

**JILID 1**

**SAMUDRA  
SOLUSI  
PROFESIONAL**

PT. SAMUDRA SOLUSI PROFESIONAL



**MEMITIGASI  
HUMAN  
ERROR**

**DALAM SISTEM MANAJEMEN K3**

**Andi Tenriola Fitri Kessi, S.K.M., M.Kes.**

**DUMMYY**

Andi Tenriola Fitri Kessi, S.K.M., M.Kes.

**JILID 1**

# **MEMITIGASI HUMAN ERROR DALAM SISTEM MANAJEMEN K3**

*Sebuah Pendekatan Sistemik untuk  
Mencegah Kecelakaan Kerja*

Diterbitkan Oleh:



PT. Samudra Solusi Profesional

## Perpustakaan Nasional RI: Katalog Dalam Terbitan (KDT)

JUDUL DAN PENANGGUNG JAWAB	Jilid 1 Memitigasi Human Error dalam Sistem Manajemen K3 / Andi Tenriola Fitri Kessi, S.K.M., M.Kes. Editor: Abdul Gafur Rinaldi, S.Ak., M.Sc., CTT., BKP.
PUBLIKASI	Malang: PT Samudra Solusi Profesional, 2026
DESKRIPSI FISIK	x + 288 Halaman; 23 cm
IDENTIFIKASI	ISBN: 978-634-7500-91-5
SUBJEK	Keselamatan dan Kesehatan Kerja (K3)

### JILID 1

#### **MEMITIGASI HUMAN ERROR DALAM SISTEM MANAJEMEN K3**

Copyright ©2026

#### **Penulis**

**Andi Tenriola Fitri Kessi, S.K.M., M.Kes.**

#### **Editor**

Abdul Gafur Rinaldi, S.Ak., M.Sc., CTT., BKP.

**Layouter:** Syafira Adzjani

**Desain Cover:** La\_Chus99

**Diterbitkan Oleh:**



Anggota IKAPI

No. Registrasi Keanggotaan: 385/JTI/2023

#### **Kantor Pusat**

Bukit Cemara Tidar Blok K1 No. 14  
Desa/Kelurahan Karangbesuki, Kec. Sukun,  
Kota Malang, Jawa Timur  
Telp/Fax: 0822-3118-6542  
Email: samudrasolusiprofesional@gmail.com

#### **Kantor Cabang**

- Workshop Jasmine, Jasmine Valley Blok 3 No. 2, Araya, Malang
- Jalan Magelang, No. 118 Karangwaru, Tegalrejo, D.I Yogyakarta

### JILID 1

**Cetakan Pertama,** Maret 2026

**ISBN:** 978-634-7500-91-5

Dilarang keras mengutip, menjiplak, atau memfotokopi baik sebagian atau seluruh isi buku ini,  
serta menjual belikannya tanpa mendapat izin tertulis dari penerbit.

# KATA PENGANTAR

Keselamatan dan Kesehatan Kerja (K3) di era industri modern menghadapi tantangan yang semakin kompleks. Sistem kerja menjadi semakin terintegrasi, berteknologi tinggi, dan sarat tekanan produksi, sementara ekspektasi terhadap kinerja keselamatan terus meningkat. Dalam konteks ini, pendekatan konvensional yang berfokus pada kesalahan individu terbukti semakin tidak memadai.

Buku *Memitigasi Human Error dalam Sistem Manajemen K3* disusun untuk memberikan landasan konseptual yang kokoh bagi pemahaman human error dalam perspektif keselamatan modern. Jilid ini secara sistematis membahas konteks K3 kontemporer, keterbatasan model sebab-akibat tradisional, serta pergeseran paradigma dari person-model menuju system-model dalam keselamatan.

Pembahasan tidak berhenti pada kritik, tetapi diarahkan untuk memperkenalkan prinsip-prinsip keselamatan berbasis sistem, termasuk konsep kondisi laten, pertahanan berlapis, budaya dan iklim keselamatan, serta peran kepemimpinan dalam membentuk keandalan sistem. Sistem Manajemen K3 (SMK3) diposisikan bukan sebagai sekadar kerangka administratif, melainkan sebagai wahana strategis untuk mengelola risiko human error secara terstruktur, proaktif, dan berkelanjutan.

Sebagai buku berjilid, Jilid 1 berfungsi sebagai pengantar intelektual dan fondasi analitis. Pemahaman yang dibangun dalam jilid ini menjadi prasyarat penting untuk memasuki pembahasan yang lebih aplikatif dan metodologis pada jilid berikutnya, yang akan menyoroti model analisis, teknik mitigasi, dan integrasi human factors secara lebih mendalam dalam praktik SMK3.

Buku ini ditujukan bagi praktisi K3, manajer, pemimpin organisasi, akademisi, serta siapa pun yang berkepentingan dalam membangun sistem kerja yang tidak hanya patuh, tetapi juga tangguh dan adaptif terhadap kompleksitas dunia nyata.

Selamat membaca dan mengaplikasikan.

Makassar, Februari 2026

**Andi Tenriola Fitri Kessi**

DUMMMY

# PRAKATA

Buku ini lahir dari sebuah kegelisahan yang kerap hadir dalam praktik Keselamatan dan Kesehatan Kerja: Mengapa, setelah puluhan tahun regulasi, standar, dan prosedur diterapkan, kecelakaan akibat human error masih terus berulang, bahkan dalam organisasi yang tampak telah “patuh” secara administratif.

Dalam banyak investigasi, kesalahan manusia sering kali dijadikan titik akhir penjelasan. Ia diberi label, dicatat dalam laporan, lalu diikuti dengan rekomendasi pelatihan ulang atau penegakan disiplin. Namun, semakin dalam penulis menelaah berbagai kasus dan literatur keselamatan modern, semakin jelas bahwa human error jarang berdiri sendiri. Ia hampir selalu merupakan manifestasi dari sistem yang dirancang tanpa sepenuhnya memahami keterbatasan, variabilitas, dan konteks kerja manusia.

Jilid pertama buku ini disusun sebagai upaya untuk menata ulang cara pandang tersebut. Alih-alih menempatkan manusia sebagai “masalah”, buku ini mengajak pembaca melihat manusia sebagai bagian inheren dari sistem dengan segala kekuatan dan keterbatasannya. Kesalahan, dalam kerangka ini, bukanlah anomali, melainkan sinyal yang menunjukkan adanya celah dalam desain sistem kerja, budaya organisasi, kepemimpinan, maupun mekanisme pengendalian risiko.

Buku ini belum menawarkan seluruh jawaban. Ia justru dimaksudkan sebagai fondasi konseptual dan filosofis: membangun bahasa bersama, kerangka berpikir sistemik, serta pemahaman kritis yang diperlukan sebelum melangkah ke strategi mitigasi yang lebih teknis dan operasional pada jilid-jilid berikutnya.

Harapannya, pembaca tidak hanya memperoleh pengetahuan, tetapi juga lensa baru untuk memaknai keselamatan sebagai hasil dari sistem yang dirancang dengan kesadaran, bukan sekadar kepatuhan.

Makassar, Februari 2026

**Andi Tenriola Fitri Kessi**

DUMMY

# DAFTAR ISI

KATA PENGANTAR.....	iii
PRAKATA.....	v
DAFTAR ISI.....	vii

## BAB 1

KONTEKS K3 DAN TANTANGAN <i>HUMAN ERROR</i> DALAM INDUSTRI <i>MODERN</i> .....	1
A. Pentingnya K3 dalam Keberlanjutan Organisasi.....	3
B. Statistik Kecelakaan Kerja: Kontribusi Dominan Faktor Manusia.....	13
C. Kritik Terhadap Model Sebab-Akibat Tradisional.....	22
D. Perlunya Pendekatan Sistemik yang Komprehensif.....	31

## BAB 2

EVOLUSI PARADIGMA <i>HUMAN ERROR</i> : DARI PERSON-MODEL KE <i>SYSTEM-MODEL</i> .....	43
A. Pendekatan Person-Model: Fokus pada Kesalahan Individu..	45
B. Kritik terhadap Blame Culture dan Pendekatan Hukuman.....	52
C. Pergeseran Paradigma ke <i>System-Model</i> .....	60
D. Prinsip Dasar Keselamatan Berbasis Sistem.....	68

## BAB 3

DEFINISI DAN TIPOLOGI <i>HUMAN ERROR</i> .....	77
A. Definisi <i>Human Error</i> dalam Konteks K3.....	79
B. Klasifikasi Kesalahan Manusia: <i>Slips</i> , <i>Lapses</i> , dan <i>Mistakes</i> .....	87
C. Klasifikasi Perilaku Berisiko: <i>Violations</i> .....	95
D. Memahami <i>Human Error</i> sebagai Variasi Perilaku Manusia ...	102

## **BAB 4**

### DASAR-DASAR PENDEKATAN SISTEMIK DALAM MITIGASI

<i>HUMAN ERROR</i> .....	113
A. Konsep Sistem dan Lingkungan Kerja.....	115
B. <i>Latent Conditions</i> (Kondisi Laten) dan <i>Active Failures</i> (Kegagalan Aktif).....	123
C. Konsep Pertahanan Berlapis ( <i>Defenses in Depth</i> ).....	130
D. Peran K3MS (Sistem Manajemen K3) sebagai Kerangka Sistemik.....	138

## **BAB 5**

### MODEL KEJU SWISS (*SWISS CHEESE MODEL*) JAMES REASON DAN RELEVANSINYA DALAM K3.....

A. Struktur dan Mekanisme Model Keju Swiss.....	151
B. Identifikasi Lubang-Lubang dalam Lapisan Pertahanan.....	158
C. Peran Kesalahan Manajemen Puncak.....	163
D. Penerapan Model untuk Prediksi dan Pencegahan Kecelakaan.....	169

## **BAB 6**

### MODEL SHELL DAN APLIKASI UNTUK ANTARMUKA MANUSIA-SISTEM.....

A. Komponen Model SHELL.....	181
B. Analisis Interaksi dan Ketidakesesuaian ( <i>Mismatch</i> ) Antarkomponen.....	188
C. Aplikasi Model SHELL dalam Perancangan Stasiun Kerja dan Tugas.....	194
D. Contoh Kasus Analisis Kecelakaan dengan Pendekatan SHELL.....	200

## **BAB 7**

### FAKTOR KOGNITIF DAN PERSEPTUAL YANG MENDORONG KESALAHAN.....

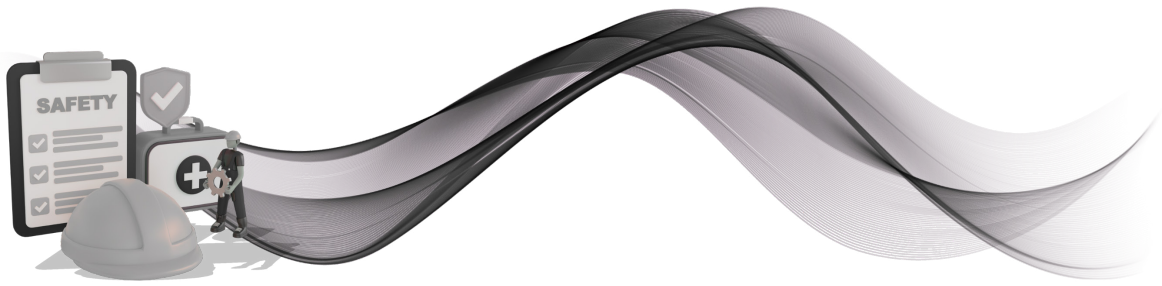
A. Keterbatasan Kapasitas Otak Manusia.....	209
---	-----

B. Peran Stres dan Kelelahan Mental .....	216
C. Fenomena <i>Cognitive Biases</i> dan <i>Mistakes</i> .....	222
D. Strategi Mitigasi Berbasis Kognisi .....	229

## **BAB 8**

PENGARUH FAKTOR ORGANISASI DAN LINGKUNGAN KERJA .....	237
A. Pengaruh Iklim Keselamatan ( <i>Safety Climate</i> ) dan Budaya Keselamatan ( <i>Safety Culture</i> ) .....	239
B. Metode Pengukuran dan Peningkatan Iklim Keselamatan .....	244
C. Dampak Jadwal Kerja, <i>Shift</i> , dan Kelelahan ( <i>Fatigue</i> ) .....	246
D. Faktor Desain Tempat Kerja (Ergonomi Fisik dan Kognitif) .....	253
E. Peran Kepemimpinan dalam Menciptakan Lingkungan yang Aman .....	259
DAFTAR PUSTAKA .....	267
GLOSARIUM .....	279
BIODATA PENULIS .....	287

**DUMMYY**



# BAB 1

## KONTEKS K3 DAN TANTANGAN *HUMAN ERROR* DALAM INDUSTRI *MODERN*

### PENDAHULUAN

Apakah mungkin menciptakan sebuah sistem kerja yang sepenuhnya kebal dari kesalahan? Pertanyaan ini sering kali menjadi titik awal perdebatan dalam diskusi keselamatan di lingkungan industri. Sebagian besar laporan investigasi kecelakaan kerja secara konsisten menunjuk pada “kesalahan manusia” sebagai faktor penyebab utama. Fenomena ini menciptakan sebuah narasi yang nyaman namun berbahaya, yaitu narasi bahwa kecelakaan terjadi karena individu di lini depan melakukan tindakan yang salah, lalai, atau tidak kompeten. Narasi ini secara implisit mengasumsikan bahwa jika saja individu tersebut lebih berhati-hati atau lebih terlatih, maka kecelakaan dapat dihindari. Konsekuensinya, solusi yang ditawarkan sering kali terbatas pada tindakan pendisiplinan, pelatihan ulang, atau penambahan prosedur yang lebih ketat.

Paradigma yang berpusat pada individu ini mulai menunjukkan keterbatasan yang signifikan dalam menghadapi kompleksitas sistem industri modern. Organisasi kontemporer merupakan sebuah jaringan interaksi yang rumit antara manusia, teknologi canggih, tekanan produksi

yang ketat, dan regulasi yang terus berubah. Menyederhanakan kegagalan sistem yang kompleks menjadi kesalahan satu atau dua individu adalah sebuah simplifikasi berlebihan yang menghalangi pembelajaran organisasi yang sejati. Fokus yang berlebihan pada kegagalan aktif individu mengabaikan kondisi-kondisi laten di dalam sistem yang sebenarnya menciptakan prasyarat bagi terjadinya kesalahan tersebut.

Bab ini akan membangun fondasi untuk memahami mengapa pendekatan tradisional tersebut tidak lagi memadai. Pembahasan akan diawali dengan penegasan kembali peran strategis Keselamatan dan Kesehatan Kerja (K3) bukan hanya sebagai kewajiban moral atau hukum, tetapi sebagai pilar fundamental bagi keberlanjutan dan daya saing organisasi. K3 yang dikelola dengan buruk dapat menimbulkan kerugian finansial yang masif dan kerusakan reputasi yang sulit dipulihkan. Sebaliknya, keunggulan dalam kinerja K3 merupakan cerminan dari keunggulan operasional secara keseluruhan.

Selanjutnya, bab ini akan menelaah data statistik kecelakaan kerja secara kritis. Meskipun statistik secara global menunjukkan kontribusi dominan faktor manusia, kita perlu mempertanyakan validitas dan interpretasi dari data tersebut. Sering kali, pelabelan "human error" dilakukan tanpa analisis yang mendalam mengenai faktor-faktor sistemik yang melatarbelakanginya. Keterbatasan dalam metodologi pelaporan dan investigasi dapat menciptakan bias yang justru memperkuat budaya menyalahkan (*blame culture*) dan menghambat upaya perbaikan yang substantif.

Kritik terhadap model-model sebab-akibat kecelakaan yang tradisional, seperti Model Domino Heinrich, juga akan menjadi fokus utama. Model-model ini, meskipun historis penting, cenderung bersifat linear dan gagal menangkap dinamika interaksi non-linear dalam sistem yang kompleks. Pandangan bahwa kecelakaan adalah hasil dari serangkaian peristiwa berurutan yang sederhana tidak lagi relevan untuk menjelaskan kegagalan katastropik di industri berisiko tinggi seperti penerbangan, nuklir, atau perminyakan.

Sebagai respons terhadap keterbatasan tersebut, bab ini akan memperkenalkan perlunya sebuah pergeseran paradigma menuju pendekatan sistemik yang komprehensif. Dalam pandangan ini, *human error* tidak dilihat sebagai penyebab, melainkan sebagai gejala dari kegagalan sistem yang lebih luas. Keselamatan tidak lagi dimaknai sebagai ketiadaan kecelakaan, tetapi sebagai kehadiran kapasitas sistem untuk mengelola variabilitas dan beradaptasi terhadap tantangan yang tak terduga. Pendekatan ini memandang organisasi sebagai sebuah ekosistem yang dinamis, di mana keselamatan diciptakan melalui desain yang proaktif, bukan melalui pengendalian reaktif.

Tujuan utama dari bab pembuka ini adalah untuk mengubah cara pandang pembaca terhadap konsep *human error*. Pembaca diharapkan dapat mulai melihat kesalahan bukan sebagai anomali yang harus dihilangkan, tetapi sebagai bagian inheren dari kinerja manusia yang harus dikelola. Dengan memahami konteks K3 modern dan keterbatasan pendekatan lama, kita dapat membangun landasan yang kokoh untuk menjelajahi model-model analisis dan strategi mitigasi berbasis sistem yang akan dibahas secara mendalam pada bab-bab berikutnya dalam buku ini.

Pergeseran ini bukanlah sekadar perubahan terminologi, melainkan sebuah perubahan filosofis yang fundamental. Ia menuntut para pemimpin dan praktisi K3 untuk menjadi arsitek sistem yang andal, bukan lagi menjadi "polisi" yang mencari pelanggar. Tantangannya adalah merancang sistem kerja yang tidak hanya meminimalkan kemungkinan terjadinya kesalahan, tetapi juga mampu menahan dan memitigasi konsekuensi dari kesalahan yang tak terhindarkan. Bab ini adalah langkah pertama untuk membekali pembaca dengan lensa analitis yang diperlukan untuk menghadapi tantangan tersebut secara efektif dan berkelanjutan.

## **A. Pentingnya K3 dalam Keberlanjutan Organisasi**

Pandangan bahwa Keselamatan dan Kesehatan Kerja (K3) hanyalah sebuah pusat biaya (*cost center*) atau sekadar pemenuhan kewajiban regulasi merupakan perspektif yang usang dan terbukti keliru dalam lanskap bisnis modern. Organisasi-organisasi terkemuka di dunia kini memandang K3

sebagai elemen inti dari strategi keberlanjutan dan keunggulan kompetitif. Investasi yang ditanamkan dalam membangun sistem manajemen K3 yang robust bukanlah beban, melainkan sebuah investasi strategis yang memberikan pengembalian signifikan dalam berbagai bentuk, mulai dari peningkatan produktivitas, efisiensi operasional, hingga penguatan citra merek. Kinerja keselamatan yang unggul sering kali berkorelasi langsung dengan tingkat disiplin operasional, kualitas produk, dan moral karyawan yang tinggi.

Sebuah lingkungan kerja yang aman dan sehat secara fundamental memengaruhi cara karyawan berinteraksi dengan pekerjaan mereka. Ketika karyawan merasa bahwa organisasi peduli terhadap kesejahteraan mereka, tingkat keterlibatan (*engagement*), loyalitas, dan motivasi cenderung meningkat secara drastis. Hal ini berdampak langsung pada penurunan tingkat absensi dan perputaran karyawan (*turnover*), yang keduanya merupakan sumber kerugian finansial yang tidak sedikit. Lebih jauh, budaya K3 yang positif mendorong karyawan untuk lebih proaktif dalam melaporkan potensi bahaya dan memberikan saran perbaikan, menciptakan siklus pembelajaran dan peningkatan berkelanjutan yang memperkuat resiliensi organisasi.

Manajemen K3 yang efektif juga berfungsi sebagai fondasi bagi inovasi dan efisiensi. Proses analisis risiko yang sistematis, seperti yang akan dibahas dalam bab-bab selanjutnya, tidak hanya mengidentifikasi bahaya keselamatan, tetapi sering kali juga menyingkap inefisiensi dalam alur kerja, desain peralatan, atau prosedur operasional. Dengan demikian, upaya untuk membuat pekerjaan lebih aman sering kali berjalan seiring dengan upaya untuk membuatnya lebih cerdas dan lebih efisien. Organisasi yang berhasil mengintegrasikan K3 ke dalam setiap aspek operasionalnya cenderung memiliki proses yang lebih andal dan terstandarisasi.

Di era di mana transparansi dan tanggung jawab sosial perusahaan menjadi sorotan utama, reputasi organisasi sangat terkait erat dengan catatan keselamatannya. Sebuah insiden kecelakaan kerja yang fatal atau berdampak luas pada lingkungan dapat menghancurkan citra perusahaan yang telah dibangun selama puluhan tahun dalam sekejap. Konsumen, investor, dan talenta terbaik semakin mempertimbangkan faktor-

faktor *Environmental, Social, and Governance* (ESG) dalam pengambilan keputusan mereka, di mana K3 merupakan komponen krusial dari pilar 'Sosial'. Organisasi yang dapat menunjukkan komitmen nyata dan kinerja K3 yang terbukti akan memiliki keunggulan dalam menarik investasi dan mempertahankan kepercayaan publik.

Integrasi K3 ke dalam strategi bisnis juga mencerminkan kematangan manajemen risiko organisasi. Kemampuan untuk mengelola risiko K3 secara proaktif menunjukkan kapabilitas organisasi dalam mengelola berbagai jenis risiko bisnis lainnya, mulai dari risiko operasional hingga risiko finansial. Sistem Manajemen K3 (SMK3) yang efektif, seperti yang diatur dalam standar internasional ISO 45001, menyediakan kerangka kerja yang terstruktur untuk identifikasi bahaya, penilaian risiko, pengendalian, dan pemantauan kinerja secara berkelanjutan. Kerangka kerja ini membantu organisasi untuk bergerak dari pendekatan reaktif menjadi prediktif.

Lebih dari sekadar metrik internal, kinerja K3 menjadi tolok ukur penting dalam rantai pasok global. Banyak perusahaan multinasional kini mewajibkan para pemasok dan mitra bisnis mereka untuk memenuhi standar K3 yang ketat sebagai syarat kerja sama. Kegagalan dalam memenuhi standar ini dapat mengakibatkan hilangnya kontrak bisnis yang vital. Oleh karena itu, keunggulan dalam K3 bukan lagi pilihan, melainkan sebuah prasyarat untuk dapat berpartisipasi dan bersaing dalam ekonomi global yang saling terhubung.

Pada akhirnya, pentingnya K3 dalam keberlanjutan organisasi berakar pada sebuah prinsip etis yang fundamental: bahwa setiap pekerja berhak untuk kembali ke rumah dalam keadaan selamat dan sehat setiap harinya. Prinsip ini harus menjadi nilai inti yang tidak dapat ditawar. Namun, buku ini berargumen bahwa pemenuhan tanggung jawab etis tersebut secara inheren juga selaras dengan pencapaian tujuan-tujuan bisnis strategis. Mengelola keselamatan dengan baik adalah praktik bisnis yang cerdas, yang melindungi aset paling berharga perusahaan, yaitu sumber daya manusianya, sekaligus memperkuat fondasi untuk pertumbuhan jangka panjang.

Komitmen terhadap K3 yang melampaui sekadar kepatuhan minimal adalah cerminan dari kepemimpinan yang visioner. Para pemimpin yang memahami ini tidak melihat K3 sebagai departemen yang terisolasi, tetapi sebagai filosofi yang menjiwai setiap keputusan dan tindakan di seluruh level organisasi. Mereka menyadari bahwa budaya keselamatan yang kuat adalah aset tak berwujud yang membedakan organisasi yang hebat dari yang sekadar baik, dan menjadi penentu utama dalam menghadapi tantangan di masa depan.

**Analogi/Contoh Kasus:** Bayangkan sebuah tim balap Formula 1. Tujuan utamanya adalah kecepatan dan kemenangan. Namun, tim yang paling sukses adalah mereka yang memiliki obsesi setara terhadap keselamatan. Sistem pengereman canggih, sasis monokok yang kuat, *halo device* pelindung kokpit, dan prosedur *pit stop* yang presisi bukanlah penghambat kecepatan. Sebaliknya, semua elemen keselamatan tersebut justru memberikan kepercayaan diri bagi pembalap untuk mendorong mobil hingga batas maksimalnya. Tim tahu bahwa sistem mereka dirancang tidak hanya untuk cepat, tetapi juga untuk bertahan dari kegagalan. Sama seperti tim balap, organisasi industri yang berinvestasi besar pada K3 (sistem pengereman yang andal, prosedur yang jelas, alat pelindung yang efektif) sebenarnya sedang membangun fondasi yang memungkinkan mereka untuk beroperasi pada tingkat produktivitas dan efisiensi tertinggi dengan risiko yang terkendali. K3 bukanlah rem, melainkan sistem navigasi dan suspensi yang memungkinkan perusahaan melaju kencang di jalur yang menantang.

### 1. K3 sebagai Investasi Bisnis dan Daya Saing

Mengalokasikan anggaran untuk program K3 sering kali diperdebatkan dalam rapat dewan direksi, dengan pertanyaan umum seputar “berapa pengembalian investasi (*return on investment* - ROI) dari program ini?”. Paradigma ini perlu digeser dari melihat K3 sebagai biaya menjadi melihatnya sebagai investasi strategis yang menghasilkan keuntungan nyata, baik yang terukur (*tangible*) maupun tidak terukur (*intangible*). Keuntungan yang terukur dapat dilihat langsung dari penurunan biaya yang terkait dengan kecelakaan, seperti biaya perawatan medis, kompensasi pekerja, perbaikan peralatan yang rusak, dan hilangnya waktu produksi.

Setiap kecelakaan yang berhasil dicegah merupakan penghematan biaya langsung bagi perusahaan.

Investasi pada K3 juga secara signifikan meningkatkan produktivitas. Lingkungan kerja yang dirancang secara ergonomis, misalnya, tidak hanya mengurangi risiko cedera muskuloskeletal, tetapi juga memungkinkan pekerja untuk bekerja lebih efisien dengan tingkat kelelahan yang lebih rendah. Prosedur kerja yang jelas dan terstandarisasi, yang merupakan elemen inti dari SMK3, meminimalkan ambiguitas dan variabilitas yang dapat menyebabkan pengerjaan ulang (*rework*) dan pemborosan material. Karyawan yang sehat dan tidak cedera jelas lebih produktif dibandingkan mereka yang sering absen atau bekerja dengan kapasitas yang berkurang akibat masalah kesehatan terkait pekerjaan.

Secara lebih luas, keunggulan dalam K3 menjadi faktor pembeda di pasar yang kompetitif. Perusahaan dengan rekam jejak keselamatan yang cemerlang cenderung lebih mudah memenangkan tender dan kontrak, terutama pada proyek-proyek besar di sektor konstruksi, pertambangan, atau manufaktur, di mana klien menetapkan standar K3 yang sangat tinggi. Reputasi sebagai perusahaan yang aman dan bertanggung jawab menarik minat investor dan lembaga keuangan yang semakin sadar akan risiko-risiko ESG. Stabilitas operasional yang ditunjukkan oleh rendahnya angka kecelakaan memberikan sinyal bahwa perusahaan tersebut dikelola dengan baik dan memiliki manajemen risiko yang matang.

Daya saing sebuah perusahaan juga sangat bergantung pada kemampuannya untuk menarik dan mempertahankan talenta terbaik. Di pasar tenaga kerja saat ini, terutama bagi generasi muda, ekspektasi terhadap kualitas lingkungan kerja semakin tinggi. Calon karyawan tidak hanya mencari kompensasi finansial yang baik, tetapi juga lingkungan kerja yang aman, sehat, dan suportif. Organisasi yang dikenal memiliki budaya K3 yang buruk akan kesulitan menarik profesional berkualitas, sementara yang memiliki reputasi sebaliknya akan menjadi pilihan utama bagi talenta-talenta unggul.

Investasi dalam teknologi keselamatan, seperti sensor otomatis, sistem pemantauan jarak jauh, atau robotika untuk tugas-tugas berbahaya, sering

kali memberikan keuntungan ganda. Selain mengurangi paparan pekerja terhadap risiko, teknologi ini juga dapat meningkatkan presisi, kecepatan, dan kualitas output produksi. Adopsi teknologi K3 yang inovatif dapat memposisikan perusahaan sebagai pemimpin industri yang berpikiran maju, yang pada gilirannya meningkatkan citra merek dan daya tarik di mata pelanggan dan mitra bisnis.

Kajian sistematis terhadap berbagai studi menunjukkan korelasi positif yang kuat antara implementasi SMK3 yang efektif dengan kinerja bisnis secara keseluruhan. Perusahaan yang secara proaktif mengelola K3 cenderung lebih tangguh dalam menghadapi disrupsi, memiliki hubungan industrial yang lebih harmonis, dan menunjukkan kinerja finansial yang lebih baik dalam jangka panjang. Ini membuktikan bahwa keselamatan dan profitabilitas bukanlah dua hal yang bertentangan, melainkan dua sisi dari mata uang yang sama: keunggulan operasional.

Oleh karena itu, setiap rupiah yang dialokasikan untuk pelatihan K3, perbaikan desain tempat kerja, penyediaan alat pelindung diri yang berkualitas, atau pengembangan sistem manajemen yang andal harus dipandang sebagai investasi pada aset paling vital perusahaan: manusia dan proses. Pengembalian dari investasi ini mungkin tidak selalu langsung terlihat dalam laporan laba rugi kuartalan, tetapi dampaknya akan terasa secara kumulatif pada kesehatan finansial, reputasi, dan keberlanjutan organisasi di masa depan.

Perusahaan yang gagal melakukan investasi ini, di sisi lain, secara tidak sadar sedang bertaruh dengan aset dan masa depan mereka. Mereka mungkin menghemat biaya dalam jangka pendek, tetapi mereka mengekspos diri pada risiko kerugian katastrofik yang dapat timbul dari satu insiden besar, yang biayanya jauh melampaui total investasi K3 yang seharusnya mereka lakukan selama bertahun-tahun.

## **2. Dampak Kecelakaan terhadap Reputasi dan Keuangan Perusahaan**

Biaya yang ditimbulkan oleh sebuah kecelakaan kerja jauh melampaui biaya langsung yang terlihat di permukaan. Model gunung es (*iceberg model*) sering digunakan untuk mengilustrasikan fenomena ini. Biaya langsung, seperti biaya medis dan kompensasi, hanyalah puncak gunung es

yang terlihat. Di bawah permukaan air terdapat biaya tidak langsung yang jauh lebih besar dan sering kali lebih merusak, yang mencakup kerusakan reputasi dan dampak finansial jangka panjang. Biaya-biaya tersembunyi ini dapat melumpuhkan sebuah organisasi, bahkan yang secara finansial sehat sekalipun.

Kerusakan reputasi adalah salah satu dampak yang paling sulit untuk dipulihkan. Di era media sosial dan siklus berita 24 jam, informasi mengenai kecelakaan kerja yang serius dapat menyebar dengan cepat dan luas, menciptakan persepsi publik yang negatif. Perusahaan dapat dicap sebagai entitas yang tidak peduli terhadap karyawannya, tidak kompeten dalam mengelola operasinya, atau serakah karena mengorbankan keselamatan demi keuntungan. Citra negatif ini dapat menyebabkan boikot konsumen, penurunan loyalitas pelanggan, dan kesulitan dalam membangun kemitraan bisnis baru.

Dampak finansial dari kecelakaan melampaui biaya kompensasi. Penyelidikan oleh pihak berwenang dapat menyebabkan penghentian sementara atau bahkan permanen dari operasi (*shutdown*), yang berarti tidak ada produksi dan tidak ada pendapatan selama periode tersebut. Denda dari regulator bisa mencapai miliaran rupiah, tergantung pada tingkat keparahan dan kelalaian yang ditemukan. Premi asuransi kompensasi pekerja dan asuransi kewajiban publik dipastikan akan melonjak tajam setelah terjadinya insiden besar, menambah beban biaya operasional untuk tahun-tahun berikutnya.

Proses hukum yang menyertai kecelakaan kerja bisa sangat panjang dan mahal. Perusahaan harus menanggung biaya pengacara, saksi ahli, dan potensi tuntutan ganti rugi perdata dari korban atau keluarga korban yang nilainya bisa sangat besar. Selain itu, manajemen senior mungkin harus menghadapi tuntutan pidana pribadi, yang tidak hanya merusak reputasi individu tetapi juga menciptakan ketidakstabilan kepemimpinan di dalam organisasi. Waktu dan energi tim manajemen yang seharusnya difokuskan untuk menjalankan bisnis akan tersita untuk menangani krisis dan proses hukum.

Moral dan produktivitas karyawan yang tersisa juga akan anjlok pasca-insiden. Menyaksikan rekan kerja terluka atau meninggal adalah pengalaman traumatis yang dapat menyebabkan stres, kecemasan, dan ketakutan di tempat kerja. Karyawan mungkin menjadi ragu-ragu dalam melakukan tugasnya, yang memperlambat laju kerja. Tingkat absensi dan keinginan untuk pindah kerja (*turnover intention*) biasanya meningkat, memaksa perusahaan mengeluarkan biaya tambahan untuk merekrut dan melatih karyawan baru. Kepercayaan antara pekerja dan manajemen dapat terkikis, menciptakan lingkungan kerja yang penuh kecurigaan dan tidak kondusif.

Nilai saham perusahaan publik sering kali bereaksi negatif terhadap berita kecelakaan kerja yang signifikan. Investor melihat insiden tersebut sebagai tanda adanya masalah fundamental dalam manajemen risiko dan kontrol operasional perusahaan. Penurunan kepercayaan investor dapat memicu aksi jual saham, yang mengikis nilai kapitalisasi pasar perusahaan secara signifikan. Akses terhadap modal baru melalui pinjaman atau penerbitan saham juga bisa menjadi lebih sulit dan mahal karena lembaga keuangan memandang perusahaan tersebut sebagai entitas berisiko lebih tinggi.

Contoh kasus historis seperti bencana Deepwater Horizon pada tahun 2010 menunjukkan bagaimana satu insiden dapat menimbulkan kerugian finansial puluhan miliar dolar bagi BP, belum termasuk kerusakan reputasi yang tak ternilai harganya. Meskipun skala insiden mungkin berbeda, prinsipnya tetap sama untuk semua organisasi. Setiap kecelakaan adalah pukulan finansial dan reputasi, dan akumulasi dari insiden-insiden kecil pun dapat secara perlahan menggerogoti kesehatan organisasi.

Dengan demikian, mengelola K3 secara proaktif adalah salah satu bentuk manajemen risiko finansial dan reputasi yang paling krusial. Anggaran yang dihabiskan untuk pencegahan adalah premi asuransi terbaik yang dapat dibeli oleh sebuah perusahaan untuk melindungi dirinya dari potensi kebangkrutan, baik secara finansial maupun moral. Setiap upaya mitigasi risiko adalah langkah untuk menjaga nama baik dan keberlangsungan hidup perusahaan di masa depan.

### 3. Kepatuhan terhadap Regulasi dan Standar K3 Global

Beroperasi sesuai dengan hukum dan peraturan yang berlaku adalah fondasi dasar dari setiap bisnis yang sah. Dalam konteks K3, kepatuhan terhadap regulasi nasional dan standar internasional bukan hanya tentang menghindari sanksi, tetapi juga tentang menetapkan standar minimum untuk melindungi tenaga kerja. Pemerintah di seluruh dunia memberlakukan undang-undang K3 untuk memastikan bahwa pengusaha menyediakan lingkungan kerja yang bebas dari bahaya yang diketahui dan dapat menyebabkan cedera atau kematian. Kegagalan untuk mematuhi peraturan ini dapat mengakibatkan konsekuensi hukum yang serius.

Sanksi hukum bagi pelanggaran K3 dapat bervariasi, mulai dari denda administratif yang ringan hingga denda pidana yang sangat besar dan hukuman penjara bagi individu yang bertanggung jawab, termasuk manajer dan direktur perusahaan. Pihak regulator, seperti Kementerian Ketenagakerjaan di Indonesia atau *Occupational Safety and Health Administration* (OSHA) di Amerika Serikat, memiliki wewenang untuk melakukan inspeksi, mengeluarkan surat perintah penghentian kerja (*stop-work order*), dan menuntut perusahaan di pengadilan. Proses hukum ini tidak hanya mahal tetapi juga menyita waktu dan merusak citra publik perusahaan.

Namun, kepatuhan seharusnya tidak dipandang sebagai tujuan akhir, melainkan sebagai titik awal. Regulasi sering kali menetapkan persyaratan minimum dan mungkin tidak selalu mencakup semua risiko yang ada di tempat kerja spesifik atau sejalan dengan praktik terbaik (*best practices*) industri terkini. Organisasi yang benar-benar berkomitmen pada keselamatan akan berusaha untuk melampaui standar minimal yang ditetapkan oleh hukum. Mereka secara proaktif mengadopsi standar-standar internasional yang lebih komprehensif, seperti ISO 45001, yang merupakan standar global untuk sistem manajemen K3.

Adopsi standar seperti ISO 45001 memberikan banyak keuntungan strategis. Standar ini menyediakan kerangka kerja yang sistematis untuk mengelola risiko K3 melalui siklus *Plan-Do-Check-Act* (PDCA). Implementasi standar ini membantu organisasi untuk mengintegrasikan K3 ke dalam

proses bisnis inti, mempromosikan partisipasi pekerja, dan mendorong budaya perbaikan berkelanjutan. Sertifikasi ISO 45001 sering kali menjadi prasyarat dalam rantai pasok global dan dapat meningkatkan daya saing perusahaan di pasar internasional.

Selain standar sistem manajemen, banyak industri, terutama yang berisiko tinggi seperti minyak dan gas, penerbangan, dan kimia, memiliki standar teknis dan praktik yang direkomendasikan (*recommended practices*) yang dikembangkan oleh asosiasi industri atau badan profesional. Kepatuhan terhadap standar-standar ini, meskipun sering kali bersifat sukarela, dianggap sebagai bukti uji tuntas (*due diligence*) dan komitmen terhadap keunggulan operasional. Mengabaikan standar industri yang diterima secara luas dapat dianggap sebagai kelalaian jika terjadi kecelakaan.

Globalisasi bisnis berarti bahwa banyak perusahaan kini beroperasi di berbagai yurisdiksi hukum yang berbeda. Hal ini menciptakan tantangan untuk memastikan kepatuhan yang konsisten di semua lokasi operasi. Perusahaan multinasional harus mengembangkan sistem manajemen K3 global yang cukup fleksibel untuk beradaptasi dengan peraturan lokal yang spesifik, sambil tetap mempertahankan standar perusahaan yang tinggi di seluruh dunia. Pendekatan ini memastikan bahwa semua karyawan, di manapun mereka berada, dilindungi oleh tingkat keselamatan yang setara.

Kepatuhan juga mencakup kewajiban untuk melaporkan data kecelakaan dan penyakit akibat kerja kepada otoritas yang berwenang. Transparansi dalam pelaporan ini sangat penting untuk pemantauan tren K3 di tingkat nasional dan sektoral, yang pada gilirannya membantu pemerintah dan badan standar untuk mengembangkan kebijakan dan program pencegahan yang lebih efektif. Menyembunyikan atau melaporkan data yang tidak akurat adalah pelanggaran serius yang dapat merusak kepercayaan dan kredibilitas perusahaan.

Pada akhirnya, kepatuhan terhadap regulasi dan standar adalah tentang membangun dan memelihara "izin untuk beroperasi" (*license to operate*) dari masyarakat, regulator, dan pemangku kepentingan lainnya. Organisasi yang secara konsisten menunjukkan komitmen terhadap kepatuhan tidak hanya melindungi dirinya dari risiko hukum, tetapi juga

membangun fondasi kepercayaan yang kuat. Kepercayaan ini adalah aset yang sangat berharga, yang memungkinkan perusahaan untuk beroperasi dengan lancar, menarik investasi, dan mempertahankan hubungan positif dengan komunitas di sekitarnya.

## **B. Statistik Kecelakaan Kerja: Kontribusi Dominan Faktor Manusia**

Data statistik kecelakaan kerja yang dikumpulkan oleh berbagai lembaga nasional dan internasional secara konsisten menyoroti sebuah narasi yang sama: faktor manusia, atau *human error*, dianggap sebagai kontributor utama dalam sebagian besar insiden. Angka-angka yang sering dikutip berkisar antara 80% hingga 95%, menunjukkan bahwa tindakan atau kelalaian individu di tempat kerja merupakan penyebab langsung dari mayoritas kecelakaan. Angka-angka ini, meskipun sering digunakan untuk menekankan pentingnya perilaku aman, perlu ditelaah dengan kaca mata kritis. Apakah statistik ini benar-benar mencerminkan akar masalah yang sebenarnya, ataukah ia merupakan produk dari sistem pelaporan dan investigasi yang memiliki bias inheren?

Memahami tren statistik kecelakaan sangat penting untuk mengarahkan sumber daya dan perhatian pada area-area yang paling berisiko. Analisis data memungkinkan organisasi dan regulator untuk mengidentifikasi pola-pola yang berulang, seperti jenis cedera yang paling umum, waktu atau hari di mana kecelakaan sering terjadi, atau departemen dengan tingkat insiden tertinggi. Informasi ini menjadi dasar bagi pengembangan program-program intervensi yang ditargetkan. Namun, jika data awal sudah bias dengan menyalahkan individu, maka intervensi yang dihasilkan pun kemungkinan besar akan salah sasaran, berfokus pada pelatihan dan pendisiplinan daripada perbaikan sistem.

Masalah utama dari statistik yang menunjuk pada dominasi *human error* adalah definisi dari istilah itu sendiri yang sering kali ambigu dan digunakan sebagai kategori "keranjang sampah". Ketika seorang investigator tidak dapat menemukan penyebab teknis yang jelas seperti kegagalan peralatan, kesimpulan bahwa "operator melakukan kesalahan" menjadi jalan keluar yang mudah. Label ini sering kali menghentikan penyelidikan lebih lanjut

untuk memahami *mengapa* operator tersebut melakukan kesalahan. Apakah karena prosedur yang membingungkan, kelelahan akibat jadwal kerja yang panjang, tekanan produksi, atau desain antarmuka yang buruk? Pertanyaan-pertanyaan krusial ini sering tidak terjawab dalam laporan statistik standar.

Pelaporan data juga dipengaruhi oleh budaya organisasi. Dalam organisasi dengan *blame culture* yang kuat, pekerja dan penyelia cenderung enggan melaporkan insiden atau *near miss* (hampir celaka) secara akurat, terutama jika laporan tersebut dapat berujung pada sanksi atau hukuman. Akibatnya, data yang terkumpul menjadi tidak lengkap dan tidak representatif. Laporan yang ada mungkin lebih mencerminkan insiden yang tidak dapat disembunyikan, sementara banyak insiden kecil dan *near miss* yang merupakan sinyal peringatan dini dari kegagalan sistem tidak pernah tercatat.

Bias lain yang melekat dalam data adalah *hindsight bias* atau bias tilik balik. Setelah sebuah kecelakaan terjadi, sangat mudah untuk melihat kembali rangkaian peristiwa dan menunjukkan di mana seseorang seharusnya bertindak berbeda. Investigator, dengan pengetahuan penuh tentang hasil akhir yang negatif, dapat dengan mudah menilai keputusan yang dibuat oleh pekerja di lapangan, yang pada saat itu beroperasi dengan informasi yang tidak lengkap dan di bawah tekanan, sebagai sebuah "kesalahan". Bias ini mengaburkan fakta bahwa tindakan yang sama mungkin dianggap normal dan dapat diterima jika tidak ada konsekuensi negatif yang terjadi.

Oleh karena itu, meskipun data statistik memberikan gambaran umum yang bermanfaat, ia harus diinterpretasikan dengan hati-hati. Menggunakan angka kontribusi *human error* sebagai pembenaran untuk tidak berinvestasi dalam perbaikan sistem adalah sebuah kesalahan fatal. Sebaliknya, angka tersebut seharusnya menjadi pemicu untuk bertanya lebih dalam: "Kondisi sistemik apa di organisasi kita yang menyebabkan 80% insiden kita dipicu oleh tindakan individu?". Pertanyaan inilah yang menggeser fokus dari menyalahkan menjadi belajar.

Pembahasan dalam subbab ini akan mengurai lebih lanjut mengenai analisis data kecelakaan global dan nasional, tantangan dalam mengatribusikan persentase kontribusi *human error* secara akurat, serta berbagai batasan dan bias yang perlu diwaspadai dalam pelaporan data kecelakaan. Tujuannya adalah untuk membekali pembaca dengan kemampuan untuk membaca data statistik tidak hanya sebagai angka, tetapi sebagai petunjuk awal untuk investigasi yang lebih mendalam terhadap kesehatan sistem K3 secara keseluruhan.

Pendekatan yang lebih matang tidak menolak fakta bahwa tindakan manusia adalah bagian dari rantai peristiwa kecelakaan. Namun, ia menolak untuk berhenti pada fakta tersebut. Sebaliknya, ia melihat tindakan tersebut sebagai titik awal untuk melacak kembali kegagalan-kegagalan tersembunyi di dalam sistem pertahanan organisasi, seperti yang akan dibahas dalam model-model sistemik di bab-bab berikutnya.

**Analogi/Contoh Kasus:** Memandang statistik *human error* sebagai penyebab utama kecelakaan sama seperti seorang dokter yang menyatakan “kegagalan jantung” sebagai penyebab kematian pada setiap pasien lansia tanpa melakukan autopsi lebih lanjut. Pernyataan itu secara teknis benar, tetapi tidak memberikan informasi yang berguna untuk pencegahan. Mengapa jantungnya gagal? Apakah karena hipertensi yang tidak terkontrol, penyakit arteri koroner akibat gaya hidup, atau kelainan genetik? Demikian pula, menyatakan “human error” sebagai penyebab kecelakaan adalah deskripsi, bukan penjelasan. Analisis yang mendalam harus “mengautopsi” insiden tersebut untuk menemukan “penyakit” organisasi yang mendasarinya, seperti prosedur yang tidak jelas (hipertensi), tekanan produksi yang berlebihan (kolesterol tinggi), atau budaya keselamatan yang lemah (faktor genetik). Statistik hanya menunjukkan gejala; tugas kita adalah mendiagnosis penyakitnya.

## 1. Analisis Data Global dan Nasional Tren Kecelakaan

Setiap tahun, Organisasi Perburuhan Internasional (*International Labour Organization* - ILO) merilis data yang melukiskan gambaran suram mengenai keselamatan kerja di seluruh dunia. Diperkirakan jutaan pekerja meninggal dunia akibat kecelakaan kerja dan penyakit akibat kerja, dan

ratusan juta lainnya mengalami cedera non-fatal. Data ini, meskipun mengejutkan, sering kali dianggap sebagai *underestimate* karena banyak negara, terutama negara berkembang, memiliki sistem pencatatan dan pelaporan yang belum memadai. Analisis tren global ini penting untuk memahami skala masalah dan membandingkan kinerja antar negara atau kawasan.

Analisis data global menunjukkan adanya perbedaan yang signifikan antar sektor industri. Sektor-sektor seperti konstruksi, pertanian, pertambangan, dan manufaktur secara konsisten menunjukkan tingkat kecelakaan fatal dan non-fatal yang lebih tinggi dibandingkan sektor jasa atau perkantoran. Hal ini dapat diatribusikan pada tingkat paparan bahaya fisik, kimia, dan biologis yang lebih tinggi di sektor-sektor tersebut. Data ini membantu lembaga-lembaga internasional dan pemerintah nasional untuk memprioritaskan sumber daya pengawasan dan program pencegahan pada industri yang paling berisiko.

Di tingkat nasional, badan-badan seperti Badan Pusat Statistik (BPS) atau BPJS Ketenagakerjaan di Indonesia mengumpulkan dan mempublikasikan data kecelakaan kerja. Analisis data ini memungkinkan pembuat kebijakan untuk melacak efektivitas program K3 nasional dari waktu ke waktu. Misalnya, penurunan angka kecelakaan di sektor tertentu mungkin menunjukkan keberhasilan kampanye keselamatan yang ditargetkan, sementara peningkatan angka dapat menjadi sinyal adanya masalah baru yang perlu segera ditangani. Data nasional juga penting bagi perusahaan untuk melakukan *benchmarking* atau membandingkan kinerja K3 mereka dengan rata-rata industri nasional.

Tren yang muncul dari analisis data sering kali mencerminkan perubahan dalam dunia kerja. Misalnya, dengan meningkatnya otomatisasi dan digitalisasi, beberapa risiko tradisional mungkin berkurang, tetapi risiko-risiko baru yang terkait dengan interaksi manusia-mesin, keamanan siber, dan stres psikososial justru meningkat. Analisis data yang cermat dapat membantu mengidentifikasi tren-tren baru ini sebelum menjadi masalah yang meluas, memungkinkan pengembangan strategi mitigasi yang proaktif.

Namun, perbandingan data antar negara harus dilakukan dengan hati-hati karena adanya perbedaan dalam definisi “kecelakaan kerja”, kriteria pelaporan, dan kualitas sistem pengumpulan data. Sebuah negara dengan sistem pelaporan yang sangat baik mungkin tampak memiliki tingkat kecelakaan yang lebih tinggi daripada negara dengan sistem yang buruk, padahal kenyataannya justru sebaliknya. Oleh karena itu, para analis sering kali lebih fokus pada tren dari waktu ke waktu dalam satu negara daripada perbandingan absolut antar negara.

Data juga dapat dipecah lebih lanjut berdasarkan demografi pekerja, seperti usia dan jenis kelamin. Analisis sering menunjukkan bahwa pekerja muda dan pekerja baru memiliki tingkat cedera yang lebih tinggi, yang mungkin disebabkan oleh kurangnya pengalaman, kesadaran risiko, atau pelatihan. Di sisi lain, pekerja yang lebih tua mungkin lebih rentan terhadap jenis cedera tertentu akibat penurunan kapasitas fisik. Informasi ini sangat berharga untuk merancang program orientasi dan pelatihan K3 yang disesuaikan dengan kebutuhan kelompok pekerja yang berbeda.

Salah satu tantangan terbesar dalam analisis data, baik di tingkat global maupun nasional, adalah kurangnya data mengenai *near misses* (hampir celaka). Insiden-insiden ini, yang tidak mengakibatkan cedera atau kerusakan, merupakan “hadiah gratis” untuk pembelajaran karena mereka menyingkap kelemahan dalam sistem pertahanan tanpa harus membayar harga yang mahal. Sayangnya, *near misses* sering kali tidak dilaporkan dan oleh karena itu tidak masuk dalam statistik resmi. Mendorong budaya pelaporan *near miss* adalah salah satu langkah paling efektif untuk mendapatkan gambaran risiko yang lebih akurat.

Pada akhirnya, analisis tren data kecelakaan adalah alat yang sangat kuat jika digunakan dengan benar. Ia memberikan gambaran makro yang membantu mengarahkan kebijakan dan strategi. Namun, para pengguna data harus selalu menyadari keterbatasannya dan tidak boleh menggunakannya sebagai satu-satunya dasar untuk pengambilan keputusan. Data statistik harus selalu dilengkapi dengan analisis kualitatif yang mendalam terhadap insiden-insiden spesifik untuk memahami konteks dan faktor-faktor sistemik yang melatarbelaknginya.

## 2. Menentukan Persentase Kontribusi Human Error

Atribusi persentase kontribusi *human error* dalam kecelakaan kerja adalah praktik yang umum, tetapi secara metodologis sangat problematik. Angka seperti “88% kecelakaan disebabkan oleh tindakan tidak aman”, yang berasal dari studi Heinrich pada tahun 1930-an, terus dikutip hingga hari ini meskipun metodologinya telah banyak dikritik. Proses penentuan persentase ini sering kali lebih bersifat subjektif dan dipengaruhi oleh bias investigator daripada berdasarkan analisis yang objektif dan terstruktur. Ada beberapa alasan mengapa klaim persentase ini perlu dipertanyakan secara fundamental.

Pertama, tidak ada definisi standar dan universal mengenai apa yang dimaksud dengan “*human error*”. Apakah sebuah tindakan dianggap sebagai kesalahan jika ia menyimpang dari prosedur, bahkan jika prosedur itu sendiri sudah usang atau tidak dapat diterapkan di lapangan? Apakah pengambilan risiko yang didorong oleh tekanan produksi yang implisit dari manajemen dihitung sebagai *human error* atau kegagalan manajemen?. Ketiadaan definisi yang jelas membuat klasifikasi menjadi tidak konsisten dan bergantung pada interpretasi individu investigator.

Kedua, proses investigasi itu sendiri sering kali dirancang untuk menemukan satu atau beberapa “penyebab utama” (*root causes*), sebuah konsep yang semakin dianggap tidak memadai untuk menjelaskan kegagalan sistem yang kompleks. Kecelakaan jarang sekali memiliki satu penyebab tunggal. Sebaliknya, mereka adalah hasil dari konvergensi berbagai faktor kontribusi dari berbagai tingkat organisasi. Ketika investigator dipaksa untuk memilih penyebab utama, tindakan individu yang paling dekat secara waktu dengan kejadian (*proximal cause*) sering kali menjadi pilihan yang paling jelas dan mudah, sehingga secara artifisial meningkatkan persentase kontribusi *human error*.

Ketiga, banyak model investigasi tidak memiliki cara yang sistematis untuk menangkap dan mengkategorikan kontribusi dari kondisi laten. Faktor-faktor seperti desain peralatan yang buruk, pelatihan yang tidak efektif, komunikasi yang lemah, atau kebijakan yang saling bertentangan adalah kontributor kuat terhadap kecelakaan, tetapi mereka sulit untuk

dihitung atau diberi label yang jelas dalam laporan statistik. Akibatnya, fokus tetap pada kegagalan aktif di ujung yang tajam (*sharp end*), yaitu tindakan operator.

Keempat, terdapat konflik kepentingan yang inheren dalam proses investigasi. Bagi sebuah organisasi, sering kali lebih mudah dan lebih murah untuk menyalahkan seorang individu daripada mengakui adanya kelemahan fundamental dalam sistem manajemennya. Mengidentifikasi *human error* sebagai penyebab dapat mengarah pada solusi yang tampaknya sederhana seperti mendisiplinkan karyawan. Sebaliknya, mengidentifikasi kegagalan sistemik mungkin menuntut investasi besar dalam perancangan ulang proses, teknologi, atau perubahan budaya, yang ingin dihindari oleh manajemen.

Sebuah pendekatan yang lebih mencerahkan adalah dengan berhenti mencoba mengisolasi *human error* sebagai sebuah kategori penyebab yang terpisah. Sebaliknya, setiap tindakan atau keputusan manusia harus dianalisis dalam konteks di mana ia terjadi. Alih-alih bertanya "Berapa persentase kecelakaan yang disebabkan oleh *human error*?", pertanyaan yang lebih produktif adalah "Dalam persentase kecelakaan berapa kita menemukan adanya ketidaksesuaian antara desain tugas dan kapabilitas manusia?" atau "Faktor-faktor organisasi apa yang secara konsisten muncul dalam investigasi insiden kita?".

Beberapa metode analisis kecelakaan modern, seperti AcciMap atau STAMP, secara eksplisit menghindari pencarian penyebab utama tunggal. Sebaliknya, mereka memetakan bagaimana keputusan dan tindakan di semua tingkat sistem, mulai dari pemerintah dan regulator, manajemen puncak, hingga pekerja di lapangan, saling berinteraksi untuk menciptakan kondisi yang memungkinkan terjadinya kecelakaan. Dalam model-model ini, tindakan individu dilihat bukan sebagai penyebab, tetapi sebagai titik di mana kegagalan sistem yang lebih luas menjadi terlihat.

Jadi, meskipun angka persentase kontribusi *human error* akan terus muncul dalam literatur dan laporan, penting bagi praktisi K3 yang kritis untuk memahami keterbatasannya. Angka tersebut lebih mencerminkan bias dalam cara kita menyelidiki dan memahami kegagalan daripada

kebenaran objektif tentang penyebab kecelakaan. Fokus yang sehat bukanlah pada persentase itu sendiri, tetapi pada upaya sistematis untuk memahami dan memperbaiki kondisi kerja yang membentuk perilaku manusia.

Penggunaan angka persentase yang tinggi tanpa kualifikasi yang tepat dapat sangat merusak. Hal itu dapat membenarkan kelambanan manajemen dalam mengatasi masalah sistemik dan melanggengkan budaya menyalahkan yang menghambat pembelajaran. Sebaliknya, mengakui bahwa setiap *human error* memiliki konteks adalah langkah pertama menuju pencegahan yang efektif dan berkelanjutan.

### 3. Batasan dan Bias dalam Pelaporan Data Kecelakaan

Kualitas dari setiap analisis statistik sangat bergantung pada kualitas data yang menjadi inputnya. Dalam konteks K3, data kecelakaan yang dilaporkan sering kali dibebani oleh berbagai batasan dan bias yang dapat secara signifikan mendistorsi gambaran nyata dari risiko di tempat kerja. Memahami batasan-batasan ini sangat penting agar tidak menarik kesimpulan yang salah dari data yang tersedia. Salah satu batasan paling fundamental adalah fenomena *under-reporting* atau kurangnya pelaporan.

*Under-reporting* terjadi karena berbagai alasan. Dalam organisasi dengan budaya keselamatan yang negatif atau *blame culture*, karyawan sangat enggan melaporkan cedera ringan atau *near miss* karena takut akan sanksi, pembalasan, atau dianggap sebagai pekerja yang ceroboh. Tekanan dari rekan kerja atau penyelia untuk menjaga catatan keselamatan tim tetap “bersih” juga dapat menekan pelaporan. Akibatnya, data resmi mungkin hanya mencerminkan sebagian kecil dari total insiden yang sebenarnya terjadi, biasanya hanya insiden yang cukup parah sehingga tidak dapat disembunyikan.

Batasan lain terletak pada klasifikasi dan kategorisasi data. Formulir laporan kecelakaan standar sering kali memiliki pilihan kategori yang terbatas dan mungkin tidak dapat menangkap nuansa atau faktor-faktor kontribusi yang kompleks dari sebuah insiden. Misalnya, sebuah formulir mungkin memiliki kotak centang untuk “kesalahan operator” tetapi tidak ada ruang untuk menjelaskan bahwa kesalahan tersebut dipicu oleh alarm

yang membingungkan atau prosedur yang bertentangan. Keterbatasan ini memaksa investigator untuk menyederhanakan realitas yang kompleks agar sesuai dengan format laporan, yang dapat menghilangkan informasi kontekstual yang penting.

Bias kognitif dari pihak investigator juga memainkan peran besar dalam membentuk data. Seperti yang telah disebutkan, *hindsight bias* (bias tilik balik) membuat tindakan pekerja tampak jelas salah setelah fakta terjadi. Ada juga *confirmation bias*, di mana investigator secara tidak sadar mencari bukti yang mendukung hipotesis awal mereka, misalnya, jika mereka sudah menduga pekerja tersebut lalai, mereka akan lebih fokus pada bukti yang mendukung kesimpulan tersebut dan mengabaikan bukti yang bertentangan, seperti kondisi peralatan yang buruk.

Data kecelakaan juga sering kali hanya fokus pada peristiwa yang mengarah langsung ke cedera, mengabaikan penyakit akibat kerja (PAK) yang berkembang secara laten dalam jangka waktu yang lama. Paparan terhadap bahan kimia berbahaya, kebisingan, atau stres ergonomis mungkin tidak menyebabkan insiden yang dapat dilaporkan secara langsung, tetapi dampaknya terhadap kesehatan pekerja bisa jauh lebih merusak dalam jangka panjang. Karena periode latensi yang panjang dan kesulitan dalam membuktikan hubungan sebab-akibat langsung, PAK secara historis sangat kurang dilaporkan dibandingkan cedera traumatis.

Fokus pada *lagging indicators* (indikator akibat) adalah batasan lain dari data kecelakaan tradisional. Metrik seperti *Lost Time Injury Rate* (LTIR) atau *Total Recordable Injury Rate* (TRIR) hanya memberitahu kita tentang kegagalan yang sudah terjadi di masa lalu. Mereka tidak memberikan informasi tentang seberapa sehat sistem pertahanan keselamatan kita saat ini atau seberapa besar kemungkinan kegagalan di masa depan. Ketergantungan yang berlebihan pada data ini dapat menciptakan ilusi keselamatan; sebuah organisasi mungkin memiliki angka LTIR yang rendah selama berbulan-bulan hanya karena keberuntungan, sementara kondisi-kondisi laten yang berbahaya terus menumpuk tanpa terdeteksi.

Selain itu, data sering kali diagregasi pada tingkat yang terlalu tinggi sehingga kehilangan makna praktisnya. Mengetahui bahwa

“angka kecelakaan di sektor manufaktur meningkat 5%” tidak banyak membantu manajer pabrik individu. Data perlu dianalisis pada tingkat mikro, berdasarkan jenis tugas, lokasi spesifik, waktu, dan peralatan, untuk dapat menghasilkan intervensi yang ditargetkan dan efektif.

Untuk mengatasi batasan-batasan ini, organisasi perlu melengkapi data kecelakaan tradisional dengan sumber informasi lain. Ini termasuk data dari audit dan inspeksi proaktif, survei persepsi keselamatan karyawan, observasi perilaku kerja, dan yang paling penting, data dari pelaporan *near miss* dan kondisi tidak aman. Dengan menciptakan sistem pelaporan yang non-hukuman dan mudah diakses, organisasi dapat membuka aliran informasi yang sangat kaya tentang kelemahan sistem sebelum kelemahan tersebut menyebabkan kerugian.

Kesimpulannya, meskipun data kecelakaan yang dilaporkan adalah sumber informasi yang diperlukan, ia tidak pernah cukup. Praktisi K3 yang cerdas akan memperlakukan data resmi dengan tingkat skeptisisme yang sehat, selalu bertanya: “Informasi apa yang tidak diceritakan oleh data ini?”. Dengan mengenali bias dan batasan yang melekat, kita dapat menghindari perangkat analisis yang dangkal dan bergerak menuju pemahaman yang lebih dalam dan lebih akurat tentang risiko.

### **C. Kritik Terhadap Model Sebab-Akibat Tradisional**

Selama beberapa dekade, pemahaman mengenai penyebab kecelakaan kerja didominasi oleh model-model sekuensial atau linear yang sederhana. Model-model ini, yang dipelopori oleh tokoh seperti Herbert W. Heinrich pada awal abad ke-20, menggambarkan kecelakaan sebagai hasil akhir dari serangkaian peristiwa yang terjadi secara berurutan, layaknya kartu domino yang jatuh dan merobohkan kartu berikutnya. Meskipun pada masanya model-model ini merupakan langkah maju yang penting dari sekadar menyalahkan nasib buruk, kini mereka dianggap terlalu menyederhanakan realitas dan bahkan dapat menghambat upaya pencegahan yang efektif dalam sistem kerja modern yang kompleks.

Pendekatan tradisional ini secara inheren berfokus pada identifikasi dan eliminasi “tindakan tidak aman” (*unsafe acts*) atau “kondisi tidak

aman" (*unsafe conditions*) yang paling dekat dengan terjadinya kecelakaan. Fokusnya adalah pada kegagalan aktif, yaitu kesalahan atau pelanggaran yang dilakukan oleh individu di lini depan. Implikasi dari model ini adalah bahwa jika kita dapat menghilangkan tindakan tidak aman melalui pelatihan, pengawasan, dan pendisiplinan, maka rantai sebab-akibat akan terputus dan kecelakaan dapat dicegah. Pendekatan ini menarik karena kesederhanaannya dan solusi yang tampaknya langsung.

Namun, kritik utama terhadap model-model ini adalah kegagalan mereka untuk mengatasi pertanyaan "mengapa". Mengapa seorang pekerja melakukan tindakan tidak aman? Mengapa kondisi tidak aman itu ada dan tidak diperbaiki? Model domino dan sejenisnya tidak memiliki kerangka kerja yang memadai untuk menganalisis faktor-faktor organisasi, manajerial, dan budaya yang lebih dalam, yang sering disebut sebagai kondisi laten, yang membentuk konteks di mana individu bekerja (Reason, 1990). Mereka melihat tindakan tidak aman sebagai titik awal masalah, bukan sebagai gejala dari masalah yang lebih dalam.

Kompleksitas sistem teknologi modern juga menantang validitas model linear. Kecelakaan besar seperti bencana Chernobyl atau meledaknya pesawat ulang-alik Challenger tidak dapat dijelaskan oleh satu kesalahan tunggal atau urutan peristiwa yang sederhana. Sebaliknya, mereka adalah hasil dari interaksi yang tidak terduga antara berbagai komponen sistem, keputusan manajemen, tekanan politik, dan budaya organisasi selama periode waktu yang panjang. Model linear gagal menangkap dinamika umpan balik (*feedback loops*), hubungan non-linear, dan sifat kemunculan (*emergence*) dari kegagalan dalam sistem sosio-teknis yang kompleks.

Fokus yang berlebihan pada tindakan individu juga secara tidak langsung mempromosikan *blame culture*. Ketika model yang digunakan mengarahkan investigator untuk menemukan "kesalahan" seseorang, maka secara alami solusi yang diusulkan adalah menghukum atau melatih ulang orang tersebut. Hal ini menciptakan siklus yang merusak: pekerja menjadi takut melaporkan masalah, manajemen tidak mendapatkan informasi tentang kelemahan sistem, kondisi laten terus ada, dan kecelakaan serupa kemungkinan besar akan terjadi lagi di masa depan pada orang yang berbeda.

Selain itu, model tradisional sering kali mengabaikan peran sentral dari desain sistem. Banyak "tindakan tidak aman" sebenarnya adalah respons yang normal dan dapat diprediksi dari manusia terhadap desain kerja yang buruk, prosedur yang tidak praktis, atau alat yang tidak ergonomis. Dalam kasus ini, mencoba untuk "memperbaiki" manusianya adalah pendekatan yang salah. Seharusnya, fokusnya adalah pada perancangan ulang sistem kerja agar lebih sesuai dengan kapabilitas dan keterbatasan manusia, sebuah prinsip inti dari disiplin ilmu *human factors* dan ergonomi.

Subbab ini akan mengupas lebih dalam keterbatasan dari Model Domino Heinrich, kegagalannya dalam mengatasi kompleksitas interaksi sistem, dan konsekuensi negatif dari fokus yang berlebihan pada tindakan tidak aman individu. Tujuannya adalah untuk menunjukkan secara meyakinkan mengapa profesi K3 perlu bergerak melampaui model-model warisan ini dan mengadopsi kerangka kerja yang lebih holistik dan sistemik untuk memahami dan mencegah kecelakaan di abad ke-21.

Pergeseran ini bukanlah penolakan total terhadap konsep bahwa tindakan individu itu penting. Tentu saja penting. Namun, ini adalah pengakuan bahwa tindakan tersebut tidak terjadi dalam ruang hampa. Mereka dibentuk, dibatasi, dan dipengaruhi oleh sistem yang lebih luas di mana mereka bekerja. Tanpa memahami sistem tersebut, upaya pencegahan kita akan selamanya dangkal dan tidak efektif.

**Analogi/Contoh Kasus:** Menggunakan Model Domino Heinrich untuk menganalisis kecelakaan kerja di pabrik modern ibarat menggunakan peta jalan dari tahun 1930 untuk menavigasi kota metropolitan saat ini. Peta lama tersebut mungkin masih menunjukkan beberapa jalan utama yang ada, tetapi ia sama sekali tidak menggambarkan jaringan jalan tol yang kompleks, jalan layang, terowongan, atau sistem transportasi publik yang saling terhubung. Mengandalkan peta lama tersebut tidak hanya tidak efisien, tetapi juga berbahaya karena akan membawa kita ke jalan buntu atau bahkan menyebabkan kecelakaan. Demikian pula, Model Domino mungkin bisa menjelaskan kecelakaan sederhana di masa lalu, tetapi ia tidak memiliki kapasitas untuk memetakan dan menjelaskan interaksi kompleks antara teknologi, manusia, dan organisasi yang menjadi ciri

khas kegagalan sistem modern. Kita membutuhkan “GPS” analisis yang lebih canggih, yaitu pendekatan sistemik.

### 1. Keterbatasan Model Domino Heinrich dan Sederhana Lainnya

Model Domino, yang diperkenalkan oleh H.W. Heinrich dalam bukunya *Industrial Accident Prevention* pada tahun 1931, adalah salah satu teori penyebab kecelakaan yang paling berpengaruh sepanjang masa. Model ini mengusulkan bahwa cedera (domino terakhir) disebabkan oleh sebuah kecelakaan, yang didahului oleh tindakan dan kondisi tidak aman, yang pada gilirannya disebabkan oleh kesalahan atau kelalaian seseorang, yang berakar pada latar belakang sosial dan keturunan individu tersebut. Ide sentralnya adalah jika salah satu domino di tengah, terutama domino “tindakan tidak aman”, dihilangkan, maka rangkaian peristiwa akan berhenti dan cedera dapat dicegah.

Meskipun revolusioner pada masanya karena mengalihkan fokus dari takdir ke pencegahan, model ini memiliki beberapa keterbatasan fundamental yang membuatnya tidak lagi relevan untuk sistem kerja kontemporer. Keterbatasan pertama dan paling utama adalah sifatnya yang linear dan sekuensial. Model ini mengasumsikan adanya satu jalur tunggal yang menyebabkan kecelakaan. Realitasnya, kecelakaan sering kali merupakan hasil dari beberapa jalur penyebab yang berinteraksi secara bersamaan dan konvergen pada satu titik waktu dan ruang. Tidak ada satu pun domino tunggal yang jika dihilangkan pasti akan mencegah kecelakaan.

Kedua, penekanan yang sangat besar pada “tindakan tidak aman” sebagai penyebab utama, Heinrich mengklaim 88% kecelakaan disebabkan olehnya, telah dikritik secara luas. Studi asli Heinrich tidak memiliki metodologi yang kuat dan transparan, dan kesimpulannya lebih didasarkan pada penilaian subjektif dari laporan penyelia, yang secara alami cenderung menyalahkan pekerja. Penekanan ini secara langsung melahirkan pendekatan *behavior-based safety* (BBS) yang, jika tidak diimplementasikan dengan benar, dapat berujung pada penyalahan korban (*victim blaming*) dan mengabaikan tanggung jawab manajemen untuk menyediakan sistem kerja yang aman.

Ketiga, model ini gagal memberikan tempat yang memadai bagi faktor-faktor organisasi dan manajerial. Dalam kerangka Heinrich, "kesalahan seseorang" ditempatkan setelah "latar belakang sosial", mengabaikan sepenuhnya pengaruh kuat dari keputusan manajemen, budaya keselamatan, tekanan produksi, desain sistem, dan komunikasi dalam membentuk perilaku pekerja. Model ini secara implisit menempatkan beban pencegahan hampir seluruhnya pada pundak pekerja di lini depan, seolah-olah mereka beroperasi secara independen dari konteks organisasi.

Model-model sederhana lainnya yang mengikuti logika serupa, seperti model "Man-Machine-Environment", juga memiliki keterbatasan. Meskipun mereka mulai memperkenalkan gagasan interaksi, mereka masih cenderung digunakan untuk mengkategorikan penyebab ke dalam kompartemen yang terpisah daripada menganalisis dinamika interaksi di antara mereka. Investigasi sering kali berakhir dengan kesimpulan seperti "penyebabnya adalah faktor manusia" atau "kegagalan mesin" tanpa menjelaskan *bagaimana* interaksi antara manusia dan mesin dalam lingkungan tertentu menyebabkan kegagalan tersebut.

Keterbatasan lainnya adalah fokus pada kegagalan tunggal. Model domino menyiratkan bahwa kecelakaan terjadi karena satu kegagalan (misalnya, satu tindakan tidak aman). Sistem modern, terutama yang berisiko tinggi, biasanya dilindungi oleh beberapa lapisan pertahanan (*defenses in depth*). Kecelakaan katastropik hampir tidak pernah terjadi karena satu kegagalan tunggal; mereka terjadi ketika serangkaian kegagalan di berbagai lapisan pertahanan ini terjadi secara bersamaan, menciptakan jalur menuju bencana, sebuah konsep yang dijelaskan jauh lebih baik oleh Model Keju Swiss yang akan dibahas nanti.

Model Heinrich juga tidak membedakan antara jenis-jenis perilaku manusia. Ia menggabungkan kesalahan yang tidak disengaja (*errors*) dengan pelanggaran yang disengaja (*violations*) ke dalam satu kategori besar "tindakan tidak aman". Perbedaan ini sangat penting karena strategi untuk mencegahnya sangat berbeda. Kesalahan sering kali diatasi dengan perbaikan desain dan prosedur, sementara pelanggaran mungkin terkait dengan masalah motivasi, budaya, atau kepraktisan prosedur itu sendiri.

Singkatnya, sementara Model Domino Heinrich memiliki nilai historis, ketergantungannya pada kausalitas linear, fokusnya yang sempit pada kesalahan individu, dan pengabaianya terhadap faktor-faktor sistemik membuatnya menjadi alat yang tidak memadai dan bahkan menyesatkan untuk menganalisis dan mencegah kecelakaan di lingkungan kerja yang kompleks saat ini. Terus mengandalkan model ini sama saja dengan mencoba memperbaiki komputer modern dengan palu dan obeng dari abad ke-19.

## 2. Model Gagal Mengatasi Kompleksitas Interaksi Sistem

Sistem kerja modern bukanlah mesin sederhana di mana hubungan sebab-akibat selalu jelas dan dapat diprediksi. Sebaliknya, mereka adalah sistem sosio-teknis yang kompleks dan adaptif. Mereka terdiri dari banyak komponen, manusia, perangkat keras, perangkat lunak, prosedur, dan lingkungan, yang saling berinteraksi secara dinamis dan sering kali non-linear. Model sebab-akibat tradisional, dengan logikanya yang linear, secara fundamental tidak mampu menangkap dan menjelaskan kompleksitas ini.

Salah satu ciri utama sistem yang kompleks adalah adanya *tight coupling* (keterkaitan erat) antar komponen. Dalam sistem seperti ini, perubahan atau kegagalan pada satu komponen dapat dengan cepat dan tidak terduga menyebar dan memengaruhi komponen lain, menciptakan efek riak atau bahkan kaskade kegagalan. Model domino tidak dapat merepresentasikan hubungan timbal balik dan umpan balik (*feedback loops*) seperti ini. Ia hanya menggambarkan panah kausalitas satu arah, padahal dalam kenyataannya, A dapat menyebabkan B, tetapi B juga dapat memengaruhi A.

Kompleksitas juga melahirkan sifat *emergence*, di mana perilaku keseluruhan sistem tidak dapat diprediksi hanya dengan memahami perilaku masing-masing komponennya secara terpisah. Kecelakaan sering kali merupakan properti *emergent* dari interaksi normal antar komponen sistem, bukan hasil dari kegagalan satu komponen saja. Misalnya, setiap keputusan yang dibuat oleh desainer, manajer, dan operator mungkin tampak rasional dan aman jika dilihat secara terpisah. Namun, kombinasi dari keputusan-keputusan ini dalam kondisi operasional tertentu dapat

menciptakan jalur yang tidak terduga menuju kegagalan. Model linear tidak memiliki cara untuk menganalisis kegagalan yang muncul dari interaksi normal ini.

Model tradisional juga gagal memperhitungkan peran adaptasi manusia. Manusia bukanlah komponen pasif dalam sistem; mereka secara aktif beradaptasi dengan kondisi kerja, mengatasi kekurangan desain, dan menemukan cara-cara baru untuk menyelesaikan pekerjaan, terutama di bawah tekanan. Sering kali, adaptasi inilah yang membuat sistem tetap berjalan dan produktif meskipun ada kekurangan. Namun, adaptasi yang sama, dalam kondisi yang sedikit berbeda, bisa menjadi pemicu kecelakaan. Model yang hanya melihat penyimpangan dari prosedur sebagai "tindakan tidak aman" gagal menghargai peran ganda dari adaptasi manusia sebagai sumber keberhasilan sekaligus kegagalan.

Contoh nyata dari kegagalan model sederhana dalam mengatasi kompleksitas adalah dalam industri penerbangan. Kecelakaan pesawat modern jarang sekali disebabkan oleh satu kesalahan pilot atau satu kegagalan mekanis. Investigasi oleh badan seperti NTSB sering kali mengungkapkan jaring kausal yang rumit yang melibatkan desain antarmuka kokpit (*human-computer interaction*), tekanan komersial, kebijakan perawatan maskapai, pelatihan simulator, komunikasi awak kabin (*crew resource management*), dan kontrol lalu lintas udara. Mencoba memaksakan semua faktor ini ke dalam lima domino Heinrich akan menjadi penyederhanaan yang absurd dan menghilangkan wawasan penting untuk pencegahan.

Ketidakmampuan model tradisional untuk mengatasi kompleksitas memiliki implikasi praktis yang serius. Rekomendasi yang dihasilkan dari investigasi berbasis model linear cenderung bersifat lokal dan dangkal, seperti "latih ulang pilot" atau "tambahkan peringatan pada prosedur". Sebaliknya, investigasi berbasis sistem akan menghasilkan rekomendasi yang lebih luas dan mendalam, seperti "rancang ulang logika sistem otomatisasi untuk memberikan umpan balik yang lebih jelas kepada pilot" atau "ubah struktur insentif maskapai agar tidak mendorong pengambilan risiko".

Dalam dunia yang semakin terhubung dan terotomatisasi, di mana interaksi antara manusia dan teknologi menjadi semakin rumit, kebutuhan akan model analisis yang dapat menangani kompleksitas menjadi semakin mendesak. Model-model seperti STAMP (*System-Theoretic Accident Model and Processes*) dan FRAM (*Functional Resonance Analysis Method*) dikembangkan secara khusus untuk tujuan ini. Mereka tidak mencari “rantai peristiwa”, melainkan menganalisis bagaimana kontrol dan batasan dalam sistem gagal, serta bagaimana variabilitas kinerja normal dapat beresonansi dan mengarah pada hasil yang tidak diinginkan.

Dengan demikian, kritik fundamental terhadap model tradisional bukanlah hanya masalah akademis. Ini adalah masalah praktis yang menentukan apakah kita benar-benar belajar dari kegagalan dan mampu merancang sistem yang lebih aman dan lebih tangguh di masa depan. Mengabaikan kompleksitas berarti mengabaikan sifat sebenarnya dari risiko yang kita hadapi.

### **3. Fokus Berlebihan pada Tindakan Tidak Aman (Unsafe Acts) Individu**

Konsekuensi paling merusak dari dominasi model sebab-akibat tradisional adalah fokus yang tidak proporsional pada “tindakan tidak aman” (*unsafe acts*) yang dilakukan oleh individu di lini depan. Dengan menempatkan tindakan ini sebagai domino sentral yang harus dihilangkan, seluruh industri K3 selama bertahun-tahun telah mengarahkan sebagian besar energinya pada upaya untuk mengamati, mengukur, dan mengoreksi perilaku pekerja. Program-program seperti *Behavior-Based Safety* (BBS) menjadi sangat populer, dengan janji bahwa jika kita dapat membuat pekerja berperilaku aman setiap saat, maka kecelakaan akan hilang.

Meskipun niat di balik program-program ini sering kali baik, fokus yang berlebihan pada perilaku individu memiliki beberapa efek samping yang negatif. Pertama, ia secara efektif mengalihkan perhatian dan tanggung jawab dari mereka yang memiliki kekuatan terbesar untuk membuat perubahan sistemik, yaitu para perancang, insinyur, manajer, dan eksekutif. Jauh lebih mudah untuk meminta pekerja memakai APD daripada merancang ulang proses untuk menghilangkan bahaya sejak awal (*hierarchy of controls*). Fokus pada perilaku individu menjadi alasan untuk

tidak melakukan investasi yang lebih sulit dan mahal dalam perbaikan rekayasa dan organisasi.

Kedua, pendekatan ini sering kali mengabaikan konteks di mana perilaku itu terjadi. Seorang pekerja mungkin tidak mengikuti prosedur bukan karena ia malas atau pemberontak, tetapi karena prosedur tersebut tidak dapat dijalankan dengan alat yang tersedia, atau karena mengikuti prosedur akan membuatnya gagal memenuhi target produksi yang tidak realistis yang ditetapkan oleh manajemen. Dalam kasus ini, "tindakan tidak aman" sebenarnya adalah sebuah adaptasi yang cerdas terhadap sistem kerja yang dirancang dengan buruk. Menghukum pekerja karena adaptasi ini tanpa memperbaiki kondisi yang mendasarinya adalah tidak adil dan tidak efektif.

Ketiga, fokus pada individu melanggengkan apa yang disebut Sidney Dekker sebagai "The Bad Apple Theory", keyakinan bahwa sistem pada dasarnya aman, dan masalahnya terletak pada beberapa individu yang tidak kompeten atau tidak termotivasi ("apel busuk"). Teori ini menyiratkan bahwa jika kita dapat menyingkirkan apel-apel busuk ini, sistem akan kembali aman. Pandangan ini secara fundamental keliru karena mengabaikan fakta bahwa sistem itu sendiri yang mungkin secara sistematis menciptakan kondisi di mana bahkan pekerja terbaik pun bisa membuat kesalahan. Orang yang berbeda yang ditempatkan dalam kondisi yang sama kemungkinan besar akan membuat kesalahan yang sama.

Keempat, penekanan pada tindakan tidak aman menciptakan lingkungan di mana kesalahan dilihat sebagai kegagalan moral. Hal ini menghambat pembelajaran. Agar sebuah organisasi dapat belajar dari kegagalan, ia membutuhkan laporan yang jujur dan terbuka tentang apa yang sebenarnya terjadi. Jika pekerja tahu bahwa mengakui kesalahan akan berujung pada sanksi atau label "tidak aman", mereka akan cenderung menyembunyikan masalah. Akibatnya, manajemen kehilangan kesempatan berharga untuk memahami kerentanan dalam sistem mereka sebelum kerentanan tersebut menyebabkan bencana.

Pendekatan yang lebih seimbang tidak mengabaikan perilaku, tetapi melihatnya sebagai produk dari sistem. Alih-alih bertanya, "Bagaimana

kita bisa mengubah perilaku pekerja?”, pertanyaan yang lebih baik adalah, “Fitur-fitur apa dari sistem kerja kita (desain, prosedur, insentif, budaya) yang mendorong perilaku berisiko?”. Pergeseran pertanyaan ini mengubah fokus dari individu ke sistem, dan dari reaktif (mengoreksi perilaku) menjadi proaktif (merancang konteks kerja yang aman).

Ini bukan berarti individu tidak memiliki tanggung jawab atau akuntabilitas. Tentu saja mereka punya. Namun, akuntabilitas tersebut harus dinilai dalam konteks peluang dan kendala yang diberikan oleh sistem. Seperti yang akan dibahas dalam bab tentang *Just Culture*, penting untuk dapat membedakan antara kesalahan manusia yang tidak disengaja, perilaku berisiko, dan pelanggaran yang sembrono. Mencampuradukkan semuanya di bawah label “tindakan tidak aman” adalah penyederhanaan yang berbahaya.

Pada akhirnya, keselamatan yang berkelanjutan tidak akan pernah tercapai hanya dengan mencoba mengendalikan perilaku setiap individu setiap saat. Manusia secara inheren tidak sempurna dan kinerjanya bervariasi. Keselamatan sejati datang dari perancangan sistem yang mengantisipasi variabilitas ini dan toleran terhadap kesalahan, sistem dengan pertahanan yang kuat, umpan balik yang jelas, dan kemampuan untuk gagal dengan aman (*fail-safe*). Inilah inti dari pergeseran dari fokus pada individu ke fokus pada sistem.

#### **D. Perlunya Pendekatan Sistemik yang Komprehensif**

Sebagai respons langsung terhadap keterbatasan model sebab-akibat tradisional, sebuah paradigma baru yang dikenal sebagai pendekatan sistemik (*systems approach*) telah muncul dan mendapatkan daya tarik yang signifikan dalam ilmu keselamatan. Pendekatan ini secara fundamental mengubah cara kita memandang, menganalisis, dan mengelola keselamatan. Alih-alih melihat kecelakaan sebagai hasil dari kegagalan komponen individual (baik manusia maupun teknis), pendekatan sistemik melihatnya sebagai manifestasi dari interaksi yang tidak memadai antara berbagai elemen dalam sebuah sistem yang kompleks. Keselamatan, dalam pandangan ini, bukanlah properti dari satu komponen, melainkan properti *emergent* dari keseluruhan sistem.

Filosofi dasar dari pendekatan sistemik adalah bahwa perilaku dan kinerja individu tidak dapat dipahami secara terpisah dari konteks atau sistem di mana mereka bekerja. Perilaku, termasuk *human error*, adalah produk dari sistem, bukan penyebab utama kegagalannya. Oleh karena itu, untuk meningkatkan keselamatan, upaya intervensi harus ditujukan untuk merancang ulang dan memperkuat sistem secara keseluruhan, bukan hanya mencoba untuk “memperbaiki” atau mengendalikan individu di dalamnya. Pergeseran ini memindahkan fokus dari pencegahan kegagalan (*avoiding failures*) ke pembangunan kapasitas untuk sukses (*ensuring success*).

Pendekatan sistemik menolak kausalitas linear dan sederhana. Sebaliknya, ia mengakui bahwa kecelakaan di sistem yang kompleks sering kali timbul dari kombinasi faktor-faktor yang tampaknya tidak berhubungan yang terjadi secara bersamaan, di mana masing-masing faktor mungkin tidak cukup berbahaya jika terjadi sendiri-sendiri. Ia menekankan pentingnya memahami hubungan, interaksi, dan umpan balik antar komponen sistem. Analisis tidak lagi berhenti pada “apa” yang gagal, tetapi menggali lebih dalam untuk memahami “mengapa” interaksi antar komponen menghasilkan hasil yang tidak diinginkan.

Salah satu konsep kunci dalam pemikiran sistemik adalah perbedaan antara *Safety-I* dan *Safety-II*. *Safety-I*, yang mencerminkan pandangan tradisional, mendefinisikan keselamatan sebagai “ketiadaan kecelakaan dan insiden”. Fokusnya adalah pada reaktivitas: menyelidiki apa yang salah dan mencoba mencegahnya terjadi lagi. Sebaliknya, *Safety-II* mendefinisikan keselamatan sebagai “kemampuan sistem untuk berhasil dalam kondisi yang bervariasi”. Fokusnya adalah pada proaktivitas: memahami mengapa sistem biasanya berhasil dan bagaimana cara memperkuat kemampuan tersebut. Pendekatan ini mengakui bahwa manusia adalah sumber resiliensi dan kesuksesan, bukan hanya sumber risiko.

Mengadopsi pendekatan sistemik membawa sejumlah manfaat yang signifikan. Pertama, ia menghasilkan rekomendasi pencegahan yang lebih kuat dan berkelanjutan karena menargetkan akar masalah di tingkat organisasi dan desain, bukan hanya gejala di tingkat individu. Kedua, ia secara inheren mempromosikan budaya pembelajaran dan perbaikan, bukan budaya menyalahkan. Dengan melihat kesalahan sebagai informasi

berharga tentang kesehatan sistem, organisasi menjadi lebih terbuka untuk melaporkan dan membahas masalah.

Ketiga, pendekatan ini lebih cocok untuk mengelola risiko di lingkungan yang dinamis dan selalu berubah. Daripada mengandalkan prosedur yang kaku, ia menekankan pentingnya membangun resiliensi, kemampuan sistem untuk mengantisipasi, memantau, merespons, dan belajar dari gangguan dan kejutan. Keempat, ia mengintegrasikan keselamatan ke dalam operasi bisnis inti. Keselamatan tidak lagi dilihat sebagai fungsi terpisah yang dilakukan oleh departemen K3, melainkan sebagai bagian integral dari cara kerja dirancang, dikelola, dan dieksekusi setiap hari.

Subbab ini akan menguraikan lebih lanjut definisi dan filosofi keselamatan berbasis sistem, menjelaskan tiga pilar utama dalam analisis kegagalan sistem, dan menyoroti manfaat dari mengintegrasikan pendekatan sistemik ke dalam Sistem Manajemen K3 (SMK3) formal. Ini akan menjadi landasan konseptual untuk sisa buku ini, yang akan mengeksplorasi berbagai model, alat, dan strategi yang berakar pada pemikiran sistemik.

Langkah menuju pendekatan sistemik bukanlah hal yang mudah. Ia menuntut perubahan pola pikir yang mendalam dari para pemimpin, manajer, dan praktisi K3. Namun, untuk menghadapi tantangan keselamatan di abad ke-21, pergeseran ini bukan lagi sebuah pilihan, melainkan sebuah keharusan.

**Analogi/Contoh Kasus:** Bayangkan seorang ahli perkebunan yang tanamannya terus-menerus gagal panen. Pendekatan tradisional (non-sistemik) akan fokus pada tanamannya: "Tanaman ini lemah, mari kita semprot dengan lebih banyak pestisida" atau "Mari kita ganti dengan bibit baru yang lebih kuat". Ini analog dengan menyalahkan dan melatih ulang pekerja. Pendekatan sistemik yang dilakukan oleh ahli perkebunan yang bijak akan berbeda. Dia akan menganalisis keseluruhan ekosistem: "Apakah kualitas tanahnya buruk? Apakah drainasenya tidak memadai? Apakah tanaman ini mendapatkan cukup sinar matahari? Apakah ada hama di lingkungan sekitar yang terus menyerang?". Dia memahami bahwa tanaman yang sehat adalah hasil dari sistem yang sehat. Demikian pula,

pendekatan sistemik dalam K3 tidak hanya melihat “pekerja yang gagal”, tetapi menganalisis “ekosistem kerja”, desain tugas, kualitas alat, tekanan produksi, dan budaya, yang memungkinkan kegagalan itu tumbuh.

### 1. Definisi dan Filosofi Keselamatan Berbasis Sistem (Systemic Safety)

Keselamatan berbasis sistem, atau *systemic safety*, adalah sebuah pendekatan untuk memahami dan mengelola keselamatan yang memandang organisasi sebagai sebuah sistem sosio-teknis yang terintegrasi. Filosofi intinya adalah bahwa keselamatan bukanlah sesuatu yang “ditambahkan” ke dalam sebuah sistem, melainkan sebuah properti yang muncul (*emergent property*) dari interaksi dinamis antara semua komponen sistem tersebut, termasuk manusia, teknologi, prosedur, budaya, dan lingkungan eksternal. Dengan kata lain, sebuah sistem tidak *memiliki* keselamatan; sistem itu *bersifat* aman atau tidak aman sebagai hasil dari strukturnya dan cara kerjanya.

Definisi ini secara fundamental berbeda dari pandangan tradisional yang sering kali menyamakan keselamatan dengan kepatuhan terhadap aturan atau ketiadaan kegagalan komponen. Dalam pandangan sistemik, adalah mungkin bagi sebuah sistem untuk mengalami kegagalan meskipun semua komponennya berfungsi sesuai spesifikasi dan semua individu mengikuti prosedur. Kecelakaan dapat terjadi karena interaksi yang tidak terantisipasi dan berbahaya antar komponen yang “berfungsi normal”. Oleh karena itu, fokus analisis bergeser dari mencegah kegagalan komponen menjadi mengendalikan interaksi antar komponen.

Filosofi keselamatan sistemik didasarkan pada beberapa prinsip kunci. Pertama, prinsip holisme, yang menyatakan bahwa keseluruhan lebih dari sekadar penjumlahan bagian-bagiannya. Kita tidak dapat memahami keselamatan sebuah sistem hanya dengan menganalisis setiap komponennya secara terpisah. Kita harus memahami bagaimana mereka terhubung dan saling memengaruhi. Ini menuntut penggunaan alat analisis yang dapat memetakan dan memvisualisasikan struktur sistem dan hubungan kausal yang kompleks di dalamnya.

Kedua, adalah prinsip kontrol dan batasan. Setiap sistem dirancang dengan serangkaian kontrol (misalnya, prosedur, alarm, pengawasan) dan

batasan untuk menjaga agar operasinya tetap berada dalam “selubung keselamatan” (*safety envelope*). Kecelakaan terjadi ketika interaksi atau gangguan menyebabkan sistem bergerak di luar batas aman ini. Tugas dari rekayasa keselamatan sistemik (*system safety engineering*) adalah merancang, mengimplementasikan, dan memelihara kontrol yang efektif di semua tingkat sistem untuk mencegah migrasi menuju kondisi berbahaya ini.

Ketiga, keselamatan dan ketidakamanan (*unsafety*) dipandang sebagai dua sisi dari mata uang yang sama. Mereka bukanlah fenomena yang terpisah. Faktor-faktor yang sama yang dalam satu konteks menciptakan efisiensi dan kesuksesan (misalnya, adaptasi manusia terhadap prosedur yang kaku) dapat dalam konteks lain menjadi sumber kegagalan. Ini mengarah pada konsep *Safety-II*, yang berpendapat bahwa kita dapat belajar paling banyak tentang keselamatan dengan mempelajari bagaimana pekerjaan biasanya berhasil setiap hari, bukan hanya dengan mempelajari kegagalan yang jarang terjadi. Dengan memahami bagaimana manusia dan sistem beradaptasi untuk menciptakan keberhasilan, kita dapat memperkuat kapasitas resiliensi tersebut.

Keempat, *human error* direkonseptualisasi. Alih-alih dilihat sebagai penyebab kegagalan, *human error* dilihat sebagai gejala dari adanya ketidakcocokan (*mismatch*) antara desain sistem dan karakteristik manusia. Kesalahan adalah konsekuensi, bukan penyebab. Oleh karena itu, respons terhadap *human error* bukanlah menyalahkan manusia, melainkan menganalisis sistem untuk menemukan mengapa tindakan tersebut tampak rasional atau tak terhindarkan bagi orang yang melakukannya pada saat itu. Ini adalah inti dari “prinsip rasionalitas lokal”: orang melakukan apa yang masuk akal bagi mereka, berdasarkan tujuan, pengetahuan, dan fokus perhatian mereka saat itu.

Filosofi ini menuntut perubahan peran bagi para profesional K3. Mereka tidak lagi hanya menjadi auditor kepatuhan atau investigator kecelakaan. Sebaliknya, mereka menjadi analis sistem, fasilitator manajemen risiko, dan arsitek proses kerja yang andal. Pekerjaan mereka menjadi lebih proaktif, lebih terintegrasi dengan desain dan operasi, dan lebih fokus pada pemahaman “bagaimana pekerjaan sebenarnya dilakukan” (*work-as-*

*done*) dibandingkan dengan “bagaimana pekerjaan seharusnya dilakukan menurut prosedur” (*work-as-imagined*).

Pada dasarnya, keselamatan berbasis sistem adalah tentang mengelola kompleksitas. Ini adalah pengakuan bahwa kita tidak dapat menghilangkan semua kegagalan atau memprediksi semua skenario. Sebaliknya, tujuan kita adalah untuk merancang sistem yang kuat, toleran terhadap kesalahan, dan mampu mendeteksi serta pulih dari penyimpangan sebelum berkembang menjadi bencana. Ini adalah pendekatan yang lebih realistis dan pada akhirnya lebih efektif untuk mencapai keselamatan yang berkelanjutan di dunia yang tidak pasti.

## **2. Tiga Pilar Utama dalam Menganalisis Kegagalan Sistem**

Untuk menerapkan pendekatan sistemik secara praktis dalam menganalisis kegagalan, para ahli telah mengidentifikasi tiga pilar atau area fokus utama. Analisis yang komprehensif harus mempertimbangkan ketiga pilar ini secara seimbang, karena kegagalan jarang sekali hanya disebabkan oleh satu pilar saja. Ketiga pilar tersebut adalah: teknologi dan desain, faktor manusia dan organisasi, serta pengaruh lingkungan dan regulasi. Memahami interaksi antara ketiga pilar ini adalah kunci untuk mengungkap akar masalah yang sebenarnya.

Pilar pertama adalah Teknologi dan Desain. Pilar ini mencakup semua aspek perangkat keras (*hardware*), perangkat lunak (*software*), dan lingkungan fisik buatan di mana pekerjaan dilakukan. Analisis dalam pilar ini berfokus pada bagaimana desain sistem berkontribusi pada potensi kegagalan. Ini termasuk evaluasi desain antarmuka manusia-mesin (*Human-Machine Interface* - HMI), ergonomi stasiun kerja, keandalan peralatan, logika sistem otomatisasi, dan efektivitas sistem peringatan (*alarms*). Pertanyaan kunci di sini adalah: “Apakah sistem ini dirancang dengan mempertimbangkan kapabilitas dan keterbatasan manusia?” dan “Apakah ada fitur desain yang secara inheren dapat memicu atau memperburuk kesalahan?”.

Pilar kedua adalah Faktor Manusia dan Organisasi. Ini adalah pilar yang paling kompleks, mencakup segala sesuatu mulai dari kinerja individu hingga budaya organisasi. Di tingkat individu, ini melibatkan

analisis faktor-faktor kognitif seperti beban kerja, stres, kelelahan, dan bias pengambilan keputusan. Di tingkat tim, ini mencakup komunikasi, koordinasi, dan kepemimpinan. Namun, yang paling penting dalam pendekatan sistemik, pilar ini menganalisis faktor-faktor organisasi yang lebih luas, seperti kebijakan dan prosedur, struktur manajemen, alokasi sumber daya, tekanan produksi, dan iklim keselamatan (*safety climate*). Pertanyaan kuncinya adalah: "Kondisi organisasi apa yang menciptakan prasyarat untuk kegagalan di lini depan?".

Pilar ketiga adalah Pengaruh Lingkungan dan Regulasi. Tidak ada organisasi yang beroperasi dalam ruang hampa. Mereka dipengaruhi oleh lingkungan eksternal yang lebih luas, yang mencakup faktor-faktor fisik, sosial, dan peraturan. Analisis pada pilar ini memeriksa bagaimana elemen-elemen eksternal ini memengaruhi keputusan dan tindakan di dalam organisasi. Ini termasuk kepatuhan terhadap regulasi pemerintah, tekanan dari pasar dan pesaing, ekspektasi dari masyarakat, dan bahkan kondisi cuaca atau geografi. Pertanyaan kunci di sini adalah: "Bagaimana tekanan dan batasan eksternal membentuk perilaku dan prioritas di dalam organisasi?".

Sebuah investigasi kecelakaan yang benar-benar sistemik akan secara sistematis memeriksa kontribusi dari ketiga pilar tersebut dan, yang terpenting, interaksi di antara mereka. Sebagai contoh, sebuah kecelakaan mungkin secara langsung dipicu oleh kesalahan operator (Pilar 2), tetapi kesalahan itu mungkin terjadi karena operator tersebut sedang berinteraksi dengan antarmuka kontrol yang dirancang dengan buruk (Pilar 1), dan pada saat yang sama berada di bawah tekanan untuk mempercepat produksi karena tuntutan pasar (Pilar 3). Tanpa melihat ketiga pilar tersebut, analisis akan tidak lengkap dan rekomendasi yang dihasilkan akan dangkal.

Model analisis kecelakaan sistemik seperti AcciMap secara eksplisit menggunakan pilar-pilar ini (atau tingkatan serupa, seperti Pemerintah, Regulator, Manajemen Perusahaan, Staf, dan Pekerjaan) untuk memetakan faktor-faktor penyebab dari sebuah insiden. Dengan memvisualisasikan bagaimana keputusan yang buruk atau kondisi laten di tingkat atas (misalnya, regulasi yang lemah) mengalir ke bawah dan menciptakan kondisi

untuk kegagalan di tingkat bawah, model ini memberikan gambaran yang sangat kuat tentang sifat sistemik dari kecelakaan.

Oleh karena itu, bagi setiap praktisi K3, membiasakan diri untuk berpikir dalam kerangka tiga pilar ini, Teknologi, Organisasi, dan Lingkungan, adalah langkah praktis pertama untuk beralih dari analisis berbasis individu ke analisis berbasis sistem. Ini memberikan sebuah struktur untuk mengajukan pertanyaan yang lebih dalam dan lebih luas selama investigasi, audit, atau penilaian risiko.

### 3. Manfaat Integrasi Pendekatan Sistemik ke dalam K3MS

Sistem Manajemen Keselamatan dan Kesehatan Kerja (SMK3), seperti yang didefinisikan oleh standar internasional ISO 45001, menyediakan kerangka kerja formal bagi organisasi untuk mengelola risiko K3 secara proaktif. Namun, sebuah kerangka kerja hanyalah sebuah kerangka; efektivitasnya sangat bergantung pada filosofi dan pendekatan yang mendasarinya. Mengintegrasikan pemikiran sistemik ke dalam setiap elemen SMK3 dapat secara dramatis meningkatkan dampaknya, mengubahnya dari sekadar latihan kepatuhan birokratis menjadi mesin yang dinamis untuk pembelajaran dan perbaikan berkelanjutan.

Salah satu manfaat utama adalah dalam proses Identifikasi Bahaya dan Penilaian Risiko. Pendekatan tradisional sering kali fokus pada bahaya-bahaya yang jelas dan terlihat di tingkat operasional. Pendekatan sistemik mendorong organisasi untuk melihat lebih jauh dan mengidentifikasi bahaya yang bersifat laten dan sistemik, seperti kelemahan dalam proses pengambilan keputusan manajemen, konflik antara tujuan produksi dan keselamatan, atau kekurangan dalam sistem pelatihan. Teknik analisis risiko sistemik, seperti STPA (*System-Theoretic Process Analysis*), dapat digunakan secara proaktif untuk mengidentifikasi skenario kecelakaan yang timbul dari interaksi yang tidak aman, bukan hanya dari kegagalan komponen.

Dalam elemen Pelatihan dan Kompetensi, integrasi pendekatan sistemik menggeser fokus dari sekadar pelatihan prosedural ("bagaimana melakukan tugas") menjadi pelatihan yang membangun pemahaman konseptual dan resiliensi ("mengapa tugas ini dirancang seperti ini" dan "apa yang harus dilakukan ketika terjadi penyimpangan"). Pelatihan menjadi

lebih fokus pada pengembangan kesadaran situasi (*situation awareness*), keterampilan pengambilan keputusan di bawah tekanan, dan pemahaman tentang bagaimana tindakan individu dapat memengaruhi keseluruhan sistem.

Pada elemen Investigasi Insiden, manfaatnya sangat jelas. Seperti yang telah dibahas, pendekatan sistemik mengubah investigasi dari “perburuan kesalahan” menjadi “peluang pembelajaran”. Organisasi mulai menggunakan alat investigasi sistemik (misalnya, AcciMap, STAMP) yang memaksa mereka untuk melihat melampaui kegagalan aktif dan menganalisis kontribusi dari semua tingkat organisasi. Hasilnya adalah rekomendasi yang jauh lebih kuat yang menargetkan perbaikan pada desain, manajemen, dan budaya, bukan hanya pada individu.

Dalam Pengukuran Kinerja K3, pendekatan sistemik mendorong pergeseran dari ketergantungan pada *lagging indicators* (angka kecelakaan) ke pengembangan *leading indicators* (indikator utama) yang lebih bermakna. Indikator-indikator ini mengukur kesehatan proses dan kapasitas sistem, bukan hanya hasil kegagalan. Contohnya termasuk metrik tentang kualitas prosedur, jumlah laporan *near miss* yang diterima dan ditindaklanjuti, waktu yang dibutuhkan untuk menutup rekomendasi audit, atau hasil survei iklim keselamatan.

Integrasi pendekatan sistemik juga memperkuat konsep Partisipasi Pekerja. Karena pendekatan ini sangat menghargai pemahaman tentang “pekerjaan sebagaimana dilakukan” (*work-as-done*), ia secara alami menempatkan pekerja di lini depan sebagai ahli dalam sistem mereka sendiri. Partisipasi mereka dalam penilaian risiko, desain prosedur, dan investigasi insiden tidak lagi dilihat sebagai formalitas, tetapi sebagai sumber data dan wawasan yang paling krusial. Ini membangun kepercayaan dan rasa kepemilikan terhadap program K3.

Manfaat lainnya adalah peningkatan Resiliensi Organisasi. Dengan fokus pada pemahaman dan pengelolaan variabilitas, sistem yang dirancang secara sistemik lebih mampu menyerap gangguan, beradaptasi dengan perubahan yang tidak terduga, dan pulih dari kegagalan dengan

cepat. Keselamatan tidak lagi rapuh dan bergantung pada kepatuhan yang sempurna, tetapi menjadi lebih tangguh dan fleksibel.

Pada akhirnya, mengintegrasikan pendekatan sistemik ke dalam SMK3 menjadikannya lebih "hidup". Ia memastikan bahwa sistem manajemen tidak hanya ada di atas kertas dalam bentuk manual dan prosedur, tetapi benar-benar mencerminkan dan membentuk cara organisasi berpikir, memutuskan, dan bertindak dalam kaitannya dengan keselamatan setiap hari. Ini adalah kunci untuk mencapai budaya keselamatan yang matang dan kinerja K3 yang unggul secara berkelanjutan.

## KESIMPULAN

Bab pertama ini telah membangun panggung untuk seluruh diskusi yang akan datang dengan menetapkan konteks fundamental mengenai peran K3 dalam industri modern dan memperkenalkan pergeseran paradigma yang krusial dari menyalahkan individu ke analisis sistem. Telah ditunjukkan bahwa K3 bukan lagi sekadar fungsi kepatuhan, melainkan pilar strategis yang menopang keberlanjutan, reputasi, dan daya saing organisasi. Investasi dalam keselamatan adalah investasi dalam keunggulan operasional, yang memberikan pengembalian finansial dan non-finansial yang signifikan.

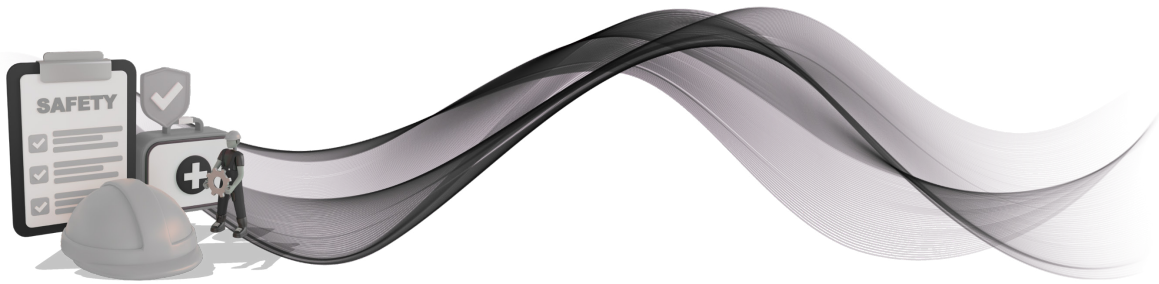
Analisis kritis terhadap data statistik kecelakaan kerja mengungkapkan bahwa narasi dominan yang menyalahkan *human error* sering kali merupakan simplifikasi yang berbahaya. Meskipun tindakan manusia tidak diragukan lagi merupakan bagian dari rantai kecelakaan, label "human error" sering kali menutupi kegagalan sistemik yang lebih dalam dan menjadi produk dari bias dalam pelaporan dan investigasi. Ketergantungan pada model sebab-akibat tradisional seperti Model Domino Heinrich semakin memperkuat fokus yang sempit ini, karena model-model tersebut secara inheren tidak mampu menangani kompleksitas interaksi dalam sistem sosio-teknis modern.

Sebagai respons, bab ini telah mengadvokasi adopsi pendekatan sistemik yang komprehensif. Pendekatan ini merekonseptualisasi kecelakaan bukan sebagai kegagalan komponen, melainkan sebagai properti emergent dari keseluruhan sistem. *Human error* dipandang sebagai gejala, bukan

penyebab, yang menandakan adanya ketidakselarasan antara desain kerja dan kapabilitas manusia. Dengan demikian, fokus intervensi bergeser dari mencoba mengubah perilaku individu menjadi merancang ulang sistem, termasuk teknologi, prosedur, dan struktur organisasi, untuk membuatnya lebih toleran terhadap kesalahan dan lebih tangguh.

Mengintegrasikan filosofi sistemik ini ke dalam kerangka Sistem Manajemen K3 formal adalah langkah selanjutnya yang logis. Hal ini memungkinkan organisasi untuk bergerak melampaui kepatuhan dan membangun kapasitas nyata untuk mengelola risiko secara proaktif, belajar dari semua peristiwa (baik sukses maupun gagal), dan secara berkelanjutan meningkatkan resiliensinya. Dengan fondasi konseptual yang telah diletakkan dalam bab ini, pembaca kini siap untuk menjelajahi model-model teoretis, alat analisis, dan strategi mitigasi spesifik yang akan diuraikan secara mendalam di bab-bab berikutnya. Perjalanan dari menyalahkan ke pemahaman sistemik telah dimulai.

**DUMMYY**



# BAB 2

## EVOLUSI PARADIGMA *HUMAN ERROR*: DARI PERSON-MODEL KE SYSTEM-MODEL

### PENDAHULUAN

Ketika sebuah insiden terjadi, respons intuitif pertama kita sering kali adalah mencari tahu “siapa” yang melakukan kesalahan. Media memberitakan “kelalaian pilot” setelah kecelakaan pesawat atau “kesalahan operator” pasca insiden pabrik. Reaksi ini, yang berakar kuat dalam psikologi manusia tentang sebab dan akibat, merupakan manifestasi dari sebuah paradigma berpikir yang telah mendominasi manajemen keselamatan selama hampir satu abad: *Person-Model* atau Model Individu. Paradigma ini memandang kesalahan manusia sebagai produk dari kekurangan individu, seperti kelalaian, kurangnya motivasi, kecerobohan, atau bahkan pelanggaran yang disengaja. Solusi yang ditawarkan pun bersifat langsung dan personal: salahkan, latih ulang, atau hukum individu yang terlibat.

Namun, seiring dengan meningkatnya kompleksitas sistem teknologi dan organisasi, keterbatasan fundamental dari pendekatan ini menjadi semakin nyata. Mengapa insiden yang sama terus berulang meskipun orang yang terlibat telah diganti? Mengapa para profesional yang sangat terlatih dan bermotivasi tinggi masih membuat kesalahan yang fatal?

Pertanyaan-pertanyaan ini tidak dapat dijawab secara memuaskan oleh *Person-Model*. Kegagalan berulang ini mendorong lahirnya sebuah revolusi konseptual dalam ilmu keselamatan, yaitu pergeseran menuju *System-Model* atau Model Sistem. Paradigma ini menawarkan lensa yang sama sekali berbeda: kesalahan manusia bukanlah penyebab utama kegagalan, melainkan gejala dari masalah yang lebih dalam yang tersembunyi di dalam sistem.

Bab ini akan menelusuri evolusi intelektual yang krusial ini. Pembahasan akan dimulai dengan membedah asumsi-asumsi dasar dari *Person-Model*, sebuah pendekatan yang melihat individu sebagai variabel yang tidak dapat diandalkan dalam sistem yang seharusnya aman. Kita akan mengeksplorasi bagaimana pandangan ini secara alami melahirkan *blame culture* atau budaya menyalahkan, sebuah lingkungan yang terbukti sangat merusak bagi upaya pembelajaran dan perbaikan keselamatan yang otentik. Kritik terhadap budaya ini akan menyoroti dampak negatifnya terhadap pelaporan insiden dan pentingnya membedakan antara hukuman dan akuntabilitas yang konstruktif.

Selanjutnya, bab ini akan memetakan pergeseran paradigma menuju *System-Model*. Dalam pandangan ini, fokus analisis beralih dari "siapa" yang gagal ke "mengapa" sistem tersebut memungkinkan terjadinya kegagalan. Konsep-konsep kunci seperti kondisi laten (*latent conditions*), "jebakan" tersembunyi yang ditinggalkan oleh para perancang, pembuat kebijakan, dan manajer, akan diperkenalkan sebagai anteseden yang jauh lebih kuat dari kecelakaan daripada kesalahan sesaat seorang individu. *Human error* akan didefinisikan ulang bukan sebagai kegagalan pribadi, tetapi sebagai manifestasi dari ketidakcocokan antara tuntutan tugas dan kapabilitas manusia.

Pergeseran ini lebih dari sekadar perdebatan akademis; ia memiliki implikasi praktis yang mendalam terhadap setiap aspek manajemen K3. Ia mengubah cara kita melakukan investigasi, merancang prosedur, melatih karyawan, dan mengukur kinerja keselamatan. *System-Model* menantang para pemimpin untuk berhenti mencari "apel busuk" dan mulai memeriksa "keranjang" tempat apel-apel itu disimpan. Ia menuntut kita untuk menjadi arsitek sistem yang andal, bukan lagi sekadar pengawas perilaku individu.

Sebagai puncaknya, bab ini akan menguraikan prinsip-prinsip dasar dari keselamatan berbasis sistem. Konsep-konsep seperti holisme, di mana sistem dipandang sebagai satu kesatuan yang saling bergantung, dan fokus pada perancangan proaktif akan dijelaskan. Pengenalan terhadap gagasan revolusioner *Safety-II*, yang mengajak kita untuk belajar dari keberhasilan sehari-hari alih-alih hanya dari kegagalan yang jarang terjadi, akan memberikan perspektif baru tentang bagaimana resiliensi dan keselamatan sebenarnya diciptakan di tempat kerja.

Memahami evolusi dari *Person-Model* ke *System-Model* adalah langkah fundamental bagi setiap praktisi K3 modern. Tanpa pemahaman ini, upaya-upaya kita untuk meningkatkan keselamatan akan tetap dangkal, reaktif, dan pada akhirnya tidak efektif. Bab ini bertujuan untuk membekali pembaca dengan kerangka berpikir baru yang menjadi landasan bagi semua model, teknik, dan strategi yang akan dibahas dalam buku ini.

## **A. Pendekatan Person-Model: Fokus pada Kesalahan Individu**

Pendekatan *Person-Model*, sering juga disebut sebagai pendekatan personal atau individualistik, merupakan cara pandang tertua dan paling intuitif dalam memahami kegagalan. Asumsi dasarnya sederhana: sistem dan teknologi pada dasarnya dirancang dengan baik dan aman, dan jika terjadi kecelakaan, itu pasti karena individu yang berinteraksi dengan sistem tersebut melakukan sesuatu yang salah. Dalam pandangan ini, manusia diposisikan sebagai sumber utama variabilitas dan risiko. Kesalahan dilihat sebagai produk dari proses mental yang menyimpang seperti lupa, tidak perhatian, motivasi yang buruk, kelalaian, atau bahkan kecerobohan yang disengaja.

Logika dari *Person-Model* sangat linear dan menarik karena kesederhanaannya. Jika kesalahan adalah penyebabnya, maka solusinya adalah menargetkan si pembuat kesalahan. Upaya mitigasi yang lahir dari paradigma ini sangat terfokus pada individu. Ini termasuk tindakan-tindakan seperti menulis lebih banyak prosedur, memberikan lebih banyak pelatihan, memasang lebih banyak poster peringatan, atau melakukan kampanye kesadaran untuk mendorong pekerja agar "lebih berhati-hati".

Jika metode-metode “lunak” ini gagal, pendekatan yang lebih “keras” akan diambil, seperti tindakan pendisiplinan, sanksi, atau bahkan pemecatan.

Fokus utama dari investigasi kecelakaan di bawah *Person-Model* adalah untuk menjawab pertanyaan “siapa yang bertanggung jawab?”. Investigator akan menelusuri rantai peristiwa ke belakang hingga mereka menemukan titik di mana seseorang melakukan tindakan yang menyimpang dari prosedur atau praktik yang diharapkan. Titik ini kemudian sering kali dilabeli sebagai “penyebab utama” (*root cause*), dan investigasi pun berhenti di sana. Tidak ada dorongan yang kuat untuk bertanya lebih lanjut: *mengapa* orang tersebut melakukan tindakan itu? Apa tekanan atau kendala yang mereka hadapi?

Pendekatan ini juga melahirkan upaya untuk mengidentifikasi dan menyaring individu yang dianggap “rawan kecelakaan” (*accident-prone*). Selama bertahun-tahun, banyak penelitian mencoba menemukan ciri-ciri kepribadian atau psikologis tertentu yang membuat seseorang lebih mungkin melakukan kesalahan. Meskipun penelitian modern telah menunjukkan bahwa konsep “kerawanan kecelakaan” sebagai sifat kepribadian yang stabil sebagian besar adalah mitos, warisan dari pemikiran ini masih bertahan dalam beberapa praktik rekrutmen atau penilaian kinerja.

Daya tarik abadi dari *Person-Model* terletak pada kemudahannya, baik secara konseptual maupun manajerial. Menyalahkan individu sering kali lebih mudah, lebih cepat, dan lebih murah daripada melakukan analisis mendalam terhadap sistem organisasi yang kompleks. Ini memungkinkan organisasi untuk mempertahankan ilusi bahwa sistem mereka pada dasarnya sehat dan hanya membutuhkan perbaikan pada beberapa “komponen manusia” yang rusak. Namun, seperti yang akan kita lihat, kemudahan ini datang dengan harga yang sangat mahal: kegagalan untuk belajar dan ketidakmampuan untuk mencegah terulangnya insiden serupa di masa depan.

*Person-Model* pada dasarnya memperlakukan gejala, yaitu kesalahan manusia, sebagai penyakit itu sendiri. Dengan hanya fokus pada gejala, ia gagal mengobati penyakit sistemik yang mendasarinya, membiarkannya

terus berkembang dan bermanifestasi kembali di waktu dan tempat yang berbeda, sering kali dengan konsekuensi yang lebih parah.

**Analogi/Contoh Kasus:** Pendekatan *Person-Model* dapat diibaratkan seperti "Teori Apel Busuk" (*Bad Apple Theory*). Bayangkan Anda memiliki satu barel penuh apel dan Anda menemukan satu apel yang busuk. Teori ini menyatakan bahwa masalahnya ada pada apel itu sendiri. Solusinya sederhana: buang apel busuk itu, dan barel akan kembali baik-baik saja. Pendekatan ini tidak pernah bertanya: "Mengapa apel itu menjadi busuk?". Mungkin kondisi penyimpanan di dalam barel itu terlalu lembab, atau ada jamur yang menyebar di seluruh barel, atau apel itu memar saat dimasukkan. *System-Model*, sebaliknya, akan memeriksa kondisi barel secara keseluruhan, karena ia memahami bahwa menempatkan apel yang segar dan bagus ke dalam barel yang buruk pada akhirnya akan menghasilkan lebih banyak apel busuk.

### 1. Asumsi Dasar dan Mekanisme Person-Model

Landasan dari *Person-Model* dibangun di atas serangkaian asumsi yang mendalam tentang sifat manusia dan kegagalan. Asumsi pertama dan yang paling fundamental adalah bahwa kesalahan adalah pilihan atau setidaknya kegagalan individu untuk menerapkan kontrol diri. Paradigma ini memandang tindakan manusia sebagai hasil dari niat sadar, dan oleh karena itu, penyimpangan dari norma yang diharapkan dilihat sebagai kegagalan dalam kehendak atau kemampuan. Istilah-istilah seperti "kelalaian", "kecerobohan", dan "ketidakpatuhan" yang sering digunakan dalam laporan investigasi berakar pada asumsi ini.

Asumsi kedua adalah bahwa dunia kerja pada dasarnya aman dan sistem dirancang dengan baik. Organisasi telah menyediakan prosedur yang benar, alat yang tepat, dan pelatihan yang memadai. Jika terjadi kecelakaan, itu karena seorang individu telah gagal memanfaatkan sumber daya ini dengan benar. Pandangan ini menciptakan dikotomi yang salah antara "sistem yang aman" dan "manusia yang tidak aman", mengabaikan kemungkinan bahwa sistem itu sendiri mungkin dirancang dengan cara yang provokatif terhadap kesalahan (*error-provoking*).

Asumsi ketiga adalah bahwa manusia dapat disempurnakan. Melalui kombinasi pelatihan, insentif, dan hukuman yang tepat, perilaku manusia dapat dibentuk untuk mencapai tingkat kepatuhan dan keandalan yang mendekati sempurna. Ini adalah dasar dari banyak program keselamatan berbasis perilaku (*Behavior-Based Safety*) yang berfokus pada pengamatan dan koreksi perilaku "tidak aman" di tempat kerja. Meskipun niatnya baik, asumsi ini sering kali mengabaikan keterbatasan kognitif dan fisiologis manusia yang inheren, seperti kapasitas memori kerja yang terbatas atau dampak kelelahan.

Mekanisme utama dari *Person-Model* adalah proses yang berfokus pada identifikasi, isolasi, dan remediasi individu. Investigasi, seperti yang disebutkan sebelumnya, bertujuan untuk menemukan individu yang tindakannya paling dekat dengan hasil negatif. Begitu "pelaku" ditemukan, mekanisme remediasi pun diaktifkan. Ini bisa berupa *counseling*, pelatihan ulang (*retraining*), penugasan kembali ke posisi yang kurang kritis, atau tindakan disipliner. Tujuannya adalah untuk "memperbaiki" individu atau, jika itu tidak mungkin, menyingkirkannya dari sistem untuk melindunginya dari kegagalan di masa depan.

Mekanisme lain adalah proliferasi pertahanan birokratis. Sebagai respons terhadap kesalahan, organisasi yang menganut *Person-Model* cenderung menambahkan lebih banyak aturan, prosedur, dan formulir. Logikanya adalah, jika prosedur yang ada dilanggar, maka prosedur tersebut perlu dibuat lebih rinci, lebih ketat, dan dengan lebih banyak lapisan persetujuan. Hasilnya sering kali adalah "hutan birokrasi" yang membuat pekerjaan menjadi lebih sulit dan rumit, yang secara ironis dapat menciptakan sumber-sumber kesalahan baru.

Pengukuran kinerja dalam *Person-Model* juga berfokus pada individu. Metrik seperti "jumlah pelanggaran K3 per orang" atau "tingkat kepatuhan terhadap prosedur" digunakan untuk mengevaluasi karyawan. Meskipun dapat berguna, metrik ini dapat mendorong perilaku yang tidak diinginkan, seperti menyembunyikan masalah untuk menghindari catatan buruk, dan mengalihkan perhatian dari pengukuran kesehatan sistem secara keseluruhan.

Secara keseluruhan, asumsi dan mekanisme *Person-Model* menciptakan sebuah siklus yang berpusat pada individu. Kesalahan terjadi, individu disalahkan, tindakan korektif diterapkan pada individu, dan sistem yang mendasarinya tetap tidak berubah. Siklus ini memberikan ilusi bahwa sesuatu sedang dilakukan untuk meningkatkan keselamatan, padahal pada kenyataannya, kerentanan yang sama tetap ada, menunggu individu berikutnya untuk jatuh ke dalam perangkap yang sama.

Pergeseran ke *System-Model* menuntut kita untuk secara radikal menantang setiap asumsi ini. Ini menuntut kita untuk menerima bahwa kesalahan bukanlah pilihan sadar, bahwa sistem sering kali jauh dari sempurna, dan bahwa tujuan kita bukanlah untuk menyempurnakan manusia, tetapi untuk merancang sistem yang mampu mengakomodasi dan mentolerir ketidaksempurnaan manusia.

## **2. Identifikasi Ciri-Ciri Individu yang Cenderung Berbuat Salah**

Sebuah konsekuensi logis dari *Person-Model* adalah pencarian "tipe" individu yang secara inheren lebih mungkin untuk melakukan kesalahan atau mengalami kecelakaan. Gagasan ini, yang dikenal sebagai teori "kerawanan kecelakaan" (*accident proneness*), pertama kali mendapatkan popularitas pada awal abad ke-20. Para peneliti pada saat itu berteori bahwa sebagian kecil populasi pekerja bertanggung jawab atas sebagian besar kecelakaan, dan bahwa kecenderungan ini adalah sifat kepribadian yang stabil dan dapat diukur.

Pencarian ini memicu gelombang penelitian yang mencoba mengidentifikasi ciri-ciri psikologis atau fisiologis dari individu yang "rawan kecelakaan". Tes-tes dikembangkan untuk mengukur berbagai atribut, mulai dari waktu reaksi dan koordinasi motorik hingga ciri-ciri kepribadian seperti impulsivitas, pengambilan risiko, atau neurotisme. Harapannya adalah bahwa dengan menggunakan tes-tes ini dalam proses seleksi, perusahaan dapat menyaring kandidat yang berisiko tinggi dan hanya mempekerjakan mereka yang dianggap "aman".

Namun, setelah beberapa dekade penelitian, bukti yang mendukung teori kerawanan kecelakaan sebagai sifat kepribadian yang stabil ternyata sangat lemah dan tidak konsisten. Para kritikus menunjukkan bahwa analisis

statistik awal yang tampaknya mendukung teori ini memiliki kelemahan metodologis yang serius. Distribusi kecelakaan yang tidak merata di antara populasi pekerja dapat dengan mudah dijelaskan oleh faktor kebetulan acak atau, yang lebih penting, oleh perbedaan dalam tingkat paparan bahaya dari pekerjaan yang berbeda. Seseorang yang bekerja sebagai penebang kayu secara alami akan memiliki lebih banyak insiden daripada seorang akuntan, bukan karena kepribadiannya, tetapi karena sifat pekerjaannya.

Meskipun konsep “kerawanan kecelakaan” sebagai sifat bawaan telah sebagian besar ditinggalkan oleh komunitas ilmiah, gema dari pemikiran ini masih bertahan. Dalam praktiknya, manajer atau penyelia mungkin masih secara informal melabeli beberapa pekerja sebagai “ceroboh” atau “pembuat masalah”. Label-label ini dapat menciptakan bias konfirmasi: begitu seseorang dicap sebagai “tidak aman”, setiap kesalahan kecil yang mereka buat akan diperhatikan dan diingat, sementara kesalahan yang dibuat oleh pekerja lain mungkin diabaikan. Hal ini dapat menyebabkan perlakuan yang tidak adil dan demoralisasi.

Fokus modern dalam psikologi K3 telah bergeser dari sifat-sifat yang stabil ke keadaan sementara (*transient states*) yang dapat memengaruhi kinerja siapa pun, terlepas dari kepribadiannya. Faktor-faktor seperti kelelahan, stres, beban kerja kognitif yang berlebihan, atau gangguan pribadi telah terbukti menjadi prediktor kesalahan yang jauh lebih kuat daripada ciri kepribadian apa pun. Ini berarti bahwa bahkan pekerja yang paling berpengalaman dan berhati-hati pun dapat melakukan kesalahan jika kondisi kerjanya tidak mendukung.

Oleh karena itu, upaya untuk meningkatkan keselamatan dengan cara mencoba mengidentifikasi dan menyingkirkan individu yang “cenderung berbuat salah” pada dasarnya adalah jalan buntu. Ini adalah manifestasi lain dari *Person-Model* yang mengalihkan perhatian dari akar masalah yang sebenarnya. Alih-alih mencoba mengubah atau menyaring pekerja, pendekatan yang jauh lebih produktif adalah dengan mengubah dan memperbaiki kondisi kerja. Fokusnya seharusnya adalah menciptakan lingkungan di mana semua jenis individu, dengan segala variabilitas dan ketidaksempurnaan mereka, dapat bekerja dengan aman dan produktif.

### 3. Kasus Kegagalan Penerapan Person-Model di Industri

Sejarah industri penuh dengan contoh-contoh di mana pendekatan *Person-Model* diterapkan setelah sebuah bencana, namun terbukti gagal mencegah terulangnya kegagalan serupa. Salah satu studi kasus yang paling sering dikutip adalah serangkaian kecelakaan yang menimpa Korean Air pada tahun 1980-an dan 1990-an. Selama periode ini, maskapai tersebut memiliki salah satu catatan keselamatan terburuk di antara maskapai-maskapai besar dunia, yang berpuncak pada kecelakaan fatal Korean Air Penerbangan 801 di Guam pada tahun 1997.

Setelah setiap kecelakaan, investigasi awal dan respons maskapai sangat khas *Person-Model*. Pilot yang terlibat disalahkan atas "kesalahan pilot", "kurangnya kesadaran situasi", atau "kegagalan untuk mengikuti prosedur". Solusi yang diterapkan berfokus pada individu: pilot diskors atau dipecat, dan pelatihan teknis ditingkatkan dengan penekanan pada kepatuhan yang lebih ketat terhadap aturan penerbangan. Manajemen percaya bahwa dengan menyingkirkan "pilot yang buruk" dan menekankan disiplin, masalah akan teratasi.

Namun, kecelakaan terus terjadi, sering kali dengan pola yang sangat mirip. Pilot-pilot yang berbeda, dalam situasi yang berbeda, terus membuat jenis kesalahan pengambilan keputusan dan komunikasi yang sama. Kegagalan pendekatan *Person-Model* menjadi sangat jelas: masalahnya bukan terletak pada individu-individu pilot, tetapi pada sistem di mana mereka beroperasi. Ini adalah masalah "barek", bukan hanya beberapa "apel busuk".

Titik baliknya datang ketika para analis, termasuk konsultan eksternal David Greenberg, mulai menerapkan lensa *System-Model*. Mereka menemukan bahwa akar masalahnya terletak pada budaya hirarkis yang kaku di dalam kokpit, yang berakar pada budaya nasional Korea. Kopilot dan insinyur penerbangan merasa sangat tidak nyaman untuk menantang atau mempertanyakan keputusan kapten, bahkan ketika mereka tahu kapten membuat kesalahan. Komunikasi bersifat tidak langsung dan terlalu sopan, yang sering menyebabkan pesan-pesan kritis tidak tersampaikan dengan jelas. Ini adalah kegagalan masif dalam *Crew Resource Management*

(CRM), sebuah konsep yang menekankan kerja tim dan komunikasi terbuka di kokpit.

Selain itu, ditemukan masalah sistemik lainnya. Jadwal penerbangan yang melelahkan, pelatihan CRM yang tidak efektif dan hanya bersifat formalitas, serta kurangnya standardisasi dalam penggunaan bahasa Inggris (bahasa standar penerbangan internasional) semuanya berkontribusi pada penciptaan kondisi laten yang membuat kesalahan menjadi lebih mungkin terjadi. Kesalahan pilot bukanlah penyebab utama; itu adalah titik akhir yang dapat diprediksi dari serangkaian kegagalan organisasi dan budaya.

Sebagai respons terhadap analisis sistemik ini, Korean Air melakukan perombakan total. Mereka mereformasi program pelatihan CRM mereka secara radikal, dengan penekanan kuat pada komunikasi yang asertif dan pemberdayaan semua anggota awak. Mereka secara aktif mendorong penggunaan bahasa Inggris di kokpit untuk menghilangkan ambiguitas budaya. Mereka merevisi kebijakan penjadwalan dan berinvestasi dalam budaya keselamatan yang lebih terbuka dan tidak menghukum. Hasilnya sangat dramatis: dalam dua dekade berikutnya, catatan keselamatan Korean Air berubah menjadi salah satu yang terbaik di dunia.

Kasus Korean Air adalah ilustrasi yang kuat tentang kegagalan *Person-Model*. Menyalahkan dan melatih ulang pilot secara individu terbukti sama sekali tidak efektif karena tidak mengatasi kondisi budaya dan organisasi yang mendasari yang membentuk perilaku mereka. Hanya ketika fokus bergeser ke perbaikan sistem secara keseluruhan, kemajuan yang nyata dan berkelanjutan dapat dicapai. Ini menunjukkan bahwa untuk mencegah kecelakaan, kita harus melihat melampaui tindakan individu dan memahami konteks yang lebih luas di mana tindakan itu terjadi.

## **B. Kritik terhadap Blame Culture dan Pendekatan Hukuman**

Budaya menyalahkan (*blame culture*) adalah produk sampingan yang tak terhindarkan dan paling merusak dari *Person-Model*. Ketika sebuah organisasi secara institusional percaya bahwa kesalahan adalah kegagalan individu, maka respons alami terhadap kesalahan adalah mencari seseorang untuk disalahkan dan dihukum. Lingkungan seperti ini mungkin tampak

memuaskan dahaga akan keadilan atau akuntabilitas yang sederhana, tetapi pada kenyataannya, ia secara aktif meracuni iklim keselamatan dan menjadi penghalang terbesar bagi pembelajaran organisasi. Budaya ini beroperasi di bawah ilusi bahwa jika orang cukup takut membuat kesalahan, mereka akan berhenti membuatnya. Kenyataannya justru sebaliknya.

Kritik utama terhadap budaya menyalahkan adalah dampaknya yang melumpuhkan terhadap aliran informasi penting. Keselamatan dalam sistem yang kompleks sangat bergantung pada kemauan orang-orang di lini depan untuk melaporkan tidak hanya kecelakaan, tetapi juga kesalahan kecil, *near misses* (hampir celaka), dan kondisi tidak aman yang mereka amati. Laporan-laporan ini adalah "sinyal gratis" atau "informasi emas" yang memberikan wawasan berharga tentang kesehatan sistem pertahanan organisasi. Mereka adalah kesempatan untuk mengidentifikasi dan memperbaiki masalah sebelum menyebabkan kerugian nyata.

Dalam *blame culture*, aliran informasi vital ini terhenti. Karyawan, karena takut akan sanksi, cemoohan, atau kerusakan reputasi, belajar bahwa hal teraman untuk dilakukan adalah menyembunyikan kesalahan dan diam tentang masalah. Siklus "tembak pembawa pesan" (*shoot the messenger*) dengan cepat mengajarkan semua orang bahwa kejujuran tidak dihargai. Akibatnya, manajemen menjadi buta terhadap risiko yang sebenarnya ada di operasi mereka. Mereka mungkin melihat data insiden yang rendah dan menyimpulkan bahwa semuanya aman, padahal di bawah permukaan, kondisi laten sedang menumpuk dan organisasi sedang melayang menuju bencana.

Pendekatan hukuman juga sering kali salah sasaran karena gagal membedakan antara berbagai jenis perilaku manusia. Ia cenderung memperlakukan kesalahan yang tidak disengaja (*honest mistake*), yang dibuat oleh seorang profesional yang bermaksud baik, dengan cara yang sama seperti pelanggaran yang disengaja dan sembrono (*reckless violation*). Perbedaan ini sangat penting untuk respons yang adil dan efektif. Menghukum seseorang karena kesalahan yang tidak disengaja tidak akan membuat mereka atau orang lain "kurang salah" di masa depan; itu hanya akan membuat mereka lebih takut.

Penting untuk ditekankan bahwa bergerak menjauh dari budaya menyalahkan bukan berarti menciptakan budaya “tanpa menyalahkan” (*no-blame culture*) yang absolut atau menghilangkan akuntabilitas. Ini adalah kesalahpahaman yang umum. Akuntabilitas sangat penting, tetapi harus dipahami secara lebih canggih. Akuntabilitas yang sejati bukanlah tentang menemukan seseorang untuk dihukum setelah kegagalan, melainkan tentang menciptakan rasa tanggung jawab bersama untuk membangun dan memelihara sistem yang aman sebelum kegagalan terjadi. Ini melibatkan penciptaan lingkungan di mana orang merasa aman untuk berbicara, melaporkan masalah, dan mengambil tanggung jawab atas tindakan mereka dalam konteks yang adil.

Subbab ini akan menguraikan lebih lanjut dampak negatif dari budaya menyalahkan, mengklarifikasi perbedaan krusial antara hukuman dan akuntabilitas, dan menyoroti pentingnya membangun lingkungan yang aman secara psikologis di mana orang tidak takut untuk berbicara. Mengatasi *blame culture* adalah prasyarat fundamental untuk menerapkan *System-Model* secara efektif.

**Analogi/Contoh Kasus:** Bayangkan sebuah kapal dengan banyak pelaut di dek. Kapten menerapkan aturan bahwa siapa pun yang melihat dan melaporkan adanya kebocoran kecil pada lambung kapal akan dicambuk, karena dianggap membawa berita buruk. Akibatnya, tidak ada pelaut yang berani melaporkan kebocoran kecil yang mereka lihat. Mereka hanya diam-diam menambalnya sebisa mungkin atau berharap orang lain yang akan melaporkannya. Kapten, di anjungan, tidak menerima laporan apa pun dan berpikir kapalnya kuat dan aman. Sementara itu, di bawah dek, puluhan kebocoran kecil perlahan-lahan membanjiri kapal. Budaya menyalahkan bekerja persis seperti ini: ia menciptakan keheningan yang mematikan, memberikan ilusi keselamatan palsu sementara kapal perlahan-lahan tenggelam.

### **1. Dampak Negatif Budaya Menyalahkan pada Pelaporan Insiden**

Dampak paling langsung dan merusak dari budaya menyalahkan adalah penekanan sistematis terhadap pelaporan insiden. Dalam lingkungan kerja di mana mengakui kesalahan atau menyoroti masalah dapat menyebabkan

hukuman, kehilangan pekerjaan, atau stigma sosial, respons manusia yang paling rasional adalah diam. Fenomena ini menciptakan apa yang oleh para ahli disebut sebagai “organisasi bisu” (*mute organization*), di mana informasi penting tentang risiko tidak pernah mencapai tingkat manajemen di mana tindakan perbaikan dapat diambil.

Ketika pelaporan ditekan, organisasi kehilangan data yang paling berharga untuk pembelajaran dan perbaikan proaktif. *Near misses* atau insiden “hampir celaka” adalah contoh utama. Insiden-insiden ini, di mana sebuah kesalahan atau kegagalan terjadi tetapi untungnya tidak mengakibatkan cedera atau kerusakan, adalah kesempatan belajar yang sempurna. Mereka menyingkapkan kelemahan dalam pertahanan sistem tanpa biaya kerugian yang sebenarnya. Dalam budaya yang sehat, pelaporan *near miss* didorong dan dirayakan sebagai kontribusi positif terhadap keselamatan. Sebaliknya, dalam *blame culture*, *near miss* disembunyikan karena dilihat sebagai bukti kegagalan individu yang hampir tertangkap.

Penekanan pelaporan juga mendistorsi metrik kinerja keselamatan organisasi. Manajemen mungkin melihat angka *Lost Time Injury* (LTI) yang rendah dan merasa puas, padahal angka tersebut mungkin rendah bukan karena sistemnya aman, tetapi karena cedera-cedera ringan dan sedang tidak dilaporkan. Karyawan mungkin berada di bawah tekanan untuk bekerja sambil menahan sakit atau mencari pengobatan di luar jalur resmi perusahaan untuk menghindari “merusak catatan keselamatan” tim atau departemen. Ini menciptakan ilusi keselamatan yang sangat berbahaya, karena manajemen membuat keputusan strategis berdasarkan data yang tidak akurat dan terlalu optimis.

Budaya menyalahkan juga menghancurkan kepercayaan, yang merupakan fondasi dari setiap program keselamatan yang efektif. Ketika karyawan tidak percaya bahwa manajemen akan menanggapi laporan mereka secara adil dan konstruktif, mereka akan berhenti berkomunikasi. Hubungan antara pekerja dan manajemen berubah dari kemitraan kolaboratif menjadi hubungan yang penuh permusuhan dan kecurigaan. Dalam kondisi seperti ini, inisiatif keselamatan baru yang diperkenalkan oleh manajemen akan disambut dengan sinisme dan kepatuhan yang dangkal, bukan dengan keterlibatan yang tulus.

Dampak negatif lainnya adalah terhambatnya inovasi dan pemecahan masalah. Dalam *blame culture*, orang takut untuk mengambil risiko yang diperhitungkan atau mencoba cara-cara baru untuk melakukan sesuatu, karena jika terjadi kesalahan, mereka tahu siapa yang akan disalahkan. Hal ini menyebabkan stagnasi, di mana orang lebih memilih untuk tetap berpegang pada prosedur yang sudah usang dan tidak efisien, bahkan jika mereka tahu ada cara yang lebih baik, karena itu adalah pilihan yang "aman" secara politis. Karyawan berhenti menggunakan kecerdasan dan kreativitas mereka untuk memecahkan masalah dan hanya melakukan apa yang diperintahkan untuk menghindari masalah.

Secara psikologis, bekerja dalam *blame culture* sangat menguras tenaga dan menimbulkan stres. Ketakutan yang konstan untuk tidak membuat kesalahan dapat menyebabkan kelelahan mental, kecemasan, dan penurunan kepuasan kerja. Ironisnya, kondisi-kondisi ini sendiri merupakan faktor kontribusi yang kuat terhadap terjadinya kesalahan. Jadi, budaya menyalahkan tidak hanya gagal mencegah kesalahan, tetapi secara aktif dapat menciptakan kondisi psikologis yang membuatnya lebih mungkin terjadi.

Pada akhirnya, dampak kumulatif dari budaya menyalahkan adalah kebutaan organisasi. Tanpa data yang jujur dari lini depan, organisasi tidak dapat melihat kerentanannya sendiri. Ia terus beroperasi dengan asumsi-asumsi yang salah tentang bagaimana pekerjaan sebenarnya dilakukan dan risiko apa yang sebenarnya dihadapi oleh karyawannya setiap hari. Kebutaan ini sering kali baru tersingkap setelah terjadinya bencana besar yang tidak dapat lagi disembunyikan.

## **2. Membedakan Hukuman dari Akuntabilitas**

Salah satu argumen yang sering dilontarkan untuk mempertahankan *blame culture* adalah bahwa hal itu diperlukan untuk menegakkan akuntabilitas. Argumen ini didasarkan pada kesalahpahaman yang mendalam tentang makna sebenarnya dari akuntabilitas. Dalam konteks keselamatan modern, penting untuk secara tegas membedakan antara pendekatan yang berfokus pada hukuman dan pendekatan yang

membangun akuntabilitas yang sejati dan adil. Keduanya memiliki tujuan dan hasil yang sangat berbeda.

Hukuman bersifat retrospektif dan retributif. Fokusnya adalah pada masa lalu: sebuah kegagalan telah terjadi, dan tujuannya adalah untuk memberikan penderitaan atau sanksi kepada individu yang dianggap bertanggung jawab sebagai bentuk pembalasan atau "keadilan". Prosesnya sering kali bersifat adversial, mencari bukti untuk menyalahkan. Hukuman cenderung mengakhiri percakapan; begitu seseorang dihukum, organisasi merasa masalahnya telah "diselesaikan" dan berhenti mencari pelajaran yang lebih dalam dari insiden tersebut. Pendekatan ini jarang sekali mengarah pada perbaikan sistemik yang berkelanjutan.

Akuntabilitas, di sisi lain, bersifat prospektif dan restoratif. Fokusnya adalah pada masa depan: bagaimana kita bisa belajar dari apa yang terjadi untuk membuat sistem lebih aman bagi semua orang? Akuntabilitas berarti mengambil tanggung jawab atas tindakan seseorang dan berkontribusi pada solusi. Ini melibatkan penjelasan yang jujur tentang apa yang terjadi dan mengapa, dari perspektif orang yang terlibat. Prosesnya bersifat kolaboratif, mencari pemahaman. Akuntabilitas yang sejati tidak mengakhiri percakapan, melainkan memulainya. Ia menggunakan insiden sebagai pemicu untuk dialog yang mendalam tentang perbaikan sistem.

Memindahkan fokus dari hukuman ke akuntabilitas bukan berarti tidak ada konsekuensi atas tindakan. Dalam kerangka kerja *Just Culture* (Budaya Adil), yang akan dibahas lebih rinci di Bab 16, ada pengakuan bahwa tidak semua tindakan diciptakan sama. Sebuah sistem respons yang adil akan membedakan antara: (1) Kesalahan manusia yang tidak disengaja (*human error*), di mana responsnya adalah memberikan dukungan dan memperbaiki sistem; (2) Perilaku berisiko (*at-risk behavior*), di mana seseorang mengambil jalan pintas yang tidak disadari risikonya, di mana responsnya adalah pembinaan dan peningkatan kesadaran; dan (3) Pelanggaran yang sembrono (*reckless violation*), di mana seseorang secara sadar mengabaikan risiko yang substansial dan tidak dapat dibenarkan, di mana tindakan disipliner mungkin diperlukan.

Perbedaan krusialnya adalah bahwa bahkan dalam kasus pelanggaran sembrono, investigasi yang berbasis akuntabilitas akan tetap bertanya: "Faktor sistem apa (misalnya, tekanan produksi yang ekstrim, pengawasan yang tidak memadai) yang mungkin telah mendorong atau memungkinkan perilaku sembrono ini?". Tujuannya adalah untuk selalu belajar dan memperbaiki sistem, bahkan ketika tindakan disipliner diperlukan.

Akuntabilitas juga merupakan jalan dua arah. Karyawan memiliki akuntabilitas untuk bekerja dengan aman dan melaporkan masalah. Di sisi lain, manajemen memiliki akuntabilitas yang setara, bahkan lebih besar, untuk menyediakan sumber daya, alat, pelatihan, dan desain sistem yang memungkinkan pekerjaan dilakukan dengan aman. Dalam *blame culture*, akuntabilitas hanya dituntut ke bawah. Dalam budaya akuntabilitas yang sejati, akuntabilitas dituntut di semua tingkat organisasi, dari dewan direksi hingga pekerja di lini depan.

Dengan demikian, meninggalkan pendekatan hukuman tidak berarti meninggalkan akuntabilitas. Sebaliknya, itu berarti merangkul bentuk akuntabilitas yang lebih canggih, lebih adil, dan yang terpenting, jauh lebih efektif dalam mendorong pembelajaran dan peningkatan keselamatan. Ini adalah tentang beralih dari pertanyaan "Siapa yang harus disalahkan?" ke pertanyaan "Apa yang bisa kita pelajari dan bagaimana kita bisa bertanggung jawab bersama untuk memperbaikinya?".

### **3. Pentingnya Lingkungan yang Aman untuk Berbicara (Speak-Up Culture)**

Sebagai penangkal langsung terhadap racun budaya menyalahkan, organisasi perlu secara proaktif membangun lingkungan yang aman untuk berbicara, atau yang sering disebut sebagai budaya *speak-up*. Konsep ini berakar pada gagasan "keamanan psikologis" (*psychological safety*), yang didefinisikan oleh Amy Edmondson dari Harvard sebagai "keyakinan bersama bahwa tim aman untuk pengambilan risiko interpersonal". Dalam konteks K3, ini berarti menciptakan lingkungan di mana setiap karyawan, terlepas dari pangkat atau posisinya, merasa yakin bahwa mereka dapat menyuarakan keprihatinan, mengajukan pertanyaan, mengakui kesalahan,

atau menantang status quo tanpa takut akan penghinaan, pembalasan, atau hukuman.

Pentingnya lingkungan seperti ini untuk keselamatan tidak dapat dilebih-lebihkan. Sistem yang kompleks dan dinamis secara konstan menghasilkan sinyal-sinyal lemah tentang potensi masalah. Sering kali, orang-orang yang pertama kali mendeteksi sinyal-sinyal ini adalah mereka yang berada di lini depan, operator mesin yang merasakan getaran aneh, perawat yang meragukan dosis obat, atau pekerja konstruksi yang melihat penyangga yang tampak tidak stabil. Dalam budaya *speak-up*, sinyal-sinyal ini akan segera disuarakan dan ditindaklanjuti. Dalam budaya diam yang diciptakan oleh rasa takut, sinyal-sinyal ini diabaikan, dan potensi bencana terus berkembang tanpa terdeteksi.

Membangun budaya *speak-up* membutuhkan komitmen yang tulus dan tindakan nyata dari kepemimpinan di semua tingkatan. Para pemimpin harus secara eksplisit mengundang masukan dan secara aktif meminta pendapat, terutama dari anggota tim yang lebih junior atau pendiam. Mereka harus menunjukkan kerentanan dengan mengakui kesalahan mereka sendiri, yang memberikan sinyal kuat bahwa kesalahan adalah bagian normal dari proses belajar, bukan sesuatu yang harus disembunyikan.

Ketika seseorang menyuarakan keprihatinan, respons pemimpin sangatlah krusial. Jika keprihatinan itu diabaikan, diremehkan, atau, lebih buruk lagi, jika orang yang menyuarakannya dihukum, maka itu akan menjadi pelajaran yang sangat kuat bagi semua orang yang menyaksikannya: "Jangan berbicara". Sebaliknya, jika pemimpin menanggapi dengan rasa ingin tahu, menghargai masukan tersebut (bahkan jika ternyata itu bukan masalah besar), dan berterima kasih kepada orang tersebut karena telah berani berbicara, itu akan memperkuat perilaku yang diinginkan. Setiap interaksi adalah kesempatan untuk membangun atau menghancurkan keamanan psikologis.

Organisasi juga perlu menciptakan saluran formal dan informal yang mudah diakses untuk pelaporan. Ini bisa berupa sistem pelaporan anonim, pertemuan rutin tentang keselamatan di mana diskusi terbuka didorong, atau kebijakan "pintu terbuka" yang benar-benar dipraktikkan oleh para

manajer. Tujuannya adalah untuk menghilangkan sebanyak mungkin hambatan bagi orang untuk berbagi apa yang mereka ketahui.

Budaya *speak-up* juga penting untuk mencegah “normalisasi penyimpangan” (*normalization of deviance*). Ini adalah fenomena di mana sebuah praktik yang menyimpang dari standar keselamatan secara bertahap menjadi diterima sebagai norma karena tidak ada hal buruk yang langsung terjadi. Bencana pesawat ulang-alik Challenger adalah contoh klasik, di mana para insinyur menyuarakan keprihatinan tentang kinerja O-ring pada suhu rendah, tetapi keprihatinan ini berulang kali dikesampingkan oleh manajemen hingga akhirnya menjadi bencana. Budaya *speak-up* yang kuat akan memberikan mekanisme untuk menantang normalisasi penyimpangan ini sebelum terlambat.

Pada akhirnya, lingkungan yang aman untuk berbicara adalah fondasi dari organisasi yang memiliki keandalan tinggi (*High Reliability Organization* - HRO). Organisasi-organisasi ini, seperti kapal induk atau unit kontrol lalu lintas udara, beroperasi di lingkungan yang sangat kompleks dan berisiko tinggi namun berhasil mempertahankan tingkat keselamatan yang luar biasa. Salah satu ciri khas mereka adalah “keasyikan dengan kegagalan” (*preoccupation with failure*), yang berarti mereka secara konstan mencari dan membahas potensi masalah, sekecil apa pun. Keasyikan ini hanya mungkin terjadi dalam lingkungan di mana setiap orang merasa aman untuk berbicara.

### **C. Pergeseran Paradigma ke *System-Model***

Keterbatasan *Person-Model* dan dampak destruktif dari budaya menyalahkan secara kolektif menciptakan kebutuhan mendesak akan cara berpikir yang baru dan lebih kuat tentang keselamatan. Kebutuhan ini dipenuhi oleh pergeseran paradigma ke *System-Model*. Pergeseran ini merupakan salah satu perkembangan paling penting dalam ilmu keselamatan selama setengah abad terakhir, mengubah secara fundamental cara kita memahami, menganalisis, dan mengelola kegagalan. Inti dari pergeseran ini adalah perubahan fokus: dari melihat kesalahan individu sebagai penyebab kecelakaan, menjadi melihatnya sebagai gejala dari masalah yang lebih dalam di dalam sistem kerja.

*System-Model* tidak menanyakan “siapa yang salah?”, melainkan “mengapa sistem ini memungkinkan kesalahan terjadi?”. Ia beroperasi di bawah asumsi dasar bahwa manusia pada dasarnya tidak sempurna dan akan selalu membuat kesalahan. Oleh karena itu, tujuan dari manajemen keselamatan bukanlah untuk menciptakan manusia yang sempurna, melainkan untuk menciptakan sistem yang toleran terhadap kesalahan (*error-tolerant*). Sistem yang baik adalah sistem yang mengantisipasi kesalahan, membuatnya sulit untuk dilakukan, mudah untuk dideteksi, dan mudah untuk dipulihkan, serta meminimalkan konsekuensi negatifnya jika tetap terjadi.

Dalam pandangan ini, kesalahan seorang individu di lini depan (kegagalan aktif atau *active failure*) tidak terjadi dalam ruang hampa. Itu adalah puncak dari gunung es. Di bawah permukaan terdapat serangkaian kondisi laten (*latent conditions*), keputusan yang buruk, desain yang cacat, prosedur yang tidak praktis, pelatihan yang tidak memadai, atau tujuan yang saling bertentangan, yang mungkin telah dibuat oleh orang-orang yang jauh dari lokasi kejadian, baik secara waktu maupun ruang. Kondisi-kondisi laten ini dapat “tertidur” di dalam sistem selama berbulan-bulan atau bahkan bertahun-tahun, seperti ranjau darat, menunggu kombinasi keadaan tertentu untuk memicunya.

Oleh karena itu, investigasi yang dipandu oleh *System-Model* tidak berhenti pada kesalahan operator. Sebaliknya, ia menggunakan kesalahan tersebut sebagai titik awal, sebagai “jendela” untuk melihat kelemahan yang lebih dalam di dalam organisasi. Proses investigasi menjadi seperti pekerjaan detektif arkeologi, melacak kembali dari kegagalan aktif di permukaan untuk menggali dan mengungkap lapisan-lapisan kondisi laten yang berkontribusi di tingkat manajemen, desain, dan kebijakan.

Pergeseran paradigma ini juga mengubah definisi *human error* itu sendiri. Ia tidak lagi dilihat sebagai cacat karakter atau kegagalan psikologis. Sebaliknya, *human error* didefinisikan sebagai hasil dari ketidakcocokan (*mismatch*) antara tuntutan sistem dan kapabilitas (dan keterbatasan) manusia. Dari perspektif ini, banyak kesalahan bukanlah hal yang acak, melainkan respons yang dapat diprediksi terhadap lingkungan kerja yang dirancang dengan buruk. Jika Anda memberikan prosedur yang

membingungkan, alat yang tidak ergonomis, dan tekanan waktu yang ekstrim kepada seseorang, Anda hampir dapat menjamin bahwa kesalahan akan terjadi.

Dengan mengadopsi *System-Model*, organisasi beralih dari pendekatan reaktif yang berfokus pada perbaikan individu menjadi pendekatan proaktif yang berfokus pada perancangan ulang sistem. Upaya keselamatan menjadi kurang tentang pengawasan dan kepatuhan, dan lebih banyak tentang *human factors engineering*, desain organisasi, dan manajemen budaya. Ini adalah pergeseran dari mencoba mengendalikan orang menjadi mencoba memahami dan mengendalikan kondisi di mana orang bekerja.

**Analogi/Contoh Kasus:** Bayangkan seorang pejalan kaki tersandung akar pohon yang menonjol di trotoar dan jatuh. *Person-Model* akan berkata, "Pejalan kaki itu ceroboh, dia seharusnya melihat ke mana dia berjalan." Solusinya adalah menempelkan poster "Hati-Hati Saat Berjalan!". *System-Model*, sebaliknya, akan bertanya, "Mengapa akar pohon itu menonjol di sana?". Jawabannya mungkin karena departemen pertamanan tidak memiliki anggaran yang cukup untuk pemeliharaan rutin, atau karena spesifikasi konstruksi trotoar tidak memperhitungkan pertumbuhan akar. Solusi sistemik adalah memperbaiki trotoar dan memastikan adanya program pemeliharaan yang efektif. Ia memperbaiki kondisi yang menciptakan "jebakan" bagi *setiap* pejalan kaki, bukan hanya menyalahkan satu orang yang kebetulan jatuh hari itu.

## 1. Kesalahan Manusia sebagai Gejala Kegagalan Sistem

Konsep inti yang membedakan *System-Model* dari pendahulunya adalah pemahaman bahwa kesalahan manusia bukanlah titik awal dari sebuah kegagalan, melainkan titik tengah atau bahkan titik akhir. Kesalahan yang dibuat oleh individu di lini depan, seorang operator menekan tombol yang salah, seorang ahli bedah salah mengidentifikasi lokasi operasi, seorang pengemudi melewati lampu merah, adalah manifestasi yang terlihat dari masalah yang lebih dalam dan sering kali tidak terlihat di dalam sistem. Dengan kata lain, kesalahan adalah gejalanya, bukan penyakitnya.

Untuk memahami bagaimana ini bekerja, kita perlu memperkenalkan "prinsip rasionalitas lokal" (*principle of local rationality*), sebuah konsep

yang dipopulerkan oleh Sidney Dekker. Prinsip ini menyatakan bahwa orang tidak dengan sengaja melakukan hal-hal yang mereka tahu akan berakhir buruk. Sebaliknya, dari sudut pandang mereka pada saat itu, tindakan mereka masuk akal. Perilaku mereka dibentuk oleh tujuan yang mereka coba capai, pengetahuan yang mereka miliki (yang sering kali tidak lengkap), dan fokus perhatian mereka (yang sering kali diarahkan oleh fitur-fitur sistem). Sebuah "kesalahan", dari sudut pandang luar setelah kejadian (*hindsight*), sebenarnya adalah hasil dari seseorang yang mencoba melakukan yang terbaik dalam situasi yang kompleks dan sering kali ambigu.

Jika kita menerima prinsip ini, maka tugas investigator kecelakaan berubah secara dramatis. Alih-alih menilai tindakan tersebut sebagai "salah" atau "bodoh", tugasnya adalah mencoba merekonstruksi rasionalitas lokal individu tersebut. Investigator harus bertanya: "Melihat dunia dari sudut pandang orang ini pada saat itu, dengan tekanan dan informasi yang mereka miliki, mengapa tindakan ini tampak sebagai hal yang benar untuk dilakukan?". Jawaban atas pertanyaan ini hampir selalu mengarah pada fitur-fitur sistem di sekitarnya.

Mungkin prosedur yang mereka coba ikuti tidak jelas atau bertentangan. Mungkin desain antarmuka memberikan informasi yang menyesatkan. Mungkin mereka kelelahan setelah bekerja 12 jam. Mungkin budaya organisasi secara implisit memberi penghargaan pada kecepatan di atas keselamatan, mendorong mereka untuk mengambil jalan pintas. Faktor-faktor inilah, desain yang buruk, prosedur yang tidak praktis, tekanan produksi, pelatihan yang tidak realistis, yang merupakan "penyakit" sistemik yang sebenarnya. Kesalahan individu hanyalah "demam" atau "ruam" yang menandakan adanya infeksi yang lebih dalam.

Dengan memandang kesalahan sebagai gejala, kita dapat menghindari dua perangkat utama dari *Person-Model*. Pertama, kita menghindari penyalahan korban (*victim blaming*). Kita mengakui bahwa individu yang membuat kesalahan sering kali adalah pewaris dari sistem yang cacat; mereka adalah "korban kedua" dari kecelakaan tersebut. Kedua, kita membuka jalan untuk perbaikan yang lebih efektif. Mengobati demam dengan kompres dingin (analog dengan melatih ulang individu) tidak

akan menyembuhkan infeksi. Kita harus memberikan antibiotik yang tepat (analog dengan merancang ulang sistem) untuk mengatasi akar penyebab penyakitnya.

Pandangan ini juga menjelaskan mengapa kecelakaan yang sama sering terulang dengan orang yang berbeda. Jika sistem kerja memiliki "jebakan" bawaan, seperti dua tombol yang tampak identik tetapi memiliki fungsi yang sangat berbeda dan ditempatkan berdampingan, hanya masalah waktu sebelum *seseorang* jatuh ke dalam perangkap itu. Menghukum orang pertama yang membuat kesalahan tidak akan mengubah desain tombol tersebut. Orang berikutnya yang ditempatkan dalam situasi yang sama, terutama di bawah tekanan, kemungkinan besar akan membuat kesalahan yang sama.

Jadi, setiap kali kita melihat sebuah *human error*, kita harus melatih diri kita untuk tidak berhenti di situ. Kita harus melihatnya sebagai sinyal, sebagai data, sebagai petunjuk berharga yang menunjuk ke arah di mana sistem kita perlu diperbaiki. Kesalahan bukan lagi sesuatu yang memalukan untuk disembunyikan, tetapi menjadi sumber informasi yang tak ternilai untuk pembelajaran dan peningkatan organisasi.

## **2. Analisis Kondisi Laten (Latent Conditions) di Tingkat Organisasi**

Jika kesalahan individu (*active failures*) adalah gejala, maka kondisi laten (*latent conditions*) adalah penyakitnya. Konsep kondisi laten, yang dikembangkan oleh James Reason, adalah salah satu kontribusi terpenting bagi *System-Model*. Kondisi laten adalah keputusan atau tindakan yang berpotensi membahayakan, yang konsekuensinya mungkin tidak langsung terlihat. Mereka adalah "patogen residu" yang dapat tetap tidak aktif di dalam sistem untuk waktu yang lama, menunggu kombinasi keadaan yang tepat untuk berkontribusi pada kecelakaan.

Berbeda dengan kegagalan aktif, yang dampaknya terasa segera dan biasanya dilakukan oleh orang-orang di lini depan (operator, pilot, perawat), kondisi laten sering kali berasal dari orang-orang di tingkat atas organisasi, yang jauh dari lokasi operasional. Mereka adalah produk sampingan dari keputusan yang dibuat oleh perancang, insinyur, penulis prosedur, manajer, dan pembuat kebijakan. Setiap keputusan ini memiliki

potensi untuk menciptakan kelemahan atau "lubang" dalam pertahanan sistem.

Contoh kondisi laten di tingkat organisasi sangat beragam. Di bidang manajemen dan kebijakan, ini bisa berupa:

- a. Tujuan yang saling bertentangan: Menetapkan target produksi yang sangat agresif tanpa menyediakan sumber daya yang memadai, sehingga secara implisit mendorong pekerja untuk mengorbankan keselamatan demi kecepatan.
- b. Jadwal kerja yang buruk: Menerapkan shift kerja 12 jam selama beberapa hari berturut-turut yang secara pasti akan menyebabkan kelelahan.
- c. Sistem pelaporan yang tidak efektif: Memiliki prosedur pelaporan insiden yang rumit dan tidak anonim, yang menghalangi orang untuk melaporkan masalah.
- d. Alokasi sumber daya yang tidak memadai: Gagal menginvestasikan dana yang cukup untuk perawatan peralatan, pelatihan, atau staf K3.

Di bidang desain dan rekayasa, kondisi laten dapat berupa:

- a. Desain antarmuka yang membingungkan: Menciptakan panel kontrol di mana alarm kritis sulit dibedakan dari alarm rutin.
- b. Peralatan yang tidak ergonomis: Menyediakan alat yang membutuhkan postur canggung atau kekuatan berlebihan, yang menyebabkan kelelahan dan cedera.
- c. Prosedur yang tidak praktis: Menulis prosedur di kantor yang tidak mencerminkan realitas dan kendala pekerjaan di lapangan.

Di bidang pelatihan dan kompetensi, kondisi laten meliputi:

- a. Pelatihan yang tidak memadai: Memberikan pelatihan yang hanya berfokus pada "apa" yang harus dilakukan, tanpa menjelaskan "mengapa" atau apa yang harus dilakukan dalam situasi tak terduga.
- b. Asumsi kompetensi yang salah: Menganggap bahwa karena seseorang memiliki sertifikat, mereka secara otomatis kompeten untuk menangani semua situasi.

Analisis kondisi laten sangat penting karena dua alasan. Pertama, mereka membantu menjelaskan mengapa kecelakaan besar jarang sekali memiliki satu penyebab tunggal. Sebaliknya, bencana adalah hasil dari penumpukan dan interaksi dari banyak kondisi laten yang berbeda. Kedua, karena kondisi laten dapat diidentifikasi dan diperbaiki *sebelum* kecelakaan terjadi, mereka menawarkan target yang jauh lebih efektif untuk intervensi proaktif. Jauh lebih efisien untuk memperbaiki keputusan manajemen yang buruk daripada mencoba mengendalikan perilaku setiap karyawan setiap saat.

Tantangan utama dalam analisis kondisi laten adalah bahwa mereka sering kali tidak terlihat dalam operasi sehari-hari. Semuanya tampak berjalan normal sampai kombinasi pemicu yang tepat, kegagalan aktif, menyingkap keberadaan mereka. Oleh karena itu, organisasi perlu secara aktif “berburu” kondisi laten melalui audit yang mendalam, penilaian risiko sistemik, dan, yang paling penting, dengan mendengarkan dengan cermat orang-orang di lini depan yang sering kali paling menyadari keberadaan “jebakan” ini dalam pekerjaan mereka sehari-hari.

### 3. Definisi Human Error dalam Konteks Interaksi Manusia-Sistem

Pergeseran ke *System-Model* menuntut kita untuk mendefinisikan kembali *human error* itu sendiri. Dalam kerangka berpikir yang baru ini, kesalahan tidak lagi dilihat sebagai sumber kegagalan yang independen atau sebagai cacat psikologis. Sebaliknya, *human error* paling baik dipahami sebagai sebuah ketidakcocokan (*mismatch*) pada antarmuka antara tuntutan tugas atau sistem dengan kapabilitas dan keterbatasan manusia. Kesalahan adalah hasil, bukan penyebab; itu adalah produk dari desain, bukan produk dari sifat manusia yang cacat.

Definisi ini memindahkan fokus dari dalam kepala individu ke interaksi antara individu dan dunia luar. Alih-alih bertanya “Apa yang salah dengan orang ini?”, kita bertanya “Apa yang salah dengan desain sistem ini sehingga memicu atau memungkinkan kesalahan ini?”. Ini adalah inti dari disiplin ilmu *Human Factors* atau Ergonomi, yang secara sistematis mempelajari interaksi manusia-sistem dengan tujuan untuk mengoptimalkan kesejahteraan manusia dan kinerja sistem secara keseluruhan.

Ada banyak jenis ketidakcocokan yang dapat menyebabkan kesalahan. Ketidakcocokan kognitif terjadi ketika tuntutan mental dari suatu tugas melebihi kapasitas kognitif manusia. Contohnya termasuk:

- a. Meminta operator untuk memantau terlalu banyak layar secara bersamaan, yang menyebabkan kelebihan beban perhatian (*attentional overload*).
- b. Prosedur yang membutuhkan pekerja untuk mengingat urutan langkah yang panjang dan rumit, yang membebani memori kerja (*working memory*).
- c. Desain alarm yang menghasilkan ratusan peringatan selama gangguan pabrik (*alarm flooding*), membuatnya mustahil bagi operator untuk mengidentifikasi masalah yang sebenarnya penting.

Ketidakcocokan fisik terjadi ketika tuntutan fisik dari suatu tugas tidak sesuai dengan anatomi atau fisiologi manusia. Contohnya termasuk:

- a. Menempatkan katup atau tuas penting di lokasi yang sulit dijangkau.
- b. Merancang alat yang membutuhkan kekuatan genggam yang berlebihan atau postur yang canggung, yang menyebabkan kelelahan dan cedera regangan berulang.
- c. Lingkungan kerja dengan pencahayaan yang buruk atau tingkat kebisingan yang tinggi, yang mengganggu persepsi dan komunikasi.

Dengan mendefinisikan ulang kesalahan sebagai produk dari ketidakcocokan, kita membuka serangkaian strategi mitigasi yang sama sekali baru dan lebih kuat. Alih-alih mencoba mengubah manusia (melalui pelatihan atau hukuman), kita fokus pada mengubah sistem agar lebih "ramah pengguna" dan "tahan kesalahan". Pendekatan ini dikenal sebagai desain yang berpusat pada manusia (*human-centred design*).

Strategi-strategi ini termasuk menyederhanakan tugas, mengurangi beban memori, membuat informasi penting lebih menonjol, merancang kontrol yang intuitif, dan mengotomatiskan tugas-tugas yang monoton atau rawan kesalahan. Salah satu contoh klasik adalah prinsip *poka-yoke* atau *mistake-proofing*, di mana sistem dirancang sedemikian rupa sehingga kesalahan secara fisik tidak mungkin dilakukan, seperti konektor USB yang hanya bisa masuk satu arah.

Pandangan ini juga mengakui bahwa variabilitas dalam kinerja manusia tidak selalu negatif. Variabilitas yang sama yang terkadang mengarah pada kesalahan juga merupakan sumber dari kreativitas, adaptasi, dan resiliensi. Manusalah yang sering kali membuat sistem yang dirancang dengan buruk tetap berfungsi dengan menemukan solusi dan cara kerja alternatif. Oleh karena-tujuan kita bukanlah untuk menghilangkan variabilitas manusia, yang merupakan hal yang mustahil. Sebaliknya, tujuannya adalah untuk memahami variabilitas tersebut dan merancang sistem yang dapat menyalurkannya ke arah yang produktif dan menangkapnya dengan aman ketika mengarah pada penyimpangan yang berisiko.

#### **D. Prinsip Dasar Keselamatan Berbasis Sistem**

Mengadopsi *System-Model* lebih dari sekadar perubahan terminologi; ini adalah tentang menerapkan serangkaian prinsip dasar yang memandu cara kita merancang, mengelola, dan meningkatkan keselamatan. Prinsip-prinsip ini memberikan kerangka kerja konseptual untuk mengubah teori sistemik menjadi praktik nyata. Mereka adalah fondasi di mana strategi mitigasi yang efektif dibangun. Tanpa pemahaman yang kuat tentang prinsip-prinsip ini, penerapan teknik-teknik keselamatan modern berisiko menjadi mekanis dan kehilangan esensinya.

Prinsip pertama adalah holisme, yang menegaskan bahwa sistem harus dipahami secara keseluruhan, bukan hanya sebagai kumpulan bagian-bagian yang terpisah. Keselamatan adalah properti *emergent*, yang berarti ia muncul dari interaksi antar komponen, bukan berada di dalam komponen itu sendiri. Memperbaiki atau mengoptimalkan satu bagian dari sistem secara terpisah bahkan dapat menimbulkan masalah baru di tempat lain. Oleh karena itu, setiap intervensi keselamatan harus mempertimbangkan dampaknya terhadap keseluruhan sistem. Ini menuntut kemampuan untuk berpikir secara interdisipliner dan melihat hubungan sebab-akibat yang tidak langsung.

Prinsip kedua adalah fokus pada desain proaktif. Pendekatan sistemik secara inheren bersifat proaktif. Daripada menunggu kegagalan terjadi dan kemudian bereaksi terhadapnya, tujuannya adalah untuk merancang keselamatan ke dalam sistem sejak awal. Ini berarti bahwa pertimbangan

*human factors* dan analisis risiko sistemik harus menjadi bagian integral dari proses desain dan pengadaan, bukan sesuatu yang ditambahkan di akhir. Hierarki kontrol, yang memprioritaskan eliminasi dan substitusi bahaya di atas kontrol administratif atau APD, adalah manifestasi praktis dari prinsip ini. Pencegahan selalu lebih baik daripada mitigasi.

Prinsip ketiga adalah pengelolaan variabilitas. Berbeda dengan *Person-Model* yang mencoba menghilangkan variabilitas kinerja manusia, pendekatan sistemik menerimanya sebagai fitur yang tak terhindarkan dan bahkan diperlukan dari sistem kerja. Tugasnya bukanlah untuk memaksa kepatuhan yang kaku, tetapi untuk memahami mengapa variabilitas terjadi dan bagaimana cara mengelolanya. Ini melibatkan penciptaan batasan atau penjaga (*safeguards*) yang jelas untuk menjaga agar variasi tetap dalam batas yang aman, sambil memberikan fleksibilitas yang cukup bagi pekerja untuk beradaptasi dengan kondisi yang tidak terduga. Konsep *Safety-II* adalah perwujudan utama dari prinsip ini, yang berfokus pada penguatan kemampuan adaptif yang membuat sistem berhasil sebagian besar waktu.

Prinsip-prinsip ini secara kolektif memberikan cetak biru untuk membangun organisasi yang tidak hanya aman, tetapi juga tangguh (*resilient*). Organisasi yang tangguh adalah organisasi yang mampu mengantisipasi, memantau, merespons, dan belajar dari tantangan dan kejutan. Mereka tidak rapuh dan mudah hancur oleh satu kegagalan. Sebaliknya, mereka memiliki kapasitas untuk menyerap gangguan, beradaptasi, dan bahkan menjadi lebih kuat setelah menghadapi kesulitan. Prinsip-prinsip keselamatan berbasis sistem adalah jalan menuju resiliensi tersebut.

**Analogi/Contoh Kasus:** Membangun sistem yang aman ibarat membangun jembatan gantung yang kokoh. Seorang insinyur yang baik tidak hanya mengandalkan kekuatan setiap kabel baja secara individu (komponen). Dia memahami bahwa kekuatan jembatan secara keseluruhan (sistem) bergantung pada bagaimana semua komponen, kabel, menara, dek, fondasi, berinteraksi di bawah berbagai tekanan seperti angin, beban, dan gempa (holisme). Dia merancang jembatan dengan margin keselamatan yang besar dan fitur-fitur redundan sejak awal (desain proaktif). Dia juga tahu bahwa jembatan akan sedikit bergoyang dan melentur sebagai

respons terhadap angin; ini adalah variabilitas yang normal dan dirancang. Tujuannya bukan untuk membuat jembatan yang kaku, tetapi yang dapat mengelola variabilitas ini dengan aman (pengelolaan variabilitas).

### **1. Sistem sebagai Kesatuan Komponen yang Saling Bergantung**

Prinsip holisme adalah landasan dari semua pemikiran sistemik. Ia mengajarkan kita bahwa untuk memahami fenomena yang kompleks seperti keselamatan, kita tidak bisa hanya membedah sistem menjadi bagian-bagiannya dan menganalisis setiap bagian secara terpisah. Melakukan hal itu akan membuat kita kehilangan esensi terpenting: interaksi dan hubungan timbal balik di antara bagian-bagian tersebut. Keselamatan, atau ketiadaannya, tidak terletak pada pekerja, mesin, atau prosedur secara individual, melainkan pada cara mereka terhubung dan berfungsi bersama sebagai satu kesatuan.

Sebuah sistem kerja dapat dianggap terdiri dari beberapa komponen utama yang saling bergantung, seperti yang dijelaskan dalam model-model seperti SHELL (yang akan dibahas di Bab 6): Manusia (*Liveware*), Teknologi (*Hardware*), Prosedur (*Software*), dan Lingkungan (*Environment*). Kegagalan sering kali terjadi di "ruang putih" antar kotak-kotak ini, yaitu pada antarmuka dan interaksi di antara mereka. Misalnya, kecelakaan mungkin terjadi bukan karena mesinnya rusak atau operatornya tidak kompeten, tetapi karena antarmuka antara mesin dan operator dirancang dengan buruk, sehingga sulit bagi operator untuk memahami status mesin.

Implikasi dari prinsip ini sangat besar. Ini berarti bahwa solusi untuk masalah keselamatan jarang sekali bersifat lokal. Memperbaiki satu komponen tanpa mempertimbangkan dampaknya pada komponen lain bisa menjadi tidak efektif atau bahkan kontra-produktif. Sebagai contoh, memperkenalkan teknologi otomatisasi baru (*Hardware*) untuk mengurangi beban kerja operator (*Liveware*) mungkin tampak seperti ide yang bagus. Namun, jika otomatisasi ini dirancang dengan buruk, ia dapat menciptakan masalah baru, seperti membuat operator menjadi pasif dan kehilangan kesadaran situasi, atau menuntut keterampilan pemecahan masalah yang sama sekali baru yang belum pernah mereka latih.

Pemikiran holistik juga menuntut kita untuk memperluas batas analisis kita. Sebuah kecelakaan di sebuah pabrik mungkin tidak dapat dipahami sepenuhnya hanya dengan melihat apa yang terjadi di dalam pabrik tersebut. Kita mungkin perlu melihat ke atas, pada keputusan yang dibuat di kantor pusat perusahaan mengenai anggaran perawatan, dan ke luar, pada tekanan pasar yang menuntut pengiriman produk lebih cepat. Sistem pabrik adalah bagian dari sistem perusahaan yang lebih besar, yang pada gilirannya adalah bagian dari sistem industri dan ekonomi yang lebih luas.

Untuk mempraktikkan holisme, para profesional K3 perlu mengembangkan keterampilan dalam pemetaan sistem. Teknik-teknik seperti diagram alir proses, analisis jejaring sosial, atau model analisis kecelakaan sistemik seperti AcciMap membantu memvisualisasikan komponen-komponen sistem dan hubungan di antara mereka. Alat-alat ini memungkinkan kita untuk melihat pola dan koneksi yang mungkin tidak terlihat jika kita hanya fokus pada satu titik kegagalan.

Pada dasarnya, prinsip ini mengubah peran praktisi K3 dari seorang "inspektur komponen" menjadi seorang "analisis sistem". Tujuannya bukan lagi hanya untuk menemukan bagian yang rusak, tetapi untuk memahami dinamika keseluruhan sistem. Ini adalah pergeseran dari pandangan dunia yang mekanistik dan reduksionis ke pandangan dunia yang lebih organik dan terintegrasi, yang jauh lebih cocok untuk menangani kompleksitas dan ketidakpastian yang menjadi ciri khas dunia kerja modern.

## **2. Fokus pada Perancangan Proses yang Mencegah Kesalahan**

Jika kita menerima bahwa kesalahan manusia adalah hasil dari ketidakcocokan antara desain sistem dan kapabilitas manusia, maka kesimpulan logisnya adalah bahwa cara paling efektif untuk mengelola kesalahan adalah melalui perancangan yang lebih baik. Prinsip ini menempatkan pencegahan proaktif di jantung manajemen keselamatan. Alih-alih menunggu orang membuat kesalahan dan kemudian mencoba mengoreksi mereka, kita harus berusaha untuk merancang sistem kerja di mana kesalahan menjadi sulit, jika bukan tidak mungkin, untuk dilakukan sejak awal. Ini adalah pergeseran dari reaktivitas ke proaktivitas.

Pendekatan ini sering diringkas dalam Hierarki Kontrol Risiko. Hierarki ini mengurutkan metode pengendalian risiko dari yang paling efektif hingga yang paling tidak efektif. Di puncak hierarki adalah Eliminasi (menghilangkan bahaya sepenuhnya) dan Substitusi (mengganti proses atau material berbahaya dengan yang lebih aman). Di bawahnya adalah Kontrol Rekayasa (mengisolasi orang dari bahaya melalui desain). Dan di bagian bawah, yang paling tidak efektif, adalah Kontrol Administratif (mengandalkan prosedur dan pelatihan) dan Alat Pelindung Diri (APD). Person-Model secara historis terlalu banyak berfokus pada bagian bawah hierarki, mencoba mengubah perilaku orang. Pendekatan sistemik mengarahkan perhatian kita ke puncak, pada perancangan ulang pekerjaan itu sendiri.

Fokus pada perancangan ini mencakup berbagai tingkatan. Pada tingkat desain fisik, ini melibatkan penerapan prinsip-prinsip ergonomi untuk memastikan bahwa stasiun kerja, alat, dan peralatan sesuai dengan ukuran, kekuatan, dan postur tubuh manusia. Ini juga mencakup desain *poka-yoke* atau *mistake-proofing*, di mana fitur-fitur fisik mencegah tindakan yang salah, seperti colokan yang hanya bisa masuk ke soket yang benar.

Pada tingkat desain kognitif, fokusnya adalah pada perancangan antarmuka dan informasi agar sesuai dengan cara otak manusia memproses informasi. Ini termasuk:

- a. Menyederhanakan tugas: Memecah proses yang kompleks menjadi langkah-langkah yang lebih kecil dan lebih mudah dikelola.
- b. Standardisasi: Menggunakan tata letak, warna, dan simbol yang konsisten untuk kontrol dan tampilan.
- c. Membuat batasan (constraints): Membatasi pilihan yang tersedia bagi pengguna untuk mencegah tindakan yang berbahaya.
- d. Memberikan umpan balik yang jelas: Memastikan bahwa sistem secara segera dan jelas memberitahu pengguna tentang hasil dari tindakan mereka.

Pada tingkat desain proses dan prosedur, ini berarti menjauh dari dokumen yang panjang dan padat teks yang ditulis di kantor. Sebaliknya, prosedur harus dikembangkan secara kolaboratif dengan pengguna akhir,

menggunakan bahasa yang sederhana, visualisasi, diagram alir, dan daftar periksa (checklists). Prosedur harus dirancang untuk digunakan dalam praktik, bukan hanya untuk memenuhi persyaratan audit.

Mengintegrasikan fokus perancangan ini ke dalam siklus hidup organisasi adalah kuncinya. Pertimbangan keselamatan dan *human factors* harus dimasukkan sejak tahap konsep awal, pengadaan, dan instalasi sistem baru. Jauh lebih mudah dan lebih murah untuk merancang keselamatan sejak awal daripada mencoba “memperbaikinya” pada sistem yang sudah ada. Ini membutuhkan keterlibatan profesional K3 dan *human factors* sebagai mitra strategis dalam tim proyek, bukan hanya sebagai pemeriksa di akhir proses.

Pada akhirnya, prinsip ini didasarkan pada pengakuan yang rendah hati: jauh lebih mudah untuk mengubah kondisi di mana orang bekerja daripada mencoba mengubah sifat dasar manusia. Dengan berfokus pada perancangan proses, tugas, dan alat yang lebih baik, kita secara proaktif menghilangkan “jebakan kesalahan” dari lingkungan kerja, menciptakan sistem yang secara inheren lebih aman dan lebih andal.

### **3. Konsep Safety-II (Mempelajari Apa yang Berjalan dengan Baik)**

Salah satu perkembangan konseptual terbaru dan paling berpengaruh dalam pemikiran sistemik adalah pengenalan konsep *Safety-I* dan *Safety-II* oleh Erik Hollnagel. Kerangka kerja ini memberikan cara baru untuk berpikir tentang apa itu keselamatan dan bagaimana kita mencapainya. Secara tradisional, manajemen keselamatan telah beroperasi hampir secara eksklusif dalam paradigma *Safety-I*.

*Safety-I* mendefinisikan keselamatan sebagai ketiadaan hasil negatif. Dalam pandangan ini, sebuah sistem dianggap aman jika tidak ada kecelakaan, insiden, atau kerugian. Akibatnya, fokus utama dari manajemen keselamatan adalah pada kegagalan. Kita menjadi ahli dalam hal-hal yang salah. Kita menginvestigasi kecelakaan, menghitung tingkat cedera, dan menganalisis laporan insiden. Pendekatannya pada dasarnya reaktif: kita menunggu sesuatu yang buruk terjadi, lalu kita mencoba mencari tahu mengapa itu terjadi dan memastikan itu tidak terjadi lagi. Meskipun penting, fokus eksklusif pada kegagalan ini memiliki keterbatasan. Kegagalan,

untungnya, adalah peristiwa yang relatif jarang. Jika kita hanya belajar dari kegagalan, kita kehilangan banyak sekali data tentang bagaimana sistem kita benar-benar berfungsi.

Sebagai alternatif, Hollnagel mengusulkan *Safety-II*, yang mendefinisikan keselamatan sebagai kehadiran kapasitas positif. Dalam pandangan ini, keselamatan adalah kemampuan sistem untuk berhasil dalam kondisi yang diharapkan maupun yang tidak terduga. Fokus *Safety-II* adalah pada pemahaman mengapa hal-hal berjalan dengan baik hampir sepanjang waktu. Mengingat bahwa 99.9% (atau lebih) dari semua aktivitas kerja selesai tanpa insiden, ada banyak sekali yang bisa dipelajari dari keberhasilan sehari-hari ini.

Pendekatan *Safety-II* mengakui bahwa pekerjaan seperti yang direncanakan dalam prosedur (*work-as-imagined*) hampir tidak pernah sama dengan pekerjaan seperti yang sebenarnya dilakukan di lapangan (*work-as-done*). Prosedur tidak pernah bisa mencakup semua kemungkinan variasi dan kejutan yang dihadapi pekerja. Untuk menyelesaikan pekerjaan, pekerja harus terus-menerus beradaptasi, menyesuaikan, dan berimprovisasi. Adaptasi dan penyesuaian inilah yang membuat sistem berfungsi dan produktif.

Dari perspektif *Safety-I*, adaptasi ini sering dilihat secara negatif sebagai "pelanggaran" atau "penyimpangan". Dari perspektif *Safety-II*, adaptasi ini dilihat sebagai sumber utama resiliensi. Manusia adalah yang menjembatani kesenjangan antara prosedur yang kaku dan realitas yang berantakan. Terkadang, adaptasi ini bisa salah dan berkontribusi pada kegagalan, tetapi sebagian besar waktu, adaptasi inilah yang menciptakan keberhasilan.

Oleh karena itu, tujuan dari manajemen *Safety-II* adalah untuk memahami bagaimana "pekerjaan-sebagaimana-dilakukan" ini berhasil. Ini melibatkan metode-metode seperti observasi etnografi, wawancara apresiatif, dan *learning teams*, di mana para manajer dan praktisi K3 pergi ke lapangan bukan untuk mencari pelanggaran, tetapi untuk bertanya kepada pekerja: "Apa tantangan terbesar dalam pekerjaan Anda? Apa saja penyesuaian yang harus Anda lakukan agar pekerjaan ini berhasil? Apa yang membuat hari ini menjadi hari yang baik?".

Dengan memahami sumber-sumber resiliensi ini, organisasi kemudian dapat secara proaktif memperkuatnya. Ini mungkin berarti memberikan lebih banyak otonomi kepada tim, meningkatkan pelatihan dalam pemecahan masalah, atau merancang sistem yang memberikan umpan balik yang lebih baik untuk mendukung adaptasi yang cerdas.

*Safety-I* dan *Safety-II* tidak saling eksklusif; keduanya diperlukan. Kita masih perlu menginvestigasi kegagalan ketika terjadi (*Safety-I*). Tetapi kita harus melengkapinya dengan pemahaman proaktif tentang keberhasilan (*Safety-II*). Dengan melakukan itu, kita beralih dari manajemen keselamatan yang hanya berfokus pada pencegahan hal-hal buruk menjadi manajemen keselamatan yang juga berfokus pada promosi hal-hal baik. Ini adalah pandangan yang lebih seimbang, lebih lengkap, dan pada akhirnya lebih kuat tentang cara menciptakan keselamatan yang berkelanjutan.

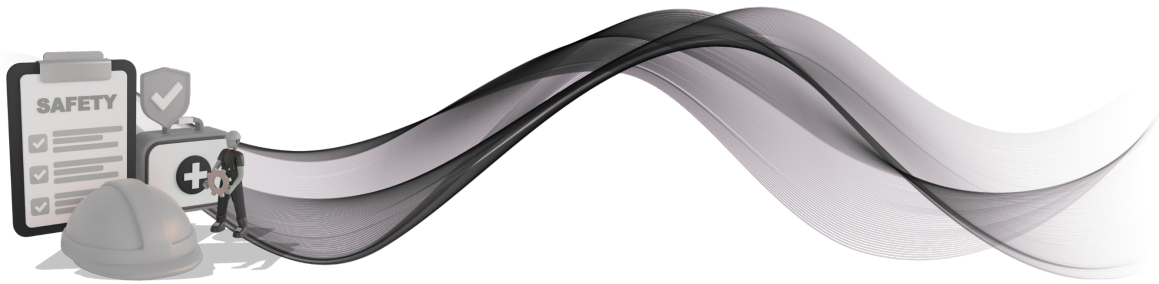
## KESIMPULAN

Bab kedua ini telah memetakan sebuah perjalanan intelektual yang fundamental dalam ilmu keselamatan: evolusi dari *Person-Model* yang usang ke *System-Model* yang lebih kuat dan relevan. Telah ditunjukkan bahwa *Person-Model*, dengan fokusnya pada kesalahan individu sebagai penyebab utama kegagalan, secara inheren terbatas. Pendekatan ini melahirkan budaya menyalahkan yang beracun, yang menekan pelaporan, menghambat pembelajaran, dan pada akhirnya gagal mencegah terulangnya kecelakaan. Upaya untuk "memperbaiki" manusia melalui hukuman atau pelatihan ulang terbukti tidak efektif karena mengabaikan konteks sistemik yang lebih luas di mana individu bekerja.

Sebagai respons, *System-Model* menawarkan sebuah paradigma yang transformatif. Dengan menyatakan bahwa kesalahan manusia adalah gejala, bukan penyebab, model ini mengalihkan fokus analisis dari individu ke sistem. Ia memaksa kita untuk mencari kondisi-kondisi laten, kelemahan tersembunyi dalam desain, manajemen, dan kebijakan, yang menciptakan prasyarat untuk kegagalan. Definisi ulang *human error* sebagai ketidakcocokan antara tuntutan sistem dan kapabilitas manusia membuka jalan bagi strategi intervensi yang jauh lebih efektif, yang berpusat pada perancangan ulang sistem kerja agar lebih toleran terhadap kesalahan dan lebih mendukung kinerja manusia.

Prinsip-prinsip dasar keselamatan berbasis sistem, holisme, desain proaktif, dan pengelolaan variabilitas, menyediakan pilar-pilar konseptual untuk menerapkan pendekatan ini dalam praktik. Pengenalan konsep *Safety-II* lebih lanjut memperkaya paradigma ini dengan mendorong kita untuk tidak hanya belajar dari kegagalan yang jarang terjadi, tetapi juga dari keberhasilan yang melimpah setiap hari. Dengan memahami bagaimana pekerja beradaptasi untuk menciptakan kesuksesan, kita dapat memperkuat resiliensi organisasi secara proaktif.

Pergeseran dari *Person-Model* ke *System-Model* bukanlah sekadar pilihan akademis, melainkan sebuah keharusan praktis bagi setiap organisasi yang serius dalam upaya mencapai tingkat keselamatan yang unggul. Ini adalah fondasi di mana semua analisis dan intervensi yang efektif harus dibangun. Dengan kerangka berpikir baru ini, pembaca kini dipersiapkan untuk mendalami model-model spesifik, seperti Model Keju Swiss dan Model SHELL pada bab-bab berikutnya, yang akan memberikan alat praktis untuk menerapkan pemikiran sistemik dalam analisis dan mitigasi *human error*.



# BAB 3

## DEFINISI DAN TIPOLOGI *HUMAN ERROR*

### PENDAHULUAN

Mengapa seorang pilot berpengalaman melewati item krusial dalam *checklist* pra-terbang? Mengapa seorang teknisi yang kompeten menyambungkan kabel yang salah meskipun telah melakukannya ratusan kali? Mengapa sebuah tim konstruksi secara kolektif mengambil jalan pintas yang berisiko? Jawaban sederhana dan tidak memuaskan untuk semua pertanyaan ini adalah "*human error*". Namun, menggunakan frasa ini sebagai penjelasan tunggal sama informatifnya dengan seorang dokter yang menyatakan "sakit" sebagai diagnosis. Frasa tersebut adalah sebuah label, bukan sebuah penjelasan. Ia mengaburkan lebih banyak daripada yang ia ungkapkan, karena ia memperlakukan semua kegagalan kinerja manusia seolah-olah mereka adalah fenomena yang sama, padahal kenyataannya sangat berbeda.

Untuk bergerak melampaui penyalahan yang dangkal dan menuju mitigasi yang efektif, kita harus terlebih dahulu membedah dan memahami berbagai bentuk dan mekanisme dari *human error*. Tidak semua kesalahan diciptakan sama. Kesalahan akibat selip perhatian saat melakukan tugas rutin secara fundamental berbeda dari kesalahan yang timbul dari keputusan

yang salah dalam situasi yang belum pernah terjadi sebelumnya. Demikian pula, penyimpangan dari prosedur yang tidak disengaja memiliki akar penyebab yang berbeda dari pelanggaran yang dilakukan secara sadar untuk menghemat waktu. Masing-masing menuntut strategi pencegahan yang sangat berbeda.

Bab ini akan berfungsi sebagai landasan taksonomi untuk sisa buku ini, dengan menyediakan definisi yang presisi dan kerangka kerja klasifikasi yang kuat untuk berbagai jenis kegagalan kinerja manusia. Tujuan utamanya adalah untuk membekali pembaca dengan "lensa diagnostik" yang lebih tajam. Dengan lensa ini, pembaca akan dapat melihat sebuah insiden dan tidak hanya melabelinya sebagai *human error*, tetapi juga mengklasifikasikannya secara spesifik: apakah ini *slip*, *lapse*, *mistake*, atau *violation*? Memahami perbedaan ini adalah langkah pertama yang krusial dalam melacak kembali ke kondisi sistemik yang mendasarinya.

Pembahasan akan dimulai dengan menetapkan definisi formal dari *human error* dalam konteks sistem, yang berpusat pada konsep niat (*intention*). Ini akan membawa kita pada pembedaan fundamental antara kesalahan (*errors*), tindakan yang tidak sesuai dengan rencana, dan pelanggaran (*violations*), yaitu penyimpangan yang disengaja dari aturan atau prosedur. Memahami perbedaan ini sangat penting karena ia mengarahkan kita pada jalur analisis yang sama sekali berbeda. Kesalahan sering kali berakar pada masalah kognitif dan desain, sementara pelanggaran sering kali terkait dengan faktor-faktor motivasi, budaya, dan organisasi.

Selanjutnya, bab ini akan menyelami taksonomi klasik yang dikembangkan oleh James Reason, yang membagi kesalahan menjadi tiga kategori utama berdasarkan mekanisme kognitifnya: *slips*, *lapses*, dan *mistakes*. Setiap kategori akan dianalisis secara mendalam, dengan contoh-contoh konkret untuk mengilustrasikan bagaimana mereka bermanifestasi dalam lingkungan kerja. Pemahaman ini akan memungkinkan kita untuk menghubungkan jenis kesalahan tertentu dengan jenis intervensi yang paling mungkin berhasil, misalnya, perbaikan desain untuk *slips*, atau alat bantu memori untuk *lapses*.

Bab ini juga akan memberikan perhatian yang sama pentingnya pada perilaku berisiko dalam bentuk pelanggaran. Pelanggaran tidak akan diperlakukan sebagai tindakan kejahatan sederhana, tetapi akan dianalisis sebagai perilaku yang sering kali dibentuk oleh konteks kerja. Klasifikasi pelanggaran menjadi rutin, situasional, dan pengecualian akan membantu kita memahami mengapa orang yang bermaksud baik pun terkadang melanggar aturan, bukan karena mereka ingin menimbulkan kerugian, tetapi sering kali karena mereka mencoba menyelesaikan pekerjaan dalam sistem yang penuh dengan kendala dan tekanan.

Pada akhirnya, bab ini akan mengintegrasikan semua tipologi ini ke dalam kerangka *System-Model* yang lebih luas. Akan ditegaskan kembali bahwa baik kesalahan maupun pelanggaran bukanlah peristiwa acak, melainkan variasi dalam kinerja manusia yang dapat diprediksi dan dipengaruhi oleh kondisi kerja, yang dikenal sebagai *Performance Shaping Factors*. Dengan memahami *human error* bukan sebagai anomali, tetapi sebagai bagian yang tak terhindarkan dari interaksi manusia-sistem, kita dapat mengalihkan fokus dari upaya sia-sia untuk menghilangkan kesalahan menjadi tujuan yang lebih realistis dan dapat dicapai: merancang sistem yang toleran terhadap kesalahan.

## **A. Definisi Human Error dalam Konteks K3**

Sebelum kita dapat mengklasifikasikan berbagai jenis *human error*, kita memerlukan definisi kerja yang jelas dan presisi. Dalam percakapan sehari-hari, istilah “kesalahan manusia” digunakan secara longgar untuk mencakup segala hal mulai dari kelupaan sederhana hingga kelalaian yang fatal. Namun, dalam ilmu keselamatan, definisi yang lebih teknis dan bermanfaat sangat diperlukan. Definisi yang paling diterima secara luas, yang dipelopori oleh psikolog kognitif James Reason, tidak berfokus pada konsekuensi dari suatu tindakan, melainkan pada niat (*intention*) di baliknya. Definisi ini memungkinkan kita untuk memisahkan tindakan itu sendiri dari hasilnya, yang merupakan langkah penting untuk analisis yang objektif.

Menurut kerangka kerja ini, *human error* didefinisikan sebagai kegagalan dari serangkaian tindakan yang direncanakan untuk mencapai

tujuan yang diinginkan, yang tidak disebabkan oleh faktor kebetulan. Secara lebih sederhana, ini adalah penyimpangan yang tidak disengaja dari apa yang seharusnya dilakukan atau direncanakan. Kata kunci di sini adalah “tidak disengaja”. Ini berarti bahwa individu tersebut memiliki niat yang benar, mereka ingin melakukan pekerjaan dengan benar dan aman, tetapi karena satu dan lain hal, tindakan yang mereka lakukan tidak sesuai dengan niat tersebut. Ini membedakan kesalahan murni dari sabotase, di mana individu tersebut dengan sengaja berniat untuk menyebabkan kerugian.

Penting untuk dipahami bahwa definisi ini memisahkan kesalahan dari hasilnya. Sebuah kesalahan tetaplah sebuah kesalahan, bahkan jika secara kebetulan tidak ada konsekuensi negatif yang terjadi. Misalnya, jika seorang teknisi salah menyambungkan kabel tetapi sistem keamanannya berhasil mencegah kerusakan, teknisi tersebut tetap melakukan kesalahan. Peristiwa ini adalah sebuah *near miss* yang berharga. Sebaliknya, sebuah tindakan yang benar dapat, karena nasib buruk atau faktor di luar kendali individu, tetap mengarah pada hasil yang negatif. Dalam kasus ini, individu tersebut tidak melakukan kesalahan. Fokus pada niat dan proses, bukan hanya pada hasil, memungkinkan analisis yang lebih adil dan akurat.

Definisi ini juga menjadi dasar untuk salah satu perbedaan paling fundamental dalam analisis kinerja manusia: perbedaan antara kesalahan (*errors*) dan pelanggaran (*violations*). Seperti yang telah disebutkan, kesalahan adalah penyimpangan yang *tidak disengaja* dari niat. Sebaliknya, pelanggaran adalah penyimpangan yang *disengaja* dari aturan, prosedur, atau praktik yang aman. Individu yang melakukan pelanggaran tahu aturannya, tetapi karena berbagai alasan, mereka memilih untuk tidak mengikutinya. Perbedaan ini sangat penting karena menunjuk pada akar penyebab dan strategi mitigasi yang sama sekali berbeda.

Selain itu, penting untuk melihat *human error* dalam sebuah kontinum. Kesalahan bisa berkisar dari selip kecil yang tidak berbahaya dan dapat segera diperbaiki, hingga kesalahan pengambilan keputusan besar yang dapat menyebabkan bencana katastropik. Meskipun mekanisme kognitifnya mungkin serupa, faktor-faktor sistemik yang memungkinkan kesalahan kecil berubah menjadi bencana besar adalah subjek utama

dari ilmu keselamatan modern. Sistem yang tangguh adalah sistem yang dapat “menangkap” kesalahan-kesalahan kecil sebelum konsekuensinya meningkat.

Memahami definisi dasar ini, berbasis niat, perbedaan antara kesalahan dan pelanggaran, dan sifat kontinumnya, memberikan kita fondasi yang kokoh. Ini memungkinkan kita untuk bergerak dari penggunaan istilah “human error” yang bersifat umum dan menghakimi, ke penggunaan kerangka kerja analitis yang dapat mengidentifikasi masalah secara spesifik dan mengarah pada solusi yang ditargetkan.

**Analogi/Contoh Kasus:** Bayangkan proses membuat secangkir kopi di pagi hari. Kesalahan (*error*) terjadi jika Anda berniat mengambil gula tetapi secara tidak sengaja mengambil garam karena wadahnya terlihat sama (*slip*). Niat Anda benar (membuat kopi manis), tetapi eksekusi tindakan Anda salah. Pelanggaran (*violation*) terjadi jika Anda tahu bahwa Anda seharusnya menggunakan satu sendok gula sesuai anjuran dokter, tetapi Anda dengan sengaja memasukkan tiga sendok karena Anda merasa lebih membutuhkannya pagi itu (*pelanggaran rutin*). Di sini, tindakan Anda sesuai dengan niat Anda (membuat kopi yang sangat manis), tetapi niat itu sendiri menyimpang dari aturan yang diketahui. Kedua tindakan tersebut menghasilkan kopi yang “salah”, tetapi alasan di baliknya sama sekali berbeda dan memerlukan “solusi” yang berbeda (misalnya, melabeli wadah garam vs. konseling gaya hidup).

### 1. Human Error sebagai Penyimpangan dari Niat (Intention)

Konsep niat (*intention*) adalah batu penjurur dari definisi modern *human error*. Untuk memahami sebuah kesalahan, kita harus terlebih dahulu memahami apa yang ingin dicapai oleh individu tersebut. James Reason menguraikan proses tindakan manusia menjadi dua tingkat: tingkat perencanaan (membentuk niat) dan tingkat eksekusi (melaksanakan rencana). Kesalahan dapat terjadi di salah satu dari dua tingkat ini.

Pada tingkat eksekusi, niat atau rencananya sudah benar, tetapi tindakan yang dilakukan untuk melaksanakannya menyimpang. Individu tersebut tahu apa yang harus dilakukan dan bagaimana melakukannya, tetapi terjadi kegagalan dalam pelaksanaan otomatis atau semi-otomatis

dari tindakan tersebut. Kegagalan pada tingkat ini disebut sebagai *slips* dan *lapses*. Sebagai contoh, seorang pengemudi berniat menginjak rem, tetapi kakinya terpeleset dan malah menginjak pedal gas. Rencananya (berhenti) benar, tetapi eksekusinya salah. Ini adalah *slip*. Kesalahan jenis ini sering terjadi pada tugas-tugas yang sudah sangat dikenal dan sering dilakukan, di mana perhatian sesaat teralihkan.

Pada tingkat perencanaan, tindakan yang dilakukan mungkin sesuai persis dengan rencana, tetapi rencana itu sendiri yang keliru atau tidak memadai untuk mencapai tujuan yang diinginkan. Kegagalan pada tingkat ini disebut sebagai *mistakes*. Individu tersebut mungkin salah mendiagnosis situasi, menerapkan aturan yang salah, atau tidak memiliki pengetahuan yang cukup untuk merumuskan rencana yang benar. Sebagai contoh, seorang dokter yang benar mendiagnosis gejala demam berdarah sebagai tifus, kemudian merumuskan dan melaksanakan rencana pengobatan untuk tifus dengan sempurna. Meskipun tindakannya sesuai dengan rencananya, rencananya salah, sehingga ini adalah sebuah *mistake*.

Dengan memusatkan definisi pada niat, kita dapat melakukan analisis yang lebih berempati dan konstruktif. Alih-alih hanya melihat tindakan yang salah dan menghakiminya, kita didorong untuk mencoba memahami apa yang ada di benak orang tersebut pada saat itu. "Apa yang mereka coba lakukan?" adalah pertanyaan pertama yang harus diajukan. Jawaban atas pertanyaan ini sering kali mengungkapkan bahwa niat mereka baik dan dapat dimengerti, meskipun hasilnya tidak diinginkan.

Fokus pada niat juga membantu kita menghindari apa yang disebut sebagai "bias hasil" (*outcome bias*). Bias hasil adalah kecenderungan kita untuk menilai kualitas sebuah keputusan atau tindakan berdasarkan hasilnya, bukan berdasarkan proses yang mengarah pada hasil tersebut. Jika seorang manajer mengambil keputusan berisiko yang kebetulan berhasil, kita cenderung memujinya sebagai visioner. Jika keputusan berisiko yang sama persis kebetulan gagal, kita mencelanya sebagai orang yang sembrono. Fokus pada niat dan proses perencanaan membantu kita mengevaluasi tindakan secara lebih objektif, terlepas dari apakah hasilnya baik atau buruk karena faktor keberuntungan.

Selain itu, kerangka kerja berbasis niat ini berlaku untuk semua tingkat keterampilan. Seorang pemula mungkin membuat kesalahan karena kurangnya pengetahuan untuk membentuk rencana yang benar (*knowledge-based mistake*). Sementara itu, seorang ahli yang sangat terampil justru lebih rentan terhadap *slips* dan *lapses* karena banyak dari tindakan mereka telah menjadi otomatis, memungkinkan pikiran mereka untuk mengembara. Ini menjelaskan mengapa para profesional yang paling berpengalaman pun tidak kebal dari kesalahan.

Memahami *human error* sebagai penyimpangan dari niat adalah langkah pertama untuk “mendekriminalisasi” kesalahan. Ini menggeser kesalahan dari ranah kegagalan moral ke ranah masalah kognitif dan interaksi sistem. Ini memungkinkan kita untuk menganalisis kesalahan sebagai fenomena psikologis yang normal dan dapat diprediksi, bukan sebagai penyimpangan perilaku yang tidak dapat dijelaskan. Pergeseran perspektif inilah yang membuka pintu bagi intervensi berbasis ilmu pengetahuan yang menargetkan mekanisme kognitif dan kondisi sistemik yang mendasari kesalahan.

## 2. Perbedaan antara Kesalahan (Error) dan Pelanggaran (Violation)

Setelah mendefinisikan kesalahan sebagai penyimpangan yang *tidak disengaja* dari niat, langkah selanjutnya yang sama pentingnya adalah membedakannya secara tajam dari pelanggaran, yang merupakan penyimpangan yang *disengaja* dari praktik yang ditentukan. Meskipun keduanya dapat menyebabkan hasil negatif yang identik, asal-usul, mekanisme, dan strategi mitigasinya sangat berbeda. Mencampuradukkan keduanya adalah resep untuk intervensi yang tidak efektif.

Kesalahan (*Errors*) pada dasarnya bersifat kognitif. Mereka berasal dari keterbatasan pemrosesan informasi otak manusia. Seperti yang telah dibahas, mereka dapat berupa kegagalan dalam eksekusi (rencana benar, tindakan salah) atau kegagalan dalam perencanaan (rencana salah). Penyebabnya sering kali terletak pada faktor-faktor seperti kurangnya perhatian, kelebihan beban memori, informasi yang tidak lengkap, atau bias kognitif. Orang yang melakukan kesalahan biasanya terkejut dan menyesal ketika mereka menyadari apa yang telah mereka lakukan; tindakan tersebut

tidak sesuai dengan apa yang mereka inginkan. Karena sifatnya yang tidak disengaja, strategi mitigasi untuk kesalahan berfokus pada perbaikan sistem, seperti desain antarmuka yang lebih baik, prosedur yang lebih jelas, atau pengurangan beban kerja.

Pelanggaran (*Violations*), di sisi lain, pada dasarnya bersifat motivasional dan kontekstual. Mereka melibatkan keputusan sadar untuk menyimpang dari aturan, kebijakan, atau prosedur. Orang yang melakukan pelanggaran tahu apa yang seharusnya mereka lakukan, tetapi memilih untuk melakukan sebaliknya. Namun, penting untuk dipahami bahwa motivasi di balik pelanggaran jarang sekali bersifat jahat atau keinginan untuk menyebabkan kerugian. Sebaliknya, pelanggaran sering kali dilakukan dengan niat yang tampaknya baik: untuk menyelesaikan pekerjaan, menghemat waktu, menghindari upaya yang tidak perlu, atau mengatasi desain sistem yang tidak praktis.

Karena sifatnya yang disengaja dan didorong oleh motivasi, strategi mitigasi untuk pelanggaran harus menargetkan konteks organisasi dan budaya yang mendorongnya. Jika prosedur secara rutin dilanggar, pertanyaan yang harus diajukan bukanlah "Mengapa para pekerja ini tidak patuh?", melainkan "Apa yang salah dengan prosedur atau sistem kerja kita sehingga orang merasa perlu untuk melanggarnya?". Mungkin prosedurnya terlalu rumit, peralatannya tidak memungkinkan pekerjaan dilakukan sesuai aturan, atau manajemen secara implisit memberi penghargaan pada kecepatan di atas kepatuhan.

Tabel berikut merangkum perbedaan utama:

<b>Fitur</b>	<b>Kesalahan (Error)</b>	<b>Pelanggaran (Violation)</b>
<b>Niat</b>	Tidak disengaja	Disengaja
<b>Asal Usul</b>	Kognitif (pemrosesan informasi)	Motivasional (dipengaruhi konteks)
<b>Sifat</b>	Kegagalan mental	Pilihan sadar
<b>Contoh</b>	Salah membaca dial, lupa langkah	Mengambil jalan pintas, tidak memakai APD
<b>Fokus Mitigasi</b>	Perbaikan desain, alat bantu kognitif	Perbaikan budaya, prosedur, pengawasan

Pembedaan ini sangat penting dalam kerangka *Just Culture*. Kesalahan yang tidak disengaja harus ditanggapi dengan dukungan dan pembelajaran, bukan hukuman. Pelanggaran, di sisi lain, memerlukan analisis yang lebih dalam tentang motivasinya. Jika itu adalah pelanggaran rutin yang didorong oleh sistem yang buruk, maka sistemlah yang harus diubah. Hanya pelanggaran yang sembrono, di mana seseorang secara sadar dan tidak dapat dibenarkan mengabaikan risiko besar, yang mungkin memerlukan tindakan disipliner.

Tanpa pembedaan yang jelas ini, organisasi cenderung memperlakukan semua penyimpangan sebagai masalah ketidakpatuhan, dan menerapkan "solusi" yang sama untuk semuanya: lebih banyak aturan dan lebih banyak hukuman. Pendekatan satu ukuran untuk semua ini dipastikan gagal, karena ia mencoba menyelesaikan masalah kognitif dengan solusi motivasional, dan sebaliknya. Memahami perbedaan antara kesalahan dan pelanggaran adalah prasyarat untuk diagnosis yang akurat dan perlakuan yang efektif.

### 3. **Kontinum Human Error: Dari Kecil hingga Katastropik**

Meskipun kita dapat mengklasifikasikan *human error* ke dalam berbagai jenis, penting juga untuk mengakui bahwa konsekuensi dari kesalahan-kesalahan tersebut ada dalam sebuah spektrum yang luas. Pada satu ujung kontinum, kita memiliki kesalahan-kesalahan kecil dan sehari-hari yang hampir tidak diperhatikan. Contohnya termasuk salah ketik dalam email, mengambil belokan yang salah saat mengemudi di rute yang dikenal, atau lupa di mana kita meletakkan kunci. Kesalahan-kesalahan ini sering kali memiliki konsekuensi yang dapat diabaikan dan dapat dengan mudah diperbaiki. Mereka adalah bagian normal dari pengalaman manusia.

Di ujung lain kontinum, kita memiliki kesalahan yang mengarah pada konsekuensi yang menghancurkan: kecelakaan industri besar, bencana transportasi, atau kesalahan medis yang fatal. Kesalahan yang terlibat dalam insiden-insiden ini, seperti salah membaca indikator kritis di ruang kontrol pembangkit listrik tenaga nuklir atau salah menghitung dosis obat, secara kognitif mungkin tidak jauh berbeda dari kesalahan kecil sehari-hari. Sebuah *lapse* memori adalah *lapse* memori, baik itu menyebabkan Anda

lupa membeli susu di toko atau lupa melakukan langkah penting dalam prosedur perawatan pesawat.

Pertanyaan krusial dalam ilmu keselamatan bukanlah “Bagaimana kita bisa menghilangkan semua kesalahan?”, karena itu adalah tujuan yang tidak mungkin. Sebaliknya, pertanyaan yang lebih penting adalah: “Faktor-faktor sistem apa yang menentukan di mana sebuah kesalahan akan mendarat di kontinum konsekuensi ini?”. Mengapa beberapa kesalahan dapat ditoleransi oleh sistem tanpa dampak, sementara kesalahan lain yang serupa dapat memicu bencana? Jawaban atas pertanyaan ini terletak pada konsep pertahanan sistem (*system defenses*).

Sistem yang dirancang dengan baik memiliki beberapa lapisan pertahanan untuk menangkap dan menahan efek dari kesalahan individu. Pertahanan ini bisa berupa teknologi (sistem alarm, interlock otomatis), prosedur (persyaratan verifikasi silang oleh dua orang), atau manusia (pengawasan, kerja tim). Ketika sebuah kesalahan kecil terjadi di sistem yang tangguh, satu atau lebih dari lapisan pertahanan ini akan menangkapnya dan mencegahnya berkembang menjadi kegagalan yang lebih besar.

Bencana katastrofik terjadi ketika serangkaian kelemahan atau “lubang” dalam berbagai lapisan pertahanan ini secara kebetulan sejajar pada satu titik waktu, menciptakan jalur tanpa hambatan bagi kesalahan awal untuk merambat melalui sistem. Ini adalah inti dari Model Keju Swiss James Reason, yang akan dibahas secara rinci di Bab 5. Dalam model ini, sebuah kesalahan operator (*active failure*) mungkin menjadi pemicu langsung, tetapi kecelakaan itu hanya mungkin terjadi karena adanya kondisi-kondisi laten yang telah melemahkan pertahanan sistem jauh sebelumnya.

Pandangan kontinum ini memiliki implikasi praktis yang penting. Ini berarti bahwa kita harus memberikan perhatian yang serius bahkan pada kesalahan-kesalahan kecil dan *near misses* yang tidak menimbulkan kerugian. Insiden-insiden ini adalah “kegagalan gratis” yang memberitahu kita di mana pertahanan kita lemah. Jika kita mengabaikannya hanya karena tidak ada yang terluka, kita kehilangan kesempatan berharga untuk menambal lubang dalam pertahanan kita sebelum kesalahan berikutnya,

yang mungkin terjadi dalam keadaan yang kurang menguntungkan, berhasil melewatinya.

Ini juga berarti bahwa fokus utama dari rekayasa keselamatan seharusnya adalah pada pembangunan pertahanan yang kuat, berlapis, dan beragam (*defense-in-depth*). Daripada hanya mencoba membuat individu di lini depan menjadi sempurna, kita harus merancang sistem yang mengakui ketidaksempurnaan mereka dan mampu mentolerir, menyerap, dan pulih dari kesalahan mereka. Tujuannya adalah untuk memastikan bahwa sebanyak mungkin kesalahan berakhir di ujung “kecil” dari kontinum konsekuensi, bukan di ujung “katastropik”.

## **B. Klasifikasi Kesalahan Manusia: *Slips*, *Lapses*, dan *Mistakes***

Setelah membedakan kesalahan dari pelanggaran, langkah selanjutnya adalah membedah kategori “kesalahan” itu sendiri. James Reason, berdasarkan penelitian dalam psikologi kognitif, mengusulkan taksonomi yang sangat berpengaruh yang membagi kesalahan (*errors*) menjadi tiga tipe utama berdasarkan mekanisme kognitif yang mendasarinya: *slips*, *lapses*, dan *mistakes*. Perbedaan ini tidak bersifat akademis semata; ia sangat penting karena setiap tipe kesalahan memiliki penyebab yang berbeda dan memerlukan jenis intervensi yang berbeda pula untuk mitigasinya.

Kerangka kerja ini didasarkan pada model tiga tingkat kinerja manusia yang diusulkan oleh Rasmussen:

### **a. *Skill-based performance* (Kinerja berbasis keterampilan)**

Ini adalah perilaku yang sangat terampil dan otomatis, yang dilakukan tanpa pemikiran sadar. Contohnya termasuk mengemudi mobil di jalan yang kosong, mengetik, atau melakukan tugas perakitan yang berulang.

### **b. *Rule-based performance* (Kinerja berbasis aturan)**

Ini melibatkan penerapan aturan atau prosedur yang telah dipelajari sebelumnya untuk menangani situasi yang dikenal. Ini adalah mode “jika X, maka lakukan Y”. Contohnya termasuk mengikuti checklist atau mendiagnosis masalah umum pada mesin.

c. **Knowledge-based performance (Kinerja berbasis pengetahuan)**

Ini diperlukan ketika menghadapi situasi baru atau tidak terduga di mana tidak ada aturan atau prosedur yang berlaku. Ini membutuhkan pemecahan masalah secara sadar, menggunakan pemahaman konseptual dan model mental dari sistem.

*Slips* dan *lapses* adalah kesalahan yang terjadi pada tingkat *skill-based*, sedangkan *mistakes* terjadi pada tingkat *rule-based* dan *knowledge-based*. Dengan kata lain, *slips* dan *lapses* adalah kesalahan dalam eksekusi (melakukan sesuatu), sementara *mistakes* adalah kesalahan dalam perencanaan (memutuskan apa yang harus dilakukan).

Memahami di tingkat mana sebuah kesalahan terjadi adalah kunci untuk diagnosis yang efektif. Jika sebuah kecelakaan disebabkan oleh *slip*, maka memberikan lebih banyak pelatihan tentang teori di balik tugas tersebut kemungkinan besar tidak akan membantu, karena masalahnya bukan pada pengetahuan, melainkan pada perhatian. Sebaliknya, jika kecelakaan disebabkan oleh *knowledge-based mistake*, maka merancang ulang tombol pada panel kontrol tidak akan mengatasi masalah mendasar dari kurangnya pemahaman. Taksonomi ini memberikan peta jalan untuk mencocokkan solusi dengan masalah yang sebenarnya.

**Analogi/Contoh Kasus:** Bayangkan seorang kasir di supermarket.

(1) Sebuah *slip* terjadi ketika dia berniat memberikan kembalian Rp 5.000, tetapi tangannya secara otomatis mengambil dan memberikan lembaran Rp 50.000 karena warnanya agak mirip dan dia sedang terganggu oleh pelanggan berikutnya. Ini adalah kesalahan eksekusi berbasis keterampilan. (2) Sebuah *lapse* terjadi ketika dia sudah memindai semua barang, tetapi lupa memindai satu item terakhir yang ada di bawah keranjang belanja. Ini adalah kesalahan memori. (3) Sebuah *mistake* terjadi ketika ada promosi baru "beli 2 gratis 1" yang aturannya rumit, dan dia salah menerapkan aturan diskon tersebut, sehingga memberikan diskon yang salah. Ini adalah kesalahan perencanaan berbasis aturan. Ketiga kesalahan ini menyebabkan kerugian finansial, tetapi sumber dan solusinya sangat berbeda.

## 1. **Slips: Kesalahan Aksi yang Tidak Disengaja (Perhatian/Skill-Based)**

*Slips* adalah jenis kesalahan yang paling umum kita alami dalam kehidupan sehari-hari. Mereka adalah kegagalan dalam pelaksanaan tindakan yang sangat terampil atau otomatis. Rencana atau niatnya benar, tetapi tindakan yang dieksekusi menyimpang darinya. *Slips* sering kali berupa tindakan yang dilakukan salah, urutan tindakan yang salah, atau tindakan yang terlewatkan. Mereka terjadi pada tingkat kinerja berbasis keterampilan (*skill-based*), di mana kita melakukan tugas-tugas yang sudah sangat kita kenal tanpa perlu banyak berpikir secara sadar.

Penyebab utama dari *slips* adalah kegagalan perhatian sesaat. Karena tugas tersebut bersifat otomatis, pikiran kita bebas untuk memikirkan hal lain. Ketika perhatian kita teralihkan pada saat yang kritis, mungkin karena gangguan eksternal (telepon berdering, seseorang berbicara kepada kita) atau gangguan internal (melamun, mengkhawatirkan masalah pribadi), program motorik otomatis kita dapat "tergelincir". Program yang salah dapat terpicu, atau program yang benar dapat dieksekusi dengan cara yang salah.

Ada beberapa jenis *slips* yang umum. Salah satunya adalah "kesalahan menangkap" (*capture error*), di mana urutan tindakan yang lebih sering dilakukan atau lebih terampil "menangkap" dan menggantikan urutan yang dimaksud, yang kurang sering dilakukan. Contoh klasiknya adalah berniat untuk mampir ke toko dalam perjalanan pulang dari kantor (rute yang jarang dilakukan), tetapi karena kebiasaan, Anda secara otomatis terus mengemudi langsung ke rumah (rute yang sering dilakukan) dan baru menyadarinya beberapa kilometer kemudian.

Jenis lain adalah "kesalahan deskripsi" (*description error*), di mana tindakan yang benar dilakukan pada objek yang salah. Ini sering terjadi ketika objek yang salah memiliki kemiripan yang kuat dengan objek yang benar. Contohnya adalah menuangkan jus jeruk ke dalam sereal Anda alih-alih susu, karena kedua karton tersebut memiliki bentuk dan berat yang serupa dan diletakkan berdampingan di lemari es. Di lingkungan industri, ini bisa berupa memutar katup yang salah karena semua katup di panel terlihat identik.

Karena *slips* berakar pada kegagalan perhatian dan desain antarmuka, strategi mitigasinya harus menargetkan area-area ini. Memberikan lebih banyak pelatihan atau menulis prosedur yang lebih panjang biasanya tidak efektif, karena masalahnya bukan pada kurangnya pengetahuan. Sebaliknya, intervensi yang efektif meliputi:

a. Perbaiki desain (*Human Factors Engineering*)

Merancang peralatan dan antarmuka untuk meminimalkan potensi kebingungan. Ini termasuk membedakan kontrol yang terlihat serupa (misalnya, dengan warna, bentuk, atau lokasi), menggunakan *forcing functions* yang membuat tindakan yang salah tidak mungkin dilakukan, dan memberikan umpan balik yang jelas.

b. Mengurangi gangguan

Menciptakan lingkungan kerja di mana gangguan diminimalkan, terutama selama langkah-langkah tugas yang kritis. Contohnya adalah kebijakan "zona steril" di kokpit pesawat selama lepas landas dan mendarat, di mana percakapan yang tidak penting dilarang.

c. Menggunakan daftar periksa (*checklists*)

Untuk tugas-tugas yang memiliki urutan langkah yang penting, penggunaan *checklist* dapat membantu memastikan tidak ada langkah yang terlewatkan atau dilakukan dalam urutan yang salah, bahkan jika perhatian teralihkan.

d. Meningkatkan kesadaran situasi

Melatih pekerja untuk secara sadar memantau kinerja mereka sendiri dan secara aktif mencari potensi kesalahan, terutama selama tugas-tugas yang monoton atau sangat rutin.

Memahami *slips* penting karena mereka menunjukkan bahwa bahkan orang yang paling terampil dan termotivasi pun bisa membuat kesalahan. Ini memperkuat argumen *System-Model* bahwa kita tidak bisa hanya mengandalkan kehati-hatian individu. Kita harus merancang sistem kerja yang mengantisipasi dan melindungi dari kegagalan perhatian yang tak terhindarkan ini.

## 2. Lapses: Kesalahan Memori yang Tidak Disengaja

*Lapses*, seperti halnya *slips*, adalah kesalahan eksekusi yang terjadi pada tingkat kinerja berbasis keterampilan (*skill-based*). Rencananya benar, tetapi ada kegagalan dalam pelaksanaannya. Perbedaan utamanya adalah jika *slips* biasanya merupakan kesalahan yang dapat diamati dalam tindakan (melakukan hal yang salah), *lapses* lebih bersifat internal dan melibatkan kegagalan memori (lupa melakukan sesuatu). *Lapse* terjadi ketika kita lupa untuk melakukan tindakan yang dimaksudkan atau kehilangan jejak di mana kita berada dalam urutan tugas.

Penyebab utama *lapses* adalah kegagalan memori kerja atau memori prospektif. Memori kerja adalah "ruang mental" kita yang berkapasitas terbatas di mana kita menyimpan informasi yang kita butuhkan untuk tugas yang sedang berjalan. Ketika memori kerja kita kelebihan beban, misalnya, karena kita mencoba melakukan terlalu banyak hal sekaligus atau karena ada gangguan, item-item dapat "jatuh" dari memori. Memori prospektif adalah kemampuan kita untuk mengingat untuk melakukan sesuatu di masa depan, seperti "ingat untuk mematikan kompor dalam 10 menit". Kegagalan dalam memori inilah yang menyebabkan *lapses*.

Contoh umum dari *lapse* dalam kehidupan sehari-hari adalah pergi ke suatu ruangan untuk mengambil sesuatu, tetapi begitu sampai di sana, Anda lupa apa yang ingin Anda ambil. Contoh lain adalah lupa membayar barang setelah mengisi bensin, karena perhatian Anda teralihkan oleh anak-anak di dalam mobil. Dalam konteks industri, *lapse* bisa sangat berbahaya. Seorang teknisi perawatan mungkin lupa untuk mengencangkan kembali baut setelah menyelesaikan perbaikan, atau seorang operator mungkin lupa untuk membuka kembali katup setelah prosedur penguncian (*lock-out/tag-out*).

Seperti *slips*, *lapses* lebih mungkin terjadi ketika melakukan tugas-tugas rutin, ketika perhatian kita tidak sepenuhnya terfokus, atau ketika kita mengalami gangguan. Kelelahan, stres, dan beban kerja mental yang tinggi juga merupakan faktor kontribusi yang signifikan karena mereka mengurangi kapasitas memori kerja kita yang sudah terbatas.

Strategi mitigasi untuk *lapses* berfokus pada mendukung fungsi memori manusia, bukan pada penyalahan atau pelatihan ulang. Intervensi yang efektif meliputi:

a. Alat bantu memori eksternal (*External memory aids*)

Ini adalah cara paling efektif untuk mengatasi keterbatasan memori. Contohnya termasuk penggunaan checklists yang terperinci, job aids (panduan visual singkat yang ditempel di dekat peralatan), dan prosedur langkah-demi-langkah yang mengharuskan pengguna untuk menandai setiap langkah yang telah selesai.

b. Desain tugas yang baik

Merancang alur kerja untuk meminimalkan beban memori. Ini bisa berarti menghindari prosedur yang mengharuskan pekerja untuk mengingat informasi dari satu langkah ke langkah lain yang jauh terpisah, atau memberikan informasi yang dibutuhkan tepat di tempat dan waktu yang dibutuhkan.

c. Peningkat otomatis

Menggunakan sistem alarm atau peningkat otomatis untuk tugas-tugas yang sensitif terhadap waktu atau mudah terlupakan.

d. Tempat untuk segala sesuatu

Menerapkan prinsip-prinsip 5S atau tata graha yang baik, di mana setiap alat memiliki tempat yang ditentukan, dapat mengurangi *lapses* yang terkait dengan mencari alat atau komponen.

Memahami *lapses* mengingatkan kita bahwa memori manusia pada dasarnya tidak dapat diandalkan, terutama di bawah tekanan. Bergantung pada ingatan individu untuk memastikan keselamatan dalam proses yang kompleks adalah strategi yang ditakdirkan untuk gagal. Sebaliknya, kita harus merancang sistem yang mengakui kelemahan ini dan menyediakan dukungan eksternal yang kuat untuk memastikan bahwa langkah-langkah kritis tidak pernah terlupakan.

### 3. Mistakes: Kesalahan Keputusan/Perencanaan (Rule/Knowledge-Based)

Berbeda secara fundamental dari *slips* dan *lapses*, *mistakes* bukanlah kesalahan dalam eksekusi, melainkan kesalahan dalam perencanaan. Dalam sebuah *mistake*, tindakan yang dilakukan mungkin dieksekusi dengan sempurna sesuai dengan rencana, tetapi sayangnya rencana itu sendiri yang cacat atau tidak tepat untuk situasi tersebut. *Mistakes* terjadi pada tingkat kinerja berbasis aturan (*rule-based*) dan berbasis pengetahuan (*knowledge-based*), di mana pemikiran sadar terlibat dalam mendiagnosis situasi dan memutuskan tindakan.

*Rule-based mistakes* (Kesalahan berbasis aturan) terjadi ketika kita menghadapi situasi yang dikenal dan menerapkan aturan atau prosedur yang salah. Ini bisa terjadi dalam dua bentuk utama. Pertama adalah "penerapan aturan yang buruk" (*misapplication of good rules*), di mana kita memiliki aturan yang benar dalam repertoar kita, tetapi kita salah memilih aturan mana yang akan diterapkan pada situasi saat ini. Ini sering terjadi karena kita salah menginterpretasikan tanda-tanda atau sinyal dari situasi tersebut. Contohnya, seorang operator mungkin melihat lampu peringatan dan, karena lampu itu mirip dengan alarm yang sering berbunyi, dia menerapkan prosedur untuk alarm rutin tersebut, padahal sebenarnya itu adalah sinyal untuk masalah yang lebih serius dan berbeda.

Bentuk kedua adalah "penerapan aturan yang buruk" (*application of bad rules*), di mana aturan yang diterapkan itu sendiri yang cacat. Aturan yang "buruk" ini mungkin telah dikembangkan dari pengalaman sebelumnya yang menyesatkan, atau dari pelatihan yang tidak memadai. Misalnya, seorang teknisi mungkin memiliki "aturan praktis" pribadi bahwa "jika mesin mengeluarkan suara X, biasanya itu hanya masalah Y", padahal kali ini suara X menandakan masalah Z yang jauh lebih berbahaya.

*Knowledge-based mistakes* (Kesalahan berbasis pengetahuan) terjadi dalam situasi yang benar-benar baru atau tidak terduga, di mana tidak ada aturan atau prosedur yang siap pakai. Individu tersebut harus kembali ke prinsip-prinsip dasar dan pengetahuan teoretisnya untuk menganalisis masalah dan menciptakan solusi baru dari awal. Ini adalah tingkat

pemrosesan kognitif yang paling menuntut dan paling rentan terhadap kesalahan.

Kesalahan pada tingkat ini sering kali disebabkan oleh keterbatasan kognitif fundamental, seperti:

a. Bias kognitif

Kecenderungan kita untuk mengambil jalan pintas mental yang dapat menyesatkan. Contohnya termasuk confirmation bias (hanya mencari informasi yang mendukung hipotesis awal kita) dan availability heuristic (terlalu mengandalkan informasi yang paling mudah diingat).

b. Model mental yang tidak akurat

Pemahaman konseptual individu tentang bagaimana sistem bekerja mungkin tidak lengkap atau salah, yang mengarah pada diagnosis dan prediksi yang keliru.

c. Informasi yang tidak memadai atau ambigu

Dalam situasi baru, informasi yang tersedia sering kali tidak lengkap, membingungkan, atau bertentangan.

Mitigasi untuk *mistakes* sangat berbeda dari *slips* dan *lapses*. Karena masalahnya terletak pada pengetahuan dan penalaran, solusinya harus menargetkan area-area ini:

a. Pelatihan yang lebih baik

Terutama pelatihan berbasis skenario dan simulasi yang memungkinkan orang untuk berlatih mengambil keputusan dalam situasi yang kompleks dan ambigu di lingkungan yang aman.

b. Sistem pendukung keputusan (Decision support systems)

Menyediakan alat, seperti sistem pakar atau diagnostik terkomputerisasi, yang dapat membantu individu menganalisis data dan mengevaluasi opsi.

c. Memperjelas prosedur dan aturan

Memastikan bahwa kriteria untuk menerapkan setiap aturan didefinisikan dengan jelas untuk menghindari salah tafsir.

d. Mendorong kolaborasi

Dalam situasi yang tidak pasti, mendorong konsultasi dengan rekan kerja atau ahli dapat membantu mengatasi bias individu dan model mental yang terbatas.

*Mistakes* sering kali memiliki konsekuensi yang lebih serius daripada *slips* dan *lapses* karena mereka dapat menempatkan sistem ke dalam jalur yang salah untuk jangka waktu yang lebih lama. Memahami perbedaan antara kesalahan berbasis aturan dan berbasis pengetahuan membantu organisasi untuk merancang pelatihan dan dukungan keputusan yang lebih ditargetkan dan efektif.

### C. Klasifikasi Perilaku Berisiko: Violations

Seperti yang telah dijelaskan, pelanggaran (*violations*) secara fundamental berbeda dari kesalahan. Mereka adalah penyimpangan yang disengaja dari prosedur, standar, atau aturan yang diketahui. Namun, sangat penting untuk tidak langsung melabeli semua pelanggaran sebagai tindakan sabotase, kelalaian, atau pembangkangan. Meskipun pelanggaran bersifat disengaja, motivasi di baliknya jarang sekali jahat. Sebagian besar pelanggaran dilakukan oleh orang-orang yang bermaksud baik yang mencoba menyelesaikan pekerjaan mereka dalam sistem yang sering kali memiliki batasan, tekanan, dan tujuan yang saling bertentangan.

Memahami *mengapa* orang merasa perlu untuk melanggar aturan adalah kunci untuk mengelola perilaku berisiko secara efektif. Menyalahkan dan menghukum pelanggar tanpa memahami konteksnya adalah pendekatan *Person-Model* yang dipastikan gagal. Sebaliknya, *System-Model* mendorong kita untuk melihat pelanggaran sebagai sinyal penting yang menunjukkan adanya ketidakcocokan antara pekerjaan seperti yang dibayangkan oleh manajemen (*work-as-imagined*) dan pekerjaan seperti yang sebenarnya harus dilakukan di lapangan (*work-as-done*).

Jika aturan secara rutin dilanggar, itu sering kali berarti ada sesuatu yang salah dengan aturan itu sendiri, atau dengan lingkungan kerja yang membuat kepatuhan menjadi sulit atau tidak praktis. Mungkin aturannya sudah usang, terlalu rumit, atau tidak mempertimbangkan kondisi

operasional yang sebenarnya. Mungkin juga tekanan untuk memenuhi target produksi sangat tinggi sehingga pekerja merasa tidak punya pilihan selain mengambil jalan pintas. Oleh karena itu, pelanggaran harus dilihat sebagai "informasi gratis" tentang di mana sistem kerja perlu diperbaiki.

Untuk memfasilitasi analisis yang lebih mendalam ini, pelanggaran dapat diklasifikasikan ke dalam beberapa jenis berdasarkan motivasi yang mendasarinya. Tipologi yang paling umum membedakan antara pelanggaran rutin, situasional, dan pengecualian. Setiap jenis memiliki penyebab yang berbeda dan, oleh karena itu, memerlukan strategi manajemen yang berbeda pula. Memahami klasifikasi ini memungkinkan organisasi untuk bergerak dari respons "nol toleransi" yang kaku menjadi pendekatan yang lebih bernuansa dan efektif untuk mengelola kepatuhan.

**Analogi/Contoh Kasus:** Bayangkan aturan batas kecepatan 50 km/jam di sebuah jalan. (1) Pelanggaran rutin terjadi ketika hampir semua orang mengemudi dengan kecepatan 60 km/jam di jalan tersebut karena jalannya lebar, lurus, dan batas kecepatannya terasa terlalu rendah. Ini telah menjadi norma sosial yang tidak tertulis. (2) Pelanggaran situasional terjadi ketika seorang pengemudi yang biasanya patuh aturan melaju dengan kecepatan 70 km/jam karena dia sedang terburu-buru mengantar anggota keluarga ke rumah sakit dalam keadaan darurat. (3) Pelanggaran pengecualian (atau sembrono) terjadi ketika seseorang dengan sengaja memacu mobilnya dengan kecepatan 120 km/jam di jalan yang sama untuk pamer atau balapan liar, dengan sadar mengabaikan risiko besar yang ditimbulkannya. Jelas, ketiga pelanggaran ini memerlukan respons yang sangat berbeda dari pihak berwenang.

### 1. Pelanggaran Rutin (Routine Violations) dan Penyebabnya

Pelanggaran rutin adalah jenis pelanggaran yang paling umum dan sering kali paling signifikan dari sudut pandang keselamatan sistemik. Ini adalah pelanggaran yang telah menjadi bagian normal dari cara kerja, sebuah kebiasaan atau norma dalam kelompok kerja. Mereka sering kali dilakukan secara terbuka dan dapat dianggap sebagai "rahasia umum". Pelanggaran ini cenderung menjadi norma karena mereka menawarkan "jalur dengan usaha terkecil" (*path of least effort*) untuk menyelesaikan

tugas. Mereka membuat pekerjaan lebih mudah, lebih cepat, atau lebih nyaman.

Pelanggaran rutin jarang sekali dimotivasi oleh keinginan untuk menentang otoritas. Sebaliknya, mereka berkembang dari waktu ke waktu karena kombinasi dari desain sistem yang buruk dan penegakan aturan yang lemah. Ketika pekerja menemukan bahwa ada cara yang lebih efisien untuk melakukan sesuatu daripada mengikuti prosedur resmi yang rumit, dan ketika mereka melihat bahwa tidak ada konsekuensi negatif (baik dalam hal keselamatan maupun sanksi) dari mengambil jalan pintas ini, perilaku tersebut secara bertahap akan menjadi standar praktik yang baru.

Penyebab utama dari pelanggaran rutin sering kali bersifat sistemik. Salah satu penyebab utamanya adalah prosedur yang tidak dapat dijalankan (*unworkable procedures*). Prosedur mungkin ditulis oleh seseorang yang jauh dari tempat kerja dan tidak memahami kendala praktisnya. Prosedur tersebut mungkin terlalu panjang, terlalu rumit, atau membutuhkan alat yang tidak selalu tersedia. Dalam kasus ini, pelanggaran bukan hanya pilihan yang mudah, tetapi satu-satunya cara yang mungkin untuk menyelesaikan pekerjaan.

Penyebab lainnya adalah lingkungan yang menoleransi pelanggaran. Ini terjadi ketika manajemen atau pengawas secara sadar atau tidak sadar "memalingkan muka" dari pelanggaran, terutama jika pelanggaran tersebut membantu mencapai target produksi. Pesan implisit yang diterima oleh pekerja adalah bahwa kepatuhan hanya penting di atas kertas, tetapi hasil produksi adalah yang benar-benar dihargai. Ini menciptakan konflik antara aturan resmi dan aturan tidak resmi, dan pekerja akan selalu mengikuti aturan tidak resmi untuk bertahan.

Keinginan untuk optimasi juga menjadi pendorong. Manusia secara alami mencari cara untuk bekerja lebih cerdas, bukan lebih keras. Pelanggaran rutin sering kali merupakan bentuk inovasi dari bawah, di mana pekerja menemukan cara yang lebih baik untuk melakukan sesuatu. Masalahnya adalah bahwa inovasi ini tidak selalu dievaluasi secara formal untuk risikonya, dan jalan pintas yang aman dalam 99% kasus mungkin memiliki konsekuensi yang tidak terduga dalam 1% kasus lainnya.

Mengelola pelanggaran rutin sangatlah menantang karena mereka telah tertanam dalam budaya kerja. Strategi yang hanya berfokus pada pendisiplinan individu (“membuat contoh”) biasanya gagal dan dapat merusak moral. Pendekatan yang lebih efektif harus bersifat sistemik:

a. Mendiagnosis akar masalah

Cari tahu mengapa aturan tersebut dilanggar. Libatkan pekerja dalam diskusi terbuka (tanpa menyalahkan) untuk memahami masalah dengan prosedur atau sistem kerja.

b. Merancang ulang pekerjaan

Jika prosedur tidak praktis, ubahlah. Jika alat tidak memadai, sediakan yang lebih baik. Buatlah kepatuhan menjadi cara yang paling mudah, bukan yang paling sulit, untuk melakukan pekerjaan.

c. Memastikan konsistensi

Manajemen harus menunjukkan komitmen yang jelas dan konsisten terhadap aturan keselamatan. Pemimpin harus menjadi teladan dan tidak pernah mendorong atau menoleransi jalan pintas.

d. Meningkatkan kesadaran risiko

Jelaskan alasan di balik aturan tersebut. Ketika pekerja memahami bahaya yang coba dicegah oleh suatu aturan, mereka lebih mungkin untuk mematuhi, bahkan jika itu membutuhkan sedikit usaha ekstra.

Pelanggaran rutin adalah cermin yang menunjukkan cacat dalam sistem kita. Mengabaikannya atau hanya menghukumnya berarti membuang kesempatan berharga untuk perbaikan.

## 2. Pelanggaran Situasional (Situational Violations) dan Tekanan Kerja

Berbeda dengan pelanggaran rutin yang bersifat habitual, pelanggaran situasional adalah penyimpangan dari aturan yang didorong oleh faktor-faktor spesifik dalam konteks pekerjaan saat itu. Pelanggaran ini biasanya dilakukan oleh individu yang normalnya patuh, tetapi merasa terpaksa untuk melanggar aturan karena tekanan atau tuntutan dari situasi tersebut. Faktor pendorong utama untuk pelanggaran jenis ini adalah tekanan waktu,

beban kerja yang tinggi, atau kurangnya sumber daya (misalnya, alat, staf, atau suku cadang).

Seorang pekerja mungkin tahu betul bahwa dia seharusnya melakukan uji isolasi energi sebelum memulai perbaikan, tetapi karena produksi telah berhenti dan manajer terus-menerus bertanya kapan mesin akan berjalan kembali, dia mungkin memutuskan untuk “hanya melihat sebentar” tanpa melalui prosedur penguncian yang memakan waktu. Dalam benaknya, dia menimbang risiko dari pelanggaran tersebut terhadap tekanan yang dia rasakan untuk segera menyelesaikan pekerjaan. Pelanggaran tersebut dilihat sebagai satu-satunya cara untuk memenuhi tuntutan situasional yang mendesak.

Penyebab pelanggaran situasional sering kali dapat dilacak kembali ke keputusan manajemen dan penjadwalan. Tekanan produksi adalah penyebab yang paling umum. Ketika organisasi secara konsisten memprioritaskan target produksi, pengiriman tepat waktu, atau tujuan finansial di atas keselamatan, mereka menciptakan lingkungan di mana pekerja secara teratur dihadapkan pada pilihan sulit antara bekerja dengan aman dan memenuhi harapan manajemen. Meskipun kebijakan resmi mungkin menyatakan “keselamatan adalah prioritas nomor satu”, tindakan dan pesan informal dari manajemen sering kali mengatakan sebaliknya.

Beban kerja yang berlebihan juga merupakan pendorong yang kuat. Ketika pekerja dibebani dengan terlalu banyak tugas dalam waktu yang terlalu sedikit, mereka secara alami akan mencari jalan pintas untuk mengatasinya. Melompati langkah-langkah keselamatan dalam prosedur mungkin tampak seperti cara yang efisien untuk mengejar ketertinggalan. Hal yang sama berlaku untuk kekurangan staf, di mana satu orang diharapkan untuk melakukan pekerjaan yang idealnya dilakukan oleh dua orang.

Ketersediaan alat dan peralatan yang tidak memadai juga dapat memicu pelanggaran situasional. Jika perancah yang benar tidak tersedia, pekerja mungkin tergoda untuk menggunakan tangga yang tidak sesuai atau berdiri di atas drum. Jika APD yang tepat tidak nyaman atau tidak

tersedia dalam ukuran yang pas, kepatuhan akan menurun, terutama ketika pekerjaan harus diselesaikan dengan cepat.

Mengelola pelanggaran situasional memerlukan fokus pada perbaikan lingkungan kerja dan manajemen tekanan. Strategi yang efektif meliputi:

- a. Manajemen beban kerja yang realistis  
Memastikan bahwa tingkat kepegawaian dan target produksi ditetapkan pada tingkat yang memungkinkan pekerjaan dilakukan dengan aman dan sesuai prosedur.
- b. Perencanaan dan penjadwalan yang lebih baik  
Mengantisipasi kebutuhan sumber daya dan memastikan alat, suku cadang, dan izin kerja tersedia saat dibutuhkan untuk menghindari penundaan yang menciptakan tekanan waktu.
- c. Memberdayakan pekerja untuk menghentikan pekerjaan  
Menciptakan budaya di mana setiap pekerja merasa berhak dan didukung untuk menghentikan pekerjaan (stop work authority) jika mereka merasa kondisi tidak aman atau mereka tidak memiliki sumber daya yang tepat untuk melanjutkan, tanpa takut akan sanksi.
- d. Komitmen kepemimpinan yang terlihat  
Manajer dan penyelia harus secara aktif menunjukkan bahwa mereka lebih menghargai keselamatan daripada produksi. Ini berarti memuji pekerja yang menghentikan pekerjaan karena alasan keselamatan, bukan mengkritik mereka karena menyebabkan penundaan.

Pelanggaran situasional adalah cerminan langsung dari tekanan yang dirasakan oleh pekerja di lini depan. Mengatasinya bukan tentang membuat pekerja lebih "tahan" terhadap tekanan, tetapi tentang mengurangi atau menghilangkan tekanan yang tidak perlu dari sistem itu sendiri.

### **3. Pelanggaran Pengecualian (Exceptional Violations) dan Risiko Tinggi**

Pelanggaran pengecualian adalah jenis pelanggaran yang paling jarang terjadi, tetapi sering kali memiliki potensi konsekuensi yang paling parah. Pelanggaran ini terjadi dalam situasi yang tidak biasa atau darurat, di mana

seorang individu dengan sengaja menyimpang dari aturan dalam upaya untuk menangani masalah yang mereka yakini tidak dapat diselesaikan dengan mengikuti prosedur standar. Ini adalah tindakan improvisasi di luar aturan yang ada.

Terkadang, pelanggaran pengecualian dapat menjadi tindakan heroik yang menyelamatkan hari. Misalnya, seorang operator di sebuah pabrik kimia mungkin melanggar prosedur untuk secara manual membuka katup pelepas tekanan selama kondisi darurat yang belum pernah terjadi sebelumnya, sehingga mencegah ledakan. Dalam kasus ini, pelanggaran tersebut adalah hasil dari keahlian dan pemahaman mendalam tentang sistem, yang memungkinkan respons adaptif yang tidak diantisipasi oleh penulis prosedur.

Namun, lebih sering, pelanggaran pengecualian adalah pertaruhan berisiko tinggi yang berakhir buruk. Ini sering terjadi ketika sesuatu telah salah, dan individu tersebut mencoba untuk "memperbaiki" situasi dengan mengambil tindakan drastis yang melanggar aturan keselamatan fundamental. Niatnya mungkin baik, untuk memulihkan operasi atau mencegah kerugian lebih lanjut, tetapi tindakan tersebut dilakukan tanpa pemahaman penuh tentang risiko yang terlibat. Bencana Chernobyl pada tahun 1986 adalah contoh tragis dari serangkaian pelanggaran pengecualian, di mana para operator dengan sengaja menonaktifkan beberapa sistem keselamatan penting untuk mencoba menyelesaikan tes reaktor yang bermasalah, dengan hasil yang menghancurkan (.).

Ada juga sub-tipe dari pelanggaran ini yang dapat dikategorikan sebagai pelanggaran optimasi atau pelanggaran sembrono (*reckless violations*). Ini adalah jenis perilaku di mana individu secara sadar dan tidak dapat dibenarkan mengabaikan risiko yang substansial demi keuntungan pribadi, sensasi, atau kemudahan. Ini berbeda dari pelanggaran pengecualian yang didorong oleh situasi darurat. Contohnya termasuk balap forklift di gudang atau masuk ke ruang terbatas tanpa pengujian atmosfer hanya karena tidak mau repot. Perilaku semacam ini tidak dapat ditoleransi dan merupakan satu-satunya jenis pelanggaran di mana tindakan disipliner yang tegas hampir selalu merupakan respons yang tepat.

Mengelola pelanggaran pengecualian sangatlah sulit karena sifatnya yang tidak dapat diprediksi. Namun, beberapa strategi dapat membantu:

a. Pelatihan berbasis skenario yang realistis

Melatih operator dan tim tanggap darurat dalam simulator atau latihan untuk menangani berbagai skenario abnormal dan darurat. Ini membantu mereka mengembangkan keterampilan pengambilan keputusan di bawah tekanan dalam lingkungan yang aman.

b. Prosedur darurat yang jelas dan kuat

Meskipun tidak mungkin untuk menulis prosedur untuk setiap kemungkinan, memiliki pedoman yang jelas tentang tindakan apa yang harus diambil dan, yang lebih penting, tindakan apa yang tidak boleh diambil selama kondisi darurat dapat memberikan batasan yang aman.

c. Mendefinisikan garis yang tidak boleh dilewati

Melalui kebijakan dan budaya, organisasi harus menetapkan dengan sangat jelas aturan-aturan keselamatan fundamental (sering disebut life-saving rules atau golden rules) yang tidak boleh dilanggar dalam keadaan apa pun.

d. Menegakkan akuntabilitas untuk perilaku sembrono

Menerapkan kebijakan nol toleransi yang konsisten untuk pelanggaran sembrono mengirimkan pesan yang kuat bahwa jenis perilaku ini tidak dapat diterima.

Memahami pelanggaran pengecualian mengingatkan kita bahwa bahkan dalam situasi yang paling ekstrem sekalipun, aturan dan batasan tetap penting. Sementara adaptasi dan keahlian terkadang diperlukan, improvisasi yang melanggar prinsip-prinsip keselamatan dasar adalah resep untuk bencana.

## **D. Memahami *Human Error* sebagai Variasi Perilaku Manusia**

Setelah membedah berbagai jenis kesalahan dan pelanggaran, penting untuk mengambil langkah mundur dan menyatukan kembali konsep-konsep ini dalam kerangka yang lebih luas. Tipologi ini bukanlah label

untuk menyalahkan individu, melainkan alat diagnostik untuk memahami fenomena yang lebih fundamental: variabilitas kinerja manusia. Kinerja manusia, bahkan pada tugas yang sama yang dilakukan oleh orang yang sama, tidak pernah 100% identik dari satu waktu ke waktu lainnya. Selalu ada sedikit variasi dalam waktu, urutan, dan presisi tindakan.

Pandangan tradisional (*Safety-I*) cenderung melihat variabilitas ini secara negatif, sebagai sumber ketidakandalan dan kesalahan. Tujuannya adalah untuk mengurangi atau menghilangkan variabilitas sebanyak mungkin melalui standardisasi dan prosedur yang ketat. Namun, pandangan yang lebih modern (*Safety-II*) mengakui bahwa variabilitas ini adalah fitur, bukan bug, dari sistem manusia. Variabilitas inilah yang memungkinkan manusia untuk beradaptasi dengan kondisi yang berubah, mengatasi kekurangan desain, dan menemukan cara-cara baru yang lebih baik untuk melakukan pekerjaan. Tanpa variabilitas, tidak akan ada pembelajaran, inovasi, atau resiliensi.

Dari perspektif ini, *human error* bukanlah kategori perilaku yang terpisah, melainkan hanyalah ujung ekor dari distribusi normal variabilitas kinerja. Kesalahan adalah variasi yang, dalam konteks tertentu, melampaui batas toleransi sistem dan menyebabkan hasil yang tidak diinginkan. Pelanggaran, terutama yang rutin, juga merupakan bentuk adaptasi dan variasi yang telah menjadi norma. Oleh karena itu, tugas manajemen keselamatan bukanlah untuk membasmi variabilitas, yang merupakan hal yang mustahil, tetapi untuk memahaminya, memantaunya, dan mengelolanya.

Ini berarti kita perlu memahami faktor-faktor apa yang memengaruhi atau membentuk variabilitas kinerja. Dalam literatur *human factors*, faktor-faktor ini dikenal sebagai *Performance Shaping Factors* (PSFs) atau *Error Producing Conditions* (EPCs). Mereka adalah karakteristik dari individu, tugas, dan lingkungan yang membuat kinerja menjadi lebih baik atau lebih buruk, dan dengan demikian membuat kesalahan menjadi lebih atau kurang mungkin terjadi. Dengan menganalisis dan memperbaiki PSFs, kita dapat "menggeser kurva" variabilitas ke arah kinerja yang lebih andal dan aman.

Pada akhirnya, pengakuan bahwa kesalahan adalah bagian alami dari variabilitas manusia mengarah pada kesimpulan yang tak terhindarkan: kita harus merancang sistem yang toleran terhadap kesalahan. Karena kita tidak akan pernah bisa mencegah semua kesalahan, kita harus membangun sistem yang dapat mendeteksi, menahan, dan pulih dari kesalahan sebelum mereka menyebabkan kerugian. Ini adalah inti dari rekayasa resiliensi dan merupakan tujuan akhir dari pendekatan sistemik terhadap mitigasi *human error*.

**Analogi/Contoh Kasus:** Bayangkan kinerja manusia seperti mengemudikan mobil di dalam sebuah lajur di jalan raya. Variabilitas normal adalah gerakan kecil dan konstan pada setir untuk menjaga mobil tetap di tengah lajur. Anda tidak pernah mengemudi dalam garis lurus yang sempurna. Kesalahan (*error*) terjadi ketika, karena sesaat terganggu, mobil Anda menyimpang dan menyentuh garis lajur. Kecelakaan terjadi jika mobil Anda keluar dari lajur dan menabrak sesuatu. Sistem yang toleran terhadap kesalahan adalah seperti memiliki lajur yang lebih lebar, bahu jalan yang rata, dan pagar pembatas. Fitur-fitur ini tidak mencegah penyimpangan awal (variabilitas), tetapi mereka memberikan ruang untuk koreksi dan menahan konsekuensi jika penyimpangan menjadi terlalu besar. Tugas kita adalah membangun "bahu jalan" dan "pagar pembatas" di dalam sistem kerja kita.

### 1. **Human Error sebagai Fungsi dari Kondisi Kerja (Performance Shaping Factors)**

Kesalahan dan pelanggaran tidak terjadi secara acak. Probabilitas terjadinya kesalahan atau pelanggaran pada tugas tertentu sangat dipengaruhi oleh kondisi di mana tugas itu dilakukan. Faktor-faktor kontekstual ini, yang secara kolektif dikenal sebagai *Performance Shaping Factors* (PSFs), adalah jembatan yang menghubungkan kondisi laten di tingkat organisasi dengan kegagalan aktif di lini depan. Menganalisis PSFs adalah cara praktis untuk menerapkan *System-Model* dan memahami *mengapa* kesalahan terjadi di lokasi dan waktu tertentu.

PSFs dapat dikategorikan ke dalam tiga kelompok utama: faktor internal (terkait individu), faktor eksternal (terkait lingkungan kerja), dan faktor stresor (terkait sifat tugas).

a. **Faktor Internal (Karakteristik Individu)**

Ini adalah keadaan sementara dari individu yang melakukan tugas. Penting untuk dicatat bahwa ini berbeda dari sifat kepribadian yang stabil. Faktor-faktor ini meliputi:

- 1) Tingkat keahlian dan pengalaman
- 2) Tingkat kelelahan dan kewaspadaan
- 3) Kesehatan fisik dan mental
- 4) Tingkat motivasi dan moral
- 5) Model mental pribadi tentang sistem

b. **Faktor Eksternal (Karakteristik Lingkungan Kerja dan Tugas)**

Ini adalah faktor-faktor yang paling dapat dikendalikan oleh organisasi melalui desain dan manajemen. Mereka memiliki pengaruh yang sangat kuat terhadap kinerja. Faktor-faktor ini meliputi:

- 1) Desain antarmuka manusia-mesin: Kejelasan tampilan, logika kontrol, dll.
- 2) Kualitas prosedur dan instruksi kerja: Kejelasan, keakuratan, dan ketersediaannya.
- 3) Kualitas alat dan peralatan: Keandalan, kesesuaian, dan perawatannya.
- 4) Faktor-faktor lingkungan fisik: Pencahayaan, kebisingan, suhu, getaran.
- 5) Budaya keselamatan dan iklim organisasi: Tingkat kepercayaan, komunikasi, dan prioritas yang dirasakan.
- 6) Kualitas pengawasan dan kepemimpinan.
- 7) Pelatihan yang diterima.

c. **Faktor Stresor (Karakteristik Tugas):** Ini adalah tuntutan yang melekat pada tugas itu sendiri. Faktor-faktor ini meliputi:

- 1) Beban kerja mental dan fisik: Seberapa menuntut tugas tersebut.
- 2) Tekanan waktu: Berapa banyak waktu yang tersedia untuk menyelesaikan tugas.

- 3) Tingkat kompleksitas tugas: Berapa banyak langkah atau keputusan yang terlibat.
- 4) Tingkat risiko yang dirasakan.

Kombinasi dari PSFs ini menciptakan konteks kinerja pada saat tertentu. Ketika banyak PSFs negatif hadir secara bersamaan, misalnya, seorang pekerja yang lelah (faktor internal) menggunakan prosedur yang membingungkan (faktor eksternal) di bawah tekanan waktu yang tinggi (faktor stresor), probabilitas terjadinya kesalahan meningkat secara dramatis. Sebaliknya, ketika PSFs positif dominan, kinerja cenderung lebih andal.

Metode *Human Reliability Assessment* (HRA), seperti HEART atau THERP (yang akan dibahas di Bab 11), secara eksplisit menggunakan PSFs (sering disebut *Error Producing Conditions* atau EPCs) untuk memodifikasi probabilitas kesalahan dasar. Misalnya, probabilitas kesalahan dasar untuk tugas tertentu mungkin 1 dalam 1000. Namun, jika dilakukan di bawah tekanan waktu yang tinggi, probabilitasnya mungkin dikalikan dengan faktor 5, menjadikannya 1 dalam 200.

Analisis PSFs memberikan target nyata untuk intervensi. Daripada hanya memberitahu pekerja untuk "lebih berhati-hati", kita dapat secara sistematis mengidentifikasi dan memperbaiki PSFs yang negatif. Kita dapat meningkatkan kualitas prosedur, mengurangi tingkat kebisingan, mengelola beban kerja, atau memberikan pelatihan yang lebih baik. Dengan melakukan ini, kita tidak mencoba untuk mengubah sifat dasar manusia; sebaliknya, kita mengubah kondisi di mana mereka bekerja untuk mendukung kinerja terbaik mereka. Ini adalah pendekatan rekayasa, bukan pendekatan moralistik, untuk mengelola *human error*.

## **2. Mengapa Variasi Adalah Bagian Alami dari Kinerja Manusia**

Upaya untuk menghilangkan variabilitas kinerja manusia adalah pengejaran yang sia-sia karena variabilitas adalah ciri yang melekat dan esensial dari menjadi manusia. Tidak seperti mesin yang dapat diprogram untuk melakukan tugas yang sama persis berulang kali, kinerja manusia secara alami berfluktuasi dari waktu ke waktu. Fluktuasi ini disebabkan oleh berbagai faktor, mulai dari keadaan fisiologis (tingkat energi, kelelahan)

dan psikologis (suasana hati, tingkat perhatian) hingga adaptasi terhadap perubahan kecil dalam lingkungan kerja.

Pandangan *Safety-II* mengajarkan kita untuk melihat variabilitas ini bukan sebagai sumber kegagalan, tetapi sebagai sumber kesuksesan dan resiliensi. Prosedur dan rencana kerja (*work-as-imagined*) hampir tidak pernah dapat menangkap kompleksitas dan ketidakpastian penuh dari dunia nyata. Selalu ada kesenjangan antara rencana dan realitas. Manusia, melalui kemampuan mereka untuk bervariasi dan menyesuaikan kinerja mereka, yang menjembatani kesenjangan ini. Kemampuan untuk sedikit menyimpang dari prosedur untuk mengakomodasi alat yang sedikit berbeda, atau untuk mempercepat satu langkah untuk mengkompensasi penundaan di langkah lain, adalah apa yang membuat sistem kerja kita benar-benar berfungsi.

Bayangkan seorang perawat yang mengikuti prosedur pemberian obat. Prosedur mungkin mengatakan "berikan obat pada pukul 09:00". Namun, pada pukul 09:00, pasien sedang tidur nyenyak setelah malam yang sulit. Perawat yang kaku dan tidak bervariasi mungkin akan membangunkan pasien, yang dapat merugikan pemulihannya. Perawat yang adaptif akan memvariasikan kinerjanya, mungkin dengan memutuskan untuk kembali dalam 30 menit. Variasi ini, penyimpangan kecil dari aturan, adalah contoh kinerja yang cerdas dan resilien.

Masalahnya adalah bahwa variasi yang sama yang biasanya menciptakan keberhasilan terkadang dapat melampaui batas dan menyebabkan kegagalan. Adaptasi yang berhasil dalam satu situasi mungkin menjadi kesalahan dalam situasi lain yang tampak serupa. Garis antara penyesuaian yang cerdas dan kesalahan berisiko sering kali sangat tipis dan hanya terlihat jelas setelah kejadian. Karena kita tidak dapat menghilangkan variabilitas, tujuannya adalah untuk mengelolanya.

Mengelola variabilitas melibatkan beberapa strategi. Pertama, memahami sumbernya. Dengan memahami mengapa kinerja bervariasi (misalnya, karena kelelahan di akhir shift, atau karena desain antarmuka yang ambigu), kita dapat menargetkan intervensi kita. Kedua, memberikan umpan balik yang lebih baik. Sistem yang memberikan informasi yang jelas

dan tepat waktu tentang di mana kinerja saat ini berada relatif terhadap batas aman memungkinkan orang untuk menyesuaikan variasi mereka sendiri secara lebih efektif.

Ketiga, menciptakan margin atau penyangga (*buffers*). Sistem yang rapuh adalah sistem yang beroperasi sangat dekat dengan batas amannya, di mana variasi kecil pun dapat menyebabkan kegagalan. Sistem yang tangguh memiliki margin, waktu ekstra, sumber daya ekstra, redundansi, yang dapat menyerap variabilitas normal tanpa konsekuensi negatif.

Menerima variabilitas sebagai bagian alami dari kinerja manusia adalah sebuah pergeseran pola pikir yang mendalam. Ini menjauhkan kita dari ideal kesempurnaan mekanistik dan menuju pemahaman yang lebih realistis dan hormat terhadap kontribusi unik yang dibawa manusia ke dalam sistem kerja. Ini adalah pengakuan bahwa orang-orang kita bukanlah sumber masalah utama kita; mereka adalah sumber utama solusi dan adaptasi kita.

### **3. Pentingnya Toleransi Kesalahan (Error Tolerance) dalam Desain Sistem**

Karena variabilitas adalah alami dan kesalahan tidak akan pernah bisa dihilangkan sepenuhnya, kesimpulan logis terakhir adalah bahwa keselamatan harus datang dari desain sistem yang toleran terhadap kesalahan. Toleransi kesalahan, kadang-kadang disebut sebagai rekayasa resiliensi, adalah prinsip desain yang mengakui kemungkinan kegagalan dan bertujuan untuk meminimalkan konsekuensinya, bukan hanya mencoba untuk mencegah terjadinya kegagalan itu sendiri. Ini adalah jaring pengaman fundamental dalam pendekatan sistemik.

Sistem yang toleran terhadap kesalahan dirancang dengan asumsi bahwa orang *akan* membuat *slips*, *lapses*, dan *mistakes*. Oleh karena itu, sistem tersebut harus memiliki fitur-fitur yang dapat:

#### **a. Mencegah kesalahan**

Membuat tindakan yang salah menjadi sulit atau tidak mungkin dilakukan. Ini adalah tingkat pertahanan pertama. Contohnya termasuk *forcing functions* (seperti kabel USB yang hanya bisa masuk satu arah) atau *interlocks* yang mencegah pengoperasian mesin jika pelindungnya tidak terpasang.

b. Mendeteksi kesalahan

Jika kesalahan tidak dapat dicegah, sistem harus membuatnya segera terlihat sehingga dapat diperbaiki. Umpan balik yang baik adalah kuncinya. Misalnya, ketika Anda mencoba menyeret file ke tempat sampah di komputer Anda, sistem akan bertanya, "Apakah Anda yakin ingin menghapus file ini?". Ini memberikan kesempatan untuk mendeteksi dan membatalkan slip yang tidak disengaja.

c. Memitigasi konsekuensi kesalahan

Jika kesalahan terjadi dan tidak terdeteksi, sistem harus dirancang untuk meminimalkan dampaknya. Ini sering dicapai melalui redundansi, di mana ada sistem cadangan yang mengambil alih jika sistem utama gagal. Pesawat modern memiliki beberapa sistem hidrolis dan komputer penerbangan sebagai contohnya.

d. Memfasilitasi pemulihan dari kesalahan

Sistem harus memudahkan pengguna untuk kembali ke keadaan aman setelah kesalahan dibuat. Tombol "Undo" (Urungkan) yang ada di mana-mana pada perangkat lunak adalah contoh sempurna dari desain yang memfasilitasi pemulihan.

Pentingnya toleransi kesalahan dapat dilihat di banyak bidang. Dalam desain mobil, fitur-fitur seperti *airbags*, zona remuk (*crumple zones*), dan sistem pengereman anti-lock (ABS) adalah contoh desain yang toleran terhadap kesalahan. Mereka tidak mencegah kecelakaan awal (kesalahan pengemudi), tetapi mereka secara dramatis mengurangi keparahan konsekuensinya.

Dalam konteks industri, toleransi kesalahan dapat diwujudkan dalam berbagai cara. Prosedur dapat dirancang untuk memiliki "langkah penahan" (*hold points*) di mana pekerjaan harus diverifikasi oleh orang kedua sebelum melanjutkan ke langkah kritis berikutnya. Sistem alarm dapat dirancang dengan prioritas yang jelas sehingga operator tidak kewalahan dan dapat fokus pada masalah yang paling penting. Tata letak fisik pabrik dapat dirancang untuk memisahkan pejalan kaki dari lalu lintas forklift, sehingga jika salah satu membuat kesalahan, konsekuensinya tidak fatal.

Membangun toleransi kesalahan ke dalam sistem membutuhkan perubahan pola pikir dari reaktivitas ke proaktivitas. Ini menuntut para perancang dan insinyur untuk secara aktif membayangkan bagaimana orang mungkin salah menggunakan sistem mereka dan kemudian merancang perlindungan terhadap skenario-skenario tersebut. Teknik-teknik seperti *Failure Mode and Effects Analysis* (FMEA) dapat diperluas untuk tidak hanya mencakup mode kegagalan peralatan, tetapi juga mode kegagalan manusia.

Pada akhirnya, toleransi kesalahan adalah pengakuan paling jujur dari pendekatan sistemik. Ini adalah penerimaan bahwa kita tidak dapat menciptakan manusia yang sempurna atau sistem yang tidak pernah gagal. Sebaliknya, tujuan kita adalah untuk menciptakan sistem yang "gagal dengan anggun" (*fail gracefully*) atau "gagal dengan aman" (*fail-safe*), sistem yang melindungi orang dari konsekuensi terburuk dari sifat mereka yang tidak sempurna. Ini adalah jalan menuju keselamatan yang sejati dan berkelanjutan.

## KESIMPULAN

Bab ketiga ini telah membongkar konsep monolitik "*human error*" menjadi sebuah taksonomi yang terstruktur dan dapat ditindaklanjuti. Dengan mendefinisikan *human error* sebagai penyimpangan yang tidak disengaja dari niat, kita telah membangun fondasi untuk membedakannya secara tegas dari pelanggaran (*violations*), yang merupakan penyimpangan yang disengaja. Pembedaan ini sangat penting, karena kesalahan berakar pada proses kognitif dan desain sistem, sementara pelanggaran sering kali didorong oleh faktor motivasi dan budaya organisasi. Keduanya memerlukan strategi mitigasi yang sangat berbeda.

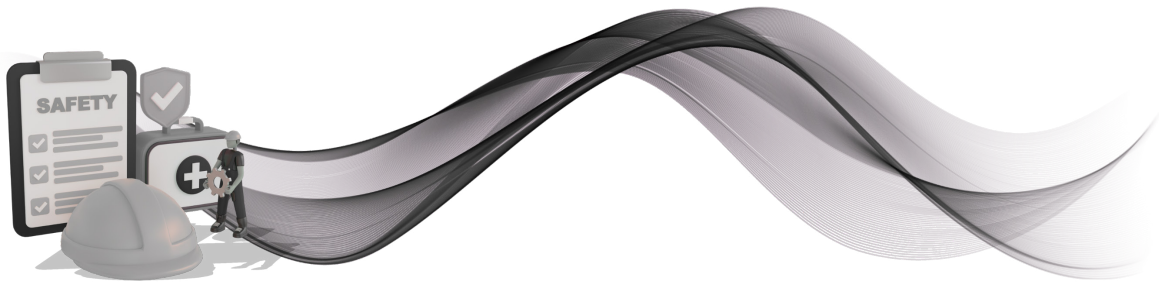
Lebih jauh lagi, kesalahan itu sendiri telah diklasifikasikan ke dalam tiga tipe utama berdasarkan mekanisme kognitifnya: *slips* (kesalahan eksekusi berbasis perhatian), *lapses* (kesalahan eksekusi berbasis memori), dan *mistakes* (kesalahan perencanaan berbasis aturan atau pengetahuan). Demikian pula, pelanggaran telah dikategorikan sebagai rutin, situasional, atau pengecualian. Kerangka kerja klasifikasi ini menyediakan sebuah "toolkit" diagnostik yang memungkinkan praktisi K3 untuk bergerak

melampaui label “kesalahan manusia” yang sederhana dan mengidentifikasi mekanisme kegagalan yang spesifik.

Namun, yang paling penting, bab ini telah mengontekstualisasikan semua jenis kegagalan kinerja ini sebagai bentuk variabilitas perilaku manusia. Kesalahan dan pelanggaran bukanlah peristiwa acak, melainkan hasil yang dapat diprediksi dari interaksi antara kapabilitas manusia dan kondisi kerja, atau *Performance Shaping Factors*. Menerima variabilitas sebagai bagian alami dan bahkan esensial dari kinerja manusia membawa kita pada kesimpulan akhir yang kuat: tujuan utama manajemen keselamatan bukanlah untuk menghilangkan kesalahan, melainkan untuk membangun sistem yang toleran terhadap kesalahan.

Dengan pemahaman yang mendalam tentang *apa* itu *human error* dan *bagaimana* berbagai bentuknya terjadi, kita sekarang siap untuk menjelajahi *mengapa* kesalahan-kesalahan ini terjadi dalam konteks sistem yang lebih luas. Bab-bab berikutnya akan membahas model-model teoritis kunci, seperti Model Keju Swiss, yang akan membantu kita memvisualisasikan bagaimana kelemahan sistemik dan kegagalan kinerja individu dapat bersekutu untuk menciptakan bencana.

**DUMMYY**



# BAB 4

## DASAR-DASAR PENDEKATAN SISTEMIK DALAM MITIGASI *HUMAN ERROR*

### PENDAHULUAN

Setelah menelusuri evolusi paradigma dari individu ke sistem dan membedah berbagai jenis *human error*, kita tiba pada sebuah pertanyaan fundamental: Bagaimana kita dapat secara praktis menerapkan pemikiran sistemik? Konsep-konsep seperti “kondisi laten” dan “kesalahan sebagai gejala” mungkin terdengar meyakinkan secara teoretis, tetapi bagaimana kita mengubahnya menjadi alat analisis dan kerangka kerja untuk tindakan nyata di tempat kerja? Bab ini bertujuan untuk menjawab pertanyaan tersebut dengan meletakkan dasar-dasar konseptual dan struktural dari pendekatan sistemik. Ini adalah bab yang akan memberikan “tata bahasa” dan “kosa kata” yang diperlukan untuk berbicara secara fasih dalam bahasa keselamatan modern.

Jika bab-bab sebelumnya adalah tentang “mengapa” kita perlu beralih ke pemikiran sistemik, bab ini adalah tentang “apa” yang menjadi pilar-pilar dari pemikiran tersebut. Kita akan bergerak dari filosofi ke arsitektur, menguraikan komponen-komponen inti yang memungkinkan kita untuk melihat organisasi bukan sebagai kumpulan individu yang terisolasi, tetapi

sebagai sebuah jaringan interaksi yang kompleks dan dinamis. Tanpa pemahaman yang kuat tentang dasar-dasar ini, model-model canggih seperti Model Keju Swiss yang akan dibahas nanti berisiko menjadi karikatur yang disalahpahami.

Pembahasan akan diawali dengan mendefinisikan secara formal apa yang kita maksud dengan “sistem” dalam konteks K3. Kita akan belajar untuk melihat melampaui bagan organisasi dan mengidentifikasi komponen-komponen kunci, manusia, teknologi, organisasi, dan lingkungan, serta, yang lebih penting, menganalisis bagaimana mereka saling terhubung melalui hubungan timbal balik dan putaran umpan balik (*feedback loops*). Pemahaman ini penting karena dalam sistem yang kompleks, penyebab dan akibat sering kali tidak berhubungan secara linear atau langsung; tindakan di satu bagian sistem dapat memiliki konsekuensi yang tidak terduga di bagian lain.

Selanjutnya, bab ini akan secara mendalam mengupas dua konsep yang menjadi jantung dari analisis kegagalan sistemik: *active failures* (kegagalan aktif) dan *latent conditions* (kondisi laten). Kita akan membedah bagaimana kegagalan aktif, kesalahan atau pelanggaran di lini depan, hanyalah pemicu terakhir dari sebuah kecelakaan. Kekuatan analisis sistemik terletak pada kemampuannya untuk melacak kembali dari kegagalan aktif ini untuk mengungkap kondisi-kondisi laten yang tersembunyi, seperti desain yang buruk, pelatihan yang tidak memadai, atau tekanan produksi, yang telah menciptakan prasyarat untuk kegagalan jauh sebelumnya.

Setelah memahami bagaimana kegagalan berkembang, kita akan beralih ke bagaimana kegagalan dapat dicegah melalui konsep pertahanan berlapis (*defenses in depth*). Prinsip rekayasa keselamatan fundamental ini mengajarkan bahwa keamanan tidak dapat diandalkan pada satu penghalang tunggal yang sempurna. Sebaliknya, sistem yang tangguh dibangun dari beberapa lapisan pertahanan yang tidak sempurna, teknis, prosedural, dan manusiawi, yang secara kolektif menciptakan jaring pengaman yang kuat. Kita akan menganalisis bagaimana kecelakaan besar hampir selalu melibatkan penembusan atau kegagalan dari beberapa lapisan pertahanan ini secara bersamaan.

Terakhir, bab ini akan menghubungkan semua konsep teoretis ini ke dalam kerangka kerja praktis yang sudah dikenal oleh banyak organisasi: Sistem Manajemen K3 (SMK3). Akan ditunjukkan bahwa SMK3, jika diimplementasikan dengan semangat sistemik, dapat menjadi struktur yang ideal untuk secara proaktif mengidentifikasi kondisi laten, memperkuat pertahanan, dan mengelola risiko *human error*. Ini adalah tentang mengubah SMK3 dari sekadar serangkaian dokumen menjadi sebuah “sistem kekebalan tubuh” organisasi yang dinamis.

Dengan menyelesaikan bab ini, pembaca akan memiliki pemahaman yang kokoh tentang arsitektur kegagalan dan pencegahan dalam pandangan sistemik. Kosa kata inti, sistem, kondisi laten, kegagalan aktif, pertahanan berlapis, akan menjadi bagian dari perangkat analisis pembaca, mempersiapkan mereka untuk menerapkan model-model spesifik dan strategi mitigasi yang akan dibahas di sisa buku ini.

## **A. Konsep Sistem dan Lingkungan Kerja**

Langkah pertama dalam menerapkan pendekatan sistemik adalah mendefinisikan dengan jelas apa yang dimaksud dengan “sistem”. Dalam konteks K3, sebuah sistem bukanlah sekadar mesin atau kumpulan orang, melainkan sebuah kesatuan yang terorganisir dari komponen-komponen yang saling berinteraksi, yang dirancang untuk mencapai tujuan tertentu. Komponen-komponen ini bekerja bersama, saling memengaruhi, dan perilaku keseluruhan sistem tidak dapat dipahami hanya dengan melihat komponen-komponennya secara terpisah. Prinsip utama di sini adalah interkoneksi; perubahan pada satu bagian sistem pasti akan memengaruhi bagian-bagian lainnya, sering kali dengan cara yang tidak terduga.

Tujuan dari sistem kerja bisa bermacam-macam, seperti memproduksi barang, menyediakan layanan, atau mengangkut orang. Namun, di samping tujuan produksi ini, setiap sistem kerja juga memiliki tujuan keselamatan, yaitu, untuk mencapai tujuan produksi tanpa menyebabkan kerugian atau cedera. Pendekatan sistemik berpendapat bahwa tujuan keselamatan ini tidak dapat dipisahkan dari tujuan produksi; keduanya adalah hasil dari dinamika sistem yang sama. Kegagalan untuk mencapai tujuan keselamatan

(kecelakaan) sering kali berakar pada konflik atau ketegangan antara berbagai tujuan sistem (misalnya, tekanan untuk memaksimalkan produksi vs. kebutuhan untuk melakukan perawatan).

Setiap sistem beroperasi dalam lingkungan yang lebih luas, dan batas antara sistem dan lingkungannya tidak selalu jelas. Menentukan batasan sistem (*system boundary*) adalah langkah analisis yang penting. Batasan ini membantu kita untuk memfokuskan analisis kita pada komponen dan interaksi yang paling relevan dengan masalah yang sedang diteliti. Misalnya, dalam menganalisis kecelakaan di sebuah anjungan minyak lepas pantai, "sistem" mungkin mencakup kru, peralatan pengeboran, dan prosedur di anjungan tersebut. "Lingkungan" mungkin mencakup cuaca, kondisi laut, keputusan dari kantor pusat di darat, dan peraturan pemerintah. Memahami bagaimana sistem berinteraksi dengan lingkungannya, menerima input (misalnya, tekanan produksi dari manajemen) dan menghasilkan output, sangat penting untuk analisis yang komprehensif.

Inti dari pemahaman sistemik adalah fokus pada interaksi dan hubungan, bukan hanya pada komponen itu sendiri. Pertanyaan yang diajukan bukan hanya "Apa saja bagian-bagian dari sistem ini?", tetapi juga "Bagaimana bagian-bagian ini terhubung? Bagaimana mereka berkomunikasi? Bagaimana mereka saling mengendalikan dan membatasi?". Hubungan ini sering kali melibatkan putaran umpan balik (*feedback loops*), di mana output dari suatu tindakan kembali memengaruhi tindakan di masa depan. Misalnya, keberhasilan mengambil jalan pintas tanpa konsekuensi negatif (output) dapat memperkuat perilaku tersebut di masa depan (umpan balik positif), yang secara bertahap mengikis margin keselamatan.

Dengan mendefinisikan pekerjaan sebagai sebuah sistem, kita dapat mulai menggunakan alat dan konsep dari pemikiran sistem untuk menganalisisnya. Kita dapat memetakan alur kerja, informasi, dan keputusan. Kita dapat mengidentifikasi titik-titik di mana interaksi antar komponen sangat erat (*tightly coupled*) dan oleh karena itu lebih rentan terhadap kegagalan berantai. Kita dapat mencari putaran umpan balik yang mungkin memperkuat perilaku berisiko. Pandangan ini mengubah cara kita melihat tempat kerja, dari sekadar lokasi fisik menjadi sebuah jaringan hubungan yang hidup dan dinamis.

**Analogi/Contoh Kasus:** Bayangkan sebuah orkestra simfoni sebagai sebuah sistem. Tujuannya adalah untuk menghasilkan musik yang indah (tujuan produksi). Komponennya meliputi para musisi (manusia), instrumen mereka (teknologi), partitur musik (prosedur), dan konduktor (manajemen). Jika seorang pemain biola memainkan nada yang salah (*active failure*), pendekatan non-sistemik akan menyalahkannya. Pendekatan sistemik akan bertanya lebih jauh. Mungkin pencahayaan di panggungnya buruk sehingga dia sulit membaca partitur (interaksi manusia-lingkungan). Mungkin konduktor memberikan isyarat yang ambigu (kegagalan manajemen/komunikasi). Atau mungkin akustik di aula membuat sulit untuk mendengar bagian lain dari orkestra (umpan balik). Kualitas musik secara keseluruhan (keselamatan dan produksi) adalah properti *emergent* dari interaksi dinamis antara semua komponen ini, bukan hanya keterampilan satu musisi.

### 1. Mendefinisikan Batasan Sistem K<sub>3</sub>

Salah satu langkah pertama yang paling praktis dan penting dalam setiap analisis sistemik adalah mendefinisikan batasan sistem (*system boundary*). Batasan ini adalah garis imajiner yang kita tarik untuk memisahkan komponen-komponen yang akan kita sertakan dalam analisis mendalam (di dalam sistem) dari elemen-elemen yang akan kita perlakukan sebagai input atau pengaruh eksternal (di luar sistem, atau di lingkungan). Keputusan tentang di mana harus menarik batasan ini bersifat pragmatis dan bergantung pada tujuan analisis kita. Tidak ada satu batasan “yang benar” secara absolut, tetapi batasan yang ditarik dengan buruk dapat menghalangi wawasan yang penting.

Jika batasan ditarik terlalu sempit, kita berisiko jatuh kembali ke dalam perangkat *Person-Model*. Misalnya, jika kita menganalisis kesalahan seorang perawat dalam memberikan obat dan mendefinisikan “sistem” hanya sebagai perawat dan pasien, kita mungkin akan melewatkan faktor-faktor krusial seperti desain kemasan obat yang membingungkan, sistem pelabelan di apotek, kebijakan kepegawaian yang menyebabkan kelelahan, atau budaya yang menghalangi perawat untuk bertanya jika ragu. Analisis kita akan berakhir dengan menyalahkan perawat karena kita telah secara artifisial mengecualikan semua pengaruh sistemik yang lebih luas.

Sebaliknya, jika batasan ditarik terlalu luas, analisis bisa menjadi tidak terkendali dan tidak praktis. Jika dalam menganalisis kecelakaan pabrik kita mencoba untuk memasukkan seluruh sistem ekonomi global atau kebijakan pendidikan nasional, kita mungkin akan tenggelam dalam kompleksitas tanpa menghasilkan rekomendasi yang dapat ditindaklanjuti untuk pabrik tersebut. Kuncinya adalah menemukan keseimbangan: cukup luas untuk menangkap pengaruh organisasi dan manajerial yang paling signifikan, tetapi cukup terfokus untuk menjaga agar analisis tetap relevan dan dapat dikelola.

Cara yang baik untuk memulai adalah dengan menggunakan pendekatan berlapis atau "kulit bawang". Kita bisa mulai dengan sistem inti di pusat, yaitu interaksi manusia-teknologi di tempat kerja (misalnya, operator dan panel kontrolnya). Lapisan berikutnya adalah tim kerja dan pengawasan langsung, yang mencakup dinamika tim, komunikasi, dan kepemimpinan di tingkat penyelia. Lapisan selanjutnya adalah manajemen lokasi atau departemen, yang mencakup kebijakan lokal, penjadwalan, dan alokasi sumber daya. Lapisan terluar yang masih berada di dalam organisasi adalah manajemen puncak dan budaya perusahaan, yang mencakup keputusan strategis, prioritas, dan nilai-nilai organisasi.

Elemen-elemen di luar batasan organisasi, seperti regulator, pemasok, pesaing, dan kondisi pasar, biasanya diperlakukan sebagai lingkungan sistem. Kita tidak menganalisis cara kerja internal regulator, tetapi kita menganalisis bagaimana peraturan yang mereka buat memengaruhi keputusan dan tindakan di dalam sistem kita.

Proses mendefinisikan batasan harus menjadi latihan yang sadar dan eksplisit di awal setiap investigasi atau penilaian risiko. Tim harus mendiskusikan dan menyepakati: "Untuk tujuan analisis ini, apa saja komponen utama yang akan kita anggap sebagai bagian dari sistem kita?". Keputusan ini harus didokumentasikan. Fleksibilitas juga penting; jika selama analisis kita menemukan bahwa pengaruh eksternal yang sebelumnya kita abaikan ternyata sangat penting, kita mungkin perlu merevisi dan memperluas batasan kita.

Mendefinisikan batasan sistem secara efektif adalah keterampilan. Ini adalah tentang membuat penilaian yang cerdas tentang apa yang penting. Dengan melakukannya dengan benar, kita memastikan bahwa kita tidak hanya melihat pohon-pohon (kegagalan individu) tetapi juga melihat keseluruhan hutan (konteks sistemik) di mana pohon-pohon itu tumbuh.

## 2. **Komponen Manusia, Teknologi, Organisasi, dan Lingkungan**

Setelah batasan sistem didefinisikan, langkah selanjutnya adalah mengidentifikasi dan menganalisis komponen-komponen utama di dalam batasan tersebut. Sebagian besar model sistem sosio-teknis menyetujui adanya empat kategori komponen utama yang saling berinteraksi. Memahami setiap komponen dan, yang lebih penting, antarmuka di antara mereka adalah inti dari analisis sistemik. Keempat komponen tersebut adalah Manusia, Teknologi, Organisasi, dan Lingkungan (sering diringkas sebagai MTOE atau serupa).

### a. **Manusia (atau *Liveware* dalam model SHELL)**

Ini adalah komponen yang paling kompleks dan variabel. Komponen manusia mencakup semua orang di dalam sistem, dari pekerja di lini depan hingga manajemen puncak. Analisis komponen ini tidak hanya melihat individu, tetapi juga tim dan kelompok. Ini mencakup atribut-atribut seperti:

- 1) Kompetensi (pengetahuan, keterampilan, pengalaman)
- 2) Keterbatasan fisik dan kognitif (misalnya, kekuatan, kapasitas memori)
- 3) Keadaan psikofisiologis (misalnya, kelelahan, stres, motivasi)
- 4) Dinamika tim dan komunikasi (misalnya, *Crew Resource Management*)
- 5) Pengambilan keputusan dan bias kognitif.

### b. **Teknologi (atau *Hardware*)**

Ini merujuk pada semua objek fisik dan alat yang digunakan dalam sistem. Ini tidak hanya mencakup mesin-mesin besar, tetapi juga peralatan tangan, kendaraan, komputer, perangkat lunak, dan alat pelindung diri (APD). Analisis komponen ini berfokus pada:

- 1) Desain dan ergonomi (apakah cocok dengan pengguna manusia?)
- 2) Keandalan dan pemeliharaan (seberapa sering gagal dan bagaimana perawatannya?)
- 3) Fungsi otomatisasi dan antarmuka (bagaimana ia berinteraksi dengan pengguna?)
- 4) Umpan balik yang diberikan kepada pengguna.

c. **Organisasi (atau *Software* dalam model SHELL, dalam arti luas)**

Komponen ini adalah “perekat” yang menyatukan manusia dan teknologi. Ini mencakup semua aturan, struktur, dan proses non-fisik yang mengatur sistem. Komponen organisasi sering kali merupakan sumber utama dari kondisi laten. Ini termasuk:

- 1) Kebijakan, prosedur, dan aturan
- 2) Struktur manajemen dan hierarki
- 3) Sistem komunikasi
- 4) Budaya organisasi dan iklim keselamatan
- 5) Sistem pelatihan dan penilaian kompetensi
- 6) Tekanan produksi dan sistem insentif.

d. **Lingkungan (*Environment*)**

Ini adalah konteks di mana ketiga komponen lainnya beroperasi. Lingkungan dapat dibagi menjadi lingkungan internal (fisik di tempat kerja) dan eksternal (di luar organisasi). Ini mencakup:

- 1) Lingkungan fisik: Pencahayaan, kebisingan, suhu, cuaca, tata letak tempat kerja.
- 2) Lingkungan sosial: Hubungan industrial, norma-norma kelompok.
- 3) Lingkungan eksternal: Peraturan pemerintah, tekanan pasar, kondisi ekonomi, ekspektasi publik.

Kecelakaan jarang sekali disebabkan oleh kegagalan satu komponen saja. Sebaliknya, mereka muncul dari ketidakcocokan (*mismatch*) pada antarmuka antara komponen-komponen ini. Misalnya, sebuah kecelakaan mungkin terjadi karena ketidakcocokan antara Manusia dan Teknologi (desain tombol yang membingungkan), atau antara Manusia dan Organisasi

(prosedur yang tidak praktis untuk diikuti), atau antara Organisasi dan Lingkungan (perusahaan gagal beradaptasi dengan peraturan baru).

Tugas seorang analis sistem adalah untuk memetakan komponen-komponen ini dalam sistem yang mereka pelajari dan kemudian secara sistematis memeriksa antarmuka di antara mereka. Di mana letak potensi gesekan atau ketidakcocokan? Di mana letak interaksi yang paling kritis dan rentan? Dengan menggunakan kerangka kerja empat komponen ini, kita dapat memastikan bahwa analisis kita bersifat komprehensif dan tidak mengabaikan area-area penting yang mungkin mengandung akar penyebab kegagalan.

### 3. Analisis Keterkaitan dan Umpan Balik dalam Sistem

Memahami komponen-komponen sistem hanyalah setengah dari cerita. Kekuatan sebenarnya dari pemikiran sistemik terletak pada analisis hubungan dan keterkaitan dinamis di antara komponen-komponen tersebut. Sistem tidak statis; mereka terus berubah dan berevolusi sebagai respons terhadap tindakan dan peristiwa. Dua konsep kunci untuk memahami dinamika ini adalah keterkaitan (*coupling*) dan putaran umpan balik (*feedback loops*).

Keterkaitan (*Coupling*) merujuk pada seberapa erat dan cepat hubungan antara dua komponen dalam sebuah sistem. Dalam sistem yang terkait erat (*tightly coupled*), tidak ada jeda atau penyangga (*buffer*). Perubahan atau kegagalan di satu bagian akan dengan cepat dan tak terhindarkan menyebar ke bagian lain. Pembangkit listrik tenaga nuklir, proses kimia kontinu, dan operasi penerbangan adalah contoh sistem yang terkait erat. Tidak ada waktu untuk berhenti dan berpikir; satu peristiwa dapat dengan cepat meningkat menjadi kaskade kegagalan. Sistem seperti ini secara inheren lebih berisiko dan membutuhkan tingkat keandalan yang sangat tinggi.

Sebaliknya, dalam sistem yang terkait longgar (*loosely coupled*), ada lebih banyak penyangga, jeda waktu, dan sumber daya cadangan. Kegagalan di satu bagian dapat diisolasi dan tidak segera memengaruhi seluruh sistem. Ada lebih banyak waktu untuk mendeteksi masalah, mendiagnosisnya, dan merumuskan respons. Sebagian besar proses konstruksi atau proyek

penelitian adalah contoh sistem yang terkait longgar. Kesalahan dalam satu tugas tidak secara otomatis menyebabkan kegagalan seluruh proyek. Menganalisis tingkat keterkaitan dalam sistem kerja kita membantu kita mengidentifikasi di mana letak risiko kaskade kegagalan yang paling besar.

Putaran Umpan Balik (*Feedback Loops*) adalah mekanisme di mana output dari sebuah sistem atau tindakan kembali menjadi input, yang memengaruhi perilaku di masa depan. Ada dua jenis utama umpan balik. Umpan balik penyeimbang atau negatif (*balancing/negative feedback*) bekerja untuk menstabilkan sistem dan menjaganya tetap dalam keadaan yang diinginkan, seperti termostat yang mematikan pemanas ketika suhu yang diinginkan tercapai. Dalam K3, investigasi kecelakaan yang efektif yang mengarah pada perbaikan sistem adalah contoh umpan balik penyeimbang.

Jenis yang sering kali lebih berbahaya adalah umpan balik penguat atau positif (*reinforcing/positive feedback*). Umpan balik ini mempercepat perubahan ke satu arah, menciptakan efek bola salju. "Normalisasi penyimpangan" adalah contoh klasik dari umpan balik penguat yang merusak. Sebuah tim mengambil jalan pintas kecil dari prosedur (penyimpangan). Tidak ada hal buruk yang terjadi (output). Keberhasilan ini memperkuat keyakinan bahwa jalan pintas itu aman, yang mendorong penyimpangan yang sedikit lebih besar di waktu berikutnya, dan seterusnya. Siklus ini terus berlanjut, secara bertahap mengikis margin keselamatan sampai akhirnya terjadi kegagalan.

Menganalisis sistem K3 berarti secara aktif mencari putaran umpan balik ini. Apakah kita memiliki mekanisme umpan balik penyeimbang yang kuat untuk belajar dari kesalahan? Apakah ada putaran umpan balik penguat yang mungkin secara diam-diam mendorong perilaku berisiko? Misalnya, jika sistem insentif hanya memberi penghargaan pada produksi (input), ini akan memperkuat perilaku yang memaksimalkan output produksi, bahkan jika itu berarti mengabaikan keselamatan.

Dengan menganalisis keterkaitan dan umpan balik, kita bergerak dari pandangan statis tentang sistem ke pemahaman yang dinamis. Kita mulai melihat bagaimana perilaku muncul dan berkembang dari waktu ke waktu

sebagai hasil dari struktur sistem itu sendiri. Pemahaman ini memungkinkan kita untuk melakukan intervensi pada "titik ungkit" (*leverage points*) yang lebih strategis, yaitu, mengubah struktur umpan balik sistem, untuk menciptakan perubahan perilaku yang berkelanjutan, alih-alih hanya mencoba mengoreksi tindakan individu secara terpisah.

## **B. *Latent Conditions* (Kondisi Laten) dan *Active Failures* (Kegagalan Aktif)**

Salah satu kontribusi paling abadi dari James Reason untuk ilmu keselamatan adalah pembedaan yang jelas antara dua jenis kegagalan: *active failures* dan *latent conditions*. Memahami perbedaan, dan yang lebih penting, hubungan antara keduanya, adalah inti dari diagnosis sistemik. Analogi medis sangat membantu di sini: *active failures* adalah gejala yang terlihat dari sebuah penyakit, seperti demam atau batuk. *Latent conditions* adalah patogen yang mendasari penyakit itu sendiri, seperti infeksi virus atau bakteri yang tidak terlihat. Mengobati gejalanya saja tidak akan pernah menyembuhkan penyakitnya.

*Active failures* adalah tindakan atau kelalaian yang memiliki dampak merugikan secara langsung dan segera. Mereka biasanya dilakukan oleh orang-orang di "ujung tajam" (*sharp end*) sistem, operator, pilot, ahli bedah, pengemudi, yang berinteraksi langsung dengan teknologi dan proses kerja. *Slips, lapses, mistakes, dan violations* yang kita diskusikan di Bab 3 adalah semua contoh dari *active failures*. Karena sifatnya yang langsung dan terlihat, *active failures* adalah hal yang paling mudah untuk diperhatikan dan disalahkan setelah sebuah insiden. Pendekatan *Person-Model* hampir secara eksklusif berfokus pada *active failures*.

*Latent conditions*, sebaliknya, adalah "jebakan" tersembunyi di dalam sistem yang mungkin tidak aktif atau tidak berbahaya selama sehari-hari, berbulan-bulan, atau bahkan bertahun-tahun. Mereka adalah konsekuensi yang tak terhindarkan dari keputusan strategis dan proses organisasi. Mereka diciptakan oleh orang-orang di "ujung tumpul" (*blunt end*) sistem, para perancang, pembuat prosedur, manajer puncak, dan regulator. Keputusan-keputusan ini, seperti memilih untuk membeli peralatan yang lebih murah tetapi kurang ergonomis, atau memotong anggaran pelatihan,

menciptakan kelemahan dalam pertahanan sistem. Kelemahan-kelemahan ini seperti “ranjau darat”, menunggu kombinasi keadaan yang tepat dan sebuah *active failure* untuk memicunya.

Kekuatan sebenarnya dari pendekatan sistemik terletak pada pengakuannya bahwa *active failures* tidak terjadi secara spontan. Mereka diciptakan dan dibentuk oleh kondisi-kondisi laten yang sudah ada sebelumnya. Seorang operator mungkin menekan tombol yang salah (*active failure*), tetapi kesalahan itu menjadi mungkin atau bahkan mungkin terjadi karena panel kontrol dirancang dengan buruk (*latent condition*). Seorang pengemudi truk mungkin tertidur di kemudi (*active failure*), tetapi ini adalah konsekuensi yang dapat diprediksi dari kebijakan perusahaan yang mendorong jam kerja yang berlebihan (*latent condition*). Menganalisis kecelakaan secara sistemik berarti menggunakan *active failure* sebagai titik awal untuk melacak kembali dan mengungkap jaringan kondisi laten yang berkontribusi.

**Analogi/Contoh Kasus:** Bayangkan tragedi Titanic. Kegagalan aktif (*active failure*) adalah tindakan para pengintai yang gagal melihat gunung es tepat waktu dan keputusan di anjungan untuk berbelok terlalu lambat. Namun, bencana ini tidak mungkin terjadi tanpa serangkaian kondisi laten (*latent conditions*) yang telah ditetapkan jauh sebelumnya. Ini termasuk: keputusan desain untuk menggunakan paku keling berkualitas rendah di beberapa bagian lambung; kebijakan perusahaan pelayaran yang memprioritaskan kemewahan di atas keselamatan dengan tidak menyediakan sekoci yang cukup; keyakinan yang arogan dari para pembuatnya bahwa kapal itu “tidak dapat tenggelam”, yang mengurangi kewaspadaan; dan praktik industri pada saat itu yang tidak mewajibkan penggunaan teropong bagi pengintai. Kegagalan para kru di malam itu adalah percikan api, tetapi tumpukan kayu bakar untuk bencana besar telah dikumpulkan selama bertahun-tahun oleh keputusan-keputusan di “ujung tumpul”.

## 1. **Identifikasi dan Dampak Kondisi Laten (Misalnya, Desain Buruk, Budaya Lemah)**

Mengidentifikasi kondisi laten adalah tugas inti dari investigasi dan audit keselamatan sistemik, namun ini merupakan tantangan karena sifatnya yang tersembunyi. Tidak seperti kegagalan aktif yang biasanya jelas dan dapat diamati, kondisi laten tertanam dalam struktur, proses, dan budaya organisasi. Mereka sering kali tampak "normal" bagi orang-orang yang bekerja di dalam sistem setiap hari, dan keberadaan mereka sebagai faktor risiko mungkin tidak disadari sampai setelah sebuah kegagalan terjadi.

Ada beberapa kategori umum di mana kondisi laten sering ditemukan, dan menggunakan kategori ini sebagai daftar periksa dapat membantu dalam proses identifikasi:

### a. **Desain dan Rekayasa**

Ini mencakup kelemahan dalam desain peralatan, teknologi, dan lingkungan kerja fisik. Contohnya termasuk antarmuka manusia-mesin yang tidak intuitif, kurangnya fitur *fail-safe*, tata letak pabrik yang tidak efisien atau berbahaya, dan peralatan yang sulit untuk dirawat.

### b. **Prosedur dan Dokumentasi**

Prosedur yang tidak akurat, tidak jelas, tidak lengkap, atau tidak tersedia adalah sumber kondisi laten yang sangat umum. Jika prosedur tidak mencerminkan *work-as-done*, mereka tidak akan diikuti dan tidak dapat berfungsi sebagai pertahanan yang efektif.

### c. **Pelatihan dan Kompetensi**

Pelatihan yang tidak memadai, tidak relevan, atau hanya berfokus pada kepatuhan daripada pemahaman dapat membuat pekerja tidak siap menghadapi situasi abnormal. Sistem untuk menilai dan memelihara kompetensi yang lemah juga merupakan kondisi laten yang signifikan.

### d. **Manajemen dan Pengawasan**

Ini adalah kategori yang luas yang mencakup keputusan dan praktik manajerial. Contohnya termasuk pengawasan yang tidak memadai, perencanaan kerja yang buruk, alokasi sumber daya yang tidak cukup,

dan kegagalan untuk menindaklanjuti masalah keselamatan yang dilaporkan sebelumnya.

e. **Komunikasi**

Hambatan komunikasi antar departemen, antar shift, atau antara manajemen dan pekerja dapat menyebabkan informasi penting hilang atau disalahartikan, menciptakan kondisi untuk kesalahpahaman dan kesalahan.

f. **Budaya Organisasi**

Ini adalah sumber kondisi laten yang paling kuat namun paling sulit diubah. Budaya yang memprioritaskan produksi di atas keselamatan, *blame culture*, atau budaya yang menoleransi pelanggaran menciptakan lingkungan di mana perilaku berisiko menjadi norma.

Dampak dari kondisi laten adalah menciptakan jebakan psikologis dan situasional bagi orang-orang di lini depan. Mereka secara bertahap mengikis pertahanan sistem dan mengurangi margin untuk kesalahan. Mereka menciptakan lingkungan kerja di mana kesalahan menjadi lebih mungkin terjadi dan lebih mungkin memiliki konsekuensi yang parah. Seorang pekerja mungkin dapat mengatasi satu atau dua kondisi laten (misalnya, prosedur yang buruk dan alat yang kurang ideal) melalui keahlian dan upaya ekstra. Namun, ketika beberapa kondisi laten menumpuk, beban kognitif menjadi terlalu besar, dan kemungkinan kegagalan aktif meningkat secara eksponensial.

Karena kondisi laten dapat tetap tidak aktif untuk waktu yang lama, organisasi dapat mengembangkan rasa aman yang palsu. Semuanya tampak berjalan lancar, dan tidak ada insiden besar yang terjadi. Namun, di bawah permukaan, "patogen" organisasi ini terus berkembang biak. Oleh karena itu, organisasi yang memiliki keandalan tinggi (*High Reliability Organizations*) tidak pernah puas dengan ketiadaan kecelakaan. Sebaliknya, mereka secara obsesif dan proaktif "berburu" kondisi laten melalui audit yang mendalam, observasi kerja, dan yang terpenting, dengan menciptakan budaya di mana pekerja di lini depan merasa aman untuk melaporkan "gejala" sistemik ini, frustrasi dengan prosedur, masalah dengan peralatan,

atau tekanan yang mereka rasakan, sebelum mereka berkontribusi pada kegagalan.

## 2. **Active Failures sebagai Pemicu Langsung Kecelakaan**

Jika kondisi laten adalah penyebab yang mendasari (*root causes*), maka kegagalan aktif (*active failures*) adalah penyebab langsung (*proximal causes*) dari sebuah kecelakaan. Mereka adalah “percikan api” yang menyulut “tumpukan kayu bakar” yang telah disiapkan oleh kondisi-kondisi laten. Kegagalan aktif adalah tindakan tidak aman, baik kesalahan (*error*) maupun pelanggaran (*violation*), yang dilakukan oleh orang di lini depan, yang dampaknya langsung terasa. Tindakan inilah yang menembus lapisan pertahanan terakhir dari sistem.

Meskipun dalam pendekatan sistemik kita menekankan pentingnya melihat melampaui kegagalan aktif, bukan berarti kegagalan aktif itu tidak penting. Mereka adalah bagian yang krusial dari teka-teki kecelakaan. Menganalisis sifat dari kegagalan aktif memberikan petunjuk penting tentang jenis kondisi laten apa yang mungkin ada di dalam sistem. Sifat dari gejala dapat membantu kita mendiagnosis penyakitnya.

Misalnya, jika investigasi menemukan bahwa kegagalan aktifnya adalah sebuah *slip* (misalnya, operator memutar saklar yang salah dari deretan saklar yang identik), ini seharusnya mengarahkan kita untuk mencari kondisi laten yang terkait dengan desain antarmuka, ergonomi, dan gangguan di lingkungan kerja. Pertanyaannya menjadi: “Desain apa yang membuat *slip* ini mungkin terjadi?”.

Jika kegagalan aktifnya adalah sebuah *mistake* (misalnya, tim teknisi salah mendiagnosis masalah mesin), ini seharusnya mendorong kita untuk menyelidiki kondisi laten yang terkait dengan pelatihan, ketersediaan informasi, dan kompleksitas tugas. Pertanyaannya menjadi: “Mengapa situasi ini begitu sulit untuk didiagnosis dengan benar? Apakah pelatihan mereka memadai? Apakah mereka memiliki data yang mereka butuhkan?”.

Dan jika kegagalan aktifnya adalah sebuah pelanggaran rutin (misalnya, kru secara teratur tidak memakai APD di area tertentu), ini adalah sinyal kuat untuk memeriksa kondisi laten yang terkait dengan kepraktisan prosedur,

pengawasan, dan budaya keselamatan. Pertanyaannya menjadi: "Apa yang membuat aturan ini begitu sulit atau tidak praktis untuk diikuti? Pesan apa yang dikirim manajemen tentang pentingnya aturan ini?".

Kegagalan aktif sering kali merupakan tindakan yang dilakukan oleh orang-orang yang bermaksud baik yang mencoba melakukan pekerjaan mereka dalam sistem yang cacat. Mereka adalah pewaris dari sistem yang dirancang oleh orang lain. Namun, penting juga untuk mengakui bahwa dalam beberapa kasus, kegagalan aktif dapat berupa pelanggaran sembrono atau sabotase. Dalam kasus-kasus ini, meskipun analisis sistemik masih relevan untuk memahami bagaimana sistem memungkinkan tindakan semacam itu terjadi, fokus pada akuntabilitas individu menjadi lebih menonjol.

Tantangan utama dalam investigasi adalah menolak godaan untuk berhenti pada kegagalan aktif. Sangat mudah bagi investigator untuk menemukan kesalahan operator dan menyimpulkan bahwa itulah penyebabnya. Ini adalah jalan keluar yang cepat dan sederhana yang menghindari pertanyaan-pertanyaan yang lebih sulit tentang tanggung jawab manajerial dan organisasi. Investigator yang terlatih secara sistemik akan selalu menggunakan identifikasi kegagalan aktif bukan sebagai titik akhir dari analisis mereka, tetapi sebagai titik awal. Mereka akan selalu bertanya, "Kesalahan ini terjadi, tetapi *mengapa* kesalahan ini masuk akal atau mungkin terjadi dalam konteks ini?".

### **3. Jendela Kecelakaan (Window of Accident Opportunity)**

Konsep "jendela peluang kecelakaan" (*window of accident opportunity*) adalah cara yang kuat untuk memvisualisasikan bagaimana kondisi laten dan kegagalan aktif berinteraksi untuk menyebabkan bencana. Bayangkan bahwa pertahanan sistem K3 kita adalah serangkaian dinding atau penghalang. Kondisi laten seperti lubang-lubang kecil yang terus-menerus dibuat di dinding-dinding ini oleh keputusan-keputusan organisasi. Dalam operasi normal, lubang-lubang ini tidak sejajar, sehingga tidak ada jalur lurus menuju kegagalan. Sistem tetap aman, meskipun pertahanannya telah melemah.

Kecelakaan terjadi pada saat yang kritis ketika, karena kombinasi keadaan, lubang-lubang di berbagai lapisan pertahanan ini secara sesaat sejajar. Kesejajaran ini menciptakan “jendela peluang”, sebuah lintasan lurus dan tanpa hambatan bagi bahaya untuk merambat melalui sistem dan menyebabkan kerugian. Kegagalan aktif sering kali merupakan peristiwa pemicu yang membuka jendela ini atau merupakan tindakan terakhir yang melewati jendela yang sudah terbuka.

Jendela ini tidak terbuka untuk waktu yang lama. Sering kali, itu adalah momen singkat di mana serangkaian faktor negatif bertemu secara bersamaan. Faktor-faktor ini bisa berupa kombinasi dari:

- a. Kegagalan teknis (misalnya, pompa cadangan gagal启动)
- b. Kondisi lingkungan yang tidak biasa (misalnya, badai yang tak terduga)
- c. Tekanan operasional (misalnya, kru bekerja di bawah tenggat waktu yang ketat)
- d. Kegagalan manusia (*active failure*)

Misalnya, seorang pilot mungkin membuat kesalahan kecil (*active failure*). Dalam 99% kasus, kesalahan ini akan ditangkap oleh kopilot, oleh sistem peringatan otomatis, atau oleh pengawas lalu lintas udara (lapisan pertahanan). Namun, pada hari yang naas itu, “jendela kecelakaan” terbuka: kopilot juga terganggu, sistem peringatan kebetulan sedang dalam perawatan (*latent condition*), dan pengawas lalu lintas udara sedang menangani terlalu banyak pesawat sekaligus (*latent condition*). Kesejajaran sesaat dari lubang-lubang ini memungkinkan kesalahan awal pilot untuk berkembang menjadi kecelakaan.

Konsep ini memiliki implikasi penting untuk manajemen risiko. Pertama, ini menjelaskan mengapa kecelakaan besar sering kali tampak “aneh” atau “tidak mungkin terjadi”. Mereka adalah hasil dari konjungsi peristiwa yang sangat tidak mungkin, yang masing-masing mungkin tidak berbahaya jika terjadi sendiri-sendiri.

Kedua, ini menekankan bahwa keselamatan bukanlah keadaan statis, melainkan dinamis. Margin keselamatan organisasi terus berfluktuasi seiring dengan bertambah atau berkurangnya jumlah kondisi laten. Tugas manajemen K3 yang proaktif adalah untuk terus-menerus mencoba

“menutup lubang” (memperbaiki kondisi laten) untuk membuat kesejajaran yang berbahaya menjadi semakin tidak mungkin terjadi.

Ketiga, ini menyoroti pentingnya resiliensi. Karena kita tidak akan pernah bisa menghilangkan semua kondisi laten, kita perlu membangun sistem yang dapat mengenali ketika “jendela kecelakaan” mulai terbuka dan dapat mengambil tindakan untuk menutupnya kembali dengan cepat. Ini melibatkan kemampuan untuk memantau tanda-tanda peringatan dini, beradaptasi dengan kejutan, dan belajar dari peristiwa kecil sebelum mereka bergabung menjadi peristiwa besar. Organisasi yang aman bukanlah organisasi yang tidak pernah memiliki lubang dalam pertahanannya, tetapi organisasi yang sangat pandai dalam mendeteksi dan menambalnya.

### **C. Konsep Pertahanan Berlapis (*Defenses in Depth*)**

Jika kondisi laten secara konstan menciptakan kelemahan dalam sistem kita, bagaimana kita bisa mencapai tingkat keselamatan yang tinggi? Jawabannya terletak pada salah satu prinsip paling fundamental dari rekayasa keselamatan: pertahanan berlapis, atau *defenses in depth*. Filosofi di balik konsep ini adalah pengakuan yang rendah hati bahwa tidak ada satu pun lapisan pertahanan yang sempurna. Setiap penghalang, baik itu teknologi, prosedur, atau manusia, memiliki kelemahan yang tidak terduga atau dapat gagal dalam keadaan tertentu. Oleh karena itu, kita tidak dapat mengandalkan satu “dinding ajaib” untuk melindungi kita.

Sebaliknya, keselamatan dan keandalan yang tinggi dicapai dengan menciptakan sistem pertahanan yang berlapis, beragam, dan tumpang tindih. Idennya adalah bahwa bahkan jika satu lapisan pertahanan gagal (dan kita harus berasumsi bahwa itu akan terjadi suatu saat), lapisan-lapisan berikutnya akan siap untuk menangkap dan menahan perkembangan kegagalan tersebut. Sangat tidak mungkin (meskipun bukan tidak mungkin) bagi semua lapisan pertahanan untuk gagal secara bersamaan. Setiap lapisan tambahan secara eksponensial mengurangi probabilitas keseluruhan dari hasil yang katastrofik.

Konsep ini berasal dari desain reaktor nuklir, di mana beberapa sistem pendingin independen, gedung penahanan (*containment building*), dan

prosedur pemadaman darurat menciptakan serangkaian penghalang yang tangguh terhadap pelepasan radiasi. Namun, prinsip ini dapat diterapkan pada sistem kerja apa pun. Di sebuah lokasi konstruksi, pertahanan terhadap jatuh dari ketinggian mungkin mencakup pagar pengaman (rekayasa), sistem penahan jatuh pribadi/harness (APD), prosedur izin kerja di ketinggian (administratif), dan pelatihan pekerja (manusia). Tidak ada satu pun dari ini yang sempurna, tetapi kombinasinya menciptakan sistem yang jauh lebih aman.

Efektivitas dari strategi pertahanan berlapis tidak hanya bergantung pada jumlah lapisan, tetapi juga pada keragaman dan independensi mereka. Jika semua lapisan pertahanan kita adalah jenis yang sama (misalnya, beberapa prosedur yang ditulis oleh orang yang sama), mereka mungkin rentan terhadap mode kegagalan yang sama (misalnya, asumsi yang salah yang dibuat oleh penulis prosedur). Oleh karena itu, penting untuk memiliki campuran pertahanan yang beragam, menggabungkan penghalang keras (rekayasa), penghalang lunak (prosedur), dan penghalang manusiawi.

Demikian pula, lapisan-lapisan tersebut harus sedapat mungkin independen. Artinya, kegagalan satu lapisan seharusnya tidak menyebabkan kegagalan lapisan berikutnya. Jika sistem alarm dan sistem pemadaman darurat ditenagai oleh sumber listrik yang sama, maka kegagalan daya tunggal dapat melumpuhkan kedua lapisan pertahanan secara bersamaan, mengalahkan tujuan dari pertahanan berlapis.

Analisis sistemik sering kali melibatkan pemetaan pertahanan yang ada (atau yang seharusnya ada) untuk tugas atau proses tertentu. Tujuannya adalah untuk mengidentifikasi di mana pertahanan itu lemah, di mana ada celah, atau di mana ada ketergantungan yang berlebihan pada satu jenis pertahanan saja (biasanya pada manusia dan prosedur).

**Analogi/Contoh Kasus:** Konsep pertahanan berlapis dapat dianalogikan dengan keamanan siber. Untuk melindungi data sensitif, sebuah perusahaan tidak hanya mengandalkan satu kata sandi (*password*) yang kuat. Mereka menggunakan pendekatan berlapis: ada firewall untuk memblokir lalu lintas yang tidak sah (pertahanan perbatasan), enkripsi data sehingga tidak dapat dibaca jika dicuri (pertahanan data), autentikasi multi-

faktor yang memerlukan kode dari telepon pengguna (pertahanan akses), dan pelatihan karyawan untuk mengenali email *phishing* (pertahanan manusiawi). Setiap lapisan dapat ditembus, tetapi seorang peretas harus berhasil menembus *semua* lapisan ini untuk mencapai tujuannya. Semakin banyak dan beragam lapisannya, semakin aman sistemnya.

### 1. Klasifikasi Jenis Pertahanan (Teknis, Prosedural, Manusiawi)

Untuk merancang sistem pertahanan berlapis yang efektif, penting untuk memahami berbagai jenis pertahanan yang tersedia. Secara umum, pertahanan K3 dapat diklasifikasikan ke dalam tiga kategori utama: pertahanan teknis (atau rekayasa), pertahanan prosedural (atau administratif), dan pertahanan manusiawi. Sistem yang paling tangguh menggunakan kombinasi yang seimbang dari ketiganya, sesuai dengan prinsip hierarki kontrol.

- a. Pertahanan Teknis (Rekayasa): Ini sering dianggap sebagai jenis pertahanan yang paling kuat dan andal karena mereka berfungsi secara independen dari perilaku manusia. Mereka "dirancang ke dalam" sistem fisik. Pertahanan teknis bekerja dengan menghilangkan bahaya atau menciptakan penghalang fisik antara bahaya dan manusia. Contohnya meliputi:
  - 1) Pelindung mesin (Machine guarding)  
Penghalang fisik yang mencegah kontak dengan bagian mesin yang bergerak.
  - 2) Interlocks  
Sakelar pengaman yang secara otomatis mematikan mesin jika pelindung dibuka atau jika seseorang memasuki zona berbahaya.
  - 3) Sistem ventilasi  
Menghilangkan kontaminan berbahaya dari udara di sumbernya.
  - 4) Sistem pemadaman kebakaran otomatis  
Mendeteksi dan memadamkan api tanpa intervensi manusia.

5) Desain ergonomis

Merancang alat dan stasiun kerja untuk mengurangi ketegangan fisik. Pertahanan teknis berada di puncak hierarki kontrol dan harus selalu menjadi pilihan pertama jika memungkinkan.

b. Pertahanan Prosedural (Administratif): Pertahanan ini bergantung pada orang-orang yang mengikuti aturan, prosedur, dan proses yang telah ditetapkan. Mereka lebih lemah daripada pertahanan teknis karena mereka bergantung pada kepatuhan manusia, yang kita tahu bervariasi. Namun, mereka adalah bagian yang penting dan tak terhindarkan dari setiap sistem keselamatan. Contohnya meliputi:

1) Prosedur Operasi Standar (SOP)

Petunjuk langkah-demi-langkah tentang cara melakukan tugas dengan aman.

2) Izin Kerja (Permit-to-Work)

Sistem formal untuk mengotorisasi dan mengendalikan pekerjaan berisiko tinggi seperti pekerjaan panas atau masuk ke ruang terbatas.

3) Checklists

Alat bantu untuk memastikan semua langkah kritis telah diselesaikan.

4) Jadwal Inspeksi dan Pemeliharaan

Proses untuk memastikan peralatan tetap dalam kondisi aman.

5) Papan Tanda dan Label Peringatan

Efektivitas pertahanan prosedural sangat bergantung pada kualitas desainnya (kejelasan, kepraktisan) dan budaya organisasi.

c. Pertahanan Manusiawi: Ini adalah lapisan pertahanan terakhir dan sering kali yang paling fleksibel, tetapi juga yang paling tidak dapat diandalkan. Pertahanan ini sepenuhnya bergantung pada keterampilan, pengetahuan, dan kewaspadaan individu dan tim untuk mendeteksi dan merespons kondisi yang tidak aman. Contohnya meliputi:

- 1) Pelatihan dan kompetensi  
Memastikan orang memiliki pengetahuan untuk mengenali dan menangani bahaya.
- 2) Pengawasan  
Penyelia memantau pekerjaan untuk memastikan kepatuhan dan mengidentifikasi masalah.
- 3) Crew Resource Management (CRM)  
Tim yang saling memeriksa silang pekerjaan satu sama lain dan berkomunikasi secara efektif untuk menangkap kesalahan.
- 4) Kesadaran situasi (Situation awareness)  
Kemampuan seorang individu untuk memahami apa yang terjadi di sekitar mereka dan memproyeksikan status masa depan. Meskipun penting, ketergantungan yang berlebihan pada pertahanan manusiawi adalah tanda dari sistem yang rapuh, karena menempatkan beban pencegahan kecelakaan pada pundak orang-orang di lini depan.

Sistem yang matang akan mencoba untuk melapisi ketiga jenis pertahanan ini. Misalnya, untuk melindungi dari tumpahan bahan kimia, mungkin ada sistem penahanan sekunder (teknis), prosedur penanganan yang aman (prosedural), dan pelatihan tanggap tumpahan (manusiawi). Menganalisis keseimbangan pertahanan ini dapat mengungkapkan area di mana organisasi terlalu bergantung pada pertahanan yang lebih lemah (prosedural dan manusiawi) dan perlu berinvestasi lebih banyak pada pertahanan teknis yang lebih kuat.

## 2. Kegagalan Ganda (Multiple Defense Failures)

Prinsip dasar dari pertahanan berlapis adalah bahwa satu kegagalan tunggal seharusnya tidak cukup untuk menyebabkan kecelakaan. Bencana besar, hampir tanpa kecuali, adalah hasil dari kegagalan ganda, serangkaian kegagalan yang terjadi di beberapa lapisan pertahanan. Analisis kecelakaan modern sering kali berfokus pada pemahaman bagaimana dan mengapa beberapa lapisan pertahanan gagal secara berurutan atau bersamaan.

Ada dua mode utama di mana kegagalan ganda dapat terjadi: kegagalan independen dan kegagalan mode bersama.

- a. Kegagalan Independen (*Independent Failures*) terjadi ketika beberapa lapisan pertahanan gagal karena alasan yang tidak saling berhubungan. Ini adalah serangkaian “nasib buruk” yang tidak terduga, di mana kelemahan-kelemahan yang berbeda di berbagai bagian sistem secara kebetulan bertemu pada satu titik waktu. Model Keju Swiss James Reason adalah representasi klasik dari kegagalan independen, di mana “lubang” (kelemahan) yang dibuat oleh kondisi laten yang berbeda secara acak sejajar, menciptakan jalur menuju kecelakaan (Reason, 1990). Meskipun setiap kegagalan bersifat independen, analisis sistemik berusaha memahami kondisi laten yang menciptakan lubang-lubang tersebut di tempat pertama.
- b. Kegagalan Mode Bersama (*Common Mode Failures*) adalah skenario yang sering kali lebih berbahaya dan lebih sulit diantisipasi. Ini terjadi ketika satu peristiwa atau penyebab tunggal menyebabkan kegagalan beberapa lapisan pertahanan secara bersamaan. Ini secara efektif meniadakan manfaat dari pertahanan berlapis karena lapisan-lapisan tersebut ternyata tidak independen satu sama lain. Mengidentifikasi dan menghilangkan potensi kegagalan mode bersama adalah prioritas utama dalam rekayasa keandalan.

Contoh kegagalan mode bersama meliputi:

1) Kegagalan Utilitas

Kehilangan daya listrik dapat secara bersamaan melumpuhkan sistem kontrol utama, sistem pendingin cadangan, dan sistem pencahayaan darurat jika semuanya bergantung pada sumber daya yang sama tanpa cadangan yang memadai.

2) Kesalahan Perawatan

Seorang teknisi yang kurang terlatih mungkin melakukan kesalahan yang sama pada sistem utama dan sistem cadangannya selama perawatan rutin, membuat keduanya tidak dapat dioperasikan.

### 3) Lingkungan Ekstrem

Kebakaran, banjir, atau gempa bumi dapat merusak beberapa sistem keselamatan yang berlokasi di area yang sama.

### 4) Kesalahan Desain

Asumsi yang salah yang dibuat oleh seorang insinyur dapat dimasukkan ke dalam beberapa sistem, membuatnya rentan terhadap kegagalan dalam kondisi operasi yang sama.

### 5) Kesalahan Manusia Tunggal

Dalam beberapa kasus, satu kesalahan manusia dapat menembus beberapa lapisan pertahanan. Misalnya, seorang operator yang salah menafsirkan alarm mungkin secara keliru menonaktifkan sistem keselamatan otomatis, secara efektif menghilangkan dua lapisan pertahanan dengan satu tindakan.

Mencegah kegagalan ganda memerlukan pendekatan dua cabang. Untuk kegagalan independen, tujuannya adalah untuk mengurangi jumlah kelemahan (lubang) secara keseluruhan di setiap lapisan pertahanan. Ini dilakukan dengan secara proaktif mencari dan memperbaiki kondisi-kondisi laten melalui audit, inspeksi, dan pelaporan. Semakin sedikit lubang, semakin kecil kemungkinan mereka akan sejajar.

Untuk kegagalan mode bersama, tujuannya adalah untuk memastikan keragaman dan independensi antar lapisan pertahanan. Ini melibatkan analisis yang cermat terhadap ketergantungan tersembunyi. Apakah sistem yang berbeda berbagi sumber daya? Apakah mereka dirancang oleh tim yang sama? Apakah mereka rentan terhadap peristiwa eksternal yang sama? Dengan mengidentifikasi ketergantungan ini, kita dapat merancang sistem yang lebih tangguh, misalnya dengan menyediakan sumber daya yang benar-benar independen atau menggunakan teknologi yang berbeda untuk sistem utama dan cadangan.

## 3. Mengoptimalkan Kualitas Setiap Lapisan Pertahanan

Memiliki banyak lapisan pertahanan tidak ada gunanya jika setiap lapisan itu sendiri lemah, penuh lubang, dan tidak dapat diandalkan. Oleh karena itu, selain menambah jumlah lapisan, sebuah organisasi harus secara

terus-menerus bekerja untuk mengoptimalkan kualitas dan efektivitas dari setiap lapisan pertahanan yang ada. Kualitas pertahanan adalah ukuran seberapa besar kemungkinan sebuah pertahanan akan berfungsi sebagaimana mestinya ketika dibutuhkan. Proses pengoptimalan ini adalah bagian inti dari siklus perbaikan berkelanjutan dalam SMK3.

Untuk pertahanan teknis, pengoptimalan melibatkan beberapa kegiatan utama. Pertama adalah desain yang kuat sejak awal, berdasarkan prinsip-prinsip *human factors* dan rekayasa keselamatan. Setelah dipasang, program pemeliharaan preventif dan prediktif yang ketat sangat penting untuk memastikan bahwa pertahanan teknis (seperti sensor atau katup pengaman) tetap dalam kondisi kerja yang prima. Pengujian rutin juga krusial untuk memverifikasi bahwa sistem keselamatan akan berfungsi dalam keadaan darurat; banyak kecelakaan terjadi karena sistem keselamatan yang ada ternyata gagal saat diuji oleh peristiwa nyata. Akhirnya, manajemen perubahan yang disiplin diperlukan untuk memastikan bahwa modifikasi pada sistem tidak secara tidak sengaja melemahkan atau menonaktifkan pertahanan yang ada.

Untuk pertahanan prosedural, pengoptimalan dimulai dengan desain prosedur yang berpusat pada pengguna. Ini berarti melibatkan pekerja di lini depan dalam penulisan dan peninjauan prosedur untuk memastikan mereka akurat, dapat dipahami, dan praktis untuk digunakan di lapangan. Prosedur harus ringkas, menggunakan bahasa yang jelas, dan memanfaatkan alat bantu visual seperti diagram dan foto. Setelah dibuat, prosedur harus mudah diakses oleh pekerja di tempat dan waktu mereka membutuhkannya. Proses peninjauan dan pembaruan berkala sangat penting untuk menjaga agar prosedur tetap relevan dengan perubahan peralatan atau proses kerja. Terakhir, kepatuhan terhadap prosedur harus dipantau melalui observasi kerja dan audit, tidak untuk menyalahkan, tetapi untuk memahami di mana prosedur tersebut gagal dan perlu diperbaiki.

Untuk pertahanan manusiawi, pengoptimalan berfokus pada peningkatan kompetensi dan dukungan keputusan. Pelatihan harus lebih dari sekadar presentasi PowerPoint; ia harus interaktif, berbasis skenario, dan memberikan kesempatan untuk praktik langsung. Penilaian kompetensi yang berkelanjutan, bukan hanya sertifikasi satu kali, memastikan bahwa

keterampilan tetap tajam. Menciptakan budaya kerja tim yang kuat, seperti prinsip-prinsip *Crew Resource Management*, mengubah individu menjadi pertahanan kolektif yang dapat saling menangkap kesalahan. Selain itu, menyediakan alat bantu keputusan dan dukungan informasi yang baik di tempat kerja dapat mengurangi beban kognitif dan membantu orang membuat pilihan yang lebih baik di bawah tekanan.

Mengoptimalkan kualitas pertahanan juga berarti memiliki sistem umpan balik yang efektif. Setiap kali sebuah insiden terjadi, sekecil apa pun, itu adalah data tentang kegagalan atau kelemahan di salah satu lapisan pertahanan kita. Demikian pula, laporan *near miss* dan kondisi tidak aman adalah informasi berharga tentang pertahanan yang hampir gagal. Organisasi harus memiliki proses yang kuat untuk menganalisis data ini dan menggunakannya untuk memperkuat lapisan pertahanan yang terbukti lemah.

Pada dasarnya, setiap lapisan pertahanan adalah sebuah produk yang membutuhkan manajemen siklus hidupnya sendiri: desain, implementasi, pemeliharaan, pemantauan, dan perbaikan. Organisasi yang aman adalah organisasi yang secara sistematis dan tanpa henti berinvestasi dalam menjaga kesehatan dan kekuatan setiap lapisan pertahanannya.

#### **D. Peran K3MS (Sistem Manajemen K3) sebagai Kerangka Sistemik**

Konsep-konsep pendekatan sistemik, sistem kerja yang kompleks, kondisi laten, kegagalan aktif, dan pertahanan berlapis, mungkin tampak abstrak. Pertanyaannya kemudian adalah: Bagaimana sebuah organisasi dapat secara sistematis dan terstruktur mengelola semua elemen ini dalam operasi sehari-harinya? Jawabannya terletak pada Sistem Manajemen Keselamatan dan Kesehatan Kerja (K3MS), seperti yang diuraikan dalam standar internasional seperti ISO 45001. K3MS menyediakan kerangka kerja operasional untuk menerapkan prinsip-prinsip sistemik dalam praktik.

Jika dipandang dengan benar, K3MS bukanlah sekadar kumpulan dokumen, prosedur, dan formulir untuk memuaskan auditor. Sebaliknya, K3MS harus dilihat sebagai "sistem saraf" atau "sistem kekebalan" organisasi

dalam hal keselamatan. Ini adalah struktur yang dirancang untuk secara konstan merasakan (mengidentifikasi bahaya), memproses (menilai risiko), merespons (mengimplementasikan kontrol), dan belajar (memantau dan meninjau) untuk menjaga kesehatan organisasi dan melindunginya dari “penyakit” kecelakaan. Ketika dijiwai dengan pemikiran sistemik, setiap elemen K3MS menjadi alat untuk mengelola interaksi kompleks dan memperkuat pertahanan.

Misalnya, klausul tentang Identifikasi Bahaya dan Penilaian Risiko dalam ISO 45001, jika dilihat melalui lensa sistemik, menuntut kita untuk mencari lebih dari sekadar bahaya fisik yang jelas. Ia mendorong kita untuk secara proaktif mengidentifikasi kondisi-kondisi laten: Apakah prosedur kita membingungkan? Apakah ada tekanan produksi yang berlebihan? Apakah desain antarmuka kita rawan kesalahan? Penilaian risiko kemudian mengevaluasi bagaimana kondisi-kondisi laten ini dapat berinteraksi dengan pemicu untuk menyebabkan kegagalan.

Elemen Kompetensi dan Pelatihan menjadi lebih dari sekadar mencatat kehadiran. Ia menjadi tentang memastikan bahwa orang tidak hanya tahu aturannya, tetapi juga memahami alasan di baliknya dan memiliki keterampilan non-teknis (seperti komunikasi dan kerja tim) untuk berfungsi sebagai pertahanan manusiawi yang efektif. Elemen Investigasi Insiden diubah dari pencarian kesalahan menjadi analisis sistemik yang mendalam, yang bertujuan untuk mengungkap dan memperbaiki kondisi laten.

Siklus Plan-Do-Check-Act (PDCA) yang menjadi inti dari ISO 45001 adalah mesin untuk perbaikan berkelanjutan dari pertahanan sistem kita. Dalam fase *Plan*, kita mengidentifikasi kelemahan dalam pertahanan kita. Dalam fase *Do*, kita mengimplementasikan perbaikan (misalnya, merancang ulang prosedur atau meningkatkan pelindung mesin). Dalam fase *Check*, kita memantau dan mengukur efektivitas perbaikan tersebut. Dan dalam fase *Act*, kita mengambil tindakan untuk menstandarisasi perbaikan atau memulai siklus baru.

Dengan demikian, K3MS bukanlah sesuatu yang terpisah dari pendekatan sistemik; itu adalah wahana untuk melaksanakannya. Tanpa K3MS, upaya sistemik bisa menjadi tidak terstruktur dan sporadis. Tanpa

pemikiran sistemik, K3MS berisiko menjadi birokrasi yang kosong dan tidak efektif. Kombinasi keduanya, sebuah K3MS yang dirancang dan diimplementasikan dengan pemahaman mendalam tentang prinsip-prinsip sistemik, adalah resep untuk manajemen K3 yang matang, proaktif, dan berkelanjutan.

**Analogi/Contoh Kasus:** Bayangkan membangun dan memelihara sebuah mobil balap berperforma tinggi (organisasi yang aman). Prinsip-prinsip sistemik adalah hukum-hukum fisika dan aerodinamika yang harus dipahami oleh para insinyur untuk merancang mobil yang cepat dan stabil. K3MS adalah rencana pemeliharaan dan buku manual operasional untuk mobil tersebut. Buku manual ini, jika ditulis dengan baik, akan didasarkan pada pemahaman mendalam tentang aerodinamika dan fisika. Ini akan menentukan jadwal inspeksi rutin untuk mencari retakan mikro pada sasis (kondisi laten), prosedur untuk memeriksa semua sistem sebelum balapan (memverifikasi pertahanan), dan proses untuk menganalisis data telemetri setelah setiap balapan untuk belajar dan meningkatkan performa (pemantauan dan peninjauan). Anda tidak dapat memiliki mobil yang andal hanya dengan memahami teori (prinsip sistemik) atau hanya dengan mengikuti manual secara buta (K3MS). Anda membutuhkan keduanya: manual yang hebat yang didasarkan pada teori yang solid.

### 1. K3MS sebagai Struktur untuk Mengelola Risiko Human Error

Sebuah Sistem Manajemen K3 (K3MS) yang efektif menyediakan struktur formal yang diperlukan untuk beralih dari sekadar berbicara tentang *human error* menjadi secara aktif mengelolanya. Alih-alih mengandalkan upaya heroik dari individu atau inisiatif keselamatan yang terfragmentasi, K3MS mengintegrasikan pengelolaan risiko *human error* ke dalam proses bisnis sehari-hari. Ia mengubah niat baik menjadi tindakan yang sistematis dan dapat diaudit.

Dalam elemen Perencanaan K3MS (misalnya, klausul 6 ISO 45001), organisasi diwajibkan untuk mengidentifikasi bahaya dan menilai risiko. Ketika diinformasikan oleh pendekatan sistemik, proses ini secara eksplisit akan mencakup identifikasi potensi human error dan Performance Shaping Factors (PSFs) yang memengaruhinya. Teknik-teknik seperti Task Analysis (Analisis Tugas) dan Human Reliability Assessment (HRA), yang akan dibahas

di Bagian III, dapat diintegrasikan ke dalam proses ini. Tujuannya adalah untuk secara proaktif mengidentifikasi di mana letak “jebakan kesalahan” dalam tugas-tugas kritis dan menilai kekuatan pertahanan yang ada untuk menangkap kesalahan tersebut.

Dalam elemen Dukungan dan Operasi (misalnya, klausul 7 & 8 ISO 45001), K3MS menyediakan mekanisme untuk menerapkan kontrol yang menargetkan human error. Ini termasuk:

a. Sumber Daya

Memastikan alokasi anggaran dan staf yang cukup untuk hal-hal yang mengurangi kesalahan, seperti perbaikan ergonomis atau pelatihan berkualitas tinggi.

b. Kompetensi

Menetapkan proses untuk memastikan bahwa pekerja tidak hanya dilatih, tetapi benar-benar kompeten untuk melakukan tugas mereka dengan aman, termasuk keterampilan non-teknis.

c. Komunikasi

Menetapkan saluran formal untuk mengkomunikasikan informasi K3, termasuk pelajaran dari insiden, perubahan prosedur, dan risiko baru.

d. Kontrol Operasional

Mengembangkan dan menerapkan prosedur dan instruksi kerja yang dirancang dengan prinsip-prinsip human-centred design untuk membuatnya jelas, ringkas, dan mudah digunakan.

Elemen Evaluasi Kinerja (misalnya, klausul 9 ISO 45001) adalah tempat K3MS memungkinkan organisasi untuk memantau seberapa baik mereka mengelola risiko *human error*. Ini melampaui sekadar melacak angka kecelakaan (*lagging indicators*). Sebaliknya, ini melibatkan pengembangan dan pemantauan indikator utama (*leading indicators*) yang mengukur kesehatan pertahanan sistem. Contohnya termasuk persentase prosedur kritis yang telah ditinjau dari perspektif *human factors*, jumlah laporan *near miss* yang diterima dan ditindaklanjuti, atau hasil audit ergonomi.

Akhirnya, elemen Peningkatan (misalnya, klausul 10 ISO 45001), terutama melalui proses investigasi insiden dan tindakan korektif,

menyediakan putaran umpan balik (*feedback loop*) yang penting. Ketika sebuah insiden yang melibatkan *human error* terjadi, K3MS menuntut adanya investigasi yang sistematis. Jika dilakukan dengan benar, investigasi ini akan mengungkap kondisi laten dan PSFs yang berkontribusi. Tindakan korektif yang dihasilkan kemudian akan menargetkan perbaikan pada sistem (misalnya, merancang ulang antarmuka, merevisi prosedur), bukan hanya pada individu.

Dengan cara ini, K3MS menciptakan siklus yang berkelanjutan: risiko *human error* diidentifikasi dalam perencanaan, kontrol diterapkan dalam operasi, efektivitas kontrol dipantau dalam evaluasi, dan setiap kegagalan digunakan sebagai peluang untuk belajar dan meningkatkan sistem. Ia menyediakan struktur, disiplin, dan akuntabilitas untuk memastikan bahwa pengelolaan *human error* adalah proses yang berkelanjutan, bukan reaksi sesaat setelah kecelakaan.

## 2. Integrasi Human Factors ke dalam Siklus PDCA K3MS

Siklus Plan-Do-Check-Act (PDCA) adalah mesin pendorong di balik standar sistem manajemen seperti ISO 45001. Untuk mengelola *human error* secara efektif, prinsip-prinsip *Human Factors* dan Ergonomi (HFE) harus diintegrasikan secara sadar ke dalam setiap tahap siklus ini. Melakukan hal ini mengubah K3MS dari kerangka kerja umum menjadi alat yang ditargetkan secara khusus untuk mengoptimalkan interaksi manusia-sistem.

### a. PLAN (Merencanakan)

Pada tahap ini, HFE diintegrasikan ke dalam proses identifikasi bahaya dan penilaian risiko. Ini berarti:

- 1) Melakukan analisis tugas (task analysis) untuk memahami tuntutan fisik dan kognitif dari pekerjaan.
- 2) Mengidentifikasi potensi mode kegagalan manusia (*slips, lapses, mistakes, violations*) untuk setiap langkah tugas kritis.
- 3) Mengevaluasi Performance Shaping Factors (PSFs) yang ada di lingkungan kerja.
- 4) Menggunakan wawasan ini untuk menetapkan tujuan dan sasaran K3 yang secara spesifik menargetkan pengurangan risiko

*human error*, seperti “mengurangi beban kerja kognitif di ruang kontrol sebesar 15%” atau “merancang ulang prosedur X untuk mengurangi waktu penyelesaian dan kemungkinan kesalahan”.

b. **DO (Melakukan)**

Pada tahap implementasi, HFE memandu desain dan penerapan kontrol. Ini berarti:

- 1) Menerapkan prinsip desain yang berpusat pada manusia (*human-centred design*) dalam pengadaan peralatan baru, pengembangan perangkat lunak, atau perancangan ulang stasiun kerja.
- 2) Melibatkan pengguna akhir secara aktif dalam penulisan dan validasi prosedur untuk memastikan kepraktisannya.
- 3) Mengembangkan program pelatihan yang tidak hanya mencakup pengetahuan teknis, tetapi juga keterampilan non-teknis seperti kesadaran situasi, pengambilan keputusan, dan kerja tim.
- 4) Mengimplementasikan solusi ergonomis untuk mengurangi ketegangan fisik dan kelelahan.

c. **CHECK (Memeriksa)**

Pada tahap pemantauan dan evaluasi, HFE memberikan metrik untuk mengukur kinerja. Ini berarti:

- 1) Mengembangkan dan melacak *leading indicators* yang terkait dengan HFE, seperti kualitas prosedur, tingkat kelelahan yang dilaporkan, atau hasil survei iklim keselamatan.
- 2) Melakukan audit dan inspeksi yang secara khusus mencari kondisi laten dan PSFs yang buruk (misalnya, pencahayaan yang tidak memadai, alarm palsu yang berlebihan).
- 3) Menganalisis data insiden dan *near miss* menggunakan alat analisis *human factors* (seperti HFACS) untuk mengidentifikasi pola kegagalan sistemik.
- 4) Mengumpulkan umpan balik kualitatif dari pekerja tentang frustrasi, kesulitan, dan tantangan dalam pekerjaan mereka.

d. **ACT (Bertindak)**

Pada tahap ini, temuan dari fase *Check* digunakan untuk mendorong perbaikan. Ini berarti:

- 1) Hasil investigasi insiden yang berfokus pada HFE mengarah pada tindakan korektif yang menargetkan perbaikan sistem, bukan menyalahkan individu.
- 2) Hasil audit HFE digunakan sebagai masukan untuk tinjauan manajemen, yang mengarah pada alokasi sumber daya untuk proyek-proyek perbaikan sistemik.
- 3) Pelajaran yang didapat digunakan untuk memperbarui penilaian risiko dan memulai kembali siklus PDCA dengan pemahaman yang lebih baik tentang risiko *human error* di organisasi.

Dengan menanamkan HFE ke dalam setiap tahap PDCA, sebuah organisasi memastikan bahwa “manusia” selalu menjadi pertimbangan inti dalam sistem manajemennya. Ini adalah cara paling sistematis untuk beralih dari sekadar bereaksi terhadap *human error* menjadi secara proaktif merancang sistem di mana orang-orang dapat berhasil.

### 3. Mengukur Kinerja Sistem, Bukan Hanya Kinerja Individu

Salah satu pergeseran paling signifikan yang dituntut oleh pendekatan sistemik adalah perubahan dalam cara kita mengukur kinerja keselamatan. Secara tradisional, metrik K3 didominasi oleh indikator akibat (*lagging indicators*) yang berfokus pada kegagalan individu atau hasil negatif. Metrik seperti *Lost Time Injury Rate* (LTIR), *Total Recordable Incident Rate* (TRIR), atau jumlah pelanggaran K3 yang tercatat, semuanya melihat ke belakang pada kegagalan yang sudah terjadi. Meskipun berguna untuk pelacakan tren, ketergantungan yang berlebihan pada metrik ini memiliki beberapa kelemahan serius.

Pertama, mereka reaktif; mereka memberitahu kita bahwa kita memiliki masalah setelah kerugian terjadi. Kedua, angka nol kecelakaan bisa menciptakan ilusi keselamatan yang berbahaya, karena mungkin hanya mencerminkan keberuntungan, bukan kehadiran sistem yang kuat. Ketiga, dan yang paling penting, mereka cenderung memperkuat *Person-Model*

dengan berfokus pada jumlah kegagalan individu, bukan pada kesehatan sistem secara keseluruhan.

K3MS yang diinformasikan oleh pemikiran sistemik akan melengkap (bukan mengganti sepenuhnya) *lagging indicators* ini dengan serangkaian indikator utama (*leading indicators*) yang proaktif. *Leading indicators* adalah pengukuran yang memantau kekuatan dan kesehatan pertahanan sistem kita. Mereka mencoba untuk mengukur kehadiran kapasitas positif dan proses yang andal, bukan hanya ketiadaan hasil negatif. Mereka mengukur kinerja sistem, bukan hanya kegagalan individu.

Mengembangkan *leading indicators* yang baik membutuhkan pemahaman mendalam tentang risiko spesifik organisasi dan pertahanan yang telah mereka terapkan. Tidak ada daftar universal yang cocok untuk semua. Namun, contoh *leading indicators* yang mengukur kesehatan sistem dalam kaitannya dengan *human error* dapat meliputi:

a. **Kualitas Pertahanan Prosedural**

- 1) Persentase prosedur untuk tugas kritis yang telah divalidasi melalui observasi kerja lapangan.
- 2) Skor rata-rata dari audit kualitas prosedur (berdasarkan kriteria seperti kejelasan, keakuratan, dan kemudahan penggunaan).

b. **Kekuatan Budaya Pelaporan**

- 1) Jumlah laporan *near miss* dan kondisi tidak aman yang diterima per periode waktu.
- 2) Waktu rata-rata yang dibutuhkan untuk menutup tindakan korektif dari laporan tersebut.

c. **Kesehatan Pertahanan Manusiawi**

- 1) Persentase penyelia yang telah menyelesaikan pelatihan kepemimpinan keselamatan tingkat lanjut.
- 2) Hasil dari survei iklim keselamatan atau persepsi keamanan psikologis.

d. **Kualitas Pertahanan Teknis**

- 1) Persentase item pemeliharaan preventif pada peralatan keselamatan kritis yang diselesaikan tepat waktu.

- 2) Jumlah alarm palsu atau mengganggu yang dilaporkan dari sistem kontrol.

Metrik-metrik ini mengalihkan percakapan dari “Berapa banyak orang yang terluka?” menjadi “Seberapa kuat pertahanan kita hari ini?”. Mereka memberikan sinyal peringatan dini tentang kondisi laten yang mungkin sedang berkembang. Misalnya, penurunan tajam dalam jumlah laporan *near miss* mungkin bukan berarti sistem menjadi lebih aman, tetapi mungkin menandakan berkembangnya *blame culture* yang menekan pelaporan.

Mengintegrasikan *leading indicators* ke dalam K3MS, terutama dalam proses pemantauan kinerja dan tinjauan manajemen, adalah langkah penting untuk mematangkan program K3. Ini memungkinkan manajemen untuk membuat keputusan berdasarkan data tentang di mana harus menginvestasikan sumber daya untuk memperkuat pertahanan, jauh sebelum pertahanan tersebut gagal. Ini adalah perwujudan praktis dari pergeseran fokus dari individu ke sistem.

## KESIMPULAN

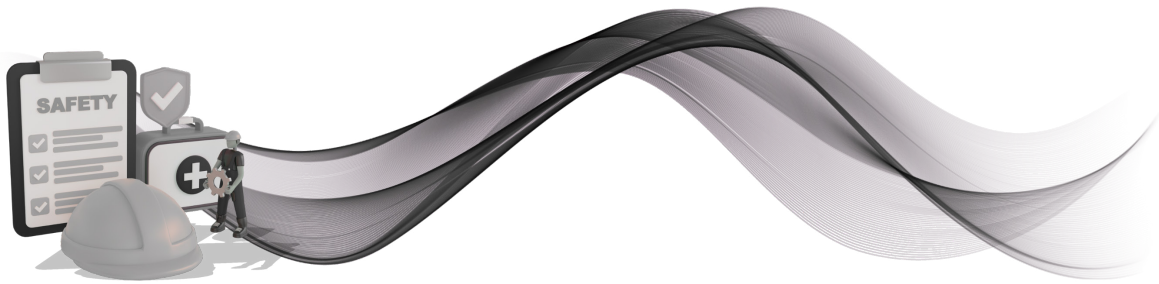
Bab keempat ini telah membekali kita dengan perangkat konseptual dasar yang diperlukan untuk membangun dan menerapkan pendekatan sistemik dalam mitigasi *human error*. Kita telah mendefinisikan sistem kerja sebagai kesatuan kompleks dari komponen manusia, teknologi, organisasi, dan lingkungan yang saling bergantung, di mana interaksi dan putaran umpan balik lebih penting daripada komponen itu sendiri. Pemahaman ini memaksa kita untuk melihat melampaui tindakan individu dan menganalisis dinamika keseluruhan sistem.

Inti dari bab ini adalah perbedaan krusial antara *active failures*, kesalahan dan pelanggaran yang terlihat di lini depan, dan *latent conditions*, yaitu kelemahan tersembunyi yang diciptakan oleh keputusan manajerial dan organisasi. Telah ditegaskan bahwa kegagalan aktif hanyalah pemicu; akar penyebab kecelakaan yang sebenarnya terletak pada kondisi-kondisi laten yang menumpuk dari waktu ke waktu. Kecelakaan terjadi ketika “jendela peluang” terbuka, memungkinkan serangkaian kelemahan ini sejajar dan ditembus.

Sebagai penangkal terhadap kegagalan ini, konsep pertahanan berlapis (*defenses in depth*) telah diperkenalkan sebagai prinsip sentral. Keselamatan tidak dicapai melalui satu penghalang tunggal, melainkan melalui kombinasi berlapis dari pertahanan teknis, prosedural, dan manusiawi. Kecelakaan besar hampir selalu melibatkan kegagalan ganda dari beberapa lapisan pertahanan ini, menyoroti pentingnya memastikan kualitas, keragaman, dan independensi dari setiap lapisan.

Terakhir, bab ini telah menunjukkan bagaimana kerja dari Sistem Manajemen K3 (K3MS) dapat berfungsi sebagai kerangka kerja praktis untuk mengimplementasikan prinsip-prinsip sistemik ini. Dengan mengintegrasikan *human factors* ke dalam setiap tahap siklus PDCA dan dengan berfokus pada pengukuran kinerja sistem melalui *leading indicators*, K3MS dapat diubah dari latihan birokrasi menjadi alat yang dinamis untuk secara proaktif mengidentifikasi kondisi laten dan memperkuat pertahanan. Dengan dasar-dasar ini, kita sekarang siap untuk menjelajahi model-model teoretis spesifik yang membantu kita memvisualisasikan dan menganalisis dinamika sistemik ini dalam praktik.

**DUMMYY**



# BAB 5

## MODEL KEJU SWISS (*SWISS CHEESE MODEL*) JAMES REASON DAN RELEVANSINYA DALAM K3

### PENDAHULUAN

Bagaimana mungkin sebuah sistem yang dilindungi oleh berbagai teknologi canggih, prosedur yang ketat, dan personel yang sangat terlatih masih bisa mengalami kegagalan katastrofik? Pertanyaan ini menghantui para praktisi keselamatan selama puluhan tahun. Konsep-konsep seperti kondisi laten dan pertahanan berlapis yang dibahas pada bab sebelumnya memberikan kerangka kerja teoretis untuk menjawabnya, tetapi mereka bisa terasa abstrak. Diperlukan sebuah model konseptual yang dapat memvisualisasikan dinamika kompleks ini dengan cara yang intuitif dan mudah dipahami. Kebutuhan inilah yang dijawab oleh Model Keju Swiss (*Swiss Cheese Model*), yang dikembangkan oleh James Reason pada tahun 1990.

Model Keju Swiss telah menjadi salah satu metafora paling kuat dan bertahan lama dalam ilmu keselamatan. Popularitasnya terletak pada kesederhanaannya yang elegan dalam menggambarkan bagaimana

kecelakaan terjadi di sistem yang kompleks dan memiliki pertahanan yang baik. Model ini secara visual merangkum seluruh filosofi pendekatan sistemik: bahwa kecelakaan bukanlah hasil dari satu kegagalan tunggal, melainkan produk akhir dari serangkaian kelemahan yang menembus berbagai lapisan pertahanan organisasi. Ia secara efektif menggeser fokus dari mencari satu “penyebab utama” menjadi memahami bagaimana berbagai faktor yang tampaknya tidak berhubungan dapat berkonspirasi untuk menciptakan bencana.

Bab ini akan mengupas Model Keju Swiss secara mendalam, tidak hanya sebagai sebuah gambar yang menarik, tetapi sebagai alat analisis yang kuat. Kita akan memulai dengan membedah struktur dan mekanisme dasar model tersebut, menjelaskan apa yang direpresentasikan oleh setiap irisan keju dan lubang-lubangnya. Konsep kunci tentang bagaimana lubang-lubang ini, yang mewakili kegagalan aktif dan kondisi laten, dapat sejajar untuk menciptakan “lintasan peluang kecelakaan” akan menjadi fokus utama. Ini akan memberikan visualisasi yang jelas tentang konsep jendela kecelakaan yang diperkenalkan pada bab sebelumnya.

Selanjutnya, kita akan bergerak dari metafora ke aplikasi praktis dengan mengidentifikasi jenis-jenis “lubang” yang umum ditemukan di berbagai lapisan pertahanan organisasi. Pembahasan akan mencakup kegagalan di tingkat pengawasan, kelemahan dalam desain prosedur dan peralatan, serta kesalahan yang dilakukan oleh pelaksana tugas di lini depan. Analisis ini akan membantu pembaca untuk mulai melihat organisasi mereka sendiri melalui lensa model ini, mengidentifikasi potensi kelemahan dalam pertahanan mereka.

Peran sentral dari manajemen puncak dalam menciptakan kondisi-kondisi laten akan mendapatkan perhatian khusus. Bab ini akan menguraikan bagaimana keputusan-keputusan yang dibuat di tingkat eksekutif, terkait alokasi sumber daya, prioritas strategis, dan pembentukan budaya, secara langsung memengaruhi ukuran dan jumlah lubang di semua lapisan pertahanan di bawahnya. Ini akan memperkuat argumen bahwa keselamatan sejati dimulai dari puncak organisasi.

Terakhir, kita akan mengeksplorasi bagaimana Model Keju Swiss dapat digunakan tidak hanya secara reaktif untuk menganalisis kecelakaan yang telah terjadi, tetapi juga secara proaktif untuk memprediksi dan mencegah kegagalan di masa depan. Penggunaan model ini dalam analisis *pre-mortem* dan untuk mengidentifikasi pertahanan kritis akan didiskusikan. Sebuah studi kasus yang mendetail akan digunakan untuk mengilustrasikan bagaimana model ini dapat diterapkan untuk mengungkap jaring kausal yang kompleks di balik sebuah kecelakaan nyata.

Meskipun model ini memiliki beberapa keterbatasan dan terkadang disederhanakan secara berlebihan, relevansinya sebagai alat pengajaran dan visualisasi tetap tak tertandingi. Dengan memahami Model Keju Swiss, praktisi K3 akan memiliki kerangka kerja yang kuat untuk mengkomunikasikan prinsip-prinsip keselamatan sistemik kepada semua tingkatan organisasi, dari ruang dewan hingga lantai pabrik.

## **A. Struktur dan Mekanisme Model Keju Swiss**

Inti dari Model Keju Swiss adalah metafora visual yang sederhana namun kuat. James Reason membayangkan pertahanan sebuah organisasi terhadap kegagalan sebagai serangkaian irisan keju Swiss yang disusun berjajar. Setiap irisan keju mewakili satu lapisan pertahanan. Dalam sistem yang ideal, setiap irisan ini akan menjadi penghalang yang kokoh dan solid. Namun, dalam dunia nyata, setiap lapisan pertahanan memiliki kelemahan atau "lubang" yang tidak dapat dihindari. Lubang-lubang ini terus-menerus muncul, menghilang, dan berpindah posisi.

Mekanisme terjadinya kecelakaan dalam model ini digambarkan sebagai berikut: dalam sebagian besar waktu, meskipun setiap lapisan pertahanan memiliki lubang, lubang-lubang tersebut tidak sejajar. Oleh karena itu, jika sebuah bahaya atau kesalahan berhasil melewati satu lapisan pertahanan (melalui sebuah lubang), ia akan dihentikan oleh lapisan berikutnya yang masih solid. Sistem tetap aman. Namun, pada kesempatan yang jarang terjadi, sebuah situasi dapat muncul di mana lubang-lubang di semua lapisan pertahanan secara sesaat sejajar. Ketika ini terjadi, sebuah "lintasan peluang kecelakaan" (*trajectory of accident opportunity*) tercipta,

memungkinkan bahaya untuk merambat tanpa hambatan melalui semua pertahanan dan menyebabkan kerugian atau kecelakaan.

Model ini secara brilian mengilustrasikan beberapa prinsip kunci dari pendekatan sistemik yang telah kita bahas. Pertama, ia menunjukkan bahwa kecelakaan adalah hasil dari banyak faktor, bukan satu penyebab tunggal. Diperlukan penembusan beberapa lapisan pertahanan agar kecelakaan terjadi. Kedua, ia secara visual membedakan antara *active failures* (kegagalan aktif) dan *latent conditions* (kondisi laten). Kegagalan aktif sering kali merupakan lubang di lapisan pertahanan terakhir (misalnya, kesalahan operator), sementara kondisi laten adalah lubang-lubang yang telah ada di lapisan pertahanan di belakangnya (misalnya, prosedur yang buruk, pengawasan yang tidak memadai).

Ketiga, model ini menyoroti sifat dinamis dari risiko. Lubang-lubang tersebut tidak statis; mereka terus bergerak dan berubah ukuran tergantung pada keputusan dan kondisi saat ini. Ini menjelaskan mengapa sebuah sistem dapat beroperasi dengan aman selama berbulan-bulan atau bertahun-tahun dengan kondisi laten yang sama, dan kemudian tiba-tiba gagal ketika serangkaian keadaan yang tidak menguntungkan menyebabkan lubang-lubang tersebut sejajar. Keselamatan bukanlah keadaan yang stabil, melainkan sebuah keseimbangan dinamis yang harus terus-menerus dikelola.

Struktur model ini juga dapat disesuaikan untuk mewakili berbagai jenis lapisan pertahanan dalam suatu organisasi. Reason sering kali menggambarkan lapisan-lapisan ini secara berurutan, mulai dari pengaruh organisasi di bagian paling belakang, bergerak maju melalui pengawasan, prasyarat untuk tindakan (misalnya, kondisi lingkungan kerja), dan akhirnya tindakan spesifik itu sendiri. Setiap lapisan ini adalah sebuah irisan keju dengan potensi lubangnya sendiri.

Dengan memahami struktur dasar dan mekanisme ini, kita dapat mulai menggunakan model ini sebagai alat analisis. Ketika sebuah kecelakaan terjadi, tugas investigator adalah untuk merekonstruksi "kesejajaran lubang" tersebut. Lapisan pertahanan apa saja yang ditembus? Apa sifat

dari lubang di setiap lapisan tersebut? Dan yang terpenting, kondisi laten apa yang menciptakan lubang-lubang tersebut di tempat pertama?

**Analogi/Contoh Kasus:** Bayangkan sebuah kastil abad pertengahan yang dilindungi oleh beberapa lapisan pertahanan: parit, tembok luar, tembok dalam, dan penjaga pribadi raja. Ini adalah irisan-irisan keju. Parit mungkin memiliki satu titik dangkal di mana musuh bisa menyeberang (lubang #1). Tembok luar mungkin memiliki satu bagian yang runtuh karena perawatan yang buruk (lubang #2, kondisi laten). Tembok dalam mungkin kebetulan tidak diawasi oleh penjaga pada shift tertentu (lubang #3, kondisi laten). Dan penjaga pribadi raja mungkin tertidur karena kelelahan (*active failure*, lubang #4). Secara terpisah, setiap kelemahan ini mungkin tidak fatal. Namun, jika seorang pembunuh yang cerdas menemukan semua kelemahan ini pada malam yang sama, dia akan memiliki jalur lurus untuk mencapai raja. Model Keju Swiss bekerja dengan logika yang sama: bencana terjadi ketika serangkaian kelemahan yang tampaknya tidak berhubungan secara kebetulan memberikan jalur yang jelas bagi bahaya.

### 1. Penggambaran Lapisan Pertahanan (Slices of Cheese)

Setiap irisan keju dalam model Reason mewakili salah satu dari banyak lapisan pertahanan, penghalang, atau penjaga (*safeguards*) yang telah diterapkan oleh sebuah organisasi untuk melindungi dirinya dari bahaya dan mencegah kecelakaan. Lapisan-lapisan ini adalah perwujudan praktis dari konsep *defenses in depth* yang dibahas di Bab 4. Mengidentifikasi dan memahami fungsi dari setiap lapisan pertahanan ini adalah langkah pertama dalam menerapkan Model Keju Swiss pada sistem kerja tertentu.

Lapisan-lapisan ini dapat dikelompokkan ke dalam beberapa kategori umum. Pertama adalah pertahanan rekayasa dan teknis. Ini adalah pertahanan yang paling "keras" dan sering kali paling andal, karena mereka dirancang untuk berfungsi secara otomatis. Contohnya termasuk sistem pemadaman darurat, katup pelepas tekanan, pelindung mesin, dan sistem alarm. Dalam metafora keju, ini adalah irisan yang paling tebal dan paling padat, meskipun mereka masih bisa memiliki lubang, seperti kegagalan mekanis, cacat desain, atau kegagalan daya.

Lapisan berikutnya adalah pertahanan administratif dan prosedural. Ini mencakup semua aturan, kebijakan, prosedur operasi standar (SOP), dan sistem izin kerja yang telah dibuat oleh organisasi. Tujuannya adalah untuk memandu perilaku ke arah yang aman dan memberikan kontrol atas aktivitas berisiko tinggi. Lapisan ini lebih "lunak" daripada pertahanan teknis karena efektivitasnya bergantung pada kualitas penulisan dan kepatuhan manusia. Lubang di lapisan ini bisa berupa prosedur yang tidak jelas, tidak akurat, atau tidak praktis.

Lapisan ketiga adalah pertahanan manusiawi. Ini adalah lapisan terakhir dan sering kali yang paling dinamis. Ini bergantung pada pengetahuan, keterampilan, dan kewaspadaan orang-orang di dalam sistem untuk mendeteksi dan memperbaiki kondisi berbahaya atau untuk merespons kegagalan yang sedang berkembang. Ini termasuk pengawasan oleh penyelia, verifikasi silang oleh rekan kerja (*peer checking*), dan kemampuan operator untuk mendiagnosis masalah dan mengambil tindakan korektif. Lapisan ini sangat fleksibel tetapi juga rentan terhadap semua jenis *human error* yang telah kita diskusikan (misalnya, *slips*, *lapses*, *mistakes*).

Reason juga sering mengategorikan lapisan pertahanan berdasarkan posisinya dalam organisasi. Lapisan paling belakang adalah pengaruh organisasi, yang mencakup budaya keselamatan, kebijakan tingkat tinggi, dan sistem manajemen. Lapisan berikutnya adalah pengawasan, yaitu praktik manajemen lini pertama. Lapisan selanjutnya adalah prasyarat untuk tindakan, yang mencakup kondisi lingkungan kerja, kebugaran personel untuk bertugas, dan ketersediaan alat yang tepat. Lapisan paling depan, yang paling dekat dengan bahaya, adalah tindakan spesifik yang dilakukan oleh individu di lini depan.

Penting untuk dipahami bahwa tidak ada satu set lapisan pertahanan yang universal untuk semua sistem. Setiap organisasi dan setiap proses berisiko tinggi akan memiliki konfigurasi pertahanannya sendiri. Bagian dari analisis keselamatan yang efektif adalah memetakan lapisan-lapisan ini secara eksplisit. Apa saja penghalang utama yang kita andalkan untuk mencegah kecelakaan X? Dengan membuat pertahanan ini terlihat, kita dapat mulai secara sistematis menilai kekuatan dan kelemahan dari setiap "irisan keju" dalam sistem kita. Ini adalah langkah penting untuk beralih

dari keselamatan yang diasumsikan ke keselamatan yang direkayasa secara sadar.

## 2. Lubang sebagai Representasi Latent Conditions dan Active Failures

Jika irisan keju adalah pertahanan kita, maka lubang-lubang di dalamnya adalah kegagalan atau kelemahan dari pertahanan tersebut. Model Keju Swiss secara visual membedakan antara dua jenis lubang utama, yang sesuai dengan konsep yang diperkenalkan di Bab 4: lubang yang disebabkan oleh *latent conditions* dan lubang yang disebabkan oleh *active failures*.

- a. Lubang dari *Latent Conditions* adalah kelemahan yang sudah ada di dalam sistem, sering kali untuk waktu yang lama, sebelum kecelakaan terjadi. Lubang-lubang ini biasanya ditemukan di irisan keju yang lebih ke belakang, lapisan pertahanan organisasi, manajerial, dan rekayasa. Mereka adalah produk sampingan yang tak terhindarkan dari keputusan yang dibuat di "ujung tumpul" organisasi. Setiap kali keputusan dibuat yang mengorbankan keselamatan demi tujuan lain (seperti penghematan biaya atau percepatan jadwal), sebuah lubang laten berpotensi diciptakan atau diperbesar.

Contoh lubang dari kondisi laten meliputi:

- 1) Prosedur yang ditulis dengan buruk: Ini adalah lubang di lapisan pertahanan prosedural.
- 2) Pelatihan yang tidak memadai: Ini menciptakan lubang di lapisan pertahanan manusiawi (kompetensi).
- 3) Sistem alarm yang dirancang dengan buruk yang menghasilkan terlalu banyak peringatan palsu: Ini adalah lubang di lapisan pertahanan teknis.
- 4) Jadwal kerja yang menyebabkan kelelahan: Ini menciptakan lubang di lapisan prasyarat untuk tindakan (kebugaran untuk bertugas).
- 5) Budaya yang tidak mendorong pelaporan masalah: Ini adalah lubang besar di lapisan pertahanan organisasi.

- b. Lubang dari *Active Failures*, di sisi lain, adalah tindakan tidak aman (kesalahan atau pelanggaran) yang dilakukan oleh orang di lini depan.

Lubang-lubang ini cenderung muncul di irisan keju paling depan, yang mewakili kinerja manusia saat itu juga. Berbeda dengan lubang laten yang bisa statis untuk waktu yang lama, lubang dari kegagalan aktif sering kali bersifat sementara dan tidak terduga, seperti selip perhatian sesaat atau lapse memori. Mereka adalah “peristiwa pemicu” yang sering kali merupakan tindakan terakhir yang menembus pertahanan yang sudah dilemahkan oleh kondisi-kondisi laten.

Penting untuk memahami hubungan antara kedua jenis lubang ini. Kondisi laten tidak hanya menciptakan lubang di pertahanan di belakang, tetapi mereka juga menciptakan jalur yang mengarah pada kegagalan aktif di lini depan. Dengan kata lain, kondisi laten meningkatkan kemungkinan terjadinya kegagalan aktif. Misalnya, prosedur yang ditulis dengan buruk (*latent condition*) membuat seorang teknisi lebih mungkin untuk melakukan kesalahan dalam mengikuti langkah-langkahnya (*active failure*). Kelelahan akibat jadwal kerja yang buruk (*latent condition*) membuat seorang pengemudi lebih rentan terhadap selip perhatian (*active failure*).

Model ini dengan demikian mengilustrasikan bahwa menyalahkan individu atas kegagalan aktif mereka adalah tindakan yang tidak adil dan tidak efektif. Mereka mungkin telah melakukan tindakan terakhir, tetapi panggung untuk kegagalan mereka telah disiapkan oleh serangkaian kondisi laten yang berada di luar kendali mereka. Fokus dari analisis sistemik, oleh karena itu, adalah untuk memahami mengapa lubang-lubang laten itu ada di tempat pertama dan bagaimana cara menutupnya.

### **3. Kondisi yang Diperlukan untuk Sejajarnya Lubang (Alignment of Holes)**

Kecelakaan dalam Model Keju Swiss adalah peristiwa yang probabilitasnya rendah karena membutuhkan terpenuhinya kondisi yang sangat spesifik: kesejajaran sesaat dari lubang-lubang di beberapa lapisan pertahanan. Jika hanya satu atau dua lubang yang sejajar, kegagalan biasanya akan ditangkap oleh lapisan berikutnya. Bencana terjadi dalam “jendela peluang” yang langka di mana semua penghalang gagal secara bersamaan, menciptakan lintasan lurus dari bahaya ke kerugian.

Kesejajaran ini bukanlah peristiwa yang sepenuhnya acak seperti memenangkan lotre. Meskipun ada elemen kebetulan di dalamnya, probabilitas kesejajaran ini sangat dipengaruhi oleh kesehatan keseluruhan sistem keselamatan. Semakin banyak dan semakin besar lubang-lubang laten di dalam sistem, semakin besar kemungkinan bahwa beberapa dari mereka akan sejajar pada waktu tertentu. Sebuah organisasi dengan budaya keselamatan yang buruk, prosedur yang usang, dan peralatan yang tidak terawat pada dasarnya sedang “memuat dadu” untuk dirinya sendiri, membuat kesejajaran yang berbahaya menjadi lebih mungkin terjadi.

Faktor-faktor yang dapat memicu atau memfasilitasi kesejajaran lubang sering kali bersifat dinamis dan terkait dengan kondisi operasional saat itu. Beberapa pemicu umum meliputi:

- a. Tekanan operasional yang tinggi: Ketika ada tekanan untuk mempercepat produksi atau mengejar tenggat waktu, orang mungkin lebih cenderung mengambil jalan pintas (membuka lubang pelanggaran) dan lebih rentan terhadap kesalahan akibat stres (membuka lubang kesalahan).
- b. Situasi abnormal atau darurat: Kondisi yang tidak terduga dapat menempatkan tekanan pada beberapa lapisan pertahanan secara bersamaan, menyingkap kelemahan-kelemahan laten yang mungkin tidak terlihat dalam operasi normal.
- c. Perubahan organisasi: Reorganisasi, pergantian personel kunci, atau pengenalan teknologi baru dapat secara sementara menciptakan kebingungan dan kelemahan di berbagai lapisan pertahanan, meningkatkan peluang untuk kesejajaran.
- d. Kegagalan teknis lokal: Kerusakan pada satu komponen dapat menciptakan serangkaian konsekuensi yang menantang berbagai lapisan pertahanan lainnya.

Konsep kesejajaran ini juga menyoroti mengapa kecelakaan besar sering kali didahului oleh serangkaian insiden kecil atau *near misses*. Peristiwa-peristiwa yang lebih kecil ini sering kali merupakan kasus di mana hanya dua atau tiga lubang yang sejajar. Mereka adalah “tembakan peringatan” yang menunjukkan bahwa pertahanan sistem sedang terkikis dan bahwa potensi untuk kesejajaran yang lebih besar sedang meningkat.

Organisasi yang bijaksana akan memperlakukan setiap *near miss* sebagai kesempatan berharga untuk menemukan dan menutup lubang-lubang ini sebelum mereka dapat bergabung dalam kesejajaran yang fatal.

Implikasi praktis dari konsep ini adalah bahwa manajemen keselamatan harus menjadi aktivitas yang proaktif dan dinamis. Tujuannya bukan hanya untuk memiliki lapisan pertahanan, tetapi untuk secara aktif memantau "posisi" dan "ukuran" lubang-lubang di dalamnya. Ini melibatkan audit yang mendalam, observasi kerja, dan mendengarkan umpan balik dari lini depan untuk merasakan di mana kelemahan baru mungkin muncul. Dengan melakukan ini, organisasi dapat mengambil tindakan untuk "menggoyangkan irisan keju", yaitu, untuk memperbaiki kelemahan dan menutup lubang, sehingga menjaga agar mereka tetap tidak sejajar.

## **B. Identifikasi Lubang-Lubang dalam Lapisan Pertahanan**

Meskipun Model Keju Swiss adalah sebuah metafora, "lubang-lubang" di dalamnya mewakili kegagalan dan kelemahan nyata yang dapat diidentifikasi di dalam sebuah organisasi. Menggunakan model ini sebagai kerangka kerja, seorang analis keselamatan dapat secara sistematis memeriksa berbagai lapisan pertahanan untuk mencari jenis-jenis lubang yang umum. Mengidentifikasi lubang-lubang ini secara proaktif, sebelum mereka sejajar, adalah inti dari manajemen risiko modern. Proses identifikasi ini sering kali mengungkapkan pola kegagalan yang berulang di seluruh organisasi.

Lubang-lubang ini dapat muncul di setiap tingkatan. Di tingkat organisasi yang tinggi, lubang mungkin berupa strategi bisnis yang secara tidak sengaja menciptakan konflik antara tujuan produksi dan keselamatan, atau kegagalan dewan direksi untuk menyediakan sumber daya yang memadai untuk K3. Di tingkat manajemen menengah, lubang dapat berupa sistem perencanaan kerja yang buruk yang secara teratur menciptakan tekanan waktu yang tidak perlu, atau proses manajemen kontraktor yang lemah. Di tingkat lini depan, lubang bisa berupa alat yang usang atau prosedur yang tidak praktis.

Mengklasifikasikan lubang-lubang ini berdasarkan lapisan pertahanan di mana mereka berada membantu untuk mengatur analisis dan menargetkan intervensi. Investigasi yang hanya berfokus pada lubang di lapisan paling depan, kesalahan operator, dipastikan akan dangkal. Investigasi yang komprehensif akan menelusuri kembali lintasan kecelakaan melalui setiap irisan keju, mengidentifikasi sifat lubang di setiap lapisan, dan bagaimana lubang-lubang ini saling berhubungan.

Bagian ini akan menguraikan beberapa jenis lubang yang paling umum ditemukan di tiga lapisan pertahanan utama: kegagalan di tingkat pengawasan dan manajemen risiko, kelemahan dalam desain prosedur dan peralatan, dan akhirnya, kesalahan yang dilakukan oleh pelaksana tugas itu sendiri, yang merupakan manifestasi akhir dari kelemahan-kelemahan yang lebih dalam ini.

**Analogi/Contoh Kasus:** Proses identifikasi lubang-lubang ini mirip dengan pemeriksaan medis yang komprehensif. Seorang dokter tidak hanya melihat gejala yang terlihat (misalnya, batuk, yang setara dengan *active failure*). Dia melakukan serangkaian tes untuk mencari masalah mendasar di berbagai "sistem" atau "lapisan" tubuh. Dia mungkin melakukan tes darah untuk memeriksa fungsi ginjal (lapisan #1), rontgen untuk memeriksa kondisi paru-paru (lapisan #2), dan EKG untuk memeriksa jantung (lapisan #3). Setiap tes dirancang untuk mencari "lubang" atau kelemahan spesifik di lapisan pertahanan biologis pasien. Diagnosis yang akurat dan rencana pengobatan yang efektif hanya mungkin dilakukan setelah gambaran keseluruhan dari berbagai kelemahan sistemik ini diperoleh.

## 1. Kegagalan Pengawasan dan Manajemen Risiko

Lapisan pertahanan pengawasan dan manajemen risiko berada tepat di belakang lini depan. Lapisan ini mewakili tugas-tugas yang dilakukan oleh manajer lini pertama, penyelia, dan perencana kerja untuk memastikan bahwa pekerjaan dapat dilakukan dengan aman. Kegagalan di lapisan ini sering kali menciptakan prasyarat langsung untuk kegagalan aktif. Jika pengawasan tidak memadai, bahkan pekerja yang bermaksud baik pun dapat menyimpang ke jalur yang tidak aman.

Salah satu lubang paling umum di lapisan ini adalah perencanaan kerja yang tidak memadai. Ini terjadi ketika pekerjaan dijadwalkan tanpa mempertimbangkan semua risiko yang terlibat, atau tanpa memastikan bahwa sumber daya yang tepat (staf, alat, bahan, izin) tersedia. Hal ini sering kali menciptakan tekanan waktu dan frustrasi di lini depan, yang merupakan pendorong kuat untuk pelanggaran situasional dan kesalahan.

Lubang lainnya adalah kegagalan untuk memperbaiki masalah yang diketahui. Seringkali, bahaya atau kekurangan prosedur telah diidentifikasi dan dilaporkan oleh pekerja jauh sebelum kecelakaan terjadi. Kegagalan manajemen untuk menanggapi laporan-laporan ini secara tepat waktu dan efektif adalah sebuah kondisi laten yang signifikan. Ini tidak hanya membiarkan bahaya tetap ada, tetapi juga mengirimkan pesan kepada pekerja bahwa keselamatan bukanlah prioritas dan bahwa melaporkan masalah adalah sia-sia.

Pengawasan yang tidak memadai di lapangan juga merupakan lubang klasik. Ini bisa berupa kurangnya kehadiran penyelia di lokasi kerja kritis, atau penyelia yang hadir secara fisik tetapi tidak terlibat secara aktif dalam memantau keselamatan. Terkadang, penyelia sendiri mungkin kurang terlatih dalam K3 atau berada di bawah tekanan yang sama untuk memprioritaskan produksi, sehingga mereka mungkin secara sengaja atau tidak sengaja menoleransi praktik kerja yang tidak aman.

Terakhir, pencocokan tugas dengan keterampilan yang tidak tepat adalah kegagalan pengawasan yang umum. Ini terjadi ketika seorang penyelia menugaskan seorang pekerja untuk melakukan tugas yang di luar tingkat kompetensi atau pengalamannya, mungkin karena kekurangan staf atau tekanan jadwal. Ini menempatkan individu tersebut dalam situasi di mana mereka lebih mungkin membuat *mistake* berbasis pengetahuan. Menilai kompetensi dan memastikan bahwa hanya orang yang memenuhi syarat yang melakukan tugas kritis adalah fungsi pengawasan fundamental yang kegagalannya dapat memiliki konsekuensi yang parah.

Menutup lubang-lubang di lapisan pengawasan ini memerlukan investasi dalam pengembangan kepemimpinan lini pertama. Penyelia perlu dilatih tidak hanya dalam aspek teknis pekerjaan, tetapi juga

dalam keterampilan manajemen risiko, komunikasi, dan kepemimpinan keselamatan. Mereka harus diberdayakan dan diberi akuntabilitas untuk menciptakan lingkungan kerja yang aman bagi tim mereka.

## 2. Kelemahan dalam Desain Prosedur dan Peralatan

Lapisan pertahanan ini mencakup semua alat, teknologi, dan dokumen yang seharusnya membantu pekerja melakukan tugas mereka dengan aman dan efisien. Lubang di lapisan ini sering kali merupakan hasil dari keputusan desain yang buruk yang dibuat jauh dari tempat kerja, yang menciptakan "jebakan" bagi pengguna di lini depan. Kelemahan di sini adalah contoh klasik dari kondisi laten.

Dalam hal prosedur, lubang yang umum termasuk prosedur yang tidak akurat atau usang. Prosedur sering kali tidak diperbarui untuk mencerminkan perubahan pada peralatan atau proses, membuatnya tidak relevan. Prosedur yang terlalu rumit, panjang, atau ditulis dengan buruk juga merupakan lubang yang signifikan. Jika sebuah prosedur sulit untuk dibaca dan dipahami, terutama di bawah tekanan, kemungkinan besar ia akan diabaikan atau disalahartikan. Tidak adanya prosedur untuk tugas-tugas yang tidak rutin tetapi berisiko tinggi adalah lubang lain yang jelas.

Dalam hal peralatan dan teknologi, lubang-lubang tersebut sering kali berkaitan dengan kegagalan untuk menerapkan prinsip-prinsip *human factors* dan ergonomi. Desain antarmuka yang buruk adalah penyebab umum dari banyak kesalahan. Ini termasuk label yang tidak jelas, kontrol yang membingungkan, atau tampilan informasi yang tidak intuitif. Desain yang tidak ergonomis, yang memaksa pekerja untuk menggunakan postur canggung atau kekuatan berlebihan, tidak hanya menyebabkan cedera regangan tetapi juga meningkatkan kelelahan, yang pada gilirannya meningkatkan kemungkinan semua jenis kesalahan.

Peralatan yang tidak dirawat dengan baik adalah lubang laten lain yang dapat menyebabkan kegagalan tak terduga pada saat kritis. Kegagalan untuk berinvestasi dalam pemeliharaan preventif yang kuat adalah keputusan organisasi yang secara langsung melemahkan lapisan pertahanan teknis. Demikian pula, kegagalan untuk menyediakan alat yang tepat untuk pekerjaan dapat memaksa pekerja untuk berimprovisasi

dengan cara yang tidak aman, yang merupakan pendorong kuat untuk pelanggaran.

Menutup lubang-lubang di lapisan ini memerlukan komitmen organisasi untuk desain yang berpusat pada manusia. Ini berarti melibatkan pengguna akhir dalam proses desain dan pengadaan peralatan. Ini berarti memiliki proses yang kuat untuk meninjau dan memvalidasi prosedur di lapangan, bukan hanya di kantor. Ini juga berarti memandang pemeliharaan bukan sebagai biaya, tetapi sebagai investasi penting dalam keandalan dan keselamatan.

### 3. Kesalahan pada Pelaksana Tugas (Operator)

Ini adalah lapisan pertahanan terakhir dan paling depan dalam Model Keju Swiss, yang mewakili kinerja individu atau tim yang berinteraksi langsung dengan bahaya. Lubang di lapisan ini adalah *active failures*, *slips*, *lapses*, *mistakes*, dan *violations*, yang menjadi pemicu langsung dari sebuah insiden. Seperti yang telah ditekankan berulang kali, lubang-lubang ini jarang sekali muncul secara spontan; mereka hampir selalu merupakan produk dari kelemahan (lubang) di lapisan pertahanan di belakangnya.

- a. Kesalahan berbasis keterampilan (*slips dan lapses*) adalah lubang yang disebabkan oleh kegagalan perhatian atau memori sesaat. Lubang-lubang ini lebih mungkin muncul ketika pelaksana tugas mengalami kelelahan, stres, atau gangguan, kondisi yang sering kali diciptakan oleh keputusan penjadwalan atau lingkungan kerja yang buruk (lubang di lapisan lain). Desain antarmuka yang buruk juga merupakan pemicu utama untuk *slips*.
- b. Kesalahan berbasis pengetahuan dan aturan (*mistakes*) adalah lubang yang berasal dari diagnosis situasi yang salah atau penerapan aturan yang keliru. Munculnya lubang ini sangat dipengaruhi oleh kualitas pelatihan yang diterima oleh pelaksana tugas, kejelasan prosedur yang mereka miliki, dan ketersediaan informasi yang akurat. Jika lapisan-lapisan ini lemah, kemungkinan terjadinya *mistake* akan meningkat secara signifikan.

Pelanggaran adalah lubang yang dibuat secara sadar ketika seorang pelaksana tugas menyimpang dari prosedur. Seperti yang dibahas di Bab

3, lubang ini sering kali merupakan respons yang dapat diprediksi terhadap prosedur yang tidak praktis, tekanan produksi yang ekstrim, atau kurangnya pengawasan. Pelanggaran rutin yang ditoleransi oleh manajemen dapat menciptakan lubang yang permanen dan menganga di lapisan pertahanan terakhir ini.

Mengidentifikasi jenis kesalahan spesifik pada pelaksana tugas sangat penting, bukan untuk menyalahkan mereka, tetapi untuk memberikan petunjuk tentang di mana harus mencari lubang di lapisan belakang. Jika kita melihat pola *slips*, kita harus memeriksa desain antarmuka. Jika kita melihat pola *mistakes*, kita harus memeriksa pelatihan dan prosedur. Jika kita melihat pola pelanggaran, kita harus memeriksa budaya dan tekanan kerja.

“Menutup” lubang di lapisan ini bukanlah tentang mencoba membuat manusia menjadi sempurna. Sebaliknya, ini adalah tentang memperkuat lapisan-lapisan di belakangnya sehingga pelaksana tugas tidak ditempatkan dalam situasi yang provokatif terhadap kesalahan. Ini juga tentang membangun pertahanan di dalam tim itu sendiri, melalui praktik kerja tim yang baik seperti komunikasi silang dan verifikasi, sehingga anggota tim dapat saling menangkap kesalahan satu sama lain sebelum menyebabkan kerugian.

### **C. Peran Kesalahan Manajemen Puncak**

Dalam Model Keju Swiss, lapisan pertahanan paling belakang dan paling berpengaruh adalah yang mewakili keputusan dan budaya organisasi. Lubang di lapisan ini, yang sering kali diciptakan oleh manajemen puncak dan menengah, memiliki efek riak yang dapat melemahkan semua lapisan pertahanan lainnya. Kesalahan atau keputusan yang buruk di tingkat ini mungkin tidak segera terlihat dampaknya, tetapi mereka adalah sumber utama dari sebagian besar kondisi laten yang pada akhirnya memungkinkan terjadinya kecelakaan. Manajemen puncak adalah arsitek utama dari sistem pertahanan organisasi; jika fondasinya retak, seluruh struktur menjadi tidak stabil.

Keputusan yang dibuat di ruang dewan, mengenai anggaran, prioritas strategis, struktur organisasi, dan penunjukan pimpinan, secara langsung membentuk konteks di mana manajer lini tengah dan pekerja lini depan membuat pilihan mereka sehari-hari. Sebuah komitmen yang tulus terhadap keselamatan di tingkat puncak akan terwujud dalam alokasi sumber daya yang memadai, sistem akuntabilitas yang adil, dan pesan yang konsisten bahwa keselamatan tidak dapat dikompromikan. Sebaliknya, jika keselamatan hanya menjadi slogan tanpa dukungan nyata, pesan yang diterima di seluruh organisasi adalah bahwa produksi dan keuntungan adalah yang benar-benar penting.

Kegagalan manajemen puncak untuk menciptakan dan memelihara budaya keselamatan yang positif adalah salah satu "lubang" paling signifikan yang bisa ada. Budaya organisasi, nilai-nilai, keyakinan, dan norma perilaku bersama, sangat menentukan apakah prosedur akan diikuti, apakah masalah akan dilaporkan, dan apakah orang akan merasa aman untuk menantang praktik yang tidak aman. Budaya ini tidak diciptakan oleh poster atau kampanye; ia diciptakan oleh tindakan, keputusan, dan prioritas yang ditunjukkan oleh para pemimpin setiap hari.

Bagian ini akan mengeksplorasi secara lebih rinci bagaimana keputusan manajemen puncak mengenai alokasi sumber daya, penetapan prioritas, dan pembentukan budaya secara langsung berkontribusi pada penciptaan kondisi laten di seluruh sistem. Memahami peran ini sangat penting, karena ini menunjukkan bahwa perbaikan keselamatan yang berkelanjutan harus dimulai dan didukung dari tingkat tertinggi organisasi.

**Analogi/Contoh Kasus:** Bayangkan manajemen puncak sebagai perancang dan operator sistem irigasi untuk sebuah lahan pertanian yang luas. Keputusan mereka di pusat kendali menentukan berapa banyak air (sumber daya) yang dialokasikan ke setiap bagian lahan, kapan air itu dialirkan (prioritas), dan seberapa baik saluran-saluran (struktur organisasi) dipelihara. Jika mereka memutuskan untuk memotong anggaran pemeliharaan, saluran-saluran akan mulai tersumbat (kondisi laten). Jika mereka mengalihkan sebagian besar air ke tanaman yang paling menguntungkan secara finansial, bagian lain dari lahan akan menjadi kering (kondisi laten). Para petani di ladang (*sharp end*) mungkin melakukan yang

terbaik, tetapi jika mereka tidak menerima air yang cukup pada waktu yang tepat karena keputusan di pusat, tanaman mereka (keselamatan dan produksi) pada akhirnya akan gagal. Kegagalan panen bukanlah kesalahan petani; itu adalah konsekuensi yang dapat diprediksi dari kesalahan manajemen sistem irigasi.

### **1. Dampak Keputusan Manajemen terhadap Kondisi Laten**

Setiap keputusan yang dibuat oleh manajemen, terutama manajemen puncak, memiliki potensi untuk menciptakan atau menutup kondisi laten. Hubungan antara keputusan ini dan kecelakaan di masa depan sering kali tidak langsung dan tertunda, sehingga sulit bagi para pembuat keputusan untuk melihat konsekuensi penuh dari tindakan mereka. Namun, analisis pasca-kecelakaan terhadap hampir semua bencana besar mengungkapkan jejak keputusan manajerial yang buruk sebagai faktor kontribusi utama.

Salah satu area di mana dampak ini paling jelas adalah dalam manajemen perubahan. Ketika organisasi memperkenalkan teknologi baru, merestrukturisasi departemen, atau mengubah proses kerja, mereka secara inheren menciptakan ketidakpastian dan potensi risiko baru. Proses manajemen perubahan (MOC) yang lemah, yang gagal menganalisis secara memadai dampak keselamatan dari perubahan, gagal melatih orang dengan benar, atau gagal memperbarui prosedur, adalah pabrik kondisi laten yang sangat efisien. Keputusan manajemen untuk melanjutkan perubahan tanpa uji tuntas K3 yang semestinya secara langsung menciptakan lubang di berbagai lapisan pertahanan.

Keputusan pengadaan dan kontrak adalah area lain yang kritis. Keputusan untuk memilih kontraktor termurah tanpa mengevaluasi kinerja keselamatannya secara ketat, atau untuk membeli peralatan berdasarkan harga terendah daripada desain *human factors* terbaik, adalah contoh keputusan yang menciptakan kondisi laten. Penghematan biaya jangka pendek ini sering kali dibayar mahal dalam bentuk peningkatan risiko kesalahan operator, biaya perawatan yang lebih tinggi, dan potensi kecelakaan di masa depan.

Kebijakan sumber daya manusia juga memiliki dampak yang mendalam. Kebijakan kompensasi yang sangat menekankan bonus produksi dapat

mendorong pengambilan risiko. Proses rekrutmen dan promosi yang tidak mempertimbangkan kompetensi dan komitmen keselamatan dapat menempatkan orang yang salah di posisi kritis. Kebijakan kepegawaian yang menyebabkan perputaran karyawan yang tinggi dapat secara konstan menguras pengalaman dari organisasi dan membuat lebih banyak pekerja pemula yang rentan kesalahan.

Bahkan keputusan yang tampaknya tidak berhubungan dengan K3 dapat memiliki dampak. Misalnya, keputusan tim pemasaran untuk menjanjikan tanggal pengiriman yang sangat ketat kepada pelanggan dapat menciptakan tekanan produksi yang luar biasa di lantai pabrik, yang pada gilirannya mendorong jalan pintas dan pelanggaran. Ini menyoroti pentingnya pemikiran terintegrasi, di mana implikasi keselamatan dari semua keputusan bisnis besar dipertimbangkan secara eksplisit.

Organisasi yang matang secara keselamatan memahami hal ini dan membangun "pertahanan" terhadap keputusan manajerial yang buruk. Ini bisa berupa proses MOC yang kuat yang mencakup tinjauan K3 wajib, persyaratan bahwa semua pengeluaran modal besar harus mencakup analisis *human factors*, atau komite keselamatan tingkat eksekutif yang meninjau implikasi K3 dari keputusan-keputusan strategis. Dengan melakukan ini, mereka mencoba untuk "menutup lubang" di irisan keju paling belakang, lapisan keputusan organisasi, sebelum lubang-lubang tersebut dapat merambat ke seluruh sistem.

## **2. Alokasi Sumber Daya dan Prioritas Keselamatan**

Salah satu cara paling nyata di mana komitmen manajemen puncak terhadap keselamatan diuji adalah melalui alokasi sumber daya, waktu, uang, dan orang. Pepatah "tunjukkan anggaran Anda, dan saya akan tahu apa prioritas Anda" sangat berlaku untuk K3. Sebuah organisasi dapat memiliki kebijakan keselamatan yang ditulis dengan indah dan poster yang mengkilap, tetapi jika departemen K3 kekurangan staf, anggaran pemeliharaan terus-menerus dipotong, dan permintaan untuk perbaikan keselamatan secara teratur ditolak karena alasan biaya, maka pesan yang sebenarnya diterima oleh karyawan sangat jelas: keselamatan adalah prioritas yang lebih rendah.

Alokasi anggaran adalah indikator yang paling jelas. Kegagalan untuk mengalokasikan dana yang cukup untuk pemeliharaan preventif, penggantian peralatan yang usang, pelatihan yang berkualitas, atau perekrutan profesional K3 yang kompeten secara langsung menciptakan kondisi laten. Keputusan untuk menunda perbaikan keselamatan yang diperlukan untuk “menghemat uang” pada kuartal ini adalah pertaruhan yang pada dasarnya memperdagangkan keuntungan jangka pendek dengan peningkatan risiko kegagalan katastrofik di masa depan. Analisis banyak bencana industri, seperti ledakan kilang minyak Texas City BP pada tahun 2005, menunjukkan bahwa pemotongan anggaran yang drastis pada pemeliharaan dan pelatihan adalah faktor penyebab utama.

Alokasi waktu dan perhatian manajemen sama pentingnya. Apakah keselamatan menjadi agenda rutin dalam rapat dewan direksi? Apakah para eksekutif senior secara teratur meluangkan waktu untuk melakukan *safety walkdowns* dan berbicara dengan pekerja di lini depan? Atau apakah keselamatan hanya dibahas setelah terjadi insiden? Ketika para pemimpin secara konsisten mendedikasikan waktu mereka untuk masalah K3, itu mengirimkan sinyal yang kuat ke seluruh organisasi tentang pentingnya masalah tersebut.

Alokasi personel juga krusial. Apakah organisasi memiliki cukup staf untuk melakukan pekerjaan dengan aman, atau apakah beban kerja yang berlebihan menjadi norma? Apakah para profesional K3 memiliki senioritas dan pengaruh yang cukup dalam organisasi untuk menantang keputusan operasional yang tidak aman, atau apakah mereka dipandang sebagai fungsi pendukung yang terpinggirkan?

Prioritas keselamatan yang dirasakan sering kali muncul dalam konflik antara tujuan produksi dan keselamatan. Dalam teori, semua manajer akan mengatakan bahwa keselamatan adalah yang utama. Namun, dalam praktik, ketika dihadapkan pada pilihan antara menghentikan produksi untuk memperbaiki masalah keselamatan atau terus berjalan untuk memenuhi target, keputusan yang dibuat mengungkapkan prioritas yang sebenarnya. Dalam organisasi dengan budaya keselamatan yang kuat, menghentikan pekerjaan untuk mengatasi masalah keselamatan akan dipuji. Dalam budaya yang lemah, itu akan dilihat sebagai penyebab masalah.

Manajemen puncak memiliki tanggung jawab untuk secara eksplisit dan berulang kali mengkomunikasikan bahwa keselamatan tidak dapat dikompromikan demi tujuan lain, dan kemudian mendukung kata-kata itu dengan alokasi sumber daya yang konsisten. Tanpa dukungan nyata ini, semua inisiatif K3 lainnya akan kekurangan fondasi dan pada akhirnya akan gagal. Alokasi sumber daya yang tidak memadai adalah salah satu lubang terbesar dan paling berbahaya yang dapat dibuat oleh manajemen di lapisan pertahanan organisasi.

### **3. Pengaruh Budaya Organisasi terhadap Kualitas Lapisan Pertahanan**

Budaya organisasi adalah "cara kita melakukan sesuatu di sini". Ini adalah kumpulan nilai-nilai, keyakinan, asumsi, dan norma perilaku bersama yang membentuk cara anggota organisasi berpikir, merasa, dan bertindak. Budaya adalah kekuatan yang sangat kuat dan sering kali tidak terlihat yang memengaruhi kualitas dari *setiap* lapisan pertahanan dalam Model Keju Swiss. Bisa dibilang, budaya organisasi adalah "jenis keju" itu sendiri; budaya yang kuat menciptakan keju yang padat dan kuat, sementara budaya yang lemah menciptakan keju yang rapuh dan penuh lubang.

Pengaruh budaya terhadap pertahanan manusiawi sangat jelas. Dalam budaya pelaporan yang positif, di mana orang merasa aman untuk menyuarkan keprihatinan tanpa takut disalahkan, karyawan menjadi sensor risiko yang sangat efektif. Mereka secara proaktif mengidentifikasi dan melaporkan kondisi tidak aman, secara efektif "menutup lubang" sebelum dapat menyebabkan kerugian. Sebaliknya, dalam blame culture, orang menyembunyikan masalah, membiarkan lubang-lubang laten tumbuh tanpa terdeteksi.

Budaya juga sangat memengaruhi pertahanan prosedural. Dalam budaya kepatuhan yang kuat, mengikuti prosedur dilihat sebagai tanda profesionalisme, dan penyimpangan tidak ditoleransi. Manajemen memimpin dengan memberi contoh dan memastikan prosedur praktis dan relevan. Sebaliknya, dalam budaya yang berfokus pada produksi, prosedur sering dilihat sebagai hambatan birokrasi. Pelanggaran rutin menjadi norma, dan lapisan pertahanan prosedural menjadi tidak relevan dalam praktik.

Bahkan pertahanan teknis dipengaruhi oleh budaya. Dalam budaya proaktif, organisasi secara aktif mencari dan berinvestasi dalam teknologi keselamatan terbaik. Program pemeliharaan dipandang sebagai hal yang penting. Sebaliknya, dalam budaya reaktif, perbaikan teknis hanya dilakukan setelah terjadi kecelakaan, dan pemeliharaan sering kali ditunda untuk menghemat biaya. Alarm dan sistem keselamatan mungkin secara rutin diabaikan atau bahkan sengaja dinonaktifkan jika dianggap mengganggu produksi.

Budaya keselamatan yang kuat memiliki beberapa karakteristik yang dapat diidentifikasi:

- a. Komitmen kepemimpinan yang terlihat: Para pemimpin secara konsisten menunjukkan bahwa keselamatan adalah nilai inti.
- b. Komunikasi terbuka: Informasi tentang risiko dan insiden dibagikan secara bebas.
- c. Keadilan (*Justness*): Ada sistem yang jelas dan adil untuk menangani kesalahan dan pelanggaran (*Just Culture*).
- d. Pembelajaran organisasi: Organisasi memiliki obsesi untuk belajar dari kegagalan dan keberhasilan.
- e. Keterlibatan karyawan: Pekerja diberdayakan dan dilibatkan secara aktif dalam semua aspek program K3.

Membangun dan memelihara budaya seperti ini adalah salah satu tanggung jawab terpenting dari manajemen puncak. Ini adalah proses jangka panjang yang membutuhkan upaya yang konsisten dan berkelanjutan. Namun, hasilnya adalah sistem pertahanan yang jauh lebih tangguh, di mana setiap lapisan diperkuat oleh komitmen bersama terhadap keselamatan. Budaya yang lemah, di sisi lain, adalah kondisi laten paling mendasar yang secara sistematis akan merusak setiap pertahanan yang coba dibangun oleh organisasi.

## **D. Penerapan Model untuk Prediksi dan Pencegahan Kecelakaan**

Nilai sebenarnya dari Model Keju Swiss tidak hanya terletak pada kemampuannya untuk menjelaskan kecelakaan secara retrospektif,

tetapi juga pada potensinya sebagai alat untuk analisis proaktif dan pencegahan. Jika kita dapat memahami bagaimana lubang-lubang dibuat dan bagaimana mereka sejajar, maka kita dapat mulai mengembangkan strategi untuk secara sengaja mencegah kesejajaran tersebut terjadi. Menggunakan model ini secara proaktif mengubahnya dari alat autopsi menjadi alat diagnosis, memungkinkan organisasi untuk mengidentifikasi dan mengatasi kelemahan sistemik sebelum mereka berkontribusi pada kegagalan.

Pendekatan proaktif ini mengharuskan organisasi untuk secara teratur dan sistematis memeriksa kesehatan lapisan pertahanannya. Ini melibatkan "berburu lubang" secara aktif, daripada menunggu lubang-lubang itu menampakkkan diri melalui sebuah insiden. Ini adalah pergeseran dari sikap reaktif ("mari kita selidiki apa yang salah") ke sikap proaktif dan bahkan prediktif ("mari kita bayangkan apa yang *bisa* salah dan perkuat pertahanan kita sekarang").

Aplikasi proaktif dari model ini dapat mengambil beberapa bentuk. Salah satu teknik yang kuat adalah analisis *pre-mortem*, di mana sebuah tim membayangkan bahwa sebuah proyek atau operasi telah gagal total dan kemudian bekerja mundur untuk mengidentifikasi kemungkinan lintasan kegagalan melalui berbagai lapisan pertahanan. Teknik ini membantu mengatasi optimisme yang berlebihan dan menyoroti kelemahan yang mungkin terlewatkan.

Model ini juga dapat digunakan untuk memprioritaskan upaya perbaikan. Dengan memetakan pertahanan yang ada untuk risiko tertentu, organisasi dapat mengidentifikasi di mana pertahanan mereka paling lemah atau di mana mereka terlalu bergantung pada satu jenis pertahanan saja (misalnya, terlalu banyak mengandalkan prosedur dan terlalu sedikit pada kontrol rekayasa). Ini memungkinkan mereka untuk mengalokasikan sumber daya secara lebih strategis untuk memperkuat pertahanan yang paling kritis atau yang paling rapuh.

Bagian ini akan membahas lebih lanjut tentang bagaimana Model Keju Swiss dapat digunakan sebagai alat proaktif untuk analisis, identifikasi pertahanan kritis, dan akan diakhiri dengan sebuah studi kasus yang

menunjukkan penerapan model ini dalam analisis kecelakaan nyata, yang mengilustrasikan bagaimana konsep-konsep ini bersatu dalam praktik.

**Analogi/Contoh Kasus:** Penerapan proaktif Model Keju Swiss mirip dengan cara tim pemadam kebakaran elit merencanakan perlindungan terhadap kebakaran hutan. Mereka tidak hanya menunggu kebakaran terjadi dan kemudian bereaksi. Secara proaktif, mereka menganalisis lanskap untuk mengidentifikasi area dengan bahan bakar kering yang menumpuk (kondisi laten). Mereka membangun jalur api (*firebreaks*) (pertahanan rekayasa). Mereka mengembangkan rencana evakuasi (pertahanan prosedural). Dan mereka melatih kru dan menempatkan menara pengintai (pertahanan manusiawi). Mereka bahkan melakukan pembakaran terkendali untuk mengurangi bahan bakar, secara sengaja “menguji” sistem mereka dalam kondisi yang terkendali. Ini semua adalah tentang mengidentifikasi dan menutup “lubang” di pertahanan mereka sebelum petir (pemicu) menyambar.

### 1. Menggunakan Model untuk Analisis Proaktif (Pre-Mortem)

Analisis *pre-mortem* adalah teknik manajemen risiko yang kuat yang membalikkan proses perencanaan tradisional. Alih-alih bertanya, “Apa yang bisa kita lakukan agar proyek ini berhasil?”, tim diminta untuk membayangkan masa depan di mana proyek atau operasi tersebut telah gagal total dan kemudian bertanya, “Apa yang salah?”. Teknik ini sangat efektif untuk mengatasi bias optimisme dan pemikiran kelompok (*groupthink*) yang sering kali menghalangi tim untuk melihat potensi risiko secara realistis.

Model Keju Swiss menyediakan kerangka kerja yang sangat baik untuk menyusun analisis *pre-mortem*. Prosesnya dapat berjalan sebagai berikut:

- a. Tetapkan Skenario Kegagalan: Tim berkumpul sebelum memulai proyek atau operasi berisiko tinggi (misalnya, *turnaround* pabrik besar, peluncuran produk baru, atau bahkan hanya tugas non-rutin yang kompleks). Fasilitator mengumumkan, “Bayangkan kita berada enam bulan di masa depan. Proyek ini telah menjadi bencana besar. Telah terjadi kecelakaan fatal, kerusakan lingkungan yang parah, dan kerugian finansial yang masif.”

- b. Identifikasi Kegagalan Aktif: Setiap anggota tim kemudian secara individu menuliskan semua alasan yang mungkin mengapa kegagalan ini terjadi, berfokus pada *active failures* yang mungkin menjadi pemicu langsung. Misalnya, "Operator salah mengkalibrasi sensor kritis," atau "Kru konstruksi melanggar prosedur izin kerja panas."
- c. Petakan Kegagalan ke Lapisan Pertahanan: Fasilitator kemudian memandu tim untuk menggunakan Model Keju Swiss sebagai peta. Untuk setiap kegagalan aktif yang diidentifikasi, tim bertanya: "Agar kesalahan ini bisa terjadi dan menyebabkan bencana, lubang apa yang harus ada di lapisan pertahanan di belakangnya?"
  - 1) Lapisan Pengawasan: "Apakah penyelia mungkin terlalu sibuk untuk memeriksa pekerjaan kalibrasi?"
  - 2) Lapisan Prosedur/Peralatan: "Apakah prosedur kalibrasi itu sendiri membingungkan? Apakah alat kalibrasi yang digunakan mungkin rusak?"
  - 3) Lapisan Organisasi: "Apakah ada tekanan jadwal yang ekstrim yang mendorong operator untuk terburu-buru? Apakah pelatihan kalibrasi kita memadai?"
- d. Bangun Lintasan Kecelakaan: Tim kemudian mencoba untuk membangun beberapa "lintasan peluang kecelakaan" yang masuk akal, menunjukkan bagaimana serangkaian lubang yang spesifik di berbagai lapisan bisa sejajar untuk menghasilkan skenario bencana yang dibayangkan.
- e. Kembangkan Rencana Mitigasi: Setelah lintasan kegagalan potensial ini diidentifikasi, tim kemudian beralih ke mode pencegahan. "Apa yang bisa kita lakukan *sekarang* untuk menutup lubang-lubang ini?". Ini menghasilkan daftar tindakan preventif yang konkret dan ditargetkan yang dapat dimasukkan ke dalam rencana proyek.

Dengan menggunakan Model Keju Swiss dalam analisis *pre-mortem*, tim dipaksa untuk berpikir secara sistemik tentang kegagalan. Ini mengalihkan fokus dari hanya mencoba mencegah kesalahan individu menjadi memperkuat seluruh sistem pertahanan. Ini adalah cara yang sangat efektif untuk secara proaktif mengidentifikasi dan mengatasi kondisi-

kondisi laten sebelum mereka memiliki kesempatan untuk berkontribusi pada kegagalan nyata.

## 2. Mengidentifikasi Pertahanan Kritis yang Perlu Diperkuat

Tidak semua lapisan pertahanan diciptakan sama. Dalam sistem apa pun, akan ada beberapa pertahanan yang dianggap kritis, yaitu, pertahanan yang jika gagal, akan secara signifikan meningkatkan kemungkinan kecelakaan. Ini mungkin karena mereka adalah satu-satunya pertahanan untuk bahaya tertentu, atau karena mereka melindungi dari konsekuensi yang sangat parah. Model Keju Swiss dapat digunakan sebagai alat untuk mengidentifikasi pertahanan-pertahanan kritis ini dan memfokuskan sumber daya yang terbatas untuk memastikan keandalannya.

Proses ini dimulai dengan pemetaan pertahanan. Untuk setiap bahaya utama atau skenario kecelakaan yang teridentifikasi dalam penilaian risiko, organisasi harus secara eksplisit memetakan semua lapisan pertahanan yang ada untuk mencegah atau memitigasi skenario tersebut. Ini dapat divisualisasikan menggunakan diagram Keju Swiss yang disesuaikan.

Setelah pertahanan dipetakan, langkah selanjutnya adalah evaluasi kualitas dan keandalan dari setiap lapisan. Pertanyaan-pertanyaan yang perlu diajukan meliputi:

- a. Seberapa kuat lapisan ini?: Apakah ini pertahanan teknis yang andal atau pertahanan prosedural yang lemah?
- b. Seberapa besar kemungkinan adanya lubang di lapisan ini?: Berdasarkan data insiden masa lalu, audit, dan umpan balik pekerja, seberapa sering pertahanan ini gagal atau dilewati?
- c. Apa konsekuensi dari kegagalan lapisan ini?: Apakah ada lapisan lain di belakangnya untuk menangkap kegagalan, atau apakah ini adalah garis pertahanan terakhir?
- d. Apakah lapisan ini rentan terhadap kegagalan mode bersama?: Apakah kegagalannya dapat menyebabkan kegagalan lapisan lain?

Analisis ini akan menyoroti pertahanan-pertahanan kritis. Pertahanan kritis sering kali adalah yang memiliki skor rendah pada kualitas atau keandalan tetapi melindungi dari konsekuensi yang tinggi. Mereka juga

bisa menjadi pertahanan yang saat ini menjadi satu-satunya penghalang untuk skenario bencana.

Setelah pertahanan kritis diidentifikasi, maka organisasi dapat mengembangkan strategi penguatan yang ditargetkan. Ini mungkin melibatkan:

- a. Menambah Redundansi: Jika sebuah pertahanan kritis adalah satu-satunya penghalang, organisasi mungkin memutuskan untuk menambahkan lapisan pertahanan baru (misalnya, menambahkan sistem alarm otomatis untuk mendukung pemeriksaan visual oleh operator).
- b. Meningkatkan Keandalan: Jika pertahanan kritis yang ada terbukti tidak dapat diandalkan (misalnya, prosedur yang sering dilanggar), upaya dapat difokuskan untuk merancang ulang prosedur tersebut agar lebih praktis dan kuat.
- c. Peningkatan Pemantauan: Pertahanan kritis harus menjadi subjek pemantauan, pengujian, dan audit yang lebih sering dan lebih ketat daripada pertahanan non-kritis. *Leading indicators* spesifik dapat dikembangkan untuk melacak kesehatan pertahanan-pertahanan ini.

Dengan menggunakan Model Keju Swiss untuk mengidentifikasi dan memprioritaskan pertahanan, organisasi dapat bergerak dari pendekatan "satu ukuran untuk semua" dalam manajemen keselamatan ke pendekatan yang lebih cerdas dan berbasis risiko. Ini memastikan bahwa sumber daya yang paling berharga, waktu, uang, dan perhatian, diarahkan ke tempat yang paling dibutuhkan untuk mencegah kegagalan yang paling signifikan.

### 3. Kasus Studi Penerapan Model Keju Swiss

Salah satu contoh paling tragis dan paling banyak dianalisis yang dapat diilustrasikan dengan Model Keju Swiss adalah bencana ledakan anjungan pengeboran Deepwater Horizon di Teluk Meksiko pada tahun 2010, yang menewaskan 11 pekerja dan menyebabkan tumpahan minyak terbesar dalam sejarah AS. Investigasi setelahnya mengungkapkan bahwa bencana ini bukanlah hasil dari satu kesalahan tunggal, melainkan kulminasi dari serangkaian kegagalan teknis, manusiawi, dan organisasi yang menembus banyak lapisan pertahanan.

Mari kita terapkan Model Keju Swiss untuk menganalisis lintasan kecelakaan ini:

a. Lapisan #1: Keputusan Organisasi & Manajemen (BP, Transocean, Halliburton)

Lubang (Kondisi Laten): Budaya yang sangat berfokus pada penghematan biaya dan kecepatan, sering kali dengan mengorbankan keselamatan dan manajemen risiko. Proyek ini sudah jauh di belakang jadwal dan melebihi anggaran, menciptakan tekanan yang luar biasa untuk mengambil jalan pintas. Keputusan dibuat untuk menggunakan desain sumur yang lebih murah tetapi lebih berisiko (misalnya, menggunakan lebih sedikit *centralizers*), dan untuk melanjutkan meskipun ada hasil tes semen yang meragukan. Ini adalah lubang-lubang besar yang diciptakan oleh manajemen puncak.

b. Lapisan #2: Pengawasan & Perencanaan di Anjungan

Lubang (Kondisi Laten): Komunikasi yang buruk dan kebingungan tanggung jawab antara berbagai perusahaan yang bekerja di anjungan (BP sebagai pemilik, Transocean sebagai operator anjungan, Halliburton sebagai kontraktor semen). Ada beberapa contoh di mana kru dari perusahaan yang berbeda salah memahami atau gagal untuk secara efektif mengkomunikasikan tanda-tanda peringatan. Perencanaan untuk tes tekanan negatif (*negative pressure test*) yang krusial tidak memadai.

c. Lapisan #3: Pertahanan Teknis & Peralatan

Lubang (Kondisi Laten & Aktif): Beberapa kegagalan pada penghalang teknis kritis. Pertama, pekerjaan penyemenan di dasar sumur, yang merupakan penghalang pertama, ternyata cacat dan gagal mengisolasi cadangan hidrokarbon. Kedua, *Blowout Preventer* (BOP), yang merupakan pertahanan teknis terakhir yang gagal-aman, gagal untuk sepenuhnya menutup sumur dalam keadaan darurat, kemungkinan karena desainnya yang kompleks dan masalah pemeliharaan.

d. Lapisan #4: Prosedur & Interpretasi Tes

Lubang (Kondisi Laten & Aktif): Prosedur untuk melakukan dan menginterpretasikan tes tekanan negatif tidak diikuti dengan benar

atau disalahartikan oleh kru di anjungan. Mereka secara keliru menyimpulkan bahwa tes tersebut berhasil dan sumur aman, padahal ada indikasi yang jelas adanya kebocoran. Ini adalah *mistake* kritis yang didorong oleh bias optimisme dan tekanan untuk menyelesaikan pekerjaan.

e. Lapisan #5: Kinerja Kru & Tindakan Darurat

Lubang (Active Failure): Begitu *blowout* dimulai dan gas serta minyak menyembur ke anjungan, kru dihadapkan pada situasi yang berkembang pesat. Ada penundaan dalam mengaktifkan sistem darurat pada BOP. Sistem alarm gas dan kebakaran tidak berfungsi sebagaimana mestinya, yang menunda evakuasi.

Pada tanggal 20 April 2010, semua lubang ini sejajar. Keputusan yang berfokus pada biaya (Lapisan 1) menyebabkan penggunaan desain sumur yang lebih berisiko dan pekerjaan semen yang cacat (Lapisan 3). Tekanan jadwal (Lapisan 1) dan kebingungan tanggung jawab (Lapisan 2) menyebabkan salah tafsir terhadap tes kunci (Lapisan 4). Ketika sumur akhirnya gagal, pertahanan terakhir yang gagal-aman, yaitu BOP (Lapisan 3), juga gagal berfungsi. Kesalahan interpretasi oleh kru (Lapisan 5) adalah kegagalan aktif terakhir yang memungkinkan bencana terjadi. Kasus ini adalah ilustrasi yang sempurna tentang bagaimana keputusan yang dibuat di ruang rapat (lubang laten) menciptakan jalur yang hampir tak terhindarkan menuju kegagalan di lini depan.

## KESIMPULAN

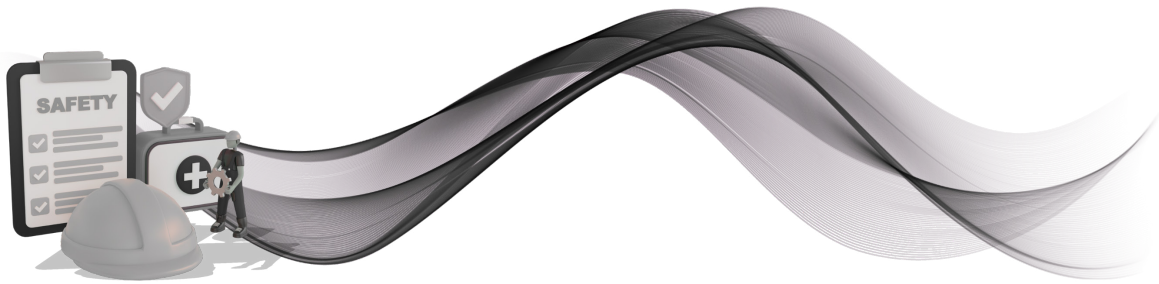
Model Keju Swiss James Reason, meskipun sederhana dalam konsepnya, memberikan kerangka kerja yang sangat kuat dan berpengaruh untuk memahami bagaimana kecelakaan terjadi di sistem yang kompleks. Bab ini telah membedah model tersebut, bergerak dari metafora visualnya ke aplikasi analitisnya. Kita telah melihat bagaimana model ini secara efektif menggambarkan pertahanan organisasi sebagai serangkaian irisan keju yang tidak sempurna, dan bagaimana kecelakaan terjadi ketika lubang-lubang di irisan ini, yang mewakili kegagalan aktif dan kondisi laten, secara sesaat sejajar.

Dengan mengidentifikasi berbagai jenis lubang di lapisan-lapisan pertahanan yang berbeda, mulai dari kegagalan pengawasan hingga kelemahan desain dan kesalahan operator, model ini memberikan peta jalan untuk investigasi kecelakaan yang sistemik. Ia secara visual memaksa kita untuk melihat melampaui kegagalan aktif di lini depan dan mencari akar penyebab yang lebih dalam pada keputusan-keputusan manajerial dan organisasi. Peran sentral manajemen puncak dalam menciptakan kondisi laten melalui keputusan tentang sumber daya, prioritas, dan budaya telah ditonjolkan sebagai faktor paling fundamental dalam membentuk kesehatan sistem pertahanan secara keseluruhan.

Lebih dari sekadar alat analisis reaktif, bab ini telah menunjukkan bagaimana Model Keju Swiss dapat digunakan secara proaktif untuk prediksi dan pencegahan. Teknik seperti analisis *pre-mortem* dan identifikasi pertahanan kritis memungkinkan organisasi untuk “berburu lubang” dan memperkuat sistem pertahanan mereka sebelum kegagalan terjadi. Studi kasus Deepwater Horizon memberikan contoh nyata yang gamblang tentang bagaimana serangkaian kegagalan di berbagai lapisan dapat berkolaborasi untuk menciptakan bencana, menggarisbawahi relevansi abadi dari model ini.

Pada dasarnya, Model Keju Swiss adalah alat untuk berpikir dan berkomunikasi tentang risiko sistemik. Ia memberikan bahasa yang sama bagi semua orang di organisasi, dari eksekutif hingga operator, untuk membahas kelemahan dan pertahanan. Dengan fondasi visual dan konseptual ini, kita sekarang siap untuk menjelajahi model-model lain yang lebih terperinci, seperti Model SHELL, yang akan membantu kita untuk lebih fokus pada antarmuka spesifik antara manusia dan komponen sistem lainnya.

**DUMMYY**



# BAB 6

## MODEL SHELL DAN APLIKASI UNTUK ANTARMUKA MANUSIA-SISTEM

### PENDAHULUAN

Jika Model Keju Swiss yang dibahas pada bab sebelumnya memberikan kita pandangan “makro” atau dari ketinggian tentang bagaimana pertahanan sistemik dapat gagal, maka kita sekarang memerlukan “mikroskop” untuk memeriksa secara detail titik di mana kegagalan itu sering kali berawal: pada antarmuka langsung antara seorang individu dan lingkungan kerjanya. Model Keju Swiss sangat baik dalam mengilustrasikan mengapa kecelakaan terjadi, tetapi ia tidak secara spesifik merinci *bagaimana* interaksi yang salah di lini depan terjadi. Untuk mengisi celah ini, kita beralih ke Model SHELL, sebuah kerangka kerja konseptual yang fundamental dalam disiplin ilmu *human factors*.

Model SHELL, yang awalnya dikembangkan oleh Edwards pada tahun 1972 dan kemudian dimodifikasi oleh Hawkins pada tahun 1984, adalah model yang berpusat pada manusia. Namanya merupakan akronim dari komponen-komponennya: **S**oftware (perangkat lunak/prosedur), **H**ardware (perangkat keras/teknologi), **E**nvironment (lingkungan), dan **L**iveware (manusia). Model ini secara visual menempatkan komponen

*Liveware* (individu) di tengah, dan menganalisis bagaimana individu ini berinteraksi dengan tiga komponen lainnya, serta dengan individu lain (*Liveware* lainnya).

Filosofi inti dari model ini adalah bahwa kecelakaan dan *human error* jarang sekali disebabkan oleh kegagalan satu komponen saja, terutama bukan karena kegagalan tunggal dari komponen manusia. Sebaliknya, masalah muncul dari ketidakcocokan (*mismatch*) pada antarmuka antara komponen-komponen tersebut. Ketika komponen-komponen sistem tidak "pas" satu sama lain, ketegangan dan tekanan tercipta pada komponen manusia yang berada di pusatnya, yang harus menjembatani kesenjangan tersebut. Ketegangan inilah yang sering kali bermanifestasi sebagai *human error*.

Bab ini akan membedah Model SHELL sebagai alat analisis dan desain yang praktis. Kita akan memulai dengan menguraikan setiap komponen model secara terperinci. Fokus utamanya adalah pada komponen *Liveware* pusat, menekankan pentingnya memahami kapabilitas dan keterbatasan manusia, baik fisik, fisiologis, maupun psikologis, yang harus diakomodasi oleh sistem, bukan sebaliknya. Komponen *Software*, *Hardware*, dan *Environment* kemudian akan didefinisikan dalam konteks interaksinya dengan manusia.

Setelah memahami komponen-komponennya, kita akan melakukan analisis sistematis terhadap potensi ketidakcocokan di setiap antarmuka: antara manusia dan mesin (L-H), manusia dan prosedur (L-S), manusia dan lingkungan (L-E), dan yang sangat penting, antara manusia dan manusia lainnya (L-L). Melalui contoh-contoh konkret, akan ditunjukkan bagaimana ketidakcocokan ini secara langsung menciptakan kondisi yang provokatif terhadap kesalahan.

Lebih dari sekadar alat analisis reaktif, Model SHELL adalah panduan yang sangat baik untuk desain proaktif. Bab ini akan mengilustrasikan bagaimana model ini dapat diterapkan dalam perancangan stasiun kerja, tugas, dan prosedur yang lebih aman dan lebih efisien. Dengan secara sadar mempertimbangkan setiap antarmuka SHELL selama proses desain,

kita dapat secara proaktif menghilangkan “jebakan kesalahan” sebelum mereka memiliki kesempatan untuk menjerat seorang operator.

Sebagai puncaknya, sebuah studi kasus mendalam dari industri penerbangan akan digunakan untuk menunjukkan kekuatan Model SHELL dalam mengungkap jaring kausal yang kompleks di balik sebuah kecelakaan nyata. Analisis ini akan menunjukkan bagaimana kegagalan di berbagai antarmuka dapat berinteraksi dan bergabung untuk menciptakan bencana, dan bagaimana wawasan dari analisis tersebut dapat mengarah pada rekomendasi mitigasi yang kuat dan berkelanjutan.

Dengan menguasai Model SHELL, praktisi K3 akan memiliki alat yang dapat digunakan sehari-hari untuk mengevaluasi tugas, menyelidiki insiden, dan berkontribusi pada desain sistem kerja yang lebih manusiawi dan tahan terhadap kesalahan.

## A. Komponen Model SHELL

Model SHELL adalah kerangka kerja konseptual yang digambarkan sebagai diagram balok bangunan, dengan komponen *Liveware* (manusia) di tengah, dikelilingi oleh komponen *Hardware*, *Software*, dan *Environment*. Keempat blok ini harus dirancang agar pas satu sama lain. Ketika tepi-tepi blok ini tidak cocok, misalnya, tepi blok *Hardware* terlalu “tajam” atau “berbentuk aneh” untuk blok *Liveware*, maka akan timbul masalah. Fokus dari analisis SHELL adalah pada antarmuka di antara blok-blok ini, karena di sinilah potensi kegagalan sistem sering kali berada.

Pusat dari model ini adalah *Liveware*, yang mewakili individu manusia. Ini adalah komponen yang paling kritis dan fleksibel, tetapi juga yang paling rentan terhadap variasi kinerja. Karakteristik dari komponen *Liveware*, seperti ukuran tubuh, kemampuan pemrosesan informasi, dan toleransi terhadap stres, sangat menentukan bagaimana ia akan berinteraksi dengan komponen-komponen lainnya. Analisis SHELL selalu dimulai dan diakhiri dengan mempertimbangkan manusia.

Komponen *Hardware* merujuk pada elemen-elemen fisik dari sistem kerja. Ini termasuk mesin, alat, panel kontrol, kursi, kendaraan, dan tata letak stasiun kerja. Antarmuka antara *Liveware* dan *Hardware* (L-H) adalah

bidang klasik dari ergonomi, yang berkaitan dengan pencocokan desain fisik teknologi dengan kapabilitas dan keterbatasan tubuh manusia.

Komponen *Software* mencakup semua aspek “lunak” atau non-fisik dari sistem yang mengatur proses kerja. Ini tidak hanya merujuk pada perangkat lunak komputer, tetapi juga prosedur, manual, *checklists*, aturan, regulasi, simbologi, dan bahkan norma-norma tidak tertulis. Antarmuka antara *Liveware* dan *Software* (L-S) adalah tentang seberapa baik manusia dapat memahami dan menggunakan “aturan main” dari sistem tersebut.

Komponen *Environment* adalah konteks di mana sistem L-H-S beroperasi. Ini mencakup lingkungan fisik, seperti pencahayaan, kebisingan, dan suhu, serta lingkungan organisasi yang lebih luas, seperti iklim keselamatan, tekanan produksi, dan hubungan industrial. Antarmuka antara *Liveware* dan *Environment* (L-E) menganalisis bagaimana faktor-faktor kontekstual ini memengaruhi kinerja manusia.

Model ini juga secara implisit dan terkadang eksplisit mencakup interaksi antara *Liveware* pusat dengan *Liveware* lainnya. Antarmuka *Liveware-Liveware* (L-L) ini sangat penting karena sebagian besar pekerjaan dilakukan dalam tim. Ini mencakup bidang-bidang seperti komunikasi, kepemimpinan, kerja sama, dan manajemen sumber daya tim. Dengan membedah sistem kerja menjadi komponen-komponen ini, Model SHELL memberikan cara yang terstruktur untuk mengidentifikasi potensi masalah dan merancang intervensi yang ditargetkan.

**Analogi/Contoh Kasus:** Bayangkan seorang koki yang bekerja di dapur restoran yang sibuk sebagai sebuah sistem SHELL. *Liveware* adalah koki itu sendiri, dengan keterampilan, tingkat kelelahan, dan stresnya. *Hardware* adalah kompor, pisau, wajan, dan tata letak dapurnya. *Software* adalah resep, pesanan dari pelanggan, dan peraturan kebersihan makanan. *Environment* adalah panas, kebisingan, dan tekanan waktu di dapur. *Liveware* lain adalah para pelayan dan koki lainnya. Masalah dapat muncul di setiap antarmuka: gagang pisau yang licin (L-H), resep yang ditulis tidak jelas (L-S), panas yang berlebihan menyebabkan dehidrasi (L-E), atau pesanan yang salah dikomunikasikan oleh pelayan (L-L). Kualitas hidangan dan keselamatan di dapur bergantung pada seberapa baik semua komponen ini “pas” bersama.

## 1. Liveware (Manusia) sebagai Pusat Model (Liveware-Self)

Dalam Model SHELL, blok pusat, *Liveware* (L), mewakili individu manusia, operator, pilot, teknisi, dokter, yang menjadi fokus analisis. Menempatkan manusia di tengah bukanlah kebetulan; ini adalah pernyataan filosofis bahwa sistem harus dirancang untuk mengakomodasi manusia, bukan sebaliknya. Sebelum kita dapat menganalisis interaksi manusia dengan komponen lain, kita harus terlebih dahulu memahami karakteristik, kapabilitas, dan keterbatasan dari komponen pusat ini.

Analisis *Liveware* mencakup berbagai dimensi. Dimensi fisik berkaitan dengan atribut tubuh manusia, sebuah bidang yang dipelajari oleh antropometri. Ini termasuk ukuran tubuh, tinggi, berat, jangkauan, dan kekuatan. Ketidakcocokan terjadi ketika desain *Hardware* tidak memperhitungkan variasi dalam dimensi-dimensi ini, misalnya, sebuah panel kontrol yang tidak dapat dijangkau oleh operator dengan tinggi badan di bawah rata-rata.

Dimensi fisiologis berkaitan dengan bagaimana tubuh manusia berfungsi dan merespons tuntutan pekerjaan. Ini termasuk kebutuhan akan oksigen, makanan, dan istirahat, serta keterbatasan indera kita (penglihatan, pendengaran). Faktor-faktor seperti kelelahan, stres, ritme sirkadian (jam tubuh), dan dampak dari penyakit atau obat-obatan sangat memengaruhi kinerja dan merupakan bagian penting dari analisis *Liveware*. Sistem kerja yang mengabaikan kebutuhan fisiologis dasar ini, misalnya, dengan jadwal kerja yang berlebihan, sedang menciptakan prasyarat untuk kesalahan.

Dimensi psikologis dan kognitif adalah yang paling kompleks. Ini mencakup bagaimana manusia memproses informasi, belajar, membuat keputusan, dan memecahkan masalah. Ini melibatkan pemahaman tentang:

### a. Kapasitas memori

Baik memori jangka pendek (kerja) yang terbatas maupun memori jangka panjang.

### b. Perhatian dan persepsi

Bagaimana kita menyaring informasi dan bagaimana persepsi kita dapat dibodohi oleh ilusi.

c. Pengambilan keputusan

Ketergantungan kita pada heuristik (jalan pintas mental) dan kerentanan kita terhadap bias kognitif.

d. Faktor kepribadian dan motivasi

Meskipun bukan prediktor kesalahan yang kuat, faktor-faktor seperti motivasi, sikap, dan kepuasan kerja dapat memengaruhi kinerja.

Selain interaksi dengan dunia luar, ada juga antarmuka internal yang penting, yang kadang-kadang disebut *Liveware-Self (L-S)*. Ini merujuk pada hubungan antara berbagai aspek individu itu sendiri. Misalnya, bagaimana kondisi fisik (kelelahan) memengaruhi kondisi psikologis (pengambilan keputusan menjadi lebih buruk). Atau bagaimana stres karena masalah pribadi (aspek psikologis) dapat bermanifestasi sebagai gejala fisik dan mengganggu kinerja. Kesadaran diri dan kemampuan untuk mengelola keadaan internal sendiri adalah bagian penting dari kinerja yang andal.

Poin paling krusial dari analisis *Liveware* adalah pengakuan akan variabilitas kinerja manusia. Tidak ada dua orang yang persis sama, dan kinerja satu orang pun tidak akan sama dari hari ke hari atau bahkan dari jam ke jam. Desain sistem yang kaku dan tidak fleksibel yang menuntut kinerja yang konsisten seperti mesin pasti akan gagal. Sebaliknya, sistem yang tangguh adalah sistem yang dirancang dengan pemahaman yang mendalam tentang variasi dan keterbatasan manusia, dan yang menyediakan toleransi dan dukungan untuk mengakomodasi variabilitas tersebut. Memahami *Liveware* adalah langkah pertama dan terpenting dalam menciptakan kesesuaian di seluruh sistem SHELL.

## 2. Interaksi dengan Software (Prosedur, Dokumen, Aturan)

Komponen *Software (S)* dalam model SHELL mencakup semua aspek non-fisik yang mengatur sistem. Ini adalah "aturan main" yang memberi tahu komponen *Liveware* bagaimana harus beroperasi di dalam sistem. Komponen ini sangat luas dan mencakup segala sesuatu mulai dari prosedur operasi standar (SOP), manual pemeliharaan, dan *checklists*, hingga peraturan pemerintah, kebijakan perusahaan, peta, dan bahkan program komputer yang memandu tugas.

Antarmuka Liveware-Software (L-S) adalah tentang seberapa baik manusia dapat memahami, menafsirkan, dan menerapkan “aturan” ini dalam praktik. Ketidakcocokan pada antarmuka ini adalah sumber yang sangat umum dari *rule-based mistakes* dan pelanggaran. Idealnya, *Software* harus dirancang agar jelas, ringkas, akurat, mudah diakses, dan relevan dengan tugas yang sedang dilakukan. Sayangnya, ini sering kali tidak terjadi.

Salah satu bentuk ketidakcocokan L-S yang paling umum adalah prosedur yang ditulis dengan buruk. Prosedur mungkin menggunakan jargon yang ambigu, kalimat yang terlalu panjang dan rumit, atau asumsi yang salah tentang pengetahuan awal pengguna. Prosedur yang ditulis oleh insinyur di kantor mungkin tidak mencerminkan realitas dan kendala yang dihadapi oleh teknisi di lapangan, menciptakan kesenjangan antara *work-as-imagined* dan *work-as-done*. Ketika prosedur tidak praktis, mereka akan diabaikan, dan pertahanan prosedural pun runtuh.

Desain *checklist* juga merupakan area kritis. *Checklist* yang dirancang dengan baik adalah alat kognitif yang sangat kuat untuk mengurangi *lapses* memori. Namun, *checklist* yang terlalu panjang, tidak terorganisir secara logis, atau berisi item-item yang tidak relevan akan menjadi beban dan mendorong orang untuk mengambil jalan pintas.

Simbologi dan penyajian informasi adalah bagian lain dari antarmuka L-S. Peta yang sulit dibaca, diagram pengkabelan yang membingungkan, atau ikon pada antarmuka perangkat lunak yang tidak intuitif semuanya dapat menyebabkan salah tafsir dan kesalahan. Standardisasi dalam simbologi sangat penting untuk meminimalkan kebingungan, terutama dalam industri di mana personel mungkin bekerja dengan berbagai jenis peralatan.

Untuk menciptakan kesesuaian yang baik pada antarmuka L-S, prinsip-prinsip desain yang berpusat pada pengguna harus diterapkan pada pengembangan semua bentuk *Software*. Ini berarti:

- a. Melibatkan pengguna akhir. Teknisi, operator, dan pilot harus menjadi bagian dari tim yang menulis dan memvalidasi prosedur yang akan mereka gunakan.

- b. Menggunakan bahasa yang jelas dan sederhana. Hindari jargon yang tidak perlu dan gunakan kalimat aktif yang singkat.
- c. Memanfaatkan format visual. Gunakan diagram alir, gambar, dan kode warna untuk membuat informasi lebih mudah dipahami.
- d. Memastikan aksesibilitas. Prosedur harus tersedia di tempat dan waktu yang dibutuhkan, dalam format yang mudah digunakan (misalnya, di tablet yang kokoh, bukan di buku tebal di kantor).
- e. Memiliki proses tinjauan dan pembaruan yang kuat. *Software* harus menjadi dokumen yang "hidup" yang terus diperbarui untuk mencerminkan perubahan dalam *Hardware* dan praktik kerja.

Antarmuka L-S pada dasarnya adalah tentang komunikasi antara perancang sistem dan pengguna akhir. Jika komunikasi ini tidak jelas, maka kesalahpahaman dan kesalahan tidak dapat dihindari.

### 3. **Interaksi dengan Hardware (Mesin, Alat, Tata Letak)**

Komponen *Hardware* (H) merujuk pada semua elemen fisik, mesin, dan teknologi dalam sistem kerja. Ini mencakup spektrum yang luas, mulai dari objek sederhana seperti palu dan obeng, hingga sistem yang sangat kompleks seperti kokpit pesawat, ruang kontrol nuklir, atau peralatan bedah robotik. Komponen ini juga mencakup desain stasiun kerja, kursi, dan tata letak fisik tempat kerja.

Antarmuka *Liveware-Hardware* (L-H) adalah tentang hubungan fisik antara manusia dan mesin. Ini adalah domain tradisional ergonomi, yang berfokus pada perancangan *Hardware* agar sesuai dengan kapabilitas dan keterbatasan fisik dan kognitif manusia. Ketidakcocokan pada antarmuka L-H adalah penyebab langsung dari banyak *slips*, *mistakes*, cedera regangan berulang, dan kelelahan. Tujuannya adalah untuk merancang *Hardware* yang terasa intuitif, nyaman, dan "alami" untuk digunakan.

Salah satu area utama dari antarmuka L-H adalah desain kontrol dan tampilan. Kontrol (tombol, tuas, sakelar) harus dirancang agar mudah dijangkau, dibedakan, dan dioperasikan. Tampilan (dial, layar, lampu peringatan) harus menyajikan informasi dengan cara yang jelas, tidak ambigu, dan tepat waktu. Ketidakcocokan yang umum terjadi meliputi:

- a. Kontrol yang mirip. Sakelar untuk fungsi yang sangat berbeda (misalnya, menaikkan roda pendarat vs. menaikkan penutup sayap/*flaps*) yang terlihat dan terasa identik dan diletakkan berdampingan.
- b. Kurangnya umpan balik. Sebuah tombol yang tidak memberikan “klik” atau sinyal visual saat ditekan, membuat operator tidak yakin apakah input mereka telah diterima.
- c. Pemetaan yang tidak wajar. Hubungan antara kontrol dan efeknya tidak intuitif. Misalnya, memutar tombol ke kanan untuk menggerakkan sesuatu ke kiri.

Area penting lainnya adalah ergonomi fisik. Ini berkaitan dengan pencocokan desain *Hardware* dengan ukuran dan bentuk tubuh manusia (antropometri) serta cara tubuh bergerak (biomekanika). Ketidakcocokan di sini dapat menyebabkan masalah kesehatan jangka panjang dan kelelahan jangka pendek. Contohnya termasuk kursi yang tidak mendukung punggung dengan baik, alat yang menyebabkan getaran berlebihan pada tangan, atau stasiun perakitan yang mengharuskan pekerja untuk terus-menerus membungkuk atau menjangkau.

Tata letak stasiun kerja secara keseluruhan juga merupakan bagian dari antarmuka L-H. Item yang paling sering digunakan harus ditempatkan dalam jangkauan yang mudah. Alur kerja harus dirancang secara logis untuk meminimalkan gerakan yang tidak perlu. Peringatan visual dan auditori harus dapat dilihat dan didengar dengan jelas dari posisi kerja normal.

Untuk memastikan kesesuaian L-H, para perancang harus secara aktif mempertimbangkan pengguna akhir. Ini melibatkan penggunaan data antropometrik untuk merancang bagi rentang populasi yang luas (bukan hanya “rata-rata” pria), melakukan pengujian kegunaan (*usability testing*) dengan prototipe, dan menerapkan prinsip-prinsip desain yang sudah mapan seperti standarisasi, konsistensi, dan umpan balik. Sebuah mesin yang dirancang dengan indah dari sudut pandang rekayasa masih merupakan desain yang buruk jika pengguna manusia tidak dapat mengoperasikannya dengan andal dan aman.

## B. Analisis Interaksi dan Ketidaksesuaian (*Mismatch*) Antarkomponen

Kekuatan sebenarnya dari Model SHELL tidak terletak pada pendefinisian komponen-komponennya secara terpisah, tetapi pada penggunaannya sebagai kerangka kerja untuk secara sistematis menganalisis antarmuka di antara mereka. Di sinilah "karet bertemu jalan", di mana teori *human factors* bertemu dengan realitas operasional. Mismatch atau ketidakcocokan pada antarmuka ini adalah di mana ketegangan dalam sistem muncul, menciptakan kondisi yang subur untuk *human error*. Seorang investigator kecelakaan atau perancang sistem dapat menggunakan model ini sebagai daftar periksa mental untuk memastikan bahwa semua interaksi kritis telah dipertimbangkan.

Analisis ini melibatkan pengambilan komponen *Liveware* pusat dan secara berurutan "mencocokkannya" dengan setiap komponen lainnya. Apakah *Liveware* cocok dengan *Hardware*? Apakah *Liveware* cocok dengan *Software*? Apakah *Liveware* cocok dengan *Environment*? Dan yang tidak kalah penting, apakah *Liveware* cocok dengan *Liveware* lain? Dengan mengajukan pertanyaan-pertanyaan ini, kita dapat bergerak dari analisis yang berfokus pada "apa yang salah dengan orang ini?" menjadi analisis yang lebih kuat tentang "apa yang salah dengan hubungan antara orang ini dan sistem di sekitarnya?".

Misalnya, seorang operator mungkin dilaporkan "tidak memperhatikan" alarm (*active failure*). Analisis SHELL akan menolak penjelasan yang dangkal ini dan memaksa kita untuk bertanya lebih dalam dengan memeriksa setiap antarmuka:

1. L-H Mismatch?: Apakah alarm itu sendiri dirancang dengan buruk? Apakah terlalu pelan, atau apakah lampu peringatannya terlalu redup atau berada di luar bidang pandang utama operator?
2. L-S Mismatch?: Apakah prosedur respons alarm terlalu rumit atau tidak jelas? Apakah operator pernah dilatih tentang arti dari alarm spesifik ini?
3. L-E Mismatch?: Apakah kebisingan di lingkungan kerja menutupi alarm pendengaran? Apakah ada terlalu banyak alarm lain yang berbunyi

pada saat yang sama (alarm flooding), menyebabkan kelebihan beban kognitif?

4. L-L Mismatch?: Apakah ada anggota tim lain yang seharusnya juga mendengar alarm tetapi gagal berkomunikasi? Apakah ada budaya di mana menunjukkan masalah dianggap negatif?

Seperti yang ditunjukkan oleh contoh ini, satu kegagalan aktif dapat memiliki akar penyebab potensial di berbagai antarmuka. Analisis yang komprehensif akan memeriksa semuanya. Bagian selanjutnya akan menyelami lebih dalam setiap jenis ketidakcocokan ini, memberikan contoh-contoh spesifik tentang bagaimana mereka bermanifestasi dan bagaimana mereka berkontribusi pada kegagalan.

**Analogi/Contoh Kasus:** Bayangkan mencoba merakit perabotan dari IKEA. Anda adalah *Liveware*. Perabotan, sekrup, dan kunci L adalah *Hardware*. Instruksi manual bergambar adalah *Software*. Pencahayaan di kamar Anda adalah *Environment*. Pasangan Anda yang mencoba "membantu" adalah *Liveware* lain. Kegagalan (misalnya, memasang papan secara terbalik) dapat disebabkan oleh ketidakcocokan di berbagai antarmuka: sekrup yang kepalanya mudah rusak (L-H); gambar di instruksi yang ambigu (L-S); ruangan yang terlalu gelap untuk melihat lubang sekrup dengan jelas (L-E); atau komunikasi yang buruk dengan pasangan Anda tentang langkah mana yang sedang dikerjakan (L-L). Menyalahkan diri sendiri karena "bodoh" (*Person-Model*) kurang produktif daripada menganalisis ketidakcocokan sistemik ini.

### 1. Mismatch L-H (Manusia dan Perangkat Keras)

Ketidakcocokan pada antarmuka *Liveware-Hardware* (L-H) adalah salah satu sumber *human error* yang paling nyata dan dapat diamati. Ini terjadi ketika desain fisik dari peralatan, mesin, atau stasiun kerja tidak sesuai dengan karakteristik fisik atau kognitif dari pengguna manusia. Ketidakcocokan ini secara aktif dapat "mengundang" kesalahan, terutama *slips* dan *mistakes*, serta menyebabkan masalah kesehatan kronis dan kelelahan akut.

Salah satu area klasik dari mismatch L-H adalah desain kontrol dan tampilan. Otak kita secara alami mencari pola dan membuat asumsi.

Ketika desain melanggar asumsi ini, kesalahan menjadi mungkin terjadi. Contohnya termasuk "efek Stroop", di mana kata "MERAH" dicetak dengan tinta biru, yang menciptakan konflik kognitif. Dalam konteks industri, ini bisa berupa sakelar yang harus didorong ke atas untuk mematikan sesuatu, yang berlawanan dengan ekspektasi umum. Contoh lain adalah kurangnya pembedaan antara kontrol-kontrol kritis, seperti yang terjadi pada kecelakaan pesawat British Midland di Kegworth, di mana pilot mematikan mesin yang salah (yang berfungsi) karena desain tampilan getaran mesin yang membingungkan pada model pesawat baru tersebut.

Kurangnya umpan balik dari *Hardware* adalah bentuk lain dari mismatch L-H. Manusia sangat bergantung pada umpan balik untuk mengetahui apakah tindakan mereka telah berhasil. Jika sebuah tombol pada layar sentuh tidak memberikan respons visual atau haptik (getaran), pengguna mungkin akan menekannya berulang kali, atau berasumsi tindakan tersebut telah terdaftar padahal belum. Umpan balik yang buruk dapat menyebabkan ketidakpastian dan kesalahan dalam tugas-tugas berurutan.

Dari perspektif ergonomi fisik, mismatch L-H dapat menyebabkan masalah kesehatan dan keselamatan yang serius. Stasiun kerja yang tidak dapat disesuaikan dapat memaksa pekerja dengan tinggi badan yang berbeda untuk bekerja dalam postur yang canggung, yang menyebabkan gangguan muskuloskeletal (MSDs) dari waktu ke waktu. Alat yang dirancang untuk pengguna tangan kanan dapat menjadi sangat sulit dan tidak efisien untuk digunakan oleh populasi kidal. Getaran yang berlebihan dari perkakas listrik dapat menyebabkan kerusakan saraf permanen (*hand-arm vibration syndrome*).

Tata letak fisik dari sebuah fasilitas juga merupakan bagian dari antarmuka L-H. Jalur pejalan kaki yang tidak jelas atau bersilangan dengan jalur forklift, penempatan katup darurat di lokasi yang sulit dijangkau, atau penyimpanan bahan kimia yang tidak kompatibel secara berdekatan adalah semua contoh mismatch L-H pada skala yang lebih besar.

Mengatasi mismatch L-H memerlukan penerapan disiplin ilmu rekayasa *human factors* secara sistematis. Ini bukan tentang membuat segalanya "lebih cantik", tetapi tentang merancang dengan pemahaman yang

mendalam tentang bagaimana manusia melihat, berpikir, dan bergerak. Solusinya sering kali bersifat teknis: memberi kode warna pada kontrol, menambahkan *interlock* pengaman, menyediakan kursi yang dapat disesuaikan, atau merancang ulang alur kerja. Berinvestasi dalam desain L-H yang baik di awal adalah salah satu cara yang paling efektif biaya untuk mencegah kesalahan dan cedera di masa depan.

## 2. Mismatch L-S (Manusia dan Prosedur)

Ketidakcocokan pada antarmuka Liveware-Software (L-S) mungkin kurang terlihat secara fisik dibandingkan dengan mismatch L-H, tetapi dampaknya terhadap keselamatan bisa sama besarnya, jika tidak lebih. Mismatch ini terjadi ketika prosedur, aturan, dan informasi yang seharusnya memandu perilaku manusia ternyata tidak jelas, tidak akurat, tidak lengkap, atau tidak praktis. Hal ini sering kali menjadi penyebab utama dari *rule-based mistakes* dan menciptakan tekanan yang kuat untuk pelanggaran rutin.

Salah satu sumber utama mismatch L-S adalah kesenjangan antara *work-as-imagined* dan *work-as-done*. Prosedur sering kali ditulis berdasarkan asumsi ideal tentang bagaimana pekerjaan seharusnya dilakukan. Mereka mungkin tidak memperhitungkan variabilitas kondisi di lapangan, keterbatasan waktu yang nyata, atau interaksi yang kompleks dengan tugas-tugas lain. Ketika teknisi di lapangan menemukan bahwa mengikuti prosedur "sesuai buku" membuat pekerjaan menjadi tidak mungkin atau sangat tidak efisien, mereka terpaksa harus berimprovisasi. Improvisasi ini, meskipun sering kali berhasil, menghilangkan pertahanan yang seharusnya disediakan oleh prosedur dan membuka pintu bagi kesalahan.

Ambiguitas dalam bahasa adalah bentuk lain dari mismatch L-S. Prosedur yang menggunakan istilah-istilah yang tidak jelas seperti "periksa secara berkala", "pastikan torsi yang tepat", atau "jika perlu" tanpa memberikan kriteria yang spesifik dan terukur sangat rentan terhadap salah tafsir. Apa yang dianggap "tepat" oleh satu orang mungkin dianggap "terlalu longgar" oleh orang lain. Instruksi yang ambigu dapat menyebabkan variabilitas kinerja yang tidak terkendali.

Kompleksitas yang berlebihan juga merupakan masalah umum. Manual teknis yang tebalnya ratusan halaman atau *checklist* pra-penerbangan dengan lebih dari seratus item dapat menyebabkan kelebihan beban kognitif. Dalam situasi seperti ini, pengguna mungkin akan melewatkan detail-detail penting atau mengembangkan “aturan praktis” mereka sendiri yang mungkin tidak selalu aman. Informasi harus disajikan dengan cara yang sesuai dengan kapasitas memori kerja manusia, dengan menyoroti langkah-langkah yang paling kritis.

Aksesibilitas informasi adalah faktor lain. Prosedur tidak ada gunanya jika tidak dapat ditemukan atau diakses pada saat dibutuhkan. Jika manual pemeliharaan yang relevan terkunci di kantor penyelia sementara teknisi berada di lapangan di tengah malam, mereka akan terpaksa bekerja berdasarkan ingatan, yang kita tahu rentan terhadap *lapses*.

Untuk mengurangi mismatch L-S, organisasi harus memperlakukan pengembangan *Software* (prosedur, manual, dll.) sebagai proses rekayasa yang serius, bukan sebagai tugas administratif. Ini melibatkan validasi di lapangan, di mana draf prosedur diuji oleh pengguna akhir dalam kondisi kerja yang realistis. Ini menuntut penggunaan prinsip-prinsip penulisan teknis yang jelas, seperti menggunakan kalimat aktif, daftar bernomor untuk urutan tindakan, dan menghindari ambiguitas. Dan yang terpenting, ini membutuhkan putaran umpan balik yang berkelanjutan, di mana pengguna didorong untuk melaporkan masalah dengan prosedur tanpa takut disalahkan, sehingga dokumen-dokumen ini dapat terus diperbaiki dan tetap menjadi alat yang berguna dan relevan.

### **3. Mismatch L-E (Manusia dan Lingkungan)**

Kinerja manusia tidak terjadi dalam ruang hampa; ia sangat dipengaruhi oleh lingkungan di mana pekerjaan itu dilakukan. Ketidakcocokan pada antarmuka Liveware-Environment (L-E) terjadi ketika kondisi lingkungan, baik fisik maupun organisasi, mengganggu kemampuan manusia untuk bekerja secara efektif dan aman. Lingkungan dapat bertindak sebagai *Performance Shaping Factor* yang signifikan, baik secara positif maupun negatif.

Lingkungan fisik adalah aspek yang paling jelas dari antarmuka ini. Faktor-faktor seperti:

a. Pencahayaan

Pencahayaan yang tidak memadai dapat menyebabkan salah membaca label atau indikator. Sebaliknya, silau atau pantulan pada layar dapat menyembunyikan informasi penting.

b. Kebisingan

Tingkat kebisingan yang tinggi dapat menutupi alarm pendengaran atau membuat komunikasi verbal menjadi sulit. Paparan kebisingan yang lama juga merupakan stresor yang signifikan dan dapat menyebabkan kelelahan.

c. Suhu dan Ventilasi

Suhu yang ekstrim, baik panas maupun dingin, dapat mengganggu kinerja kognitif dan fisik. Ventilasi yang buruk dapat menyebabkan paparan terhadap kontaminan berbahaya atau kekurangan oksigen.

d. Getaran

Getaran seluruh tubuh (misalnya, pada pengemudi truk) dapat menyebabkan kelelahan dan masalah punggung, sementara getaran tangan-lengan dari alat dapat merusak saraf.

Selain lingkungan fisik, lingkungan organisasi atau psikososial sering kali memiliki dampak yang lebih kuat dan lebih meresap. Ini adalah aspek "iklim" atau "budaya" dari tempat kerja. Mismatch L-E di tingkat organisasi meliputi:

- a. Tekanan waktu dan produksi: Seperti yang telah dibahas, tekanan yang tidak realistis adalah pendorong utama untuk pelanggaran situasional dan kesalahan akibat ketergesa-gesaan.
- b. Budaya keselamatan: Apakah organisasi memiliki *blame culture* atau *just culture*? Apakah pelaporan masalah didorong atau dihukum? Iklim ini secara langsung memengaruhi kemauan individu untuk berkomunikasi tentang risiko.
- c. Hubungan interpersonal: Konflik dengan rekan kerja atau pengawas dapat menjadi sumber stres yang signifikan dan mengalihkan perhatian dari tugas-tugas keselamatan kritis.

- d. Jadwal kerja: Shift kerja yang panjang, kerja malam, atau rotasi shift yang cepat dapat mengganggu ritme sirkadian tubuh, yang menyebabkan penurunan kewaspadaan dan peningkatan risiko kesalahan secara signifikan.

Mengelola antarmuka L-E memerlukan pendekatan dua cabang. Untuk lingkungan fisik, solusinya sering kali melibatkan kontrol rekayasa, meningkatkan pencahayaan, memasang peredam suara, atau meningkatkan sistem ventilasi. Untuk lingkungan organisasi, solusinya terletak pada kepemimpinan dan manajemen. Ini melibatkan penetapan target yang realistis, membangun budaya kepercayaan dan komunikasi terbuka, merancang jadwal kerja yang mempertimbangkan keterbatasan fisiologis manusia, dan secara aktif menunjukkan bahwa keselamatan adalah nilai yang tidak dapat dinegosiasikan. Seringkali, memperbaiki lingkungan organisasi adalah intervensi yang paling kuat untuk mengurangi *human error* di seluruh sistem.

### **C. Aplikasi Model SHELL dalam Perancangan Stasiun Kerja dan Tugas**

Selain menjadi alat analisis reaktif yang sangat baik untuk investigasi insiden, kekuatan sebenarnya dari Model SHELL terletak pada aplikasinya yang proaktif dalam desain. Dengan menggunakan model ini sebagai kerangka kerja selama tahap perancangan sistem, stasiun kerja, atau tugas, kita dapat secara sistematis mengidentifikasi dan menghilangkan potensi ketidakcocokan sebelum mereka memiliki kesempatan untuk menyebabkan kesalahan. Ini adalah perwujudan dari prinsip “mencegah lebih baik daripada mengobati” dalam konteks *human factors*. Pendekatan ini dikenal sebagai desain yang berpusat pada manusia (*human-centred design*) atau makroergonomi, yang mempertimbangkan seluruh sistem kerja, bukan hanya komponen-komponen yang terisolasi.

Proses desain yang dipandu oleh SHELL dimulai dengan pertanyaan sentral: “Siapa pengguna kita?” (analisis *Liveware*). Memahami karakteristik populasi pengguna, ukuran fisik mereka, tingkat keterampilan, latar belakang budaya, dan keterbatasan kognitif, adalah fondasi dari semua keputusan desain selanjutnya. Merancang sistem untuk “operator rata-rata”

yang tidak ada adalah resep untuk kegagalan; sebaliknya, desain harus mengakomodasi rentang variasi manusia yang luas.

Setelah pengguna dipahami, desainer dapat secara sistematis memeriksa setiap antarmuka SHELL untuk memandu keputusan mereka. Daripada merancang *Hardware* terlebih dahulu dan kemudian menulis *Software* (prosedur) untuk menjelaskannya, pendekatan SHELL mendorong proses desain yang lebih terintegrasi. Bagaimana desain kontrol fisik (*Hardware*) akan memengaruhi kemudahan mengikuti *checklist* (*Software*)? Bagaimana kondisi pencahayaan di *Environment* akan memengaruhi keterbacaan tampilan pada *Hardware*? Bagaimana kebutuhan akan komunikasi tim (*Liveware-Liveware*) dapat didukung oleh tata letak stasiun kerja (*Hardware*)?

Menggunakan SHELL secara proaktif mengubah peran profesional K3 dan *human factors*. Alih-alih hanya dipanggil untuk menyelidiki kecelakaan setelah terjadi, mereka menjadi mitra penting dalam tim desain dan rekayasa sejak awal. Kontribusi mereka membantu memastikan bahwa sistem tidak hanya berfungsi secara teknis, tetapi juga dapat dioperasikan secara efektif, efisien, dan aman oleh manusia yang akan menjalankannya setiap hari. Investasi dalam analisis SHELL di muka mungkin tampak seperti biaya tambahan, tetapi itu jauh lebih murah daripada biaya perancangan ulang sistem setelah insiden mahal atau serangkaian masalah kegunaan yang terus-menerus.

**Analogi/Contoh Kasus:** Merancang stasiun kerja menggunakan Model SHELL ibarat seorang arsitek merancang sebuah rumah untuk keluarga tertentu. Arsitek pertama-tama akan mempelajari keluarga tersebut (*Liveware*): berapa banyak orang, berapa usia mereka, apakah ada anggota keluarga dengan kebutuhan khusus? Kemudian, dia akan merancang setiap aspek rumah dengan mempertimbangkan interaksi. Tata letak dapur (*Hardware*) harus memungkinkan alur kerja yang efisien. Tombol lampu (*Hardware*) harus intuitif. Jendela (*Hardware*) harus ditempatkan untuk memaksimalkan cahaya alami (*Environment*). Ruang keluarga harus dirancang untuk memfasilitasi interaksi sosial (*Liveware-Liveware*). Arsitek tidak hanya merancang empat dinding dan atap; dia merancang sebuah sistem terintegrasi untuk kehidupan. Demikian pula, perancang stasiun

kerja tidak hanya menempatkan mesin di sebuah ruangan; dia merancang sebuah sistem terintegrasi untuk bekerja.

### **1. Mendesain Hardware yang Sesuai dengan Keterbatasan Manusia**

Aplikasi proaktif dari analisis antarmuka Liveware-Hardware (L-H) adalah inti dari rekayasa ergonomi. Tujuannya adalah untuk merancang dunia fisik agar sesuai dengan manusia, bukan sebaliknya. Proses ini dimulai dengan pemahaman mendalam tentang populasi pengguna (Liveware) dan menerapkan prinsip-prinsip desain yang sudah mapan untuk menciptakan kesesuaian yang optimal.

Salah satu prinsip pertama adalah desain antropometrik. Ini melibatkan penggunaan data tentang ukuran tubuh manusia (misalnya, tinggi, jangkauan, lebar genggam) untuk menentukan dimensi stasiun kerja, kursi, dan peralatan. Praktik terbaik adalah merancang untuk rentang populasi yang luas, biasanya dari persentil ke-5 wanita hingga persentil ke-95 pria. Ini berarti bahwa desain harus dapat disesuaikan. Misalnya, merancang meja kerja atau kursi yang ketinggiannya dapat diatur memastikan bahwa baik pekerja yang paling pendek maupun yang paling tinggi dapat mempertahankan postur yang netral dan nyaman.

Prinsip kedua adalah desain biomekanik, yang berfokus pada kekuatan dan gerakan tubuh. Tujuannya adalah untuk meminimalkan kekuatan yang dibutuhkan, mengurangi gerakan berulang, dan menghindari postur yang canggung. Ini dapat dicapai dengan menyediakan alat bantu angkat mekanis untuk benda berat, merancang alat dengan pegangan yang sesuai dengan bentuk tangan, atau menempatkan komponen yang sering diakses dalam "zona jangkauan utama" untuk menghindari peregangan yang berlebihan.

Prinsip ketiga, dan yang semakin penting, adalah desain kognitif. Ini berkaitan dengan perancangan antarmuka *Hardware* agar sesuai dengan cara otak manusia memproses informasi. Beberapa pedoman utama meliputi:

- a. Pemetaan alami (*Natural mapping*): Hubungan antara kontrol dan efeknya harus intuitif. Untuk menggerakkan sesuatu ke atas pada layar,

Anda harus menekan tombol panah atas. Kontrol pada kompor harus ditata dalam pola yang sama dengan pembakarnya.

- b. Umpan balik (*Feedback*): Setiap tindakan kontrol harus menghasilkan umpan balik yang segera dan jelas (visual, auditori, atau haptik) untuk memberi tahu pengguna bahwa tindakan tersebut telah berhasil.
- c. Konsistensi: Kontrol dan tampilan untuk fungsi yang sama harus terlihat dan berfungsi dengan cara yang sama di seluruh sistem. Ini mengurangi beban belajar dan mencegah kebingungan.
- d. Meminimalkan beban memori: Informasi yang dibutuhkan harus terlihat, tidak perlu diingat. Hindari mode operasi yang tersembunyi.

Terakhir, prinsip desain untuk kesalahan (*design for error*) secara eksplisit mengakui bahwa manusia akan membuat kesalahan. Oleh karena itu, *Hardware* harus dirancang untuk menjadi toleran terhadap kesalahan. Ini termasuk menggunakan *forcing functions* atau *poka-yoke* yang membuat tindakan yang salah secara fisik tidak mungkin dilakukan, serta memastikan bahwa konsekuensi dari kesalahan yang umum tidak bersifat katastropik. Dengan menerapkan prinsip-prinsip ini, kita dapat secara proaktif merancang *Hardware* yang tidak hanya mengurangi risiko cedera fisik, tetapi juga secara signifikan mengurangi kemungkinan *human error* kognitif.

## 2. Menyusun Software (Prosedur) yang Mudah Dipahami dan Diikuti

Prosedur dan instruksi kerja (*Software*) adalah pertahanan kritis dalam banyak sistem, tetapi mereka hanya efektif jika dirancang dengan mempertimbangkan pengguna akhir (*Liveware*). Proses penyusunan *Software* yang berpusat pada manusia adalah aplikasi proaktif dari analisis antarmuka *Liveware-Software* (L-S). Tujuannya adalah untuk mengubah dokumen yang sering kali dilihat sebagai beban birokrasi menjadi alat bantu kinerja yang benar-benar berguna dan digunakan.

Langkah pertama yang krusial adalah keterlibatan pengguna. Orang-orang yang akan menggunakan prosedur harus dilibatkan dalam setiap tahap, mulai dari penyusunan draf awal hingga pengujian dan validasi akhir. Mereka adalah ahli dalam *work-as-done* dan dapat memberikan wawasan yang tak ternilai tentang apa yang praktis dan apa yang tidak.

Keterlibatan ini tidak hanya menghasilkan prosedur yang lebih baik tetapi juga menciptakan rasa kepemilikan, yang meningkatkan kemungkinan kepatuhan.

Prinsip kejelasan dan kesederhanaan adalah yang terpenting. Penulis teknis harus mengikuti pedoman yang sudah mapan untuk memastikan keterbacaan. Ini termasuk:

- a. Menggunakan bahasa yang sederhana dan lugas, menghindari jargon yang tidak perlu.
- b. Menggunakan kalimat pendek dan aktif (misalnya, "Putar katup A" daripada "Katup A harus diputar").
- c. Menggunakan daftar bernomor untuk tindakan berurutan dan daftar berpoin untuk item-item yang tidak berurutan.
- d. Mendefinisikan akronim dan istilah teknis saat pertama kali digunakan.

Format dan tata letak visual memainkan peran besar dalam seberapa mudah informasi dapat dicerna. Dinding teks yang padat sangat mengintimidasi dan tidak efektif. Sebaliknya, prosedur yang baik harus memanfaatkan ruang putih, judul, dan subjudul untuk memecah informasi menjadi bagian-bagian yang dapat dikelola. Penggunaan alat bantu visual, seperti foto, diagram alir, dan ilustrasi, dapat secara dramatis meningkatkan pemahaman, terutama untuk tugas-tugas spasial atau mekanis. Peringatan dan perhatian harus dibuat menonjol secara visual agar tidak terlewatkan.

Struktur prosedur harus logis dan berorientasi pada tugas. Prosedur harus mengikuti alur kerja alami dari tugas tersebut. Informasi latar belakang harus dipisahkan dari langkah-langkah tindakan yang sebenarnya. *Checklists* harus dirancang dengan cermat, mengelompokkan item-item terkait dan menyoroti langkah-langkah "pembunuh" (*killer items*) yang paling kritis.

Terakhir, proses validasi dan verifikasi sangat penting sebelum prosedur dirilis secara resmi. Ini harus melampaui tinjauan di meja. Validasi terbaik melibatkan simulasi atau walkthrough, di mana pengguna mencoba untuk melakukan tugas di lingkungan kerja yang sebenarnya (atau disimulasikan) hanya dengan menggunakan draf prosedur. Proses ini dengan cepat akan mengungkap ambiguitas, langkah-langkah yang

hilang, atau ketidakpraktisan yang mungkin terlewatkan dalam tinjauan teoritis. Dengan mengikuti pendekatan yang ketat dan berpusat pada pengguna ini, organisasi dapat menyusun *Software* yang berfungsi sebagai pertahanan yang kuat, bukan sebagai sumber frustrasi dan pelanggaran.

### 3. Mengelola Environment (Kebisingan, Suhu, Cahaya)

Merancang sistem yang aman dan efisien memerlukan pengelolaan proaktif dari antarmuka Liveware-Environment (L-E). Ini berarti secara sadar merekayasa dan mengendalikan lingkungan kerja, baik fisik maupun organisasi, untuk mendukung kinerja manusia, bukan menghambatnya. Banyak standar K3 nasional dan internasional memberikan pedoman spesifik untuk mengelola faktor-faktor lingkungan fisik, yang harus dianggap sebagai persyaratan minimum.

Untuk pencahayaan, tujuannya adalah untuk memberikan iluminasi yang cukup untuk tugas yang dilakukan tanpa menciptakan silau atau bayangan yang mengganggu. Kebutuhan pencahayaan bervariasi secara dramatis tergantung pada tugasnya; pekerjaan perakitan detail membutuhkan tingkat cahaya yang jauh lebih tinggi daripada koridor umum. Kualitas cahaya (misalnya, rendering warna) juga bisa menjadi penting dalam tugas-tugas yang memerlukan pembedaan warna yang akurat. Audit pencahayaan secara teratur menggunakan *lux meter* adalah praktik yang baik untuk memastikan standar terpenuhi.

Untuk kebisingan, tujuannya adalah untuk menjaga tingkat kebisingan di bawah batas yang dapat merusak pendengaran dan mengganggu komunikasi atau konsentrasi. Hierarki kontrol harus diterapkan: solusi pertama harus selalu mencoba untuk mengurangi kebisingan di sumbernya (misalnya, menggunakan mesin yang lebih senyap atau memasang peredam). Jika itu tidak memungkinkan, jalur transmisi dapat diblokir dengan penutup atau penghalang akustik. Mengandalkan alat pelindung pendengaran (APD) harus menjadi pilihan terakhir. Penting juga untuk memastikan bahwa alarm pendengaran yang kritis dapat didengar di atas kebisingan latar belakang.

Untuk lingkungan termal (suhu dan kelembaban), tujuannya adalah untuk menjaga kondisi dalam zona nyaman untuk mencegah stres panas

(*heat stress*) atau stres dingin (*cold stress*). Keduanya dapat secara signifikan mengganggu kinerja fisik dan kognitif. Solusinya dapat mencakup ventilasi yang lebih baik, pendingin udara, pemanas, atau penyediaan pakaian pelindung yang sesuai. Untuk pekerjaan di lingkungan yang panas, kebijakan untuk istirahat dan hidrasi yang teratur sangat penting.

Selain lingkungan fisik, mengelola lingkungan organisasi secara proaktif adalah kunci untuk mengurangi kesalahan dan pelanggaran. Ini berarti:

- a. Merancang jadwal kerja yang sehat. Menggunakan prinsip-prinsip manajemen risiko kelelahan (*Fatigue Risk Management Systems - FRMS*) untuk merancang shift kerja yang meminimalkan gangguan pada ritme sirkadian dan memberikan waktu istirahat yang cukup.
- b. Membangun budaya keselamatan yang positif. Para pemimpin secara aktif mempromosikan pelaporan, melakukan tinjauan yang adil terhadap insiden, dan menunjukkan melalui tindakan mereka bahwa keselamatan adalah nilai inti.
- c. Mengelola beban kerja. Memastikan bahwa tingkat kepegawaian dan harapan kinerja realistis, sehingga pekerja tidak terus-menerus berada di bawah tekanan waktu yang berlebihan.

Dengan menganggap lingkungan sebagai variabel desain yang dapat dikendalikan, bukan sebagai kondisi yang "diberikan", organisasi dapat secara signifikan meningkatkan keandalan dan kesejahteraan komponen *Liveware* mereka.

#### **D. Contoh Kasus Analisis Kecelakaan dengan Pendekatan SHELL**

Untuk mengilustrasikan kekuatan analitis dari Model SHELL, kita dapat menerapkannya pada salah satu bencana paling terkenal dalam sejarah penerbangan: tabrakan dua pesawat Boeing 747 di landasan pacu Bandara Los Rodeos (sekarang Bandara Tenerife Utara) pada tanggal 27 Maret 1977. Kecelakaan ini, yang menewaskan 583 orang, adalah contoh klasik tentang bagaimana serangkaian kegagalan interaksi di berbagai antarmuka SHELL, bukan satu kesalahan tunggal, dapat berkolaborasi untuk menciptakan bencana.

Kecelakaan itu melibatkan KLM Penerbangan 4805 dan Pan Am Penerbangan 1736. Serangkaian peristiwa yang tidak biasa telah memaksa banyak penerbangan besar, termasuk dua 747 ini, untuk dialihkan ke bandara regional kecil di Tenerife, yang tidak dilengkapi untuk menangani lalu lintas sebesar itu. Kabut tebal kemudian turun, secara drastis mengurangi jarak pandang. Dalam kebingungan dan tekanan untuk berangkat, pesawat KLM memulai lepas landas saat pesawat Pan Am masih berada di landasan pacu yang sama, yang mengarah ke tabrakan berkecepatan tinggi.

Analisis *Person-Model* yang dangkal mungkin hanya menyalahkan kapten KLM karena lepas landas tanpa izin. Namun, analisis SHELL mengungkapkan jaring kausal yang jauh lebih kompleks, menunjukkan berbagai ketidakcocokan sistemik yang menciptakan panggung untuk kesalahan kapten. Analisis ini tidak untuk memaafkan tindakan tersebut, tetapi untuk memahami *mengapa* tindakan tersebut terjadi sehingga pelajaran yang bermakna dapat dipetik untuk mencegah terulangnya kejadian serupa.

Bagian berikut akan membedah kecelakaan ini dengan menerapkan lensa SHELL pada setiap antarmuka, dengan penekanan khusus pada antarmuka Liveware-Liveware, yang memainkan peran yang sangat penting dalam tragedi ini. Ini akan menunjukkan bagaimana model tersebut dapat mengubah narasi dari "kesalahan pilot" menjadi "kegagalan sistem".

## 1. Studi Kasus Industri Penerbangan atau Maritim

Konteks kecelakaan Tenerife sangat penting untuk dipahami karena ia menciptakan berbagai tekanan dan kondisi abnormal yang menguji sistem penerbangan hingga batasnya. Bandara Los Rodeos adalah fasilitas regional yang tidak terbiasa menangani beberapa jumbo jet secara bersamaan. Hal ini menyebabkan kemacetan parah di area parkir dan taxiway, memaksa pesawat untuk melakukan manuver yang tidak biasa, seperti berputar 180 derajat di landasan pacu dan melakukan *backtrack* (melaju di sepanjang landasan pacu ke arah yang berlawanan sebelum berbalik untuk lepas landas).

Tekanan waktu adalah faktor lingkungan organisasi yang sangat besar. Kapten KLM, Jacob van Zanten, adalah salah satu pilot paling senior dan

dihormati di maskapai, kepala instruktur 747 mereka. Namun, ia berada di bawah tekanan dari peraturan pembatasan waktu tugas awak yang ketat. Jika pesawatnya tidak segera berangkat, penerbangan harus dibatalkan, yang akan menyebabkan gangguan besar dan biaya bagi maskapai. Kecemasan untuk menghindari penundaan ini kemungkinan besar memengaruhi pengambilan keputusannya, sebuah contoh dari antarmuka L-Self (stres memengaruhi penilaian).

Faktor lingkungan fisik yang paling kritis adalah kabut tebal yang tiba-tiba turun, mengurangi jarak pandang di landasan pacu menjadi hanya beberapa ratus meter. Yang penting, bandara ini tidak memiliki radar darat, yang berarti menara pengawas lalu lintas udara (ATC) tidak memiliki cara untuk melihat posisi pesawat secara visual. Mereka sepenuhnya bergantung pada laporan posisi melalui radio, sebuah fakta yang krusial untuk memahami kegagalan komunikasi yang akan terjadi.

Mari kita mulai analisis SHELL:

a. Liveware (Pusat)

Awak KLM dan Pan Am, serta pengendali ATC. Kapten KLM adalah seorang figur otoritas yang sangat dominan. Pengendali ATC memiliki aksen Spanyol yang kental dan bekerja di bawah tekanan tinggi dengan peralatan yang terbatas.

b. Hardware

Dua pesawat Boeing 747, menara ATC dengan radio tetapi tanpa radar darat.

c. Software

Prosedur komunikasi radio penerbangan standar (yang ternyata tidak sepenuhnya diikuti), peraturan waktu tugas awak.

d. Environment

Kemacetan bandara, kabut tebal, tekanan waktu.

Dengan elemen-elemen ini, kita dapat mulai memeriksa antarmuka. Ada mismatch L-E yang jelas: sistem (bandara, kru) dipaksa untuk beroperasi dalam kondisi lingkungan (kabut, kemacetan) yang jauh di luar norma desainnya. Ada mismatch L-H: menara ATC tidak memiliki *Hardware* (radar

darat) yang diperlukan untuk mengelola lalu lintas dengan aman dalam kondisi jarak pandang rendah. Namun, kegagalan yang paling fatal terjadi pada antarmuka L-L.

## 2. Identifikasi Kegagalan Interaksi L-L (Liveware-Others)

Antarmuka Liveware-Liveware (L-L) adalah tentang interaksi antara individu di dalam tim (intra-tim) dan antara tim yang berbeda (antar-tim). Ini mencakup komunikasi, kepemimpinan, kerja tim, dan budaya. Kecelakaan Tenerife adalah studi kasus definitif dalam kegagalan L-L di berbagai tingkatan.

### a. Kegagalan L-L Intra-Tim (di dalam Kokpit KLM)

Di dalam kokpit KLM, ada gradien otoritas yang curam antara Kapten van Zanten dan kopilot serta insinyur penerbangannya yang jauh lebih junior. Van Zanten adalah seorang legenda di maskapai, dan bawahannya sangat enggan untuk secara tegas menantang keputusannya, bahkan ketika mereka memiliki keraguan. Setelah menerima izin ATC yang ambigu, insinyur penerbangan memang sempat bertanya, "Apakah dia [Pan Am] belum keluar [dari landasan pacu]?". Van Zanten dengan tegas menjawab, "Oh, ya," dan melanjutkan lepas landas. Ketidakberanian insinyur untuk menantang lebih jauh adalah kegagalan L-L klasik. Ini menunjukkan bahwa tim tersebut lebih merupakan hierarki daripada sebuah tim kolaboratif.

### b. Kegagalan L-L Antar-Tim (Kru KLM dan ATC)

Komunikasi antara kokpit KLM dan menara ATC adalah inti dari bencana ini. Terjadi serangkaian kesalahpahaman fatal yang disebabkan oleh penggunaan fraseologi non-standar. Setelah menyelesaikan *backtrack* dan bersiap di ujung landasan pacu, kopilot KLM memberitahu ATC, "Kami sedang berada di posisi untuk lepas landas" (*we're now at takeoff*), sebuah frasa yang ambigu. Dia mungkin bermaksud "kami siap", tetapi ATC mungkin mendengarnya sebagai "kami sedang lepas landas".

ATC merespons dengan instruksi untuk "bersiap untuk lepas landas, saya akan hubungi Anda" (*stand by for takeoff, I will call you*), yang dengan

jelas memberitahu mereka untuk menunggu. Namun, tepat pada saat yang sama, kru Pan Am mengirim pesan radio, "Kami masih melaju di landasan pacu" (*we're still taxiing down the runway*). Kedua transmisi ini tumpang tindih di kokpit KLM, menciptakan suara siulan yang keras (*heterodyne*) yang mengaburkan bagian penting dari pesan ATC. Kopilot KLM hanya mendengar "OK..." dari ATC (yang merupakan respons terhadap pesan lain) dan kemudian kapten, yang sudah tidak sabar, berkata, "Kita berangkat" (*We're going*) dan mulai mendorong tuas daya. Ini adalah kegagalan komunikasi multi-pihak yang katastrofik.

Kombinasi dari gradien otoritas yang tinggi di dalam kokpit (mencegah verifikasi internal) dan komunikasi yang ambigu dan terganggu dengan pihak eksternal (ATC dan Pan Am) menciptakan badai yang sempurna. Ini menunjukkan bahwa keselamatan tidak hanya bergantung pada keterampilan individu, tetapi secara kritis bergantung pada kualitas interaksi di antara mereka.

### 3. Merumuskan Rekomendasi Mitigasi Berdasarkan Setiap Elemen SHELL

Analisis SHELL terhadap bencana Tenerife tidak hanya menjelaskan mengapa kecelakaan itu terjadi, tetapi juga secara langsung mengarah pada serangkaian rekomendasi mitigasi yang kuat yang telah mengubah industri penerbangan secara fundamental. Rekomendasi-rekomendasi ini menargetkan perbaikan di setiap antarmuka yang gagal.

#### a. Untuk Mismatch L-L (Liveware-Liveware)

- 1) Rekomendasi: Pengembangan dan implementasi wajib dari pelatihan Manajemen Sumber Daya Awak (*Crew Resource Management - CRM*).
- 2) Tindakan: CRM mengubah dinamika kokpit dari hierarki satu orang menjadi tim terkelola. Pelatihan ini secara eksplisit mengajarkan keterampilan komunikasi, pengambilan keputusan bersama, dan kepemimpinan. Kopilot dan anggota awak lainnya dilatih untuk bersikap asertif dan secara hormat menantang kapten jika mereka yakin ada masalah keamanan. Ini secara langsung mengatasi masalah gradien otoritas yang terlihat di kokpit KLM.

b. **Untuk Mismatch L-S (Liveware-Software)**

- 1) Rekomendasi: Penegakan ketat terhadap fraseologi radio penerbangan standar internasional.
- 2) Tindakan: Industri penerbangan memberlakukan aturan yang lebih ketat tentang penggunaan bahasa Inggris standar dan frasa yang tepat dan tidak ambigu untuk semua komunikasi penting antara pilot dan ATC. Frasa ambigu seperti "OK" atau "we're at takeoff" dihilangkan. Penggunaan kata-kata kunci kritis seperti "takeoff" dan "clear" sekarang sangat dibatasi hanya untuk izin yang sebenarnya, mengurangi kemungkinan salah tafsir.

c. **Untuk Mismatch L-E (Liveware-Environment)**

- 1) Rekomendasi: Peningkatan infrastruktur bandara untuk operasi dalam jarak pandang rendah.
- 2) Tindakan: Bandara-bandara besar di seluruh dunia diwajibkan untuk memasang radar darat (ground radar). Teknologi ini memungkinkan ATC untuk "melihat" posisi semua pesawat dan kendaraan di lapangan secara elektronik, bahkan dalam kabut tebal sekalipun, menghilangkan ketergantungan pada laporan posisi visual atau verbal yang rawan kesalahan.

d. **Untuk Mismatch L-Self dan Lingkungan Organisasi**

- 1) Rekomendasi: Peningkatan sistem manajemen untuk risiko kelelahan dan tekanan komersial.
- 2) Tindakan: Meskipun sudah ada sebelumnya, tragedi ini memperkuat pentingnya Sistem Manajemen Risiko Kelelahan (*Fatigue Risk Management Systems*). Maskapai penerbangan dan regulator menjadi lebih sadar akan bagaimana tekanan komersial dan jadwal dapat secara negatif memengaruhi pengambilan keputusan pilot.

Tragedi Tenerife, jika dianalisis melalui Model SHELL, menjadi pelajaran yang sangat berharga. Ia menunjukkan bahwa keselamatan penerbangan modern yang luar biasa tidak dibangun di atas asumsi bahwa pilot tidak akan membuat kesalahan, tetapi di atas pembangunan sistem yang tangguh, dengan CRM (L-L), fraseologi standar (L-S), dan radar darat (L-H/L-E), yang

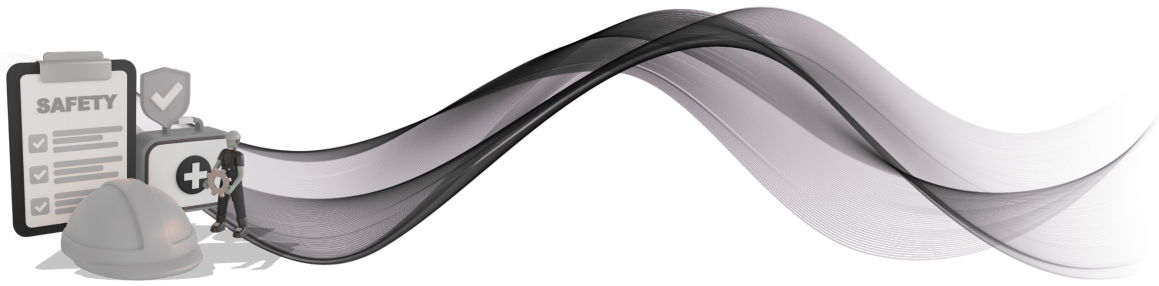
dirancang untuk menangkap dan menahan kesalahan tersebut sebelum dapat menyebabkan bencana.

## KESIMPULAN

Model SHELL memberikan "mikroskop" analitis yang sangat diperlukan untuk melengkapi pandangan "teleskopik" dari Model Keju Swiss. Dengan menempatkan manusia (*Liveware*) di pusatnya, model ini memaksa kita untuk secara sistematis memeriksa kualitas interaksi antara individu dan setiap komponen lain dari sistem kerjanya: *Hardware*, *Software*, *Environment*, dan *Liveware* lainnya. Bab ini telah menunjukkan bahwa *human error* jarang sekali merupakan kegagalan yang terisolasi, melainkan manifestasi dari ketidakcocokan atau "gesekan" pada antarmuka-antarmuka ini.

Melalui analisis komponen dan antarmuka, Model SHELL memberikan kerangka kerja yang terstruktur untuk investigasi insiden dan, yang lebih penting, untuk desain proaktif. Ia mengubah pertanyaan dari "Siapa yang salah?" menjadi "Di mana letak ketidakcocokan antara sistem dan penggunanya?". Studi kasus bencana Tenerife secara dramatis mengilustrasikan bagaimana kegagalan di berbagai antarmuka, terutama komunikasi L-L yang buruk, prosedur L-S yang ambigu, dan lingkungan L-E yang menantang, dapat bergabung untuk menciptakan bencana. Pelajaran yang dipetik dari analisis semacam itu telah secara fundamental membentuk praktik keselamatan modern, terutama melalui pengembangan CRM.

Pada akhirnya, Model SHELL adalah alat praktis untuk menerapkan filosofi desain yang berpusat pada manusia. Ia mengingatkan kita bahwa sistem yang aman dan efisien adalah sistem yang dirancang dengan pemahaman yang mendalam tentang kapabilitas dan keterbatasan manusia. Dengan fondasi ini, kita sekarang siap untuk menjelajahi faktor-faktor kognitif dan perseptual yang lebih dalam yang mendorong terjadinya kesalahan di tingkat individu, yang akan menjadi fokus dari bab berikutnya.



# BAB 7

## FAKTOR KOGNITIF DAN PERSEPTUAL YANG MENDORONG KESALAHAN

### PENDAHULUAN

Pernahkah Anda berjalan ke dapur dengan niat yang jelas untuk mengambil sesuatu, hanya untuk berdiri bingung di tengah ruangan, sama sekali lupa apa tujuan Anda? Atau pernahkah Anda begitu fokus pada sebuah tugas sehingga Anda sama sekali tidak mendengar seseorang memanggil nama Anda berulang kali? Insiden-insiden kecil ini, yang sering kita abaikan sebagai keanehan pikiran, sebenarnya adalah jendela yang membuka pemahaman kita tentang arsitektur dasar dari kognisi manusia. Otak manusia, meskipun merupakan organ yang luar biasa kuat dan adaptif, bukanlah komputer yang sempurna. Ia beroperasi dengan serangkaian batasan dan "aturan praktis" bawaan yang, meskipun sangat efisien dalam sebagian besar waktu, dapat menjadi sumber kesalahan yang dapat diprediksi dalam kondisi tertentu.

Jika bab-bab sebelumnya telah membangun pandangan "makro" tentang kegagalan, dengan memeriksa bagaimana sistem pertahanan organisasi dapat ditembus (Model Keju Swiss) dan bagaimana komponen-komponen sistem berinteraksi (Model SHELL), maka bab ini akan melakukan

“zoom in” ke tingkat mikro. Kita akan menjelajahi “mesin” di pusat Model SHELL itu sendiri: *Liveware*, atau pikiran manusia. Tujuan kita bukanlah untuk menyalahkan “perangkat keras” biologis ini, melainkan untuk memahami spesifikasi teknisnya, kekuatan dan kelemahannya, sehingga kita dapat merancang sistem kerja yang kompatibel dengannya.

Fokus bab ini adalah pada faktor-faktor kognitif dan perseptual, proses-proses mental yang kita gunakan untuk merasakan, memahami, mengingat, dan membuat keputusan tentang dunia di sekitar kita. Kita akan memulai dengan memeriksa keterbatasan fundamental dari kapasitas pemrosesan informasi otak manusia. Konsep-konsep seperti memori kerja yang terbatas, rentang perhatian yang sempit, dan beban kerja kognitif akan dibedah untuk menunjukkan mengapa bahkan para profesional yang paling cerdas pun dapat mengalami kelebihan beban mental, yang secara dramatis meningkatkan kemungkinan kesalahan.

Selanjutnya, kita akan menganalisis bagaimana keadaan fisiologis dan emosional, seperti stres dan kelelahan, dapat secara signifikan menurunkan kinerja kognitif kita. Kelelahan bukanlah sekadar perasaan subjektif; ia adalah gangguan fisiologis yang dapat melemahkan penilaian dan waktu reaksi sebanding dengan keracunan alkohol. Memahami dampak dari stresor-stresor ini sangat penting, terutama dalam lingkungan kerja 24/7 yang menuntut kewaspadaan tinggi.

Bab ini juga akan menyelami dunia bias kognitif yang menarik, jalan pintas mental atau heuristik yang digunakan otak kita untuk membuat keputusan dengan cepat. Meskipun sering kali berguna, bias-bias ini dapat secara sistematis menyesatkan kita dalam situasi yang kompleks atau ambigu. Fenomena seperti *confirmation bias* (kecenderungan untuk mencari bukti yang mendukung keyakinan kita) akan dianalisis untuk menunjukkan bagaimana hal itu dapat mendistorsi investigasi insiden dan diagnosis masalah. Pentingnya kesadaran situasi (*situation awareness*), pemahaman yang akurat tentang apa yang sedang terjadi dan apa yang mungkin terjadi selanjutnya, akan ditekankan sebagai penangkal utama terhadap kesalahan pengambilan keputusan.

Pada akhirnya, pemahaman harus mengarah pada tindakan. Bab ini akan ditutup dengan menguraikan serangkaian strategi mitigasi yang secara khusus dirancang untuk mendukung kognisi manusia dan melindungi dari kegagalannya. Ini termasuk teknik untuk memvisualisasikan tugas yang kompleks, prinsip-prinsip untuk merancang antarmuka yang mengurangi beban memori, dan metode pelatihan mental yang bertujuan untuk meningkatkan fokus dan ketahanan terhadap stres.

Dengan memahami mekanisme internal dari kesalahan, kita dapat beralih dari sekadar melabeli tindakan sebagai *human error* ke diagnosis yang lebih dalam tentang mengapa tindakan tersebut masuk akal bagi individu pada saat itu. Ini adalah pergeseran dari menyalahkan individu ke pemahaman empati terhadap tantangan kognitif yang mereka hadapi, sebuah langkah penting dalam merancang sistem kerja yang benar-benar manusiawi dan aman.

## **A. Keterbatasan Kapasitas Otak Manusia**

Otak manusia sering dianalogikan dengan superkomputer, yang mampu melakukan prestasi kreativitas dan pemecahan masalah yang luar biasa. Namun, dari perspektif rekayasa, “perangkat keras” kognitif kita memiliki beberapa keterbatasan desain yang sangat signifikan. Keterbatasan ini bukanlah cacat, melainkan hasil dari evolusi yang mengoptimalkan otak untuk bertahan hidup di lingkungan yang sangat berbeda dari ruang kontrol industri atau kokpit pesawat modern. Mengabaikan keterbatasan bawaan ini saat merancang tugas dan sistem kerja sama berbahayanya dengan merancang jembatan tanpa memahami batas beban baja. Kecelakaan sering kali terjadi bukan karena orang bertindak tidak normal, tetapi karena mereka ditempatkan dalam situasi yang melebihi batas normal dari kapasitas kognitif mereka.

Keterbatasan yang paling fundamental terletak pada kapasitas kita untuk pemrosesan informasi secara sadar. Sementara otak kita dapat memproses sejumlah besar informasi sensorik secara tidak sadar, “layar” kesadaran kita, tempat kita berpikir, bernalar, dan membuat keputusan secara aktif, sangatlah sempit. Kita hanya dapat secara sadar memperhatikan dan memanipulasi sejumlah kecil informasi pada satu waktu. Ketika tuntutan

tugas melebihi kapasitas saluran terbatas ini, kinerja mulai menurun, dan kesalahan menjadi lebih mungkin terjadi.

Masalah ini diperparah oleh fakta bahwa di banyak lingkungan kerja modern, jumlah informasi yang harus diproses oleh operator telah meledak. Seorang operator di ruang kontrol mungkin dihadapkan pada ratusan variabel proses yang ditampilkan di beberapa layar, sementara seorang dokter di unit gawat darurat harus mengintegrasikan data dari monitor pasien, hasil lab, dan riwayat medis secara bersamaan. Ketika sistem dirancang tanpa mempertimbangkan keterbatasan pemrosesan manusia, mereka secara efektif sedang menyiapkan pengguna mereka untuk kegagalan.

Bagian ini akan menguraikan tiga keterbatasan kapasitas kognitif yang paling kritis dan relevan dengan K3: kapasitas memori jangka pendek yang terbatas, yang bertindak sebagai "meja kerja" mental kita; rentang perhatian kita yang sempit, yang menentukan seberapa banyak yang bisa kita tangani sekaligus; dan konsep beban kerja kognitif, yang merupakan ukuran dari seberapa banyak "daya pemrosesan" mental yang dibutuhkan oleh suatu tugas. Memahami ketiga pilar keterbatasan ini adalah prasyarat untuk merancang intervensi yang efektif.

**Analogi/Contoh Kasus:** Bayangkan kapasitas pemrosesan sadar otak Anda sebagai seorang juru masak tunggal di dapur yang sangat kecil dengan hanya satu talenan. Talenan ini adalah memori kerja Anda; ia hanya dapat menampung beberapa bahan (informasi) pada satu waktu. Perhatian Anda adalah seperti tatapan mata sang juru masak; dia hanya bisa fokus pada satu bahan yang sedang diiris pada satu waktu. Beban kerja kognitif adalah seberapa rumit resep yang harus dia ikuti dan seberapa cepat pesanan datang. Jika resepnya terlalu rumit atau pesanan datang terlalu cepat, juru masak akan kewalahan. Dia mungkin akan salah mengambil bahan (slip), lupa menambahkan bumbu penting (lapse), atau salah membaca resep (mistake). Masalahnya bukan pada juru masaknya, tetapi pada sistem dapur yang tidak dirancang untuk mendukungnya.

## 1. Kapasitas Memori Jangka Pendek dan Dampaknya pada Tugas Kompleks

Memori manusia bukanlah sebuah gudang tunggal. Secara umum, ia dibagi menjadi memori jangka panjang, yang merupakan gudang pengetahuan dan pengalaman kita yang luas, dan memori jangka pendek atau memori kerja (*working memory*), yang merupakan "ruang mental" sementara tempat kita menyimpan dan memanipulasi informasi yang kita butuhkan untuk tugas yang sedang kita lakukan. Memori kerja sangat penting untuk aktivitas seperti penalaran, pemecahan masalah, dan pemahaman bahasa. Namun, ia memiliki dua keterbatasan yang parah: durasi yang singkat dan kapasitas yang sangat terbatas.

Informasi dalam memori kerja akan hilang dalam waktu sekitar 15-30 detik kecuali jika kita secara aktif mengulanginya (misalnya, terus-menerus mengulang nomor telepon di kepala kita). Keterbatasan yang lebih signifikan adalah kapasitasnya. Penelitian klasik oleh George Miller menunjukkan bahwa kita hanya dapat menyimpan sekitar tujuh, plus atau minus dua, "potongan" (*chunks*) informasi dalam memori kerja pada satu waktu. Sebuah "potongan" bisa berupa satu digit, satu kata, atau bahkan konsep yang lebih kompleks jika kita sudah familiar dengannya. Namun, intinya tetap sama: ada batas yang tegas pada seberapa banyak informasi baru yang dapat kita proses secara sadar sekaligus.

Dampak dari keterbatasan ini pada tugas-tugas kompleks di tempat kerja sangat besar. Setiap kali sebuah tugas mengharuskan seorang pekerja untuk mengingat informasi dari satu langkah untuk digunakan di langkah lain, memori kerja mereka sedang dibebani. Pertimbangkan seorang teknisi yang membaca nilai torsi dari manual di kantor, lalu berjalan ke lantai pabrik untuk mengencangkan baut. Selama perjalanan itu, jika dia terganggu oleh pertanyaan dari rekan kerja atau panggilan radio, ada kemungkinan besar bahwa angka yang dia simpan di memori kerjanya akan hilang atau rusak.

Tugas-tugas yang melibatkan urutan langkah yang panjang, perhitungan mental, atau perbandingan antara berbagai sumber informasi sangat membebani memori kerja. Ketika kapasitasnya terlampaui, kinerja akan menurun drastis. Gejalanya termasuk lupa langkah-langkah penting

dalam prosedur, kehilangan jejak di mana kita berada dalam suatu tugas, atau membuat kesalahan dalam perhitungan mental. Desain sistem yang tidak mempertimbangkan keterbatasan ini secara langsung berkontribusi pada *lapses* memori.

Oleh karena itu, salah satu tujuan utama dari desain yang berpusat pada manusia adalah untuk mengurangi beban memori kerja. Ini bukan tentang membuat pekerja menjadi "lebih pintar", tetapi tentang merancang tugas dan alat yang tidak menuntut kapasitas memori yang tidak realistis. Strategi untuk mencapai ini termasuk:

- a. Menyediakan informasi di tempat dan waktu yang dibutuhkan (*just-in-time information*).
- b. Menggunakan *checklists* untuk tugas-tugas multi-langkah.
- c. Merancang tampilan yang menyajikan informasi yang relevan secara bersamaan sehingga tidak perlu diingat.
- d. Menggunakan alat bantu hitung eksternal alih-alih mengandalkan perhitungan mental.

Dengan "memindahkan" beban memori dari kepala pekerja ke dunia luar (misalnya, ke prosedur atau tampilan), kita membebaskan sumber daya kognitif mereka yang berharga untuk fokus pada aspek-aspek tugas yang lebih kritis, seperti pemecahan masalah dan kesadaran situasi.

## 2. Keterbatasan Rentang Perhatian (Attention Span)

Perhatian adalah mekanisme kognitif yang memungkinkan kita untuk secara selektif fokus pada sebagian kecil dari informasi sensorik yang membombardir kita setiap saat, sambil mengabaikan sisanya. Ini adalah "lampu sorot" mental kita. Seperti halnya memori kerja, perhatian adalah sumber daya yang terbatas. Kita tidak dapat memperhatikan segalanya sekaligus. Keterbatasan dalam kemampuan kita untuk mengalokasikan dan mempertahankan perhatian adalah sumber utama dari banyak *human error*, terutama *slips*.

Ada beberapa jenis perhatian yang relevan dengan K3. Perhatian selektif (*Selective attention*) adalah kemampuan untuk fokus pada satu sumber informasi sambil mengabaikan gangguan. Ketika seorang operator

ruang kontrol mencoba untuk fokus pada satu alarm kritis di tengah “banjir alarm” (*alarm flooding*), dia sedang menggunakan perhatian selektif. Kegagalan dalam perhatian selektif terjadi ketika gangguan yang tidak relevan berhasil “menangkap” lampu sorot mental kita.

Perhatian terbagi (*Divided attention*), atau *multitasking*, adalah kemampuan untuk memantau atau memproses lebih dari satu sumber informasi pada saat yang sama. Penelitian secara konsisten menunjukkan bahwa manusia pada dasarnya sangat buruk dalam *multitasking* yang sebenarnya. Apa yang kita anggap sebagai *multitasking* sebenarnya adalah proses beralih perhatian dengan sangat cepat bolak-balik antara tugas-tugas. Setiap kali kita beralih, ada biaya kognitif, waktu yang hilang dan peningkatan kemungkinan kesalahan. Tugas-tugas yang menuntut perhatian terbagi yang konstan, seperti mengemudi sambil menggunakan ponsel, secara inheren rawan kesalahan.

Perhatian berkelanjutan (*Sustained attention*), atau kewaspadaan (*vigilance*), adalah kemampuan untuk mempertahankan fokus pada suatu tugas dalam jangka waktu yang lama, terutama jika tugas tersebut monoton. Ini adalah jenis perhatian yang dibutuhkan oleh penjaga keamanan yang memantau layar, atau operator sonar. Kinerja pada tugas-tugas kewaspadaan menurun secara dapat diprediksi seiring waktu, sebuah fenomena yang dikenal sebagai penurunan kewaspadaan (*vigilance decrement*). Setelah sekitar 20-30 menit, kemampuan untuk mendeteksi sinyal yang jarang muncul mulai menurun.

Di lingkungan kerja, banyak faktor yang dapat mengganggu atau melebihi kapasitas perhatian kita. Gangguan eksternal seperti kebisingan atau interupsi, serta gangguan internal seperti kelelahan, stres, atau kebosanan, semuanya dapat menyebabkan kegagalan perhatian. Ketika perhatian kita teralihkan dari tugas yang sangat terampil atau otomatis, kita rentan terhadap *slips of action*, seperti kesalahan menangkap (*capture errors*).

Strategi untuk mengelola keterbatasan perhatian meliputi:

- a. Merancang lingkungan untuk meminimalkan gangguan yang tidak relevan.

- b. Membuat sinyal dan peringatan penting menonjol dan mudah dibedakan dari kebisingan latar belakang.
- c. Menghindari desain tugas yang menuntut *multitasking* yang berlebihan.
- d. Untuk tugas kewaspadaan, menjadwalkan istirahat secara teratur, merotasi tugas, atau memperkenalkan variasi untuk menjaga agar operator tetap waspada.

Memahami bahwa perhatian adalah sumber daya yang berharga dan mudah habis membantu kita untuk merancang sistem yang tidak menyia-nyiakannya, tetapi mengarahkannya ke tempat yang paling dibutuhkan.

### 3. **Beban Kerja Kognitif (Cognitive Workload) Berlebihan**

Beban kerja kognitif atau beban kerja mental adalah konsep yang merangkum jumlah total sumber daya mental yang dibutuhkan untuk melakukan suatu tugas dalam periode waktu tertentu. Ini adalah "harga" kognitif dari suatu aktivitas. Beban kerja bukanlah konsep tunggal; ia dipengaruhi oleh kompleksitas tugas, tekanan waktu, dan keadaan individu (seperti tingkat kelelahan atau keahlian). Kinerja manusia cenderung mengikuti kurva U terbalik dalam kaitannya dengan beban kerja (Hukum Yerkes-Dodson).

Pada beban kerja yang sangat rendah, ketika tugasnya terlalu sederhana atau monoton, orang bisa menjadi bosan, puas diri, dan perhatian mereka cenderung mengembara. Hal ini dapat menyebabkan hilangnya kesadaran situasi dan kegagalan untuk mendeteksi perubahan atau masalah yang berkembang secara perlahan. Ini adalah masalah umum dalam sistem yang sangat terotomatisasi, di mana operator hanya bertindak sebagai pemantau pasif.

Pada beban kerja yang optimal, orang merasa tertantang tetapi tidak kewalahan. Mereka waspada, terlibat, dan mampu mengerahkan sumber daya kognitif yang cukup untuk melakukan tugas dengan baik. Ini adalah zona kinerja puncak.

Namun, ketika beban kerja menjadi berlebihan, kinerja mulai menurun secara drastis. Ketika tuntutan tugas melebihi kapasitas pemrosesan informasi yang tersedia, berbagai gejala negatif mulai muncul:

- a. Penyempitan perhatian (*Attentional narrowing*) atau “visi terowongan” (*tunnel vision*). Orang mulai fokus hanya pada apa yang mereka anggap sebagai aspek paling penting dari tugas, sambil mengabaikan informasi lain di periferal yang mungkin juga kritis.
- b. Pemindaian informasi yang lebih buruk. Mereka memeriksa lebih sedikit sumber informasi dan melakukannya dengan cara yang kurang sistematis.
- c. Penurunan kapasitas memori kerja. Kemampuan untuk mengingat informasi baru atau melacak status tugas menurun.
- d. Regresi ke kebiasaan lama. Di bawah tekanan tinggi, orang cenderung kembali ke respons yang lebih familiar atau lebih dulu dipelajari, bahkan jika itu tidak sesuai untuk situasi saat ini (strategi “*strong but wrong*”).
- e. Pengambilan keputusan yang disederhanakan. Mereka mungkin membuat keputusan yang tergesa-gesa tanpa mempertimbangkan semua opsi atau konsekuensi.

Beban kerja yang berlebihan dapat disebabkan oleh berbagai faktor: terlalu banyak informasi yang harus diproses, tugas yang terlalu kompleks, atau terlalu sedikit waktu untuk melakukan tugas tersebut. Ini adalah keadaan yang sangat berbahaya di lingkungan berisiko tinggi. Banyak kecelakaan terjadi selama periode aktivitas yang sangat tinggi (misalnya, selama gangguan pabrik atau pendaratan darurat), di mana beban kerja kognitif para operator melonjak hingga tingkat yang tidak dapat dikelola.

Mengelola beban kerja kognitif adalah tujuan utama dari desain sistem yang baik. Strategi mitigasi meliputi:

- a. Menyederhanakan tugas dan antarmuka. Menghilangkan langkah-langkah, informasi, dan kontrol yang tidak perlu.
- b. Otomatisasi, menggunakan teknologi untuk mengambil alih tugas-tugas yang sangat menuntut atau berulang, sambil menjaga agar operator tetap “dalam lingkaran” (*in the loop*).
- c. Menyediakan alat bantu keputusan. Memberikan dukungan untuk membantu operator mendiagnosis masalah atau mengevaluasi opsi.
- d. Pelatihan dalam manajemen beban kerja. Melatih individu dan tim untuk mengenali tanda-tanda kelebihan beban dan untuk berkomunikasi

serta mendistribusikan kembali tugas secara efektif selama periode sibuk.

## B. Peran Stres dan Kelelahan Mental

Jika keterbatasan kapasitas kognitif adalah “spesifikasi perangkat keras” dasar dari otak kita, maka stres dan kelelahan adalah faktor-faktor yang dapat secara drastis “menurunkan kinerja” perangkat keras tersebut. Stres dan kelelahan bukanlah sekadar perasaan subjektif atau tanda kelemahan pribadi; mereka adalah keadaan psikofisiologis yang nyata dengan konsekuensi yang dapat diukur dan sering kali parah terhadap kemampuan kita untuk berpikir jernih dan bertindak dengan aman. Mereka adalah *Performance Shaping Factors* negatif yang sangat kuat yang dapat memengaruhi siapa saja, terlepas dari tingkat keterampilan atau motivasi mereka. Di lingkungan kerja modern yang sering kali menuntut lebih banyak dengan lebih sedikit, pengelolaan stres dan kelelahan telah menjadi salah satu tantangan K3 yang paling signifikan.

Stres dapat didefinisikan sebagai respons tubuh terhadap tuntutan atau tekanan apa pun. Sejumlah kecil stres (sering disebut *eustress*) dapat bermanfaat, meningkatkan kewaspadaan dan kinerja. Namun, ketika stres menjadi berlebihan atau kronis, ia mulai menguras sumber daya kognitif dan fisik kita. Kelelahan adalah keadaan penurunan kapasitas mental atau fisik akibat pengerahan tenaga, kurang tidur, atau stres yang berkepanjangan. Keduanya sering kali saling terkait erat; stres yang kronis dapat menyebabkan kelelahan, dan kelelahan membuat kita lebih sulit untuk mengatasi stres.

Dampak gabungan dari stres dan kelelahan pada fungsi kognitif sangat merusak. Mereka secara efektif mengurangi kapasitas memori kerja kita yang sudah terbatas, mempersempit rentang perhatian kita, dan memperlambat waktu reaksi kita. Mereka juga mengganggu fungsi eksekutif tingkat tinggi dari korteks prefrontal otak kita, bagian yang bertanggung jawab atas penalaran logis, perencanaan, dan pengendalian impuls. Akibatnya, di bawah pengaruh stres atau kelelahan, kita lebih cenderung untuk membuat keputusan yang impulsif, mengandalkan jalan pintas mental yang berisiko, dan gagal melihat gambaran besar.

Mengabaikan peran stres dan kelelahan dalam analisis keselamatan adalah sebuah kelalaian besar. Banyak kecelakaan yang pada awalnya diatribusikan pada “kelalaian operator” ternyata, setelah diselidiki lebih dalam, melibatkan individu yang telah bekerja berjam-jam tanpa istirahat yang cukup atau berada di bawah tekanan psikologis yang luar biasa. Bagian ini akan membahas secara lebih rinci bagaimana stres dan kelelahan secara spesifik memengaruhi pengambilan keputusan dan kinerja, serta bagaimana kita dapat mulai mengukur dan mengelola risiko-risiko tak terlihat ini.

**Analogi/Contoh Kasus:** Bayangkan seorang pengemudi mobil balap. Keterbatasan kognitif dasar adalah seperti batas cengkraman ban mobil di lintasan kering, ada batas fisik seberapa cepat dia bisa melewati tikungan. Stres akut (misalnya, mobil lain berputar di depannya) adalah seperti hujan tiba-tiba yang membuat lintasan menjadi licin; batas cengkraman menurun drastis, dan dia harus memperlambat dan menjadi jauh lebih berhati-hati. Kelelahan adalah seperti mengemudi dengan ban yang sudah aus setelah 200 putaran; cengkramannya menjadi tidak dapat diprediksi, waktu reaksinya melambat, dan dia lebih mungkin membuat kesalahan kecil yang bisa berakibat fatal. Sistem yang aman tidak hanya bergantung pada keterampilan pengemudi, tetapi juga pada pengelolaan kondisi lintasan (stres) dan pemeliharaan ban (kelelahan).

### 1. Stres K3 dan Pengaruhnya pada Pengambilan Keputusan

Stres di tempat kerja dapat muncul dalam dua bentuk utama: stres akut dan stres kronis. Stres akut adalah respons “lawan atau lari” (*fight-or-flight*) tubuh terhadap ancaman atau keadaan darurat yang tiba-tiba dan intens. Dalam beberapa situasi K3, respons ini bisa menyelamatkan nyawa, karena ia membanjiri tubuh dengan adrenalin, mempertajam indera tertentu, dan mempercepat reaksi fisik. Namun, respons yang sama ini juga memiliki sisi negatif yang signifikan terhadap fungsi kognitif yang lebih tinggi.

Di bawah stres akut, aliran darah dialihkan dari korteks prefrontal (pusat pemikiran rasional) ke bagian otak yang lebih primitif dan reaktif. Hal ini menyebabkan beberapa efek yang berpotensi berbahaya bagi pengambilan keputusan dalam situasi yang kompleks:

- a. Persepsi waktu yang terdistorsi. Waktu bisa terasa melambat atau justru melesat.
- b. Penyempitan perseptual. Terjadi “visi terowongan” baik secara visual maupun kognitif. Orang hanya fokus pada sumber ancaman yang paling jelas dan mungkin gagal memproses informasi penting lainnya.
- c. Penurunan kemampuan berpikir analitis. Kemampuan untuk mempertimbangkan berbagai opsi, memikirkan konsekuensi jangka panjang, atau melakukan pemecahan masalah yang kreatif menjadi sangat terganggu. Sebaliknya, orang cenderung mengandalkan respons yang paling sederhana atau paling sering dilatih.

Stres kronis, di sisi lain, adalah hasil dari paparan jangka panjang terhadap stresor di tempat kerja, seperti beban kerja yang tinggi, kurangnya kontrol atas pekerjaan, konflik interpersonal, atau ketidakamanan kerja. Meskipun tidak sedramatis stres akut, dampaknya bisa lebih merusak dalam jangka panjang. Stres kronis menguras sumber daya mental dan fisik, yang mengarah pada kelelahan, penurunan motivasi, dan masalah kesehatan. Dari perspektif kognitif, stres kronis dapat mengganggu memori, konsentrasi, dan kemampuan untuk belajar hal-hal baru.

Pengaruh gabungan dari stres akut dan kronis pada pengambilan keputusan sangat signifikan. Orang yang sudah lelah karena stres kronis akan memiliki lebih sedikit “cadangan” kognitif untuk mengatasi keadaan darurat akut ketika terjadi. Mereka lebih mungkin untuk “membeku”, membuat keputusan yang prematur, atau gagal mengenali tanda-tanda peringatan dini dari suatu masalah yang berkembang.

Oleh karena itu, strategi mitigasi harus menargetkan kedua jenis stres. Untuk stres akut, pelatihan berbasis simulasi yang sangat realistis sangat penting. Pelatihan ini memungkinkan personel untuk berlatih membuat keputusan di bawah tekanan di lingkungan yang aman, sehingga respons yang benar menjadi lebih otomatis dan kurang rentan terhadap degradasi akibat stres. Untuk stres kronis, solusinya terletak pada desain organisasi dan manajemen. Ini melibatkan memastikan beban kerja yang dapat dikelola, memberikan dukungan sosial dan pengawasan yang baik, meningkatkan kontrol dan otonomi pekerja, serta menciptakan lingkungan kerja yang adil dan saling menghormati.

## 2. Dampak Kurang Tidur dan Kelelahan (*Fatigue*) pada Kinerja

Kelelahan (*fatigue*) adalah salah satu ancaman yang paling meresap dan paling sering diremehkan terhadap keselamatan di tempat kerja. Ini lebih dari sekadar merasa lelah atau mengantuk; kelelahan adalah keadaan penurunan kapasitas mental dan fisik yang dapat secara serius mengganggu hampir setiap aspek kinerja kognitif. Penyebab utamanya adalah kurang tidur, tetapi juga dapat diperburuk oleh pengerahan tenaga fisik atau mental yang berkepanjangan dan stres. Di banyak industri yang beroperasi 24/7, seperti transportasi, perawatan kesehatan, dan manufaktur, kelelahan adalah risiko pekerjaan yang endemik.

Dampak kelelahan pada kinerja sering dibandingkan dengan dampak alkohol, dan perbandingan ini tidak berlebihan. Penelitian telah menunjukkan bahwa setelah sekitar 17-19 jam terjaga, kinerja pada beberapa tes dapat menurun ke tingkat yang setara dengan kadar alkohol dalam darah 0,05%. Setelah 24 jam terjaga, penurunannya setara dengan kadar alkohol 0,10%, yang jauh di atas batas legal untuk mengemudi di sebagian besar negara.

Dampak kognitif spesifik dari kelelahan meliputi:

- a. Penurunan kewaspadaan dan perhatian. Kemampuan untuk mempertahankan konsentrasi menurun, dan orang menjadi lebih rentan terhadap gangguan. Ada juga peningkatan episode "*microsleeps*", yaitu periode tidur singkat yang berlangsung beberapa detik yang mungkin tidak disadari oleh individu.
- b. Waktu reaksi yang melambat. Dibutuhkan waktu lebih lama untuk merespons sinyal atau peristiwa yang tidak terduga.
- c. Gangguan memori jangka pendek. Menjadi lebih sulit untuk mengingat informasi baru atau melacak tugas yang kompleks.
- d. Penurunan kemampuan komunikasi. Berbicara menjadi lebih monoton, dan kemampuan untuk mengekspresikan ide-ide kompleks menurun.
- e. Peningkatan pengambilan risiko. Orang yang lelah cenderung kurang mampu menilai risiko secara akurat dan mungkin membuat pilihan yang lebih impulsif.

- f. Penurunan kemampuan untuk mengatasi situasi tak terduga. Kemampuan untuk berpikir fleksibel dan kreatif untuk memecahkan masalah baru sangat terganggu.

Risiko kelelahan sangat tinggi pada pekerja shift, terutama mereka yang bekerja pada shift malam atau shift yang berotasi. Kerja malam secara langsung bertentangan dengan ritme sirkadian alami tubuh, yang secara biologis memprogram kita untuk tidur di malam hari. Akibatnya, tidur di siang hari sering kali lebih pendek dan kualitasnya lebih buruk, yang menyebabkan akumulasi "utang tidur" dari waktu ke waktu.

Mengelola risiko kelelahan memerlukan pendekatan sistemik, yang dikenal sebagai Sistem Manajemen Risiko Kelelahan (*Fatigue Risk Management System* - FRMS). Ini melampaui sekadar memberitahu pekerja untuk "tidur yang cukup". FRMS yang komprehensif mencakup:

- a. Kebijakan kelelahan. Komitmen tertulis dari manajemen untuk mengelola risiko kelelahan.
- b. Edukasi dan pelatihan. Mengajarkan manajer dan pekerja tentang bahaya kelelahan dan strategi untuk meningkatkan kualitas tidur.
- c. Desain jadwal shift yang ilmiah. Merancang jadwal yang mempertimbangkan prinsip-prinsip sirkadian untuk meminimalkan gangguan tidur.
- d. Sistem pelaporan kelelahan. Menyediakan saluran yang non-hukuman bagi pekerja untuk melaporkan ketika mereka merasa tidak layak untuk bekerja karena kelelahan.
- e. Investigasi insiden. Secara rutin mempertimbangkan kelelahan sebagai faktor kontribusi potensial dalam semua investigasi kecelakaan.

### 3. Mengukur Tingkat Stres Kognitif Pekerja

Salah satu tantangan dalam mengelola stres dan beban kerja kognitif adalah bahwa mereka sering kali merupakan pengalaman internal yang tidak terlihat. Seorang operator mungkin tampak tenang di luar, tetapi secara mental berjuang di bawah beban yang luar biasa. Untuk beralih dari manajemen yang reaktif ke proaktif, organisasi memerlukan cara untuk mengukur dan memantau tingkat stres dan beban kerja kognitif.

Pengukuran ini dapat dikelompokkan menjadi tiga kategori: pengukuran subjektif, pengukuran kinerja, dan pengukuran fisiologis.

Pengukuran Subjektif adalah metode yang paling umum dan paling mudah diterapkan. Metode ini bergantung pada penilaian individu itu sendiri tentang seberapa menuntut suatu tugas. Alat yang paling banyak digunakan adalah NASA Task Load Index (NASA-TLX). Setelah menyelesaikan suatu tugas, seorang pekerja akan menilai tugas tersebut pada enam skala: tuntutan mental, tuntutan fisik, tuntutan temporal (tekanan waktu), tingkat kinerja, tingkat usaha, dan tingkat frustrasi. Skor gabungan memberikan indikator yang andal tentang beban kerja yang dirasakan (Hart & Staveland, 1988). Alat subjektif lainnya termasuk kuesioner stres kerja atau survei persepsi.

Pengukuran Kinerja secara tidak langsung mengukur beban kerja dengan melihat bagaimana kinerja pada suatu tugas berubah. Idanya adalah bahwa ketika beban kerja menjadi terlalu tinggi, kinerja akan mulai menurun. Metrik kinerja dapat mencakup jumlah kesalahan, waktu yang dibutuhkan untuk menyelesaikan tugas, atau variabilitas dalam respons. Salah satu teknik yang umum adalah metode "tugas sekunder". Peserta diminta untuk melakukan tugas utama sambil secara bersamaan melakukan tugas sekunder yang sederhana (misalnya, menekan tombol setiap kali mereka mendengar nada). Penurunan kinerja pada tugas sekunder diasumsikan mencerminkan peningkatan beban kerja dari tugas utama.

Pengukuran Fisiologis menawarkan cara yang paling objektif untuk mengukur respons tubuh terhadap stres dan beban kerja. Metode-metode ini sering kali lebih kompleks dan intrusif, tetapi dapat memberikan wawasan yang berharga. Beberapa pengukuran yang umum digunakan meliputi:

a. Ukuran kardiovaskular

Variabilitas detak jantung (*Heart Rate Variability* - HRV) adalah indikator yang sensitif terhadap beban kerja mental. Ketika beban kerja meningkat, variabilitas detak jantung cenderung menurun.

b. Ukuran okular

Teknologi pelacakan mata (*eye-tracking*) dapat mengukur pergerakan mata, diameter pupil, dan frekuensi kedipan. Diameter pupil, misalnya, cenderung meningkat dengan meningkatnya kesulitan tugas.

c. Aktivitas otak

Elektroensefalografi (EEG) dapat digunakan untuk mengukur aktivitas listrik di otak dan mengidentifikasi pola yang terkait dengan kewaspadaan atau beban kerja mental.

Dalam praktiknya, pendekatan terbaik sering kali melibatkan penggunaan kombinasi dari metode-metode ini. Misalnya, organisasi dapat secara teratur menggunakan survei subjektif untuk mendapatkan gambaran umum tentang "titik panas" beban kerja, dan kemudian menggunakan pengukuran kinerja atau fisiologis untuk menganalisis tugas-tugas yang paling kritis secara lebih mendalam. Tujuan dari pengukuran ini bukanlah untuk memata-matai pekerja, tetapi untuk mengidentifikasi tugas dan proses yang dirancang dengan buruk yang secara konsisten membebani sumber daya kognitif manusia, sehingga memungkinkan intervensi desain yang ditargetkan.

### C. Fenomena *Cognitive Biases* dan *Mistakes*

Otak manusia tidak memproses informasi seperti komputer yang logis dan tidak memihak. Sebaliknya, untuk mengatasi kompleksitas dunia dan membuat keputusan dengan cepat, otak kita sangat bergantung pada heuristik, jalan pintas mental atau "aturan praktis" yang telah berevolusi. Dalam banyak situasi, heuristik ini sangat efisien dan mengarah pada penilaian yang cukup akurat. Namun, dalam konteks tertentu, ketergantungan pada heuristik ini dapat menyebabkan kesalahan yang sistematis dan dapat diprediksi dalam penilaian dan pengambilan keputusan. Kesalahan sistematis ini dikenal sebagai bias kognitif.

Bias kognitif bukanlah tanda kebodohan atau penalaran yang ceroboh; mereka adalah fitur bawaan dari arsitektur kognitif manusia. Mereka memengaruhi semua orang, dari pemula hingga ahli. Memahami bias-bias ini sangat penting dalam K3 karena mereka dapat secara signifikan

mendistorsi persepsi kita terhadap risiko, memengaruhi diagnosis kita terhadap masalah, dan menyesatkan investigasi kita terhadap insiden. Bias-bias ini adalah sumber utama dari *mistakes*, atau kesalahan dalam perencanaan dan penilaian.

Berbeda dengan *slips* dan *lapses* yang merupakan kegagalan dalam eksekusi, *mistakes* adalah hasil dari proses berpikir yang salah. Individu tersebut mungkin telah mengeksekusi rencananya dengan sempurna, tetapi sayangnya rencananya itu sendiri didasarkan pada pemahaman yang keliru tentang situasi. Bias kognitif adalah salah satu alasan utama mengapa pemahaman kita bisa menjadi keliru. Mereka bertindak seperti "filter" tak terlihat yang membentuk cara kita melihat dan menafsirkan informasi, sering kali tanpa kita sadari.

Bagian ini akan mengeksplorasi beberapa bias kognitif yang paling relevan dengan keselamatan, seperti *confirmation bias*, dan akan menghubungkan fenomena ini dengan jenis-jenis *mistakes* yang dibahas sebelumnya. Kita juga akan membahas konsep kesadaran situasi (*situation awareness*) sebagai kerangka kerja untuk memahami bagaimana proses kognitif yang baik dapat gagal, dan mengapa mempertahankannya sangat penting untuk pencegahan *mistakes*. Mengenali keberadaan bias-bias ini adalah langkah pertama untuk mengembangkan strategi untuk memitigasi dampaknya.

**Analogi/Contoh Kasus:** Bayangkan Anda sedang mencari kunci mobil Anda yang hilang. Bias kognitif seperti menggunakan senter dengan sinar yang sangat sempit dalam ruangan yang gelap. Senter (perhatian dan penalaran Anda) mungkin berfungsi dengan baik, tetapi karena Anda memiliki hipotesis awal bahwa Anda meninggalkannya di meja dapur (*confirmation bias*), Anda hanya menyinari area di sekitar meja dapur. Anda mungkin melewatkan fakta bahwa kunci tersebut sebenarnya tergantung di gagang pintu tepat di sebelah Anda, karena itu berada di luar sorotan sempit Anda. Bias kognitif membuat kita "buta" terhadap informasi yang tidak sesuai dengan harapan atau model mental awal kita, bahkan jika informasi itu berada tepat di depan mata kita.

## 1. **Confirmation Bias dan Dampaknya pada Investigasi Insiden**

*Confirmation bias* atau bias konfirmasi adalah salah satu bias kognitif yang paling kuat dan meresap. Ini adalah kecenderungan alami kita untuk mencari, menafsirkan, mendukung, dan mengingat informasi dengan cara yang mengkonfirmasi keyakinan atau hipotesis kita yang sudah ada sebelumnya, sambil memberikan perhatian yang jauh lebih sedikit pada informasi yang bertentangan dengannya. Pada dasarnya, kita tidak melihat dunia sebagaimana adanya; kita melihatnya sebagaimana kita yakini.

Dampak dari bias konfirmasi pada investigasi insiden bisa sangat merusak objektivitas. Seorang investigator yang memulai penyelidikan dengan asumsi awal, misalnya, "ini pasti kesalahan operator karena dia masih baru" atau "peralatan ini selalu bermasalah", secara tidak sadar akan mulai mencari bukti yang mendukung teori awalnya. Dia mungkin akan lebih banyak mengajukan pertanyaan yang mengarahkan saksi untuk mengkonfirmasi kecurigaannya. Dia mungkin akan memberikan bobot yang lebih besar pada data log yang tampaknya menunjukkan kesalahan operator, sambil mungkin mengabaikan atau meremehkan data lain yang menunjukkan adanya kegagalan teknis yang intermiten.

Bias konfirmasi menciptakan efek "visi terowongan" dalam investigasi. Setelah sebuah hipotesis awal terbentuk, menjadi sangat sulit secara psikologis untuk melepaskannya, bahkan di hadapan bukti yang bertentangan. Bukti yang ambigu akan ditafsirkan sebagai pendukung, sementara bukti yang jelas bertentangan mungkin diabaikan sebagai "anomali" atau "tidak relevan". Hal ini dapat menyebabkan investigasi berhenti secara prematur pada penyebab yang paling jelas atau yang paling sesuai dengan prasangka, gagal mengungkap kondisi laten yang lebih dalam dan lebih penting.

Bias ini tidak hanya memengaruhi investigasi setelah kejadian. Dalam diagnosis masalah secara *real-time*, bias konfirmasi juga berbahaya. Seorang operator ruang kontrol yang percaya bahwa alarm tertentu adalah alarm palsu (karena sering terjadi di masa lalu) akan mencari bukti yang mengkonfirmasi bahwa itu memang palsu, dan mungkin memerlukan bukti

yang luar biasa kuat untuk diyakinkan sebaliknya, bahkan ketika situasi yang sebenarnya memburuk.

Mitigasi terhadap bias konfirmasi tidak mudah karena ia beroperasi di tingkat bawah sadar. Namun, beberapa strategi dapat membantu:

- a. Membentuk tim investigasi yang beragam. Tim yang terdiri dari orang-orang dengan latar belakang dan keahlian yang berbeda (misalnya, insinyur, operator, spesialis *human factors*) lebih mungkin untuk menantang asumsi satu sama lain.
- b. Secara aktif mencari bukti yang menyangkal. Salah satu teknik yang paling kuat adalah secara sadar memaksa diri sendiri atau tim untuk bertanya, "Bukti apa yang, jika kita temukan, akan membuktikan hipotesis kita salah?". Ini mendorong pencarian informasi yang lebih seimbang.
- c. Mempertimbangkan beberapa hipotesis secara bersamaan. Daripada mengunci satu "teori utama" sejak awal, investigator harus mencoba untuk mengembangkan beberapa penjelasan yang mungkin dan mengevaluasinya secara paralel.
- d. Pelatihan kesadaran bias. Meskipun tidak dapat menghilangkan bias, pelatihan dapat membuat orang lebih sadar akan keberadaannya dan lebih mungkin untuk mengenali kapan mereka mungkin jatuh ke dalam perangkapnya.

Mengatasi bias konfirmasi adalah inti dari pelaksanaan investigasi yang benar-benar sistemik dan tidak memihak.

## 2. ***Rule-Based Mistakes* (Kesalahan Penerapan Aturan)**

*Rule-based mistakes* atau kesalahan berbasis aturan adalah jenis *mistake* yang sering terjadi pada personel yang berpengalaman dan kompeten. Mereka terjadi bukan karena kurangnya pengetahuan, tetapi karena penerapan aturan atau prosedur yang salah pada suatu situasi. Seperti yang dijelaskan di Bab 3, ini bisa berupa penerapan aturan yang buruk pada situasi yang tepat, atau penerapan aturan yang baik pada situasi yang salah. Fenomena ini sering kali didorong oleh bias kognitif yang kuat.

Salah satu pendorong utama adalah heuristik pencocokan pola (*pattern matching*). Otak kita adalah mesin pencari pola yang luar biasa. Ketika kita menghadapi situasi baru, kita secara otomatis mencoba untuk mencocokkannya dengan pola-pola yang telah kita lihat di masa lalu dari pengalaman atau pelatihan. Jika kita menemukan kecocokan, kita dengan cepat menerapkan solusi atau aturan yang terkait dengan pola tersebut. Proses ini sangat efisien dan biasanya berhasil.

Namun, di sinilah letak jebakannya. Terkadang, sebuah situasi mungkin terlihat sangat mirip dengan pola yang familiar, tetapi memiliki satu atau dua perbedaan kritis yang tidak kentara. Karena kita begitu cepat “mengunci” pola yang familiar, kita mungkin gagal memperhatikan perbedaan-perbedaan penting ini. Akibatnya, kita menerapkan aturan yang “kuat tetapi salah” (*strong but wrong*), aturan yang biasanya benar untuk pola yang familiar, tetapi sama sekali salah untuk situasi yang sebenarnya kita hadapi.

Contoh klasiknya adalah dalam diagnostik medis atau pemecahan masalah teknis. Seorang dokter mungkin melihat serangkaian gejala yang 90% cocok dengan flu biasa, dan dengan cepat mendiagnosisnya sebagai flu. Dia mungkin melewatkan satu gejala atipikal yang sebenarnya merupakan tanda dari penyakit yang jauh lebih serius tetapi jarang terjadi. Demikian pula, seorang teknisi mungkin mendengar suara aneh dari sebuah mesin yang biasanya berarti bantalan perlu dilumasi, dan dia menerapkan solusi tersebut, tanpa menyadari bahwa kali ini suara tersebut disebabkan oleh retakan mikro pada poros.

Frekuensi dan pengalaman dapat secara ironis meningkatkan kerentanan terhadap jenis kesalahan ini. Semakin sering kita berhasil menerapkan aturan tertentu, semakin otomatis dan kuat aturan itu menjadi, dan semakin besar kemungkinan kita akan menerapkannya secara tidak tepat pada situasi yang tampak serupa.

Mitigasi untuk *rule-based mistakes* berfokus pada peningkatan kemampuan diagnosis dan pencegahan penguncian prematur pada satu solusi:

- a. Checklists diagnostik: Menyediakan daftar periksa yang memaksa individu untuk secara sistematis memeriksa semua kemungkinan, bukan hanya yang paling jelas.
- b. Pelatihan berbasis skenario: Memberikan kesempatan kepada peserta untuk berlatih membedakan antara masalah yang tampak serupa tetapi memiliki akar penyebab yang berbeda.
- c. Mendorong "second opinion": Menciptakan norma di mana meminta kolega untuk memeriksa ulang diagnosis yang sulit adalah praktik standar, bukan tanda kelemahan.
- d. Desain antarmuka: Merancang tampilan yang menyoroti parameter-parameter yang tidak normal atau menyimpang untuk membantu memecah pola pikir yang sudah mapan.

Memahami *rule-based mistakes* mengingatkan kita bahwa keahlian bisa menjadi pedang bermata dua; pengalaman yang luas terkadang dapat membuat kita buta terhadap hal-hal baru.

### 3. Pentingnya Kesadaran Situasi (*Situation Awareness*)

Jika ada satu konsep tunggal yang merangkum tujuan dari semua proses kognitif dalam lingkungan kerja yang dinamis, itu adalah kesadaran situasi atau *situation awareness* (SA). SA bukanlah sekadar "memperhatikan"; ini adalah konsep yang jauh lebih kaya. Didefinisikan oleh Mica Endsley, SA adalah "persepsi elemen-elemen di lingkungan dalam volume waktu dan ruang, pemahaman maknanya, dan proyeksi status mereka di masa depan yang dekat". Definisi ini secara efektif menguraikan SA menjadi tiga tingkatan.

#### a. SA Tingkat 1

Persepsi: Ini adalah tingkat yang paling dasar. Ini adalah tentang secara benar mempersepsi informasi yang relevan dari lingkungan kerja. Ini berarti melihat indikator di panel kontrol, mendengar alarm, atau merasakan getaran dari mesin. Kegagalan pada tingkat ini sering kali disebabkan oleh data yang tidak tersedia, sulit dideteksi, atau kegagalan perhatian.

b. SA Tingkat 2

Pemahaman: Ini melampaui sekadar melihat data; ini adalah tentang memahami atau menginterpretasikan makna dari data tersebut dalam konteks tujuan saat ini. Ini melibatkan pengintegrasian beberapa potong informasi untuk membentuk gambaran holistik tentang apa yang sedang terjadi. Misalnya, memahami bahwa alarm suhu tinggi (data 1) yang terjadi bersamaan dengan penurunan tekanan (data 2) berarti ada kebocoran di sistem pendingin (pemahaman). Kegagalan pada tingkat ini sering kali merupakan *mistakes* yang disebabkan oleh model mental yang salah atau kurangnya pengetahuan.

c. SA Tingkat 3

Proyeksi: Ini adalah tingkat SA yang tertinggi. Ini adalah tentang kemampuan untuk memproyeksikan atau mengantisipasi apa yang kemungkinan besar akan terjadi di masa depan yang dekat berdasarkan pemahaman saat ini tentang situasi. Misalnya, seorang pilot dengan SA Tingkat 3 yang baik tidak hanya tahu di mana dia berada dan seberapa cepat dia melaju, tetapi dia juga secara mental “melihat ke depan” untuk mengantisipasi potensi konflik dengan pesawat lain atau perubahan cuaca.

Kehilangan kesadaran situasi (*Loss of Situation Awareness - LSA*) telah diidentifikasi sebagai penyebab utama dalam sebagian besar kecelakaan penerbangan dan insiden di industri berisiko tinggi lainnya. LSA terjadi ketika ada perbedaan antara persepsi operator tentang keadaan sistem dan keadaan sistem yang sebenarnya. Seseorang dapat kehilangan SA karena berbagai alasan: beban kerja yang berlebihan, gangguan, informasi yang ambigu, atau bias kognitif.

Mempertahankan SA adalah proses yang aktif dan dinamis. Ini membutuhkan pemindaian informasi yang konstan, pembaruan model mental, dan pemikiran “bagaimana-jika”. Mengingat pentingnya SA, strategi mitigasi sangat berfokus pada mendukungnya:

- a. Desain tampilan: Merancang antarmuka yang menyajikan informasi dengan cara yang terintegrasi dan mendukung pemahaman, bukan hanya menampilkan data mentah. Tampilan “prediktif” yang

menunjukkan di mana sistem akan berada di masa depan adalah contoh yang baik.

- b. Pelatihan: Pelatihan berbasis simulasi yang secara khusus dirancang untuk menantang dan mengukur SA. Sesi *debriefing* setelah simulasi dapat berfokus pada di mana SA hilang dan mengapa.
- c. Kerja Tim (CRM): Tim yang efektif secara konstan berbagi informasi dan memeriksa silang pemahaman mereka tentang situasi, menciptakan model mental tim yang sama. Ini adalah salah satu pertahanan terkuat terhadap hilangnya SA oleh individu.

Pada dasarnya, semua keterbatasan kognitif dan bias yang telah kita diskusikan berkontribusi pada potensi hilangnya SA. Oleh karena itu, semua upaya untuk mendukung memori, mengelola perhatian, dan mengurangi bias pada akhirnya adalah upaya untuk membangun dan mempertahankan kesadaran situasi yang tinggi.

#### **D. Strategi Mitigasi Berbasis Kognisi**

Memahami berbagai cara di mana proses kognitif dan perseptual kita dapat gagal hanyalah setengah dari pertempuran. Pemahaman ini tidak banyak gunanya kecuali jika ia mengarah pada pengembangan dan implementasi strategi mitigasi yang efektif. Jika masalahnya terletak pada keterbatasan bawaan dari “perangkat keras” mental kita dan “perangkat lunak” heuristik kita, maka solusinya tidak bisa hanya berupa seruan untuk “berpikir lebih keras” atau “lebih berhati-hati”. Sebaliknya, solusinya harus bersifat sistemik, berfokus pada perancangan ulang sistem kerja agar lebih sesuai dengan arsitektur kognitif manusia. Pendekatan ini dikenal sebagai ergonomi kognitif atau rekayasa *human factors*.

Tujuan dari strategi mitigasi berbasis kognisi bukanlah untuk menghilangkan kebutuhan akan pemikiran manusia, tetapi untuk mendukung dan memperkuatnya. Ini adalah tentang menciptakan lingkungan kerja di mana sumber daya kognitif kita yang terbatas tidak disia-siakan untuk hal-hal sepele, tetapi dapat difokuskan pada aspek-aspek tugas yang benar-benar membutuhkan kecerdasan dan penilaian

manusia. Ini adalah tentang menyediakan “alat-alat kognitif” eksternal yang dapat mengkompensasi kelemahan internal kita.

Strategi-strategi ini dapat diterapkan di berbagai tingkatan. Di tingkat desain antarmuka, tujuannya adalah untuk menyajikan informasi dengan cara yang meminimalkan beban memori dan perhatian serta mempromosikan kesadaran situasi. Di tingkat desain tugas, tujuannya adalah untuk menyusun alur kerja dengan cara yang logis dan mengurangi kemungkinan kesalahan. Dan di tingkat pelatihan, tujuannya adalah untuk membekali individu dengan keterampilan mental, bukan hanya pengetahuan prosedural, untuk mengelola perhatian, mengatasi stres, dan mengenali bias dalam pemikiran mereka sendiri.

Bagian ini akan menguraikan beberapa strategi mitigasi berbasis kognisi yang paling kuat dan dapat ditindaklanjuti. Ini termasuk teknik untuk memetakan tugas secara visual, prinsip-prinsip untuk merancang antarmuka yang mengurangi beban kognitif, dan metode untuk pelatihan mental. Penerapan strategi-strategi ini secara sistematis adalah cara paling efektif untuk mengurangi *human error* pada sumbernya.

**Analogi/Contoh Kasus:** Bayangkan seorang pilot pesawat tempur. Dia dihadapkan pada sejumlah besar informasi yang kompleks di bawah tekanan waktu yang ekstrim. Sistem pesawat tempur modern adalah sebuah keajaiban ergonomi kognitif, yang dirancang untuk mendukung pilot, bukan membebani. Informasi yang paling penting ditampilkan di *Head-Up Display* (HUD), diproyeksikan ke pandangan depannya sehingga dia tidak perlu melihat ke bawah (mengurangi beban perhatian). Simbol-simbol yang terintegrasi menunjukkan status pesawat dan ancaman secara visual (mendukung pemahaman SA). Sistem peringatan menggunakan isyarat auditori yang berbeda untuk berbagai tingkat ancaman (menyajikan informasi secara intuitif). Sistem ini adalah contoh sempurna dari mitigasi berbasis kognisi: ia tidak menggantikan pilot, tetapi memberinya “indera super” kognitif untuk melakukan pekerjaannya dengan aman dan efektif.

## 1. Teknik Cognitive Mapping dan Visualisasi Tugas

Salah satu tantangan terbesar dalam tugas yang kompleks adalah membangun dan memelihara model mental yang akurat tentang

bagaimana semua bagian yang bergerak saling cocok. Ketika tugas hanya ada sebagai serangkaian langkah dalam prosedur tertulis atau di dalam kepala beberapa ahli, sulit bagi tim untuk memiliki pemahaman bersama dan mengidentifikasi potensi masalah. Analisis tugas kognitif (*Cognitive Task Analysis*) dan teknik visualisasi terkait adalah metode untuk mengekstraksi dan membuat model mental ini menjadi eksplisit dan terlihat oleh semua orang.

Analisis tugas hierarkis (*Hierarchical Task Analysis - HTA*), yang akan dibahas lebih lanjut di Bab 10, adalah salah satu teknik dasar. Ini memecah tugas menjadi tujuan utama, sub-tujuan, dan operasi spesifik. Membuat diagram HTA secara visual membantu tim untuk memahami struktur tugas dan mengidentifikasi langkah-langkah kritis.

Teknik yang lebih canggih adalah pemetaan kognitif (*cognitive mapping*). Ini adalah proses menciptakan representasi visual dari hubungan, proses, dan keputusan yang terlibat dalam suatu tugas. Peta ini dapat berupa diagram alir, diagram sebab-akibat, atau diagram jaringan. Tujuannya adalah untuk menunjukkan bagaimana informasi mengalir, di mana keputusan kunci dibuat, dan apa saja ketergantungan antar langkah.

Manfaat dari teknik-teknik ini sangat banyak:

a. Pemahaman Bersama

Dengan memvisualisasikan tugas, seluruh tim dapat mengembangkan model mental bersama (*shared mental model*). Ini sangat penting untuk koordinasi dan komunikasi yang efektif, karena semua orang bekerja dari "peta" yang sama.

b. Identifikasi Titik Rawan Kesalahan

Peta visual memudahkan untuk melihat titik-titik dalam proses di mana beban kerja kognitif mungkin tinggi, di mana ada potensi ambiguitas, atau di mana ada ketergantungan pada satu individu. Ini adalah "hotspot" yang memerlukan pertahanan tambahan.

c. Dasar untuk Desain

Peta tugas kognitif adalah alat yang sangat baik untuk tim desain. Mereka dapat digunakan untuk merancang antarmuka, prosedur, atau

alat bantu keputusan yang secara langsung mendukung tuntutan kognitif yang telah diidentifikasi.

d. Alat Pelatihan

Peta visual adalah alat bantu pelatihan yang sangat baik, terutama untuk pemula. Mereka membantu peserta didik untuk memahami “mengapa” di balik langkah-langkah prosedural, bukan hanya “apa” yang harus dilakukan.

Dalam praktiknya, proses ini sering kali melibatkan wawancara dengan para ahli materi pelajaran (*Subject Matter Experts* - SMEs) dan observasi kerja untuk memahami bagaimana tugas sebenarnya dilakukan. Informasi ini kemudian digunakan untuk membangun model visual secara kolaboratif. Dengan membuat pengetahuan tak terucapkan (*tacit knowledge*) dari para ahli menjadi terlihat, teknik visualisasi tugas memungkinkan pengetahuan tersebut untuk dianalisis, ditingkatkan, dan dibagikan ke seluruh organisasi.

## 2. Mendesain Antarmuka yang Mengurangi Beban Memori

Mengingat bahwa memori kerja manusia sangat terbatas, salah satu kontribusi terbesar yang dapat diberikan oleh desain sistem adalah mengurangi atau menghilangkan kebutuhan untuk mengingat informasi. Prinsip dasarnya sederhana: letakkan pengetahuan di dunia, bukan di dalam kepala. Setiap kali seorang pengguna harus mengingat sesuatu, itu adalah peluang untuk terjadinya *lapse*. Antarmuka yang dirancang dengan baik berfungsi sebagai “memori eksternal” bagi pengguna, menyajikan informasi yang mereka butuhkan pada saat mereka membutuhkannya.

Beberapa prinsip desain kunci untuk mengurangi beban memori meliputi:

a. Visibilitas (*Visibility*)

Buat semua opsi dan status sistem yang relevan menjadi terlihat. Pengguna tidak seharusnya harus mengingat cara menuju fungsi tertentu atau apa arti dari mode operasi yang tersembunyi. Menu yang terstruktur dengan baik dan ikon yang jelas adalah contoh dari visibilitas yang baik.

b. Pengenalan daripada Mengingat (*Recognition over Recall*)

Manusia jauh lebih baik dalam mengenali sesuatu ketika mereka melihatnya daripada mencoba mengingatnya dari awal. Inilah sebabnya mengapa menu *drop-down* jauh lebih mudah digunakan daripada antarmuka baris perintah, yang mengharuskan pengguna untuk mengingat perintah yang tepat.

c. Batasan (*Constraints*)

Batasi tindakan yang mungkin dilakukan oleh pengguna untuk mencegah kesalahan. Batasan bisa bersifat fisik (colokan yang hanya bisa masuk satu arah) atau logis (opsi menu yang “berwarna abu-abu” dan tidak dapat dipilih dalam konteks tertentu). Ini mengurangi kebutuhan pengguna untuk mengingat apa yang boleh dan tidak boleh dilakukan.

d. Konsistensi

Gunakan terminologi, tata letak, dan urutan tindakan yang konsisten di seluruh antarmuka. Konsistensi memungkinkan pengguna untuk mentransfer pembelajaran dari satu bagian sistem ke bagian lain, mengurangi jumlah hal baru yang harus mereka ingat.

Dalam konteks industri, prinsip-prinsip ini dapat diterapkan dalam banyak cara. Label yang jelas dan permanen pada semua kontrol, katup, dan pemutus sirkuit mengurangi ketergantungan pada ingatan. Tampilan proses terintegrasi yang menunjukkan hubungan antara berbagai parameter membantu operator untuk memahami gambaran besar tanpa harus mengingat nilai-nilai individu. Prosedur berbasis komputer yang interaktif dapat memandu pengguna langkah demi langkah, hanya menyajikan informasi yang relevan untuk langkah saat ini dan secara otomatis mencatat apa yang telah dilakukan.

Setiap elemen desain yang memaksa pengguna untuk berhenti dan mencoba mengingat sesuatu adalah “gesekan” kognitif dan titik rawan kesalahan. Dengan secara sistematis mencari dan menghilangkan gesekan ini, kita dapat menciptakan sistem yang tidak hanya lebih aman tetapi juga lebih mudah dan lebih cepat untuk digunakan.

### 3. Pelatihan Mental untuk Peningkatan Fokus dan Perhatian

Sementara banyak strategi mitigasi berfokus pada perancangan ulang dunia eksternal, ada juga semakin banyak minat pada strategi yang bertujuan untuk meningkatkan kapasitas kognitif internal kita. Ini bukan tentang mengubah arsitektur dasar otak kita, tetapi tentang melatih keterampilan mental yang dapat membantu kita untuk lebih baik dalam mengelola sumber daya kita yang terbatas, seperti perhatian, dan untuk lebih tahan terhadap dampak negatif dari stres.

Salah satu bidang yang menjanjikan adalah pelatihan perhatian dan kesadaran (*attention and mindfulness training*). Praktik-praktik seperti meditasi kesadaran, yang pada dasarnya adalah latihan dalam memfokuskan dan memfokuskan kembali perhatian, telah terbukti dalam penelitian klinis dapat meningkatkan fungsi eksekutif, memori kerja, dan kemampuan untuk mempertahankan konsentrasi. Dalam konteks K3, program-program yang diadaptasi dari praktik ini dapat membantu pekerja untuk lebih baik dalam:

- a. Mengenali kapan pikiran mereka mengembara dari tugas yang ada.
- b. Secara sadar mengarahkan kembali fokus mereka ke saat ini.
- c. Mengelola respons emosional mereka terhadap stresor, sehingga tidak terlalu reaktif.

Bidang lain yang sangat penting adalah pelatihan manajemen stres. Teknik-teknik seperti biofeedback, latihan pernapasan dalam, dan restrukturisasi kognitif (belajar untuk menantang dan membongkar ulang pikiran-pikiran yang menimbulkan stres) dapat diajarkan kepada pekerja di lingkungan berisiko tinggi. Tujuannya bukanlah untuk menghilangkan stres, yang tidak mungkin, tetapi untuk memberi mereka alat untuk mengelola respons fisiologis dan psikologis mereka terhadap stres, sehingga mereka dapat mempertahankan kinerja kognitif yang lebih baik di bawah tekanan.

Pelatihan berbasis simulasi tetap menjadi salah satu alat yang paling kuat untuk pelatihan mental. Simulasi yang dirancang dengan baik tidak hanya mengajarkan prosedur; mereka melatih proses kognitif. Mereka memungkinkan peserta untuk:

- a. Membangun model mental yang akurat tentang bagaimana sistem bekerja.

- b. Berlatih pengambilan keputusan dalam skenario yang kompleks dan ambigu.
- c. Mengalami dan belajar untuk mengelola beban kerja kognitif yang tinggi di lingkungan yang aman.
- d. Berlatih keterampilan kerja tim dan komunikasi (CRM) di bawah tekanan.

Penting untuk ditekankan bahwa pelatihan mental bukanlah pengganti untuk desain sistem yang baik. Kita tidak dapat “melatih” seseorang untuk mengatasi antarmuka yang dirancang dengan sangat buruk atau jadwal kerja yang melelahkan. Namun, sebagai pelengkap dari sistem yang dirancang dengan baik, pelatihan keterampilan mental dapat memberikan lapisan pertahanan manusiawi tambahan, meningkatkan kemampuan individu dan tim untuk menjadi lebih waspada, fokus, dan tangguh dalam menghadapi tantangan operasional.

## **KESIMPULAN**

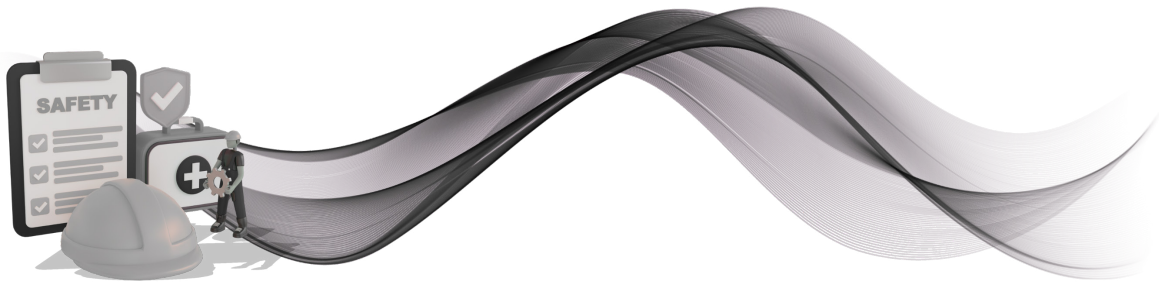
Bab ketujuh ini telah membawa kita ke dalam “kotak hitam” pikiran manusia untuk memahami mekanisme internal yang mendasari *human error*. Kita telah melihat bahwa otak, meskipun luar biasa, beroperasi di bawah serangkaian keterbatasan perangkat keras yang jelas: memori kerja yang sempit, perhatian yang terbatas, dan kerentanan terhadap kelebihan beban kognitif. Keadaan seperti stres dan kelelahan semakin memperburuk keterbatasan ini, secara signifikan menurunkan kemampuan kita untuk berpikir jernih dan bertindak dengan aman.

Selain itu, “perangkat lunak” pemikiran kita dipenuhi dengan bias kognitif, jalan pintas mental yang, meskipun efisien, dapat secara sistematis menyesatkan penilaian kita. Fenomena seperti bias konfirmasi dapat mendistorsi investigasi, sementara kesalahan pencocokan pola dapat menyebabkan *mistakes* bahkan di antara para ahli. Kegagalan untuk membangun dan memelihara kesadaran situasi (*situation awareness*) yang akurat telah diidentifikasi sebagai jalur umum menuju bencana.

Pemahaman mendalam tentang faktor-faktor kognitif dan perseptual ini bukanlah sebuah latihan akademis. Ia memiliki implikasi praktis yang mendalam, yang paling penting adalah bahwa kita tidak dapat dan tidak

boleh menyalahkan individu karena memiliki otak manusia. Sebaliknya, pengetahuan ini harus mendorong kita untuk merangkul ergonomi kognitif sebagai prinsip inti dari manajemen keselamatan. Tujuannya adalah untuk merancang sistem, tugas, dan antarmuka yang bekerja selaras dengan cara pikiran kita bekerja, mendukung kekuatannya dan mengkompensasi kelemahannya.

Strategi-strategi seperti visualisasi tugas, desain antarmuka yang mengurangi beban memori, dan pelatihan mental menunjukkan jalan ke depan. Mereka mewakili pergeseran dari upaya yang sia-sia untuk mengubah sifat manusia menjadi upaya yang jauh lebih produktif untuk mengubah kondisi di mana manusia bekerja. Dengan dasar pemahaman tentang keterbatasan individu ini, kita sekarang siap untuk kembali ke tingkat sistem dan mengeksplorasi bagaimana faktor-faktor organisasi dan lingkungan yang lebih luas berinteraksi dengan faktor-faktor kognitif ini, yang akan menjadi fokus dari bab berikutnya.



# BAB 8

## PENGARUH FAKTOR ORGANISASI DAN LINGKUNGAN KERJA

### PENDAHULUAN

Seorang operator yang sangat terlatih dan waspada, bekerja dengan peralatan yang dirancang secara ergonomis, masih dapat membuat kesalahan fatal. Mengapa? Jawaban atas pertanyaan ini sering kali tidak terletak pada individu atau pada antarmuka mesinnya, melainkan pada kekuatan-kekuatan tak terlihat yang membentuk konteks pekerjaannya. Bayangkan seorang pemain catur jenius yang dipaksa bermain di tengah badai, dengan jam catur yang terus dipercepat oleh wasit, dan dengan penonton yang terus-menerus meneriakan nasihat yang saling bertentangan. Betapapun hebatnya pemain itu, kualitas permainannya pasti akan menurun. Konteks, bukan hanya kompetensi, sering kali menjadi penentu antara keberhasilan dan kegagalan.

Bab-bab sebelumnya telah membawa kita dari pandangan makro sistemik (Model Keju Swiss) ke tingkat mikro interaksi manusia-mesin (Model SHELL) dan bahkan lebih dalam lagi ke dalam proses kognitif individu. Sekarang, kita akan memperluas lensa kita kembali untuk memeriksa kekuatan-kekuatan kontekstual yang paling kuat yang membentuk perilaku

manusia di tempat kerja: faktor organisasi dan lingkungan. Ini adalah “cuaca” dan “iklim” di mana pekerjaan dilakukan. Faktor-faktor ini adalah sumber utama dari kondisi-kondisi laten, menciptakan tekanan dan kendala yang secara sistematis dapat membuat kesalahan menjadi lebih mungkin dan pelanggaran menjadi lebih menarik.

Perjalanan dalam bab ini akan dimulai dengan eksplorasi konsep budaya dan iklim keselamatan. Budaya keselamatan adalah “kepribadian” organisasi dalam hal risiko, yaitu nilai-nilai dan keyakinan bersama yang menentukan “cara kita melakukan sesuatu di sini”. Iklim keselamatan, di sisi lain, adalah manifestasi yang lebih terlihat dari budaya tersebut, persepsi karyawan tentang prioritas keselamatan yang sebenarnya. Kita akan membedah karakteristik budaya keselamatan yang kuat dan menganalisis bagaimana norma-norma organisasi dapat secara kuat mendorong perilaku aman atau, sebaliknya, menoleransi pengambilan risiko.

Selanjutnya, perhatian akan dialihkan ke salah satu musuh keselamatan yang paling meresap di era modern: kelelahan (*fatigue*). Dampak dari jadwal kerja yang buruk, shift kerja yang panjang, dan gangguan ritme sirkadian akan dianalisis secara mendalam. Kelelahan bukanlah masalah kemauan atau ketangguhan individu; ini adalah risiko fisiologis yang dapat dikelola yang memerlukan pendekatan sistemik, yang dikenal sebagai *Fatigue Risk Management System* (FRMS).

Desain tempat kerja, yang melampaui sekadar mesin dan alat, juga akan menjadi fokus. Ergonomi fisik dan kognitif akan dibahas sebagai disiplin ilmu yang bertujuan untuk merancang keseluruhan lingkungan kerja, mulai dari posisi kerja hingga cara informasi disajikan, untuk mendukung kinerja manusia. Pengaruh faktor-faktor lingkungan ambien seperti pencahayaan dan kebisingan, yang sering dianggap sepele, akan ditunjukkan sebagai kontributor signifikan terhadap kesalahan dan stres.

Terakhir dan yang paling penting, bab ini akan menyoroiti peran kepemimpinan yang tak tergantikan dalam membentuk semua faktor lainnya. Pemimpin, terutama manajemen puncak, adalah “arsitek” utama dari lingkungan kerja. Melalui komitmen mereka yang terlihat, alokasi sumber daya, dan gaya kepemimpinan mereka, para pemimpin

memiliki kekuatan untuk menciptakan lingkungan yang secara sistematis memperkuat pertahanan keselamatan atau, sebaliknya, mengikisnya. Perbedaan antara kepemimpinan transaksional dan transformasional dalam konteks K3 akan dianalisis untuk menunjukkan bagaimana para pemimpin dapat menginspirasi komitmen terhadap keselamatan yang melampaui sekadar kepatuhan.

Memahami pengaruh faktor-faktor organisasi dan lingkungan adalah langkah terakhir yang krusial dalam melengkapi gambaran sistemik kita. Ini adalah pengakuan bahwa untuk mengelola *human error* secara efektif, kita tidak dapat hanya fokus pada pekerja di lini depan. Kita harus secara proaktif merancang dan mengelola budaya, jadwal, lingkungan fisik, dan kepemimpinan yang secara kolektif menciptakan kondisi di mana orang-orang dapat berhasil.

### **A. Pengaruh Iklim Keselamatan (*Safety Climate*) dan Budaya Keselamatan (*Safety Culture*)**

Dalam analisis kegagalan sistemik, budaya keselamatan (*safety culture*) sering disebut sebagai kondisi laten paling fundamental yang memengaruhi semua lapisan pertahanan lainnya. Budaya keselamatan adalah fondasi di mana semua upaya K3 dibangun; jika fondasinya rapuh, struktur yang paling canggih sekalipun pada akhirnya akan runtuh. Ini adalah konsep yang sulit dipahami karena sebagian besar tidak terlihat, namun pengaruhnya sangat nyata. Budaya keselamatan adalah ekspresi dari nilai-nilai dan keyakinan bersama tentang risiko, kecelakaan, dan keselamatan di dalam sebuah organisasi. Ia menjawab pertanyaan: "Seberapa pentingkah keselamatan di sini?".

Sementara budaya adalah konsep yang lebih dalam dan lebih stabil, "iklim keselamatan" (*safety climate*) adalah manifestasinya yang lebih permukaan dan dapat diukur pada waktu tertentu. Iklim keselamatan adalah persepsi yang dimiliki oleh karyawan tentang kebijakan, prosedur, dan praktik keselamatan di tempat kerja mereka. Ini adalah "perasaan" atau "suasana" keselamatan saat ini. Jika budaya adalah kepribadian organisasi, iklim adalah suasana hatinya. Iklim keselamatan yang positif, di mana karyawan percaya bahwa manajemen benar-benar peduli terhadap

kesejahteraan mereka, adalah prediktor kuat dari perilaku aman dan hasil keselamatan yang lebih baik.

Pengaruh iklim dan budaya meresap ke dalam setiap keputusan dan tindakan sehari-hari. Dalam budaya keselamatan yang kuat, seorang pekerja tidak akan ragu untuk menghentikan pekerjaan jika dia melihat kondisi yang tidak aman, karena dia tahu tindakannya akan didukung oleh manajemen. Dalam budaya yang lemah, pekerja yang sama mungkin akan tetap diam karena takut ditegur karena menyebabkan penundaan. Budaya menentukan norma-norma, aturan-aturan tidak tertulis tentang perilaku yang dapat diterima, yang sering kali lebih kuat daripada aturan tertulis dalam prosedur.

Membangun budaya keselamatan yang kuat bukanlah proyek jangka pendek; ini adalah proses evolusi jangka panjang yang membutuhkan komitmen yang tak tergoyahkan dari kepemimpinan. Ini melibatkan penciptaan kepercayaan, komunikasi terbuka, dan sistem yang adil untuk menangani kesalahan. Mengabaikan budaya dan hanya berfokus pada kontrol teknis dan prosedural adalah resep untuk kegagalan, karena pada akhirnya manusialah yang harus membuat pertahanan tersebut berfungsi, dan perilaku mereka sangat dibentuk oleh budaya di mana mereka bekerja.

**Analogi/Contoh Kasus:** Budaya keselamatan sebuah organisasi dapat diibaratkan seperti tanah di sebuah kebun. Anda dapat membeli benih terbaik (personel yang kompeten), sistem penyiraman tercanggih (teknologi keselamatan), dan buku petunjuk penanaman yang paling detail (prosedur). Namun, jika Anda menanam semuanya di tanah yang berbatu, asam, dan tidak subur (budaya keselamatan yang buruk), tanaman Anda akan tumbuh kerdil, sakit-sakitan, dan tidak akan pernah mencapai potensi penuhnya. Sebaliknya, tanah yang subur dan kaya nutrisi (budaya keselamatan yang positif) akan mendukung pertumbuhan yang sehat, membuat tanaman lebih tahan terhadap penyakit (kegagalan), dan menghasilkan panen yang melimpah (kinerja keselamatan yang unggul). Budaya bukanlah tanaman itu sendiri, tetapi merupakan medium esensial yang menentukan apakah segala sesuatu yang lain akan berhasil atau gagal.

## 1. Definisi dan Karakteristik Budaya Keselamatan yang Kuat

Budaya keselamatan pertama kali menjadi sorotan global setelah bencana nuklir Chernobyl pada tahun 1986. Laporan investigasi menyimpulkan bahwa salah satu akar penyebab utama adalah “budaya keselamatan yang kurang” di kalangan operator dan manajemen. Sejak saat itu, konsep ini telah menjadi pusat perhatian dalam manajemen risiko. Secara formal, budaya keselamatan dapat didefinisikan sebagai “produk dari nilai-nilai, sikap, persepsi, kompetensi, dan pola perilaku individu dan kelompok yang menentukan komitmen terhadap, serta gaya dan kemahiran dari, program kesehatan dan keselamatan suatu organisasi”. Ini adalah tentang apa yang dilakukan orang ketika tidak ada yang mengawasi.

Budaya keselamatan bukanlah konsep tunggal, melainkan terdiri dari beberapa sub-komponen yang saling terkait. James Reason mengidentifikasi beberapa karakteristik kunci dari sebuah organisasi dengan budaya keselamatan yang matang dan positif. Karakteristik ini menyediakan cetak biru tentang seperti apa “keadaan baik” itu. Sebuah organisasi yang aman tidak hanya memiliki prosedur dan teknologi, tetapi juga menjiwai nilai-nilai ini dalam praktik sehari-harinya, menciptakan pertahanan yang tangguh terhadap kesalahan.

Pertama, ada budaya yang terinformasi (*informed culture*). Dalam budaya ini, organisasi secara aktif mengumpulkan, menganalisis, dan menyebarkan data dari berbagai sumber untuk memahami risiko yang dihadapinya. Para pemimpin dan pekerja sama-sama memiliki kesadaran yang akurat tentang bahaya yang melekat dalam operasi mereka. Mereka tidak hanya mengandalkan data kecelakaan di masa lalu, tetapi juga secara proaktif mencari sinyal-sinyal lemah dari masalah yang mungkin berkembang. Informasi ini tidak disembunyikan atau dimanipulasi, melainkan dibagikan secara terbuka untuk mendorong pembelajaran.

Selanjutnya adalah budaya pelaporan (*reporting culture*). Ini adalah lingkungan di mana orang merasa aman dan bahkan didorong untuk melaporkan kesalahan, *near misses*, dan kondisi tidak aman tanpa takut akan hukuman. Organisasi memahami bahwa laporan-laporan ini adalah “hadiah gratis”, wawasan berharga tentang kelemahan sistem. Untuk

menumbuhkan budaya ini, proses pelaporan harus mudah, bermanfaat (pelapor mendapatkan umpan balik), dan yang terpenting, non-hukuman. Kepercayaan adalah mata uang dari budaya pelaporan.

Budaya pelaporan harus didukung oleh budaya yang adil (*just culture*). Seperti yang dibahas sebelumnya, ini adalah suasana di mana ada pemahaman bersama tentang di mana garis ditarik antara kesalahan manusia yang tidak dapat diterima dan yang dapat diterima. Organisasi memiliki sistem yang jelas dan transparan untuk membedakan antara kesalahan yang tidak disengaja (yang harus ditanggapi dengan pembelajaran), perilaku berisiko (yang memerlukan pembinaan), dan pelanggaran sembrono (yang memerlukan tindakan disipliner). Keadilan ini membangun kepercayaan yang diperlukan untuk pelaporan yang jujur.

Budaya keselamatan yang kuat juga merupakan budaya yang fleksibel (*flexible culture*). Ini adalah kemampuan organisasi untuk beradaptasi dan mengubah strukturnya dalam menghadapi situasi darurat atau risiko yang meningkat. Dalam operasi normal, organisasi mungkin beroperasi secara hierarkis. Namun, dalam keadaan darurat, budaya yang fleksibel memungkinkan otoritas untuk beralih ke orang-orang dengan keahlian yang paling relevan pada saat itu, terlepas dari pangkat formal mereka. Ini mencegah pengambilan keputusan yang kaku dan tidak efektif di bawah tekanan.

Terakhir, semua komponen ini menyatu dalam budaya pembelajaran (*learning culture*). Ini adalah kemauan dan kompetensi organisasi untuk menarik kesimpulan yang benar dari informasi keselamatannya, dan kemauan untuk menerapkan reformasi besar ketika diperlukan. Organisasi yang belajar tidak puas dengan status quo. Mereka memiliki "keasyikan dengan kegagalan" (*preoccupation with failure*), yang berarti mereka secara konstan waspada terhadap kemungkinan kesalahan dan memperlakukan setiap insiden, sekecil apa pun, sebagai peluang untuk meningkatkan pertahanan mereka.

## **2. Peran Nilai dan Norma Organisasi terhadap Perilaku Aman**

Nilai dan norma adalah inti dari budaya organisasi. Nilai adalah keyakinan yang dipegang teguh tentang apa yang penting, benar, dan

diinginkan. Norma adalah aturan tidak tertulis tentang perilaku yang diharapkan atau "normal" dalam suatu kelompok. Bersama-sama, nilai dan norma membentuk "kompas" internal yang memandu keputusan dan tindakan karyawan, sering kali pada tingkat bawah sadar. Peran mereka dalam membentuk perilaku aman sangatlah besar, sering kali melebihi pengaruh prosedur tertulis atau ancaman hukuman.

Ketika keselamatan adalah nilai inti yang dianut secara tulus oleh sebuah organisasi, ia menjadi pertimbangan non-negosiasi dalam semua keputusan. Ini berarti bahwa jika terjadi konflik antara keselamatan dan tujuan lain seperti produksi atau biaya, keselamatan secara konsisten akan diprioritaskan. Nilai ini harus ditanamkan dan diperkuat mulai dari puncak. Ketika para pemimpin secara konsisten membuat keputusan yang menunjukkan bahwa mereka menghargai kesejahteraan karyawan di atas keuntungan jangka pendek, nilai ini akan meresap ke seluruh organisasi. Sebaliknya, jika para pemimpin mengatakan keselamatan itu penting tetapi tindakan mereka menunjukkan sebaliknya, karyawan akan dengan cepat belajar bahwa nilai yang sebenarnya adalah produksi.

Norma perilaku kemudian muncul dari nilai-nilai ini. Di tempat kerja dengan norma keselamatan yang kuat, perilaku seperti memakai APD dengan benar, melakukan pemeriksaan pra-tugas, dan saling mengingatkan tentang bahaya menjadi perilaku standar yang diharapkan dari semua orang. Anggota baru dengan cepat belajar bahwa "inilah cara kita melakukan sesuatu di sini". Norma-norma ini diperkuat melalui tekanan rekan kerja (*peer pressure*) yang positif. Seorang pekerja yang mencoba mengambil jalan pintas mungkin akan ditegur oleh rekan kerjanya, bukan karena mereka ingin menjadi "polisi keselamatan", tetapi karena perilaku tidak aman tersebut melanggar norma kelompok yang diterima.

Sebaliknya, di tempat kerja dengan norma keselamatan yang lemah, yang terjadi adalah sebaliknya. Pengambilan jalan pintas, mengabaikan prosedur, atau tidak melaporkan *near misses* dapat menjadi perilaku "normal". Tekanan rekan kerja mungkin justru bekerja ke arah yang negatif, di mana pekerja yang mencoba untuk mengikuti aturan keselamatan dengan ketat mungkin diejek sebagai orang yang "lambat" atau "tidak menjadi bagian dari tim". Norma-norma negatif ini bisa sangat sulit

untuk diubah karena mereka sering kali didukung oleh keuntungan yang dirasakan, seperti menyelesaikan pekerjaan lebih cepat.

Nilai dan norma juga memengaruhi persepsi risiko. Dalam sebuah organisasi di mana kecelakaan dilihat sebagai sesuatu yang tak terhindarkan atau “biaya menjalankan bisnis”, karyawan cenderung menjadi lebih pasrah dan menerima risiko yang lebih tinggi. Sebaliknya, dalam sebuah organisasi yang menganut nilai bahwa semua cedera dapat dicegah, karyawan akan lebih proaktif dalam mengidentifikasi dan mengendalikan bahaya. Norma-norma tentang komunikasi juga penting; jika norma yang ada adalah untuk menghindari konflik dan tidak menyampaikan berita buruk kepada atasan, maka masalah keselamatan yang kritis mungkin tidak akan pernah dilaporkan ke atas.

Oleh karena itu, upaya untuk meningkatkan perilaku aman tidak dapat hanya berfokus pada pelatihan individu tentang aturan. Upaya tersebut harus mencakup intervensi yang bertujuan untuk mengubah nilai dan norma kolektif. Ini adalah proses jangka panjang yang melibatkan kepemimpinan yang konsisten, dialog terbuka tentang nilai-nilai, pengakuan dan penghargaan terhadap perilaku yang diinginkan, serta memastikan bahwa sistem dan proses organisasi (seperti penilaian kinerja dan promosi) selaras dengan nilai-nilai keselamatan yang dinyatakan.

## **B. Metode Pengukuran dan Peningkatan Iklim Keselamatan**

Karena budaya keselamatan adalah konsep yang dalam dan sulit diukur secara langsung, banyak organisasi memilih untuk fokus pada pengukuran iklim keselamatan. Iklim keselamatan, sebagai persepsi bersama karyawan tentang keselamatan pada waktu tertentu, lebih mudah diukur dan dapat berfungsi sebagai “proksi” atau indikator utama dari budaya yang mendasarinya. Mengukur iklim keselamatan secara teratur memungkinkan organisasi untuk mendiagnosis kekuatan dan kelemahan dalam program K3 mereka, melacak kemajuan dari waktu ke waktu, dan membandingkan (*benchmark*) diri mereka dengan unit bisnis lain atau standar industri.

Metode yang paling umum untuk mengukur iklim keselamatan adalah melalui survei persepsi keselamatan (*safety climate surveys*). Survei ini

biasanya terdiri dari serangkaian pernyataan di mana karyawan diminta untuk menilai tingkat persetujuan mereka (misalnya, pada skala Likert 1-5). Pernyataan-pernyataan ini dirancang untuk mengukur persepsi karyawan tentang berbagai dimensi iklim keselamatan. Dimensi yang umum diukur meliputi:

- a. Komitmen manajemen: "Manajemen di sini menganggap keselamatan sama pentingnya dengan produksi."
- b. Tindakan pengawas: "Penyelia saya secara teratur memuji perilaku kerja yang aman."
- c. Komunikasi keselamatan: "Kami secara teratur mengadakan pertemuan untuk membahas masalah keselamatan."
- d. Partisipasi karyawan: "Saya merasa nyaman untuk melaporkan masalah keselamatan tanpa takut akan sanksi."
- e. Tekanan produksi: "Kami sering diminta untuk mengabaikan aturan keselamatan untuk menyelesaikan pekerjaan lebih cepat."

Hasil survei, yang harus selalu dijaga kerahasiaannya untuk mendorong jawaban yang jujur, kemudian dianalisis secara statistik. Hasilnya dapat memberikan gambaran yang kuat tentang di mana letak "titik panas" masalah dalam organisasi. Misalnya, jika skor untuk komitmen manajemen tinggi tetapi skor untuk tekanan produksi sangat rendah, ini menunjukkan adanya konflik pesan yang perlu ditangani. Hasil juga dapat dipecah berdasarkan departemen, shift, atau lokasi untuk mengidentifikasi area dengan iklim keselamatan yang paling buruk.

Metode pengukuran lain yang melengkapi survei termasuk wawancara dan kelompok fokus (*focus groups*). Metode kualitatif ini memungkinkan organisasi untuk menggali lebih dalam "mengapa" di balik skor survei. Diskusi terbuka dengan kelompok-kelompok kecil karyawan dapat mengungkap nuansa, contoh spesifik, dan saran-saran untuk perbaikan yang mungkin tidak tertangkap oleh survei kuantitatif.

Observasi perilaku kerja adalah metode lain, di mana pengamat yang terlatih secara sistematis mengamati dan mencatat frekuensi perilaku aman dan tidak aman di tempat kerja. Meskipun ini lebih mengukur perilaku

daripada persepsi, hasilnya dapat menjadi indikator yang baik dari iklim keselamatan yang mendasarinya.

Setelah iklim keselamatan diukur dan area-area untuk perbaikan diidentifikasi, langkah selanjutnya adalah peningkatan. Peningkatan harus menjadi proses yang partisipatif. Berbagi hasil survei secara transparan dengan karyawan dan melibatkan mereka dalam mengembangkan rencana tindakan adalah kunci untuk mendapatkan dukungan dan komitmen. Rencana tindakan harus spesifik, terukur, dapat dicapai, relevan, dan terikat waktu (SMART). Tindakan dapat berkisar dari pelatihan kepemimpinan untuk penyelia, perbaikan proses komunikasi, hingga perancangan ulang sistem insentif. Siklus pengukuran dan peningkatan ini, yang idealnya dilakukan setiap tahun, mengubah iklim keselamatan menjadi bagian yang dapat dikelola dan ditingkatkan dari K3MS.

### **C. Dampak Jadwal Kerja, *Shift*, dan Kelelahan (*Fatigue*)**

Dalam ekonomi global 24/7, pekerjaan tidak lagi berhenti saat matahari terbenam. Banyak industri kritis, mulai dari manufaktur dan transportasi hingga layanan darurat dan perawatan kesehatan, bergantung pada pekerja shift untuk menjaga operasi tetap berjalan sepanjang waktu. Meskipun penting secara ekonomi, model kerja ini datang dengan biaya fisiologis dan keselamatan yang signifikan. Tubuh manusia secara biologis tidak dirancang untuk aktif di malam hari dan tidur di siang hari. Mengabaikan realitas biologis ini dan merancang jadwal kerja yang buruk adalah salah satu cara paling pasti untuk menciptakan kondisi laten yang mengarah pada kelelahan (*fatigue*), yang pada gilirannya secara dramatis meningkatkan risiko *human error*.

Kelelahan lebih dari sekadar rasa lelah; ini adalah gangguan kompleks yang melibatkan interaksi antara waktu dalam sehari (ritme sirkadian), jumlah tidur yang diperoleh, dan lamanya waktu terjaga. Dampaknya terhadap fungsi kognitif, seperti yang dibahas di Bab 7, bisa setara dengan keracunan alkohol, yang mengganggu perhatian, penilaian, dan waktu reaksi. Kecelakaan-kecelakaan besar seperti bencana nuklir Chernobyl, tumpahan minyak Exxon Valdez, dan ledakan pesawat ulang-alik Challenger semuanya memiliki kelelahan sebagai faktor kontribusi yang signifikan.

Tantangan dalam mengelola kelelahan adalah bahwa ia sering kali dianggap sebagai masalah pribadi atau tanda kelemahan, bukan sebagai risiko pekerjaan yang sah. Banyak budaya kerja bahkan mengagungkan kemampuan untuk bekerja berjam-jam tanpa istirahat. Pendekatan sistemik menolak pandangan ini dan sebaliknya memperlakukan kelelahan sebagai bahaya di tempat kerja yang harus dikelola melalui kontrol rekayasa, administratif, dan praktik kerja, sama seperti bahaya lainnya.

Bagian ini akan menyelami lebih dalam risiko yang terkait dengan kerja shift dan kelelahan. Kita akan menganalisis bagaimana jadwal kerja mengganggu ritme sirkadian alami kita, memperkenalkan kerangka kerja formal untuk mengelola risiko ini (*Fatigue Risk Management System - FRMS*), dan membahas kebijakan spesifik terkait istirahat dan rotasi kerja yang dapat membantu memitigasi dampak terburuk dari tuntutan kerja 24 jam.

**Analogi/Contoh Kasus:** Bayangkan baterai ponsel Anda. Setiap malam, Anda mengisi ulanginya hingga 100% (tidur). Sepanjang hari, setiap aplikasi yang Anda gunakan (tugas mental dan fisik) menguras daya. Jika Anda tidak mengisi ulang baterai sepenuhnya, Anda memulai hari berikutnya dengan daya, katakanlah, 70%. Jika Anda juga menjalankan aplikasi yang sangat berat (beban kerja tinggi) atau menjaga layar tetap menyala terus-menerus (waktu terjaga yang lama), baterai akan terkuras lebih cepat. Bekerja pada shift malam ibarat mencoba mengisi ulang ponsel Anda dengan pengisi daya yang salah yang hanya mengisi hingga 50%. Kelelahan adalah keadaan ketika tingkat daya baterai Anda sangat rendah. Ketika ini terjadi, ponsel (otak Anda) mulai melambat, aplikasi macet (kesalahan), dan akhirnya mungkin mati sama sekali (*microsleep*). FRMS adalah seperti aplikasi manajemen baterai yang cerdas: ia memantau tingkat daya, memperingatkan Anda ketika rendah, dan menyarankan cara untuk menghemat daya (misalnya, mengambil istirahat).

## 1. Analisis Risiko Shift Work dan Ritme Sirkadian

Tubuh manusia beroperasi berdasarkan jam internal 24 jam yang dikenal sebagai ritme sirkadian. Jam master ini, yang terletak di hipotalamus otak, mengatur berbagai fungsi fisiologis dan psikologis, termasuk siklus

tidur-bangun, suhu tubuh, pelepasan hormon, dan kewaspadaan. Ritme ini secara alami disinkronkan dengan siklus terang-gelap lingkungan, yang memberi sinyal pada tubuh kita untuk aktif di siang hari dan beristirahat di malam hari.

**Kerja shift**, terutama kerja shift malam, secara langsung bertentangan dengan pemrograman biologis ini. Ketika seorang pekerja harus tetap terjaga dan waspada pada saat tubuhnya secara fisiologis berada pada titik terendah (biasanya antara jam 2 dan 6 pagi), mereka berjuang melawan dorongan tidur yang kuat. Sebaliknya, ketika mereka mencoba untuk tidur di siang hari, jam sirkadian mereka, bersama dengan cahaya dan kebisingan lingkungan, memberi sinyal pada tubuh mereka untuk bangun. Akibatnya, tidur di siang hari hampir selalu lebih pendek dan kualitasnya lebih buruk daripada tidur di malam hari.

Konflik antara tuntutan kerja dan ritme sirkadian ini menyebabkan beberapa konsekuensi negatif:

- a. Penurunan Kinerja: Kewaspadaan, waktu reaksi, memori, dan fungsi kognitif lainnya secara signifikan lebih buruk selama shift malam dibandingkan shift siang, bahkan setelah beberapa malam berturut-turut. Risiko kesalahan dan kecelakaan terbukti secara statistik lebih tinggi pada shift malam.
- b. Utang Tidur Kronis: Karena kualitas tidur yang buruk di siang hari, pekerja shift sering mengalami defisit tidur kronis. Utang tidur ini terakumulasi dari waktu ke waktu, yang semakin memperburuk kelelahan dan penurunan kinerja.
- c. Masalah Kesehatan Jangka Panjang: Gangguan sirkadian kronis telah dikaitkan dengan peningkatan risiko berbagai masalah kesehatan, termasuk penyakit kardiovaskular, gangguan metabolisme seperti diabetes, masalah pencernaan, dan bahkan beberapa jenis kanker.

Selain waktu dalam sehari, desain jadwal shift itu sendiri merupakan faktor risiko yang penting. Beberapa karakteristik jadwal yang sangat berisiko meliputi:

- a. Shift yang sangat panjang (misalnya, lebih dari 12 jam).
- b. Awal shift yang sangat pagi (misalnya, dimulai sebelum jam 6 pagi).

- c. Rotasi shift yang cepat, terutama rotasi yang berlawanan arah jarum jam (misalnya, dari shift malam ke shift sore ke shift pagi), yang paling sulit bagi jam tubuh untuk beradaptasi.
- d. Waktu istirahat yang tidak cukup antara shift (misalnya, kurang dari 11 jam).

Analisis risiko kerja shift harus menjadi bagian standar dari proses penilaian risiko K3 di setiap organisasi yang beroperasi 24/7. Ini melibatkan identifikasi tugas-tugas yang paling sensitif terhadap kelelahan (misalnya, tugas-tugas yang membutuhkan kewaspadaan tinggi atau bersifat monoton) dan mengevaluasi bagaimana jadwal kerja saat ini dapat meningkatkan risiko kegagalan pada tugas-tugas tersebut. Alat-alat pemodelan biomatematis dapat digunakan untuk memprediksi tingkat kelelahan yang mungkin dialami oleh pekerja berdasarkan jadwal tertentu, yang memungkinkan perbandingan dan optimalisasi jadwal sebelum diimplementasikan.

## **2. Strategi Manajemen Kelelahan (Fatigue Risk Management System - FRMS)**

Menyadari bahwa kelelahan adalah risiko K3 yang kompleks dan multidimensional, pendekatan modern telah beralih dari sekadar membatasi jam kerja ke kerangka kerja yang lebih holistik dan berbasis data yang dikenal sebagai Sistem Manajemen Risiko Kelelahan (*Fatigue Risk Management System - FRMS*). FRMS didefinisikan sebagai “seperangkat praktik manajemen berbasis data untuk mengidentifikasi dan mengurangi risiko kelelahan, sambil mengelola dampak operasionalnya” (IPIECA, 2011). Ini adalah pendekatan sistemik yang mengakui tanggung jawab bersama antara organisasi dan karyawan dalam mengelola kelelahan.

FRMS yang efektif biasanya dibangun di atas beberapa pilar utama, sering kali dalam format sistem manajemen yang mirip dengan ISO 45001.

### **a. Kebijakan FRMS**

Ini adalah pernyataan komitmen dari manajemen puncak untuk mengelola risiko kelelahan. Kebijakan ini harus menetapkan tujuan, sasaran, dan akuntabilitas untuk FRMS di seluruh organisasi.

b. Pelatihan dan Edukasi

Semua personel, dari manajer hingga pekerja, harus menerima pelatihan tentang ilmu tidur dan ritme sirkadian, penyebab dan konsekuensi kelelahan, serta strategi pribadi untuk meningkatkan kualitas tidur (misalnya, higiene tidur). Manajer dan penyelia memerlukan pelatihan tambahan tentang cara mengenali tanda-tanda kelelahan pada tim mereka dan cara merancang jadwal yang lebih aman.

c. Sistem Pelaporan Kelelahan

Organisasi harus menyediakan saluran yang rahasia dan non-hukuman bagi karyawan untuk melaporkan insiden yang berhubungan dengan kelelahan atau untuk menyatakan bahwa mereka merasa tidak layak untuk bekerja karena kelelahan. Data dari laporan ini sangat penting untuk memahami di mana letak masalah kelelahan terbesar.

d. Proses Manajemen Risiko Kelelahan

Ini adalah inti dari FRMS. Proses ini melibatkan:

- 1) Identifikasi Bahaya Kelelahan: Menganalisis jadwal kerja, jenis tugas, dan faktor-faktor lain untuk mengidentifikasi di mana dan kapan risiko kelelahan paling tinggi.
- 2) Penilaian Risiko: Mengevaluasi tingkat risiko yang terkait dengan bahaya-bahaya ini.
- 3) Implementasi Kontrol: Menerapkan serangkaian kontrol untuk memitigasi risiko. Kontrol ini bisa berupa desain jadwal yang lebih baik, penyediaan fasilitas istirahat, atau penerapan teknologi pemantauan kelelahan (dengan pertimbangan etis yang cermat).

e. Investigasi Insiden

Memasukkan kelelahan sebagai faktor potensial untuk diselidiki dalam semua investigasi kecelakaan dan insiden.

f. Pemantauan dan Peninjauan

Secara teratur meninjau data (misalnya, data pelaporan, data kinerja, data jadwal) untuk menilai efektivitas FRMS dan melakukan perbaikan berkelanjutan.

Penerapan FRMS memungkinkan organisasi untuk bergerak dari pendekatan preskriptif yang kaku (misalnya, "tidak boleh bekerja lebih dari X jam") ke pendekatan berbasis kinerja yang lebih fleksibel dan efektif, di mana tingkat risiko kelelahan yang sebenarnya dinilai dan dikelola secara proaktif.

### 3. Kebijakan Istirahat dan Rotasi Kerja yang Efektif

Salah satu kontrol paling kritis dalam FRMS adalah desain jadwal kerja itu sendiri, yang mencakup kebijakan tentang waktu istirahat dan rotasi shift. Merancang jadwal yang baik adalah tentang menyeimbangkan tuntutan operasional dengan batasan fisiologis manusia. Meskipun tidak ada satu jadwal "sempurna" yang cocok untuk semua, ada beberapa prinsip berbasis bukti yang dapat memandu pengembangan kebijakan yang lebih aman.

#### a. Waktu Istirahat di Dalam Shift

Istirahat pendek dan sering terbukti lebih efektif dalam mempertahankan kinerja daripada satu kali istirahat makan siang yang panjang. Istirahat memberikan kesempatan bagi otak untuk pulih dari kelelahan mental. Untuk tugas-tugas yang menuntut kewaspadaan tinggi atau bersifat monoton, istirahat harus dijadwalkan secara proaktif, bukan hanya diambil ketika pekerja sudah merasa lelah. Memberikan akses ke "ruang tidur siang" (*nap room*) untuk istirahat singkat (15-20 menit) selama shift malam dapat menjadi strategi yang sangat efektif untuk meningkatkan kewaspadaan.

#### b. Waktu Istirahat Antar Shift

Sangat penting untuk memberikan waktu pemulihan yang cukup di antara periode kerja. Sebagian besar pedoman merekomendasikan minimal 10-11 jam libur antara akhir satu shift dan awal shift berikutnya untuk memungkinkan waktu perjalanan, makan, interaksi sosial, dan setidaknya 7-8 jam kesempatan untuk tidur. Periode istirahat yang lebih lama (misalnya, 2-3 hari libur berturut-turut) diperlukan setelah serangkaian shift malam atau shift yang panjang untuk memungkinkan pemulihan penuh dari utang tidur.

### c. **Desain Rotasi Shift**

Jika rotasi shift tidak dapat dihindari, desainnya harus mencoba untuk bekerja selaras dengan jam tubuh, bukan melawannya. Prinsip-prinsip utama meliputi:

#### 1) **Rotasi maju (*Forward rotation*)**

Rotasi harus bergerak searah jarum jam, dari shift pagi ke shift sore ke shift malam. Arah ini lebih mudah bagi jam sirkadian untuk beradaptasi daripada rotasi mundur.

#### 2) **Kecepatan rotasi**

Rotasi yang cepat (misalnya, bekerja 2-3 hari pada setiap shift sebelum berotasi) sering kali lebih disukai daripada rotasi mingguan yang lambat. Rotasi yang cepat tidak memberikan cukup waktu bagi jam tubuh untuk beradaptasi sepenuhnya ke jadwal malam, yang ironisnya membuatnya lebih mudah untuk kembali ke jadwal normal pada hari libur.

#### 3) **Batasi jumlah shift malam berturut-turut**

Sebagian besar ahli merekomendasikan untuk tidak menjadwalkan lebih dari 3 atau 4 shift malam berturut-turut untuk mencegah penumpukan kelelahan yang parah.

**Fleksibilitas:** Jika memungkinkan, memberikan tingkat fleksibilitas dan kontrol kepada pekerja atas jadwal mereka dapat meningkatkan kepuasan dan mengurangi stres. Namun, fleksibilitas ini harus dikelola dalam kerangka batasan jam kerja yang aman untuk mencegah jam kerja yang berlebihan.

Implementasi kebijakan ini memerlukan kolaborasi antara manajemen, perencana jadwal, dan perwakilan karyawan. Alat pemodelan biomatematis dapat digunakan untuk mengevaluasi berbagai skenario jadwal dan memprediksi dampaknya terhadap kelelahan sebelum diimplementasikan. Dengan memperlakukan desain jadwal sebagai kontrol rekayasa untuk risiko kelelahan, organisasi dapat secara signifikan mengurangi salah satu kondisi laten yang paling umum di tempat kerja modern.

## D. Faktor Desain Tempat Kerja (Ergonomi Fisik dan Kognitif)

Desain tempat kerja secara fundamental membentuk cara kita berinteraksi dengan pekerjaan kita. Setiap aspek, mulai dari ketinggian kursi hingga tata letak layar komputer, dapat membuat pekerjaan lebih mudah dan lebih aman, atau lebih sulit dan lebih berbahaya. Disiplin ilmu ergonomi (atau *human factors*) adalah ilmu terapan yang berfokus pada perancangan dan penataan hal-hal yang digunakan orang sehingga interaksi antara manusia dan hal-hal tersebut menjadi optimal. Tujuannya ganda: untuk meningkatkan kesejahteraan manusia (dengan mengurangi stres, kelelahan, dan cedera) dan untuk meningkatkan kinerja sistem secara keseluruhan (dengan membuat pekerjaan lebih efisien dan mengurangi kesalahan).

Pendekatan ergonomis secara inheren bersifat sistemik dan berpusat pada manusia. Ia menolak gagasan untuk mencoba "memperbaiki" atau "menyesuaikan" manusia agar cocok dengan sistem yang dirancang dengan buruk. Sebaliknya, ia menuntut agar sistemlah yang harus dirancang agar sesuai dengan kapabilitas dan keterbatasan manusia. Dalam konteks mitigasi *human error*, ergonomi adalah salah satu alat pencegahan proaktif yang paling kuat yang kita miliki. Dengan merancang tempat kerja yang sesuai dengan kebutuhan fisik dan kognitif kita, kita secara langsung menghilangkan banyak "jebakan kesalahan" dari lingkungan.

Ergonomi secara tradisional dibagi menjadi dua bidang utama yang saling melengkapi. Ergonomi fisik berfokus pada anatomi, antropometri, dan biomekanika manusia dalam kaitannya dengan aktivitas fisik. Ini adalah tentang merancang untuk tubuh. Ergonomi kognitif, yang telah kita singgung di bab sebelumnya, berfokus pada proses mental seperti persepsi, memori, dan penalaran. Ini adalah tentang merancang untuk pikiran.

Tempat kerja yang dirancang dengan buruk dari kedua perspektif ini adalah pabrik kondisi laten. Desain yang buruk tidak hanya menyebabkan masalah kesehatan jangka panjang seperti gangguan muskuloskeletal, tetapi juga meningkatkan kelelahan, stres, dan beban kerja kognitif dalam jangka pendek, yang semuanya merupakan prekursor yang diketahui untuk

*human error*. Bagian ini akan menguraikan lebih lanjut bagaimana prinsip-prinsip ergonomi fisik dan kognitif dapat diterapkan untuk menciptakan lingkungan kerja yang lebih aman.

**Analogi/Contoh Kasus:** Bayangkan mendesain sebuah mobil. Ergonomi fisik adalah tentang memastikan bahwa kursi dapat disesuaikan agar pengemudi dengan berbagai ukuran dapat duduk dengan nyaman dan mencapai pedal, bahwa setir mudah digenggam, dan bahwa spion memberikan bidang pandang yang baik. Desain yang buruk di sini menyebabkan sakit punggung dan kelelahan fisik. Ergonomi kognitif adalah tentang memastikan bahwa *dashboard* mudah dibaca, bahwa simbol-simbolnya intuitif, bahwa sistem navigasi mudah dioperasikan, dan bahwa peringatan (seperti peringatan bahan bakar rendah) jelas dan tidak ambigu. Desain yang buruk di sini menyebabkan kebingungan, gangguan, dan kesalahan navigasi. Sebuah mobil yang dirancang dengan baik harus unggul dalam kedua aspek ergonomi untuk menjadi aman dan menyenangkan untuk dikendarai. Tempat kerja pun demikian.

### 1. Ergonomi Fisik: Posisi Kerja dan Desain Alat

Ergonomi fisik adalah aspek ergonomi yang paling dikenal luas. Fokus utamanya adalah mencegah gangguan muskuloskeletal terkait kerja (*Work-related Musculoskeletal Disorders - WMSDs*), seperti cedera punggung, *carpal tunnel syndrome*, dan tendinitis. WMSDs berkembang dari waktu ke waktu sebagai akibat dari ketegangan berulang atau postur yang canggung. Namun, dampak dari ergonomi fisik yang buruk melampaui cedera kronis; ia juga menyebabkan kelelahan, ketidaknyamanan, dan penurunan kinerja dalam jangka pendek, yang dapat meningkatkan kemungkinan kesalahan.

Prinsip inti dari ergonomi fisik adalah untuk menjaga tubuh dalam postur netral sebanyak mungkin. Postur netral adalah postur di mana sendi-sendi berada dalam posisi yang rileks dan tidak tegang, dan otot-otot tidak perlu bekerja keras untuk menahan posisi. Bekerja dengan pergelangan tangan yang tertekuk, punggung yang membungkuk, atau lengan yang

terangkat adalah contoh postur non-netral yang meningkatkan risiko cedera dan kelelahan.

Penerapan ergonomi fisik dalam desain stasiun kerja melibatkan beberapa elemen kunci:

a. **Dapat disesuaikan (*Adjustability*)**

Karena tidak ada dua orang yang memiliki ukuran tubuh yang sama, stasiun kerja harus dapat disesuaikan. Ini adalah prinsip "sesuaikan pekerjaan dengan pekerja". Contohnya termasuk kursi kantor dengan berbagai penyesuaian (tinggi, sandaran punggung, sandaran tangan), meja kerja yang ketinggiannya dapat diubah, dan monitor komputer pada lengan yang dapat diatur posisinya.

b. **Desain untuk Gerakan**

Tubuh manusia tidak dirancang untuk tetap statis dalam satu posisi untuk waktu yang lama. Desain yang baik mendorong variasi postur dan gerakan. Ini mungkin melibatkan penyediaan opsi untuk bekerja sambil duduk atau berdiri, atau merancang alur kerja yang mengharuskan pekerja untuk bergerak secara berkala.

c. **Mengurangi Kekuatan Berlebihan**

Tugas-tugas yang memerlukan pengerahan kekuatan yang tinggi atau berulang harus direkayasa ulang. Ini dapat dicapai dengan menyediakan alat bantu angkat mekanis (misalnya, *hoist* atau konveyor), menggunakan alat dengan pegangan yang lebih baik untuk meningkatkan cengkraman, atau mengurangi berat benda yang harus ditangani.

Desain alat tangan adalah sub-bidang penting lainnya. Alat yang dirancang dengan baik akan pas dengan nyaman di tangan, meminimalkan tekanan pada pergelangan tangan, dan mengurangi getaran. Alat yang dirancang dengan buruk dapat menjadi sumber utama WMSDs.

Dengan secara proaktif menerapkan prinsip-prinsip ergonomi fisik, organisasi tidak hanya dapat secara drastis mengurangi biaya yang

terkait dengan WMSDs (seperti biaya kompensasi dan absensi), tetapi juga menciptakan tenaga kerja yang lebih nyaman, tidak terlalu lelah, dan oleh karena itu, kurang rentan untuk membuat kesalahan akibat ketidaknyamanan atau kelelahan fisik.

## 2. Ergonomi Kognitif: Desain Informasi dan Pengambilan Keputusan

Ergonomi kognitif, atau rekayasa kognitif, berfokus pada perancangan sistem agar sesuai dengan kekuatan dan kelemahan pikiran manusia. Tujuannya adalah untuk membuat interaksi dengan teknologi dan informasi menjadi seintuitif dan sebebaskan mungkin dari kesalahan. Di dunia yang semakin dipenuhi dengan data dan sistem yang kompleks, pentingnya ergonomi kognitif terus meningkat. Desain yang buruk dalam domain ini adalah penyebab utama dari kelebihan beban kognitif, hilangnya kesadaran situasi, dan *mistakes*.

Salah satu bidang inti dari ergonomi kognitif adalah desain tampilan informasi. Tujuannya adalah untuk menyajikan data dengan cara yang tidak hanya memungkinkan orang untuk membacanya, tetapi juga untuk memahaminya dengan cepat dan akurat. Beberapa prinsip utama meliputi:

### a. Prinsip Kedekatan (*Proximity Compatibility*)

Informasi yang perlu diproses atau dibandingkan bersama harus ditempatkan berdekatan secara spasial.

### b. Prinsip Keterlihatan (*Legibility*)

Teks dan simbol harus cukup besar dan kontrasnya cukup tinggi untuk dapat dibaca dengan mudah dalam kondisi pencahayaan yang diharapkan.

### c. Prinsip Minimalisme

Hindari kekacauan visual. Tampilan seharusnya hanya menyajikan informasi yang diperlukan untuk tugas saat ini, menghilangkan data yang tidak relevan yang dapat mengganggu.

### d. Prinsip Representasi Grafis

Gunakan grafik, diagram, dan bagan jika memungkinkan, karena otak manusia sering kali dapat memproses informasi visual-spasial lebih cepat daripada teks atau angka mentah.

Desain sistem pendukung keputusan adalah aplikasi lain yang penting. Sistem ini tidak membuat keputusan untuk manusia, tetapi membantu mereka membuat keputusan yang lebih baik dengan mengatasi keterbatasan kognitif. Contohnya termasuk sistem diagnostik medis yang menyarankan kemungkinan diagnosis berdasarkan gejala, atau sistem di ruang kontrol yang dapat memprediksi tren proses di masa depan berdasarkan data saat ini. Sistem-sistem ini dapat membantu melawan bias konfirmasi dengan menyajikan hipotesis alternatif dan mengurangi beban memori kerja.

Desain alarm adalah sub-bidang kritis dalam ergonomi kognitif. Di banyak industri, "banjir alarm" (*alarm flooding*), di mana ratusan atau ribuan alarm berbunyi selama gangguan pabrik, adalah masalah serius. Hal ini membuat operator tidak mungkin untuk mengidentifikasi alarm mana yang benar-benar penting. Desain alarm yang baik melibatkan rasionalisasi dan prioritas alarm, memastikan bahwa hanya alarm yang memerlukan respons operator yang disajikan, dan menggunakan isyarat auditori dan visual yang berbeda untuk berbagai tingkat urgensi.

Dengan menerapkan prinsip-prinsip ergonomi kognitif, kita dapat merancang sistem yang bekerja sebagai "mitra" kognitif bagi pengguna, bukan sebagai "lawan" yang membingungkan. Ini menghasilkan pengambilan keputusan yang lebih cepat, kesadaran situasi yang lebih baik, dan pengurangan signifikan dalam *mistakes* yang mahal.

### **3. Pengaruh Lingkungan Kerja (Pencahayaannya, Kebisingan) terhadap Kesalahan**

Meskipun pencahayaan dan kebisingan sering dianggap sebagai masalah kenyamanan atau kesehatan jangka panjang (seperti kerusakan pendengaran), dampaknya terhadap kinerja dan *human error* dalam jangka pendek juga sangat signifikan. Kondisi lingkungan yang tidak sesuai dapat bertindak sebagai stresor, mengganggu komunikasi, dan secara langsung menyebabkan kesalahan perseptual. Mereka adalah bagian integral dari antarmuka Liveware-Environment yang harus dikelola secara aktif.

Pencahayaan yang buruk adalah penyebab langsung dari banyak kesalahan. Tingkat pencahayaan yang terlalu rendah dapat membuat sulit

untuk membaca label, instruksi, atau tampilan instrumen, yang mengarah pada salah tafsir. Ini juga dapat menyembunyikan bahaya tersandung atau bahaya fisik lainnya di lingkungan kerja. Di sisi lain, pencahayaan yang terlalu terang atau silau juga bermasalah. Silau dari jendela atau lampu di atas kepala yang memantul dari layar komputer atau permukaan kerja yang mengkilap dapat membuat informasi menjadi tidak terbaca dan menyebabkan kelelahan mata serta sakit kepala. Kualitas cahaya, seperti rendering warna, juga penting. Di lingkungan di mana kode warna digunakan untuk keselamatan (misalnya, pada pengkabelan atau perpipaan), sumber cahaya yang mendistorsi warna dapat menyebabkan kesalahan identifikasi yang berbahaya.

Kebisingan memiliki efek ganda yang merusak. Pertama, ia dapat menutupi (*masking*) sinyal auditori yang penting. Ini adalah masalah keselamatan yang serius. Alarm peringatan, teriakan peringatan dari rekan kerja, atau suara aneh dari mesin yang menandakan adanya masalah mungkin tidak terdengar di atas kebisingan latar belakang industri. Kedua, kebisingan, terutama yang tidak terduga atau tidak dapat dikendalikan, adalah stresor fisiologis dan kognitif yang kuat. Paparan kebisingan yang terus-menerus dapat meningkatkan tingkat stres, tekanan darah, dan kelelahan. Ini juga secara langsung mengganggu kinerja pada tugas-tugas yang membutuhkan perhatian dan memori kerja, karena kebisingan yang tidak relevan “mencuri” sebagian dari sumber daya kognitif kita yang terbatas.

Mitigasi untuk masalah lingkungan ini harus selalu mengikuti hierarki kontrol. Untuk pencahayaan, solusinya meliputi penyediaan pencahayaan tugas (*task lighting*) yang dapat disesuaikan di stasiun kerja, menggunakan pelindung anti-silau pada layar, dan memilih warna cat dan permukaan akhir yang tidak memantulkan. Untuk kebisingan, prioritasnya adalah kontrol rekayasa seperti memasang peredam suara pada mesin atau membangun penutup akustik. Mengandalkan alat pelindung diri (APD) seperti penyumbat telinga harus menjadi pilihan terakhir, karena APD itu sendiri dapat menciptakan masalah baru dengan menghalangi komunikasi verbal.

Mengelola faktor-faktor lingkungan ini bukanlah “kemewahan”, melainkan komponen esensial dari perancangan sistem kerja yang aman. Dengan menyediakan lingkungan sensorik yang optimal, kita memberikan fondasi di mana proses perseptual dan kognitif dapat berfungsi dengan baik, sehingga mengurangi kemungkinan kesalahan.

## **E. Peran Kepemimpinan dalam Menciptakan Lingkungan yang Aman**

Jika faktor-faktor organisasi dan lingkungan adalah kekuatan kontekstual yang membentuk perilaku, maka kepemimpinan adalah tangan yang mengarahkan kekuatan-kekuatan tersebut. Tidak ada faktor tunggal yang lebih berpengaruh dalam membentuk budaya keselamatan, menetapkan prioritas, dan menciptakan lingkungan kerja yang positif selain perilaku dan komitmen para pemimpin di semua tingkatan, dari penyelia lini pertama hingga CEO. Kepemimpinan bukanlah sekadar posisi atau jabatan; itu adalah serangkaian tindakan dan perilaku yang memengaruhi dan memotivasi orang lain untuk mencapai tujuan bersama. Dalam konteks K3, tujuan itu adalah menciptakan tempat kerja di mana tidak ada yang terluka.

Para pemimpin adalah “arsitek” dan “penjaga” budaya. Apa yang dikatakan oleh para pemimpin, apa yang mereka lakukan, apa yang mereka ukur, dan apa yang mereka hargai secara kolektif mengirimkan sinyal yang sangat kuat kepada seluruh organisasi tentang apa yang benar-benar penting. Jika ada ketidaksesuaian antara kata-kata pemimpin (misalnya, “keselamatan adalah prioritas nomor satu”) dan tindakan mereka (misalnya, memberi penghargaan kepada manajer yang mencapai target produksi dengan mengabaikan aturan keselamatan), karyawan akan selalu memperhatikan tindakan, bukan kata-kata. Ketidaksesuaian ini adalah sumber sinisme yang merusak dan secara aktif melemahkan iklim keselamatan.

Peran kepemimpinan dalam keselamatan melampaui sekadar memastikan kepatuhan terhadap aturan. Kepemimpinan yang efektif menginspirasi tingkat komitmen terhadap keselamatan yang melampaui kepatuhan minimum. Ini adalah tentang menciptakan lingkungan di mana

karyawan secara proaktif terlibat dalam keselamatan, merasa diberdayakan untuk menyuarakan keprihatinan, dan mengambil kepemilikan pribadi atas kesejahteraan mereka sendiri dan rekan kerja mereka.

Gaya kepemimpinan yang berbeda memiliki dampak yang berbeda pula terhadap hasil keselamatan. Bagian ini akan mengeksplorasi perbedaan antara gaya kepemimpinan transaksional dan transformasional, menyoroti pentingnya komitmen manajemen puncak yang nyata dan terlihat, dan membahas praktik kepemimpinan spesifik seperti *safety walkdowns* yang dapat menerjemahkan niat baik menjadi dampak nyata di lini depan.

**Analogi/Contoh Kasus:** Seorang pemimpin dalam organisasi ibarat seorang kapten kapal. Kapten tidak hanya berdiri di anjungan dan memberikan perintah; dia menetapkan tujuan (visi keselamatan nol kecelakaan), memetakan jalur (strategi K3), dan yang terpenting, dia menciptakan iklim di atas kapal (budaya). Jika kapten tenang dan kompeten selama badai, kru akan merasa percaya diri. Jika kapten secara teratur memeriksa setiap bagian kapal dan berbicara dengan para pelaut (visibilitas), mereka akan tahu dia peduli. Jika dia secara adil menangani kesalahan dan tidak hanya menghukum, kru akan melaporkan masalah dengan jujur. Sebaliknya, jika kapten hanya bersembunyi di kabinnya, meneriakkan perintah yang tidak realistis, dan menyalahkan kru atas setiap masalah, maka kapalnya akan dipenuhi oleh ketakutan, ketidakpercayaan, dan pada akhirnya, lebih mungkin untuk mengalami bencana. Arah dan nasib kapal, seperti halnya keselamatan organisasi, sangat ditentukan oleh kepemimpinan di pucuk pimpinan.

### 1. **Kepemimpinan Transaksional vs. Transformasional dalam K3**

Dalam literatur manajemen, dua gaya kepemimpinan yang sering dikontraskan adalah transaksional dan transformasional. Keduanya dapat berperan dalam manajemen K3, tetapi kepemimpinan transformasional terbukti memiliki dampak yang lebih mendalam dan berkelanjutan terhadap budaya dan kinerja keselamatan.

Kepemimpinan Transaksional didasarkan pada pertukaran atau "transaksi" antara pemimpin dan pengikut. Pemimpin menetapkan harapan dan tujuan yang jelas, memantau kinerja, dan kemudian memberikan

penghargaan (misalnya, bonus, pujian) untuk kinerja yang baik atau sanksi (misalnya, teguran) untuk kinerja yang buruk. Dalam konteks K3, ini sering kali terwujud dalam bentuk program keselamatan berbasis perilaku (*behavior-based safety*) di mana perilaku aman diamati dan diberi imbalan, atau dalam sistem di mana kepatuhan terhadap aturan ditegakkan melalui pengawasan dan disiplin.

Kepemimpinan transaksional penting untuk menetapkan dasar kepatuhan. Ia memastikan bahwa aturan-aturan dasar diikuti dan ada akuntabilitas untuk kinerja. Namun, jika hanya mengandalkan gaya ini, keselamatan bisa menjadi sekadar latihan “mencentang kotak”. Karyawan mungkin berperilaku aman hanya ketika mereka diawasi, untuk mendapatkan imbalan atau menghindari hukuman. Ini mendorong kepatuhan, tetapi tidak selalu menginspirasi komitmen.

Kepemimpinan Transformasional, di sisi lain, melampaui sekadar pertukaran. Pemimpin transformasional menginspirasi dan memotivasi pengikut untuk mencapai hasil yang luar biasa dengan mengubah keyakinan, nilai, dan kebutuhan mereka. Mereka melakukannya melalui beberapa perilaku kunci:

a. **Pengaruh yang Diidealkan (Karisma)**

Pemimpin bertindak sebagai panutan yang kuat untuk nilai-nilai keselamatan. Mereka “menjalankan apa yang mereka katakan” dan mendapatkan rasa hormat serta kepercayaan.

b. **Motivasi Inspirasional**

Pemimpin mengartikulasikan visi keselamatan yang menarik (misalnya, “kita akan menjadi yang teraman di industri”) dan menginspirasi karyawan untuk menjadi bagian dari visi tersebut.

c. **Stimulasi Intelektual**

Pemimpin menantang status quo, mendorong karyawan untuk berpikir secara kritis tentang risiko, dan secara aktif mencari cara-cara baru yang lebih baik untuk meningkatkan keselamatan.

#### d. **Pertimbangan Individual**

Pemimpin benar-benar peduli terhadap kesejahteraan setiap individu. Mereka bertindak sebagai mentor, mendengarkan keprihatinan, dan memberikan dukungan.

Dalam konteks K3, pemimpin transformasional tidak hanya menuntut kepatuhan; mereka membangun kepercayaan, memberdayakan karyawan, dan menumbuhkan rasa kepemilikan bersama atas keselamatan. Karyawan termotivasi untuk berperilaku aman bukan karena mereka takut dihukum, tetapi karena mereka secara internal percaya bahwa itu adalah hal yang benar untuk dilakukan dan mereka ingin berkontribusi pada kesuksesan tim. Penelitian secara konsisten menunjukkan bahwa kepemimpinan transformasional berkorelasi kuat dengan iklim keselamatan yang lebih positif, tingkat partisipasi keselamatan yang lebih tinggi, dan angka kecelakaan yang lebih rendah.

## 2. **Komitmen dan Keterlibatan Manajemen Puncak**

Meskipun kepemimpinan di semua tingkatan itu penting, komitmen dan keterlibatan aktif dari manajemen puncak adalah faktor penentu tunggal yang paling penting bagi keberhasilan program K3. Manajemen puncak, CEO, dewan direksi, dan tim eksekutif lainnya, memiliki kekuatan untuk menetapkan arah, mengalokasikan sumber daya, dan membentuk budaya dengan cara yang tidak dapat dilakukan oleh tingkat manajemen lainnya. Tanpa dukungan mereka yang tulus dan terlihat, inisiatif K3 terbaik sekalipun akan gagal.

Komitmen harus lebih dari sekadar pernyataan dalam kebijakan perusahaan. Itu harus dapat dibuktikan melalui keputusan dan tindakan. Seperti yang dibahas sebelumnya, cara manajemen puncak mengalokasikan sumber daya adalah ujian lakmus sejati dari komitmen mereka. Apakah mereka bersedia berinvestasi dalam teknologi keselamatan yang lebih baik, bahkan jika itu tidak memberikan pengembalian finansial langsung? Apakah mereka memastikan departemen K3 memiliki staf yang memadai dan berpengaruh? Jawaban atas pertanyaan-pertanyaan ini mengungkapkan komitmen yang sebenarnya.

Komitmen juga ditunjukkan melalui penetapan akuntabilitas. Apakah kinerja K3 merupakan bagian dari evaluasi kinerja untuk para manajer senior? Apakah para pemimpin dimintai pertanggungjawaban atas catatan keselamatan di area mereka, sama seperti mereka dimintai pertanggungjawaban atas target finansial? Ketika keselamatan menjadi bagian integral dari sistem akuntabilitas manajemen, ia akan mendapatkan tingkat perhatian yang layak.

Keterlibatan berarti bahwa para pemimpin puncak tidak mendelegasikan keselamatan sepenuhnya dan kemudian melupakannya. Mereka harus terlihat dan terdengar dalam upaya K3. Ini berarti:

- a. Menjadikan keselamatan sebagai agenda pertama dalam setiap rapat penting.
- b. Berkomunikasi secara teratur dengan seluruh tenaga kerja tentang kinerja dan prioritas K3.
- c. Secara pribadi memimpin atau berpartisipasi dalam tinjauan investigasi kecelakaan besar.
- d. Berada di lapangan secara teratur, berbicara dengan pekerja, dan mendengarkan keprihatinan mereka secara langsung.

Ketika karyawan melihat CEO mengenakan APD yang benar dan mengajukan pertanyaan yang mendalam tentang bahaya selama kunjungan ke lokasi, itu mengirimkan pesan yang jauh lebih kuat daripada seribu email atau poster. Keterlibatan pribadi ini menunjukkan rasa hormat terhadap risiko yang dihadapi oleh pekerja dan memperkuat kredibilitas komitmen organisasi. Tanpa komitmen dan keterlibatan dari puncak, upaya K3 akan kekurangan legitimasi dan sumber daya yang diperlukan untuk berhasil, dan budaya keselamatan yang positif tidak akan pernah dapat berakar.

### **3. Safety Walkdowns dan Visibilitas Pemimpin di Lapangan**

Salah satu alat kepemimpinan yang paling sederhana namun paling efektif untuk menunjukkan komitmen dan meningkatkan iklim keselamatan adalah interaksi keselamatan di lapangan, yang sering kali berbentuk *safety walkdowns* atau *safety tours*. Ini adalah praktik di mana para pemimpin, dari penyelia hingga manajer senior, secara teratur dan terjadwal meninggalkan

kantor mereka untuk berjalan-jalan di area kerja dengan tujuan tunggal untuk berinteraksi dengan karyawan tentang masalah K3.

Penting untuk membedakan *safety walkdowns* dari audit atau inspeksi keselamatan tradisional. Tujuannya bukanlah untuk mencari pelanggaran atau “menangkap” orang yang melakukan kesalahan. Sebaliknya, tujuannya adalah untuk terlibat dalam dialog dua arah yang positif. Fokusnya adalah pada mendengarkan, bukan pada memberi kuliah. Pemimpin ada di sana untuk belajar tentang realitas pekerjaan, tantangan yang dihadapi karyawan, dan ide-ide mereka untuk perbaikan.

Selama *walkdown* yang efektif, seorang pemimpin mungkin akan mengajukan pertanyaan terbuka seperti:

- a. “Apa hal yang paling berbahaya yang Anda lakukan hari ini?”
- b. “Jika Anda memiliki tongkat ajaib, satu hal apa yang akan Anda ubah untuk membuat pekerjaan ini lebih aman?”
- c. “Apakah Anda memiliki semua alat dan sumber daya yang Anda butuhkan untuk melakukan pekerjaan ini dengan aman?”
- d. “Ceritakan tentang *near miss* terakhir yang Anda atau rekan Anda alami.”

Manfaat dari praktik ini sangat banyak. Pertama, ia memberikan visibilitas kepemimpinan yang sangat dibutuhkan. Ketika karyawan melihat manajer senior secara teratur di area kerja mereka, itu menunjukkan bahwa para pemimpin tersebut peduli dan terlibat. Ini membangun kepercayaan dan menghancurkan persepsi bahwa manajemen “terputus” dari realitas lini depan.

Kedua, ini adalah saluran umpan balik yang sangat kaya. Para pemimpin mendapatkan wawasan langsung dan tanpa filter tentang bagaimana *work-as-done* berbeda dari *work-as-imagined*. Mereka dapat melihat sendiri di mana prosedur tidak praktis, di mana peralatan menyebabkan frustrasi, dan di mana kondisi lingkungan sub-optimal. Informasi kualitatif ini sering kali lebih berharga daripada laporan statistik.

Ketiga, ini adalah peluang untuk penguatan positif. Ketika seorang pemimpin melihat perilaku kerja yang aman, mereka dapat memberikan

pujian dan pengakuan di tempat. Penguatan positif ini jauh lebih efektif dalam membentuk perilaku daripada hanya berfokus pada hal-hal negatif.

Agar *walkdowns* berhasil, ada beberapa aturan penting. Mereka harus dilakukan secara teratur dan terjadwal, bukan hanya sesekali. Pemimpin harus dilatih tentang cara mengajukan pertanyaan yang baik dan mendengarkan secara aktif. Dan yang paling penting, harus ada tindak lanjut yang terlihat. Jika karyawan menyuarakan keprihatinan yang sah, mereka harus melihat bahwa tindakan diambil untuk mengatasinya. Kegagalan untuk menindaklanjuti akan dengan cepat merusak kredibilitas seluruh proses dan mengajarkan karyawan bahwa berbicara adalah sia-sia. Ketika dilakukan dengan benar, *safety walkdowns* adalah alat yang ampuh untuk mengubah kepemimpinan keselamatan dari konsep abstrak menjadi praktik yang nyata dan berdampak.

## KESIMPULAN

Bab kedelapan ini telah memperluas analisis kita untuk mencakup kekuatan-kekuatan kontekstual yang paling kuat yang membentuk kinerja manusia: faktor organisasi dan lingkungan. Telah ditunjukkan bahwa tindakan individu di lini depan tidak terjadi dalam ruang hampa, melainkan sangat dipengaruhi oleh "iklim" dan "arsitektur" organisasi tempat mereka bekerja. Faktor-faktor ini adalah sumber utama dari kondisi-kondisi laten yang secara sistematis dapat meningkatkan atau mengurangi kemungkinan terjadinya *human error*.

Kita telah mengeksplorasi budaya dan iklim keselamatan sebagai fondasi dari semua pertahanan organisasi. Budaya yang kuat, yang ditandai dengan pelaporan yang jujur, keadilan, fleksibilitas, dan pembelajaran, menciptakan lingkungan di mana pertahanan dapat berkembang. Sebaliknya, budaya yang lemah secara aktif mengikis pertahanan tersebut. Demikian pula, faktor-faktor fisiologis seperti jadwal kerja dan kelelahan telah diidentifikasi bukan sebagai masalah pribadi, melainkan sebagai risiko sistemik yang memerlukan solusi manajemen yang terstruktur seperti FRMS.

Pentingnya desain tempat kerja yang ergonomis, baik secara fisik maupun kognitif, juga telah ditegaskan. Dengan secara proaktif merancang pekerjaan agar sesuai dengan kapabilitas dan keterbatasan tubuh dan

pikiran manusia, kita dapat secara langsung menghilangkan banyak jebakan kesalahan dari sistem. Pengelolaan lingkungan fisik seperti pencahayaan dan kebisingan melengkapi pendekatan holistik ini.

Pada akhirnya, semua faktor ini menyatu dan dipengaruhi oleh satu kekuatan tunggal yang paling dominan: kepemimpinan. Perilaku, komitmen, dan visibilitas para pemimpin di semua tingkatan menentukan prioritas yang sebenarnya dari organisasi dan membentuk budaya keselamatan. Kepemimpinan transformasional, yang didukung oleh komitmen yang nyata dari manajemen puncak, telah diidentifikasi sebagai katalisator utama untuk mencapai keunggulan K3 yang berkelanjutan.

Dengan pemahaman yang komprehensif tentang pengaruh individu, teknologi, dan organisasi ini, kita sekarang telah menyelesaikan eksplorasi kita terhadap model-model teoretis dan faktor-faktor penyebab. Kita siap untuk beralih ke Bagian III, yang akan fokus pada alat dan teknik praktis yang digunakan untuk menganalisis, menilai, dan memprediksi *human error* dalam praktik.

# DAFTAR PUSTAKA

- ACSNI Human Factors Study Group. (1993). *Organising for Safety: Third Report of the ACSNI Human Factors Study Group*. HMSO.
- Akerstedt, T. (2003). Shift work and disturbed sleep/wakefulness. *Occupational Medicine*, 53(2), 89-94. <https://doi.org/10.1093/occmed/kqg046>
- Akerstedt, T. (2003). Shift work and disturbed sleep/wakefulness. *Occupational Medicine*, 53(2), 89-94. <https://doi.org/10.1093/occmed/kqg046>
- Arnedt, J. T., et al. (2001). How do sleep deprivation and alcohol affect driving performance? *Journal of Sleep Research*, 10(3), 235-241. <https://doi.org/10.1046/j.1365-2869.2001.00257.x>
- Arnsten, A. F. T. (2015). Stress weakens prefrontal networks: an organizing principle. *Nature Neuroscience*, 18(10), 1376–1385. <https://doi.org/10.1038/nn.4117>
- Baddeley, A. D. (2012). Working memory: theories, models, and controversies. *Annual Review of Psychology*, 63, 1-29. <https://doi.org/10.1146/annurev-psych-120710-100422>
- Baker, J. A., et al. (2007). *The Report of the BP U.S. Refineries Independent Safety Review Panel*. BP.
- Baysari, M. T., et al. (2021). The 'Swiss cheese' model of medication errors: is there a need for a new metaphor? *Journal of Patient Safety and Risk Management*, 26(3), 118-123. <https://doi.org/10.1177/25160435211024976>
- Bridger, R. S. (2018). *Introduction to Human Factors and Ergonomics* (4th ed.). CRC Press.
- Carayon, P. (2006). Human factors of complex sociotechnical systems. *Applied Ergonomics*, 37(4), 525-535. <https://doi.org/10.1016/j.apergo.2006.04.011>

- Chan, D., Baghbaderani, A., & Sarvari, H. (2022). An Empirical Study of the Human Error-Related Factors Leading to Site Accidents in the Iranian Urban Construction Industry. *Buildings*, 12(11), 1858. <https://doi.org/10.3390/buildings12111858>
- Checkland, P. (1999). *Systems Thinking, Systems Practice: Includes a 30-Year Retrospective*. John Wiley & Sons.
- Clarke, S. (2013). Safety leadership: A meta-analytic review of transformational and transactional leadership styles as antecedents of safety behaviours. *Journal of Occupational and Organizational Psychology*, 86(1), 22-49. <https://doi.org/10.1111/j.2044-8325.2012.02064.x>
- Crandall, B., Klein, G., & Hoffman, R. R. (2006). *Working Minds: A Practitioner's Guide to Cognitive Task Analysis*. MIT Press.
- Czeisler, C. A. (2013). Perspective: Casting light on sleep deficiency. *Nature*, 497(7450), S13. <https://doi.org/10.1038/497S13a>
- Dawson, D., & Reid, K. (1997). Fatigue, alcohol and performance impairment. *Nature*, 388(6639), 235. <https://doi.org/10.1038/40775>
- De Mattos, L., Rocha, R., Castro, F., Duarte, M., Anselmo, L., & Mattos, D. (2024). Human error and violation of rules in industrial safety: A systematic literature review. *Work*, 79(4), 1237-1253. <https://doi.org/10.3233/wor-230186>
- De Mattos, L., Rocha, R., Castro, F., Duarte, M., Anselmo, L., & Mattos, D. (2024). Human error and violation of rules in industrial safety: A systematic literature review. *Work*, 79(4), 1237-1253. <https://doi.org/10.3233/wor-230186>
- Dekker, S. W. A. (2003). Failure to adapt or adaptations that fail: contrasting models on procedures and safety. *Applied Ergonomics*, 34(3), 233-238. [https://doi.org/10.1016/S0003-6870\(03\)00030-3](https://doi.org/10.1016/S0003-6870(03)00030-3)
- Dekker, S. W. A. (2017). *Just Culture: Restoring Trust and Accountability in Your Organization* (3rd ed.). CRC Press.
- Dekker, S. W. A. (2017). *Just Culture: Restoring Trust and Accountability in Your Organization* (3rd ed.). CRC Press.
- Dekker, S. W. A. (2022). *Foundations of Safety Science: A Century of Understanding Accidents and Disasters* (3rd ed.). CRC Press.
- Dekker, S. W. A. (2022). *Foundations of Safety Science: A Century of Understanding Accidents and Disasters* (3rd ed.). CRC Press.

- Dienagha, I., & Onyeke, F. (2025). Human Factors and Safety Culture in High-Risk Energy Operations: Strategies to Minimize Human Error and Enhance Compliance. *International Journal of Research and Innovation in Social Science*, 9(1). <https://doi.org/10.47772/ijriss.2025.9010118>
- Edmondson, A. C. (1999). Psychological safety and learning behavior in work teams. *Administrative Science Quarterly*, 44(2), 350-383. <https://doi.org/10.2307/2666999>
- Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. *Human Factors*, 37(1), 32-64. <https://doi.org/10.1518/001872095779049543>
- Flin, R., Mearns, K., O'Connor, P., & Bryden, R. (2000). Measuring safety climate: identifying the common features. *Safety Science*, 34(1-3), 177-192. [https://doi.org/10.1016/S0925-7535\(00\)00012-6](https://doi.org/10.1016/S0925-7535(00)00012-6)
- Folkard, S., & Tucker, P. (2003). Shift work, safety and productivity. *Occupational Medicine*, 53(2), 95-101. <https://doi.org/10.1093/occmed/kqg047>
- Gander, P., et al. (2011). An evidence-based approach to fatigue risk management. *Safety Science*, 49(2), 232-241. <https://doi.org/10.1016/j.ssci.2010.08.006>
- Geller, E. S. (2001). *The Psychology of Safety Handbook*. CRC Press.
- Gladwell, M. (2008). *Outliers: The Story of Success*. Little, Brown and Company.
- Goel, P., & Singh, P. (2020). The relationship between occupational health and safety management and business performance: A literature review. *Journal of Safety Research*, 73, 143-154. <https://doi.org/10.1016/j.jsr.2020.03.001>
- Goh, Y. M., Love, P. E. D., Stagbouer, G., & An, C. H. (2012). The safety leading indicators of construction projects: The case of Singapore. *Safety Science*, 50(9), 1642-1652. <https://doi.org/10.1016/j.ssci.2012.04.004>
- Greenwood, M., & Woods, H. M. (1919). *The Incidence of Industrial Accidents upon Individuals with Special Reference to Multiple Accidents*. Industrial Fatigue Research Board, Report No. 4.
- Griffin, M. A., & Neal, A. (2000). Perceptions of safety at work: a framework for linking safety climate to safety performance, knowledge, and

- motivation. *Journal of Occupational Health Psychology*, 5(3), 347–358. <https://doi.org/10.1037/1076-8998.5.3.347>
- Hale, A. R., & Glendon, A. I. (1987). *Individual Differences in Safety and Accident Behaviour*. In *Individual Behaviour in the Control of Danger* (pp. 100-120). Elsevier.
- Halim, A., Ghazi, T., Yassin, F., & Tohir, M. (2024). Study of human error from incident investigation in upstream facilities. *Process Safety Progress*, 43(S1), S22-S34. <https://doi.org/10.1002/prs.12584>
- Hart, S. G., & Staveland, L. E. (1988). Development of NASA-TLX (Task Load Index): Results of empirical and theoretical research. In P. A. Hancock & N. Meshkati (Eds.), *Human Mental Workload* (pp. 139-183). North-Holland.
- Hawkins, F. H., & Orlady, H. W. (Eds.). (1993). *Human Factors in Flight* (2nd ed.). Ashgate.
- Hendrick, H. W., & Kleiner, B. M. (2001). *Macroergonomics: An Introduction to Work System Design*. Human Factors and Ergonomics Society.
- Hoffmeister, K., et al. (2014). The differential effects of transformational leadership on follower's safety behaviors. *Safety Science*, 62, 29-38. <https://doi.org/10.1016/j.ssci.2013.08.003>
- Holden, R. J. (2021). The rusty sword of professional autonomy: A system-level critique of a cherished healthcare value. *Applied Ergonomics*, 92, 103339. <https://doi.org/10.1016/j.apergo.2020.103339>
- Hollnagel, E. (2017). *The ETTO Principle: Efficiency-Thoroughness Trade-Off: Why Things That Go Right Sometimes Go Wrong*. CRC Press.
- Hollnagel, E. (2021). *Safety-II in Practice: Developing the Resilience Potentials*. Routledge.
- Hollnagel, E. (2021). *Safety-II in Practice: Developing the Resilience Potentials*. Routledge.
- Hollnagel, E. (2021). *Safety-II in Practice: Developing the Resilience Potentials*. Routledge.
- Hopkins, A. (2012). *Disastrous Decisions: The Human and Organisational Causes of the Gulf of Mexico Blowout*. CCH Australia.
- Inness, M., LeBlanc, M. M., & Barling, J. (2022). "It won't happen to me": The role of optimistic bias in managers' safety-related decisions. *Journal of*

*Occupational Health Psychology*, 27(1), 1-12. <https://doi.org/10.1037/ocp0000287>

- International Labour Organization. (2023). *A Call for Safer and Healthier Working Environments*. ILO.
- Investigasi Kecelakaan Pesawat Spanyol. (1978). *Report on the Collision between PAN AM B-747 and KLM B-747 at Tenerife Airport, Spain, on March 27, 1977*. Subsecretaría de Aviación Civil, Spain.
- IPIECA. (2011). *Fatigue Management in the Workplace*. International Petroleum Industry Environmental Conservation Association.
- Kaila, H. (2025). Human Error or Cultural Failure that Cause Serious Incidents and Implications for Industry. *SAMVAD: Journal of Management and Social Sciences*, 29. <https://doi.org/10.53739/samvad/2024/v29/174605>
- Khan, F., et al. (2021). A hybrid risk assessment model for process industries. *Safety Science*, 143, 105436. <https://doi.org/10.1016/j.ssci.2021.105436>
- Kim, M., Kim, S., & Cho, G. (2023). A Study on the Analysis of Chemical Accident Based on Swiss Cheese Model -Focusing on the case of India's Bhopal accident-. *Journal of the Korea Academia-Industrial cooperation Society*, 24(11), 124-131. <https://doi.org/10.5762/kais.2023.24.11.124>
- Kim, M., Kim, S., & Cho, G. (2023). A Study on the Analysis of Chemical Accident Based on Swiss Cheese Model -Focusing on the case of India's Bhopal accident-. *Journal of the Korea Academia-Industrial cooperation Society*, 24(11), 124-131. <https://doi.org/10.5762/kais.2023.24.11.124>
- Kirwan, B. (1994). *A Guide to Practical Human Reliability Assessment*. CRC Press.
- Kirwan, B. (1994). *A Guide to Practical Human Reliability Assessment*. CRC Press.
- Klein, G. (2007). Performing a project premortem. *Harvard Business Review*, 85(9), 18-19.
- Kontogiannis, T., & Malakis, S. (2022). A proactive approach to assessing the resilience of a safety management system in an airline. *Safety Science*, 147, 105615. <https://doi.org/10.1016/j.ssci.2021.105615>
- Kumar, P., Gupta, S., & Gunda, Y. (2020). Estimation of human error rate in underground coal mines through retrospective analysis of mining accident reports and some error reduction strategies. *Safety Science*, 123, 104555. <https://doi.org/10.1016/j.ssci.2019.104555>

- Ladell, M., Jacobson, N., Yale, S., McDermott, K., Papautsky, E., Catchpole, K., & Scanlon, M. (2025). The problem with how we view medical (and diagnostic) error in emergency medicine. *Academic Emergency Medicine*, 32(3), 340-347. <https://doi.org/10.1111/acem.15076>
- Lardner, R., & Maitland, T. (2013). *Effective Safety Conversations: A guide for leaders and safety professionals*. The Keil Centre.
- LeBlanc, V. R. (2009). The effects of acute stress on performance: implications for health professions education. *Academic Medicine*, 84(10 Suppl), S25-S33. <https://doi.org/10.1097/ACM.0b013e3181b37b8f>
- Leveson, N. (2020). *An Introduction to STAMP*. MIT Press.
- Leveson, N. (2020). *An Introduction to STAMP*. MIT Press.
- Leveson, N. (2020). *An Introduction to STAMP*. MIT Press.
- Marx, D. (2001). *Patient Safety and the "Just Culture": A Primer for Health Care Executives*. National Institutes of Health.
- Marx, D. (2001). *Patient Safety and the "Just Culture": A Primer for Health Care Executives*. National Institutes of Health.
- Miller, G. A. (1956). The magical number seven, plus or minus two: Some limits on our capacity for processing information. *Psychological Review*, 63(2), 81-97. <https://doi.org/10.1037/h0043158>
- Morrison, E. W., & Milliken, F. J. (2000). Organizational silence: A barrier to change and development in a pluralistic world. *Academy of Management Review*, 25(4), 706-725. <https://doi.org/10.5465/amr.2000.3707697>
- Musungwa, T., & Kowe, P. (2022). Effects of occupational health and safety management systems implementation in accident prevention at a Harare beverage company. *Cogent Engineering*, 9(1). <https://doi.org/10.1080/23311916.2022.2124638>
- National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling. (2011). *Deep Water: The Gulf Oil Disaster and the Future of Offshore Drilling*.
- Nickerson, R. S. (1998). Confirmation bias: A ubiquitous phenomenon in many guises. *Review of General Psychology*, 2(2), 175-220. <https://doi.org/10.1037/1089-2680.2.2.175>
- NIOSH. (2015). *Hierarchy of Controls*. National Institute for Occupational Safety and Health. Retrieved from <https://www.cdc.gov/niosh/topics/hierarchy/default.html>

- Noboa, A. (2025). Neuroergonomics applied to construction: Preventing human error to protect health and safety of high-risk workers. *World Journal of Advanced Research and Reviews*, 26(3). <https://doi.org/10.30574/wjarr.2025.26.3.2316>
- Norman, D. A. (1981). Categorization of action slips. *Psychological Review*, 88(1), 1–15. <https://doi.org/10.1037/0033-295X.88.1.1>
- Norman, D. A. (1988). *The Psychology of Everyday Things* (later retitled *The Design of Everyday Things*). Basic Books.
- Norman, D. A. (1988). *The Psychology of Everyday Things* (later retitled *The Design of Everyday Things*). Basic Books.
- Norman, D. A. (1988). *The Psychology of Everyday Things*. Basic Books.
- O'Connor, P., et al. (2020). The relationship between safety culture and safety performance—A systematic review. *Journal of Safety Research*, 75, 127-141. <https://doi.org/10.1016/j.jsr.2020.08.010>
- O'Connor, P., et al. (2020). The relationship between safety culture and safety performance—A systematic review. *Journal of Safety Research*, 75, 127-141. <https://doi.org/10.1016/j.jsr.2020.08.010>
- Orikpete, O., & Ewim, D. (2024). Interplay of human factors and safety culture in nuclear safety for enhanced organisational and individual Performance: A comprehensive review. *Nuclear Engineering and Design*, 419, 112797. <https://doi.org/10.1016/j.nucengdes.2023.112797>
- Perkins, A., et al. (2022). Organizational learning from incidents: A systematic literature review. *Safety Science*, 154, 105843. <https://doi.org/10.1016/j.ssci.2022.105843>
- Perrow, C. (1999). *Normal Accidents: Living with High-Risk Technologies*. Princeton University Press.
- Pratama, A., & Sari, D. P. (2022). Implementasi Sistem Manajemen K3 untuk Meningkatkan Daya Saing Perusahaan di Era Industri 4.0. *Jurnal Teknik Industri*, 23(1), 45-56.
- Probst, T. M., & Brubaker, T. L. (2001). The effects of job insecurity on employee safety outcomes: Cross-sectional and longitudinal explorations. *Journal of Occupational Health Psychology*, 6(2), 139–159. <https://doi.org/10.1037/1076-8998.6.2.139>
- Probst, T. M., & Brubaker, T. L. (2001). The effects of job insecurity on employee safety outcomes: Cross-sectional and longitudinal

- explorations. *Journal of Occupational Health Psychology*, 6(2), 139–159. <https://doi.org/10.1037/1076-8998.6.2.139>
- Probst, T. M., Petitta, L., & Barbaranelli, C. (2021). The interactive effects of safety climate and blame culture on underreporting of occupational injuries. *Journal of Safety Research*, 77, 236–243. <https://doi.org/10.1016/j.jsr.2021.03.007>
- Rasmussen, J. (1983). Skills, rules, and knowledge; signals, signs, and symbols, and other distinctions in human performance models. *IEEE Transactions on Systems, Man, and Cybernetics*, SMC-13(3), 257–266.
- Rasmussen, J. (1997). Risk management in a dynamic society: a modelling problem. *Safety Science*, 27(2-3), 183–213. [https://doi.org/10.1016/S0925-7535\(97\)00052-0](https://doi.org/10.1016/S0925-7535(97)00052-0)
- Reason, J. (1990). *Human Error*. Cambridge University Press.
- Reason, J. (1990). *Human Error*. Cambridge University Press.
- Reason, J. (1990). *Human Error*. Cambridge University Press.
- Reason, J. (1990). *Human Error*. Cambridge University Press.
- Reason, J. (1990). *Human Error*. Cambridge University Press.
- Reason, J. (1990). *Human Error*. Cambridge University Press.
- Reason, J. (1997). *Managing the Risks of Organizational Accidents*. Ashgate.
- Reason, J. (1997). *Managing the Risks of Organizational Accidents*. Ashgate.
- Reason, J. (1997). *Managing the Risks of Organizational Accidents*. Ashgate.
- Reason, J. (1997). *Managing the Risks of Organizational Accidents*. Ashgate.
- Reason, J., Manstead, A., Stradling, S., Baxter, J., & Campbell, K. (1990). Errors and violations on the roads: a real distinction? *Ergonomics*, 33(10-11), 1315–1332. <https://doi.org/10.1080/00140139008925335>
- Robson, L. S., et al. (2021). The effectiveness of occupational health and safety management systems: A systematic review. *Safety Science*, 140, 105289. <https://doi.org/10.1016/j.ssci.2021.105289>
- Robson, L. S., et al. (2021). The effectiveness of occupational health and safety management systems: A systematic review. *Safety Science*, 140, 105289. <https://doi.org/10.1016/j.ssci.2021.105289>

- Salas, E., et al. (2008). Does team training improve team performance? A meta-analysis. *Human Factors*, 50(6), 903-933. <https://doi.org/10.1518/001872008X375009>
- Saleh, J. H., & Cummings, A. M. (2021). A critique of the Swiss cheese model of accident causation and its contribution to safety investigation and analysis. *Journal of System Safety*, 57(1), 14-25.
- Salvendy, G. (Ed.). (2012). *Handbook of Human Factors and Ergonomics* (4th ed.). John Wiley & Sons.
- Salvendy, G. (Ed.). (2012). *Handbook of Human Factors and Ergonomics* (4th ed.). John Wiley & Sons.
- Sandberg, J., & Albrechtsen, E. (2021). The challenge of managing change for process safety: A case study of a major oil and gas company. *Journal of Loss Prevention in the Process Industries*, 72, 104555. <https://doi.org/10.1016/j.jlp.2021.104555>
- Sanders, M. S., & McCormick, E. J. (1993). *Human Factors in Engineering and Design* (7th ed.). McGraw-Hill.
- Sarter, N. B., & Woods, D. D. (1991). Situation awareness: A critical but ill-defined phenomenon. *The International Journal of Aviation Psychology*, 1(1), 45-57.
- Schein, E. H. (2010). *Organizational Culture and Leadership* (4th ed.). Jossey-Bass.
- Schein, E. H. (2010). *Organizational Culture and Leadership* (4th ed.). Jossey-Bass.
- Stanton, N. A. (2013). *Human Factors in Alarm Design*. CRC Press.
- Sujan, M., et al. (2019). A new perspective on the causes of medical accidents: a study of the role of organisational and engineering factors. *Reliability Engineering & System Safety*, 190, 106509. <https://doi.org/10.1016/j.res.2019.106509>
- Szabo, C., et al. (2021). The impact of industrial noise on cognitive performance: A systematic review. *Noise & Health*, 23(104), 1-13. [https://doi.org/10.4103/nah.nah\\_7\\_21](https://doi.org/10.4103/nah.nah_7_21)
- Takahashi, M. (2003). The role of prescribed napping in sleep and wakefulness. *Journal of Physiological Anthropology and Applied Human Science*, 22(2), 75-81. <https://doi.org/10.2114/jpa.22.75>

- Tversky, A., & Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases. *Science*, 185(4157), 1124-1131. <https://doi.org/10.1126/science.185.4157.1124>
- Vaughan, D. (1996). *The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA*. University of Chicago Press.
- Vaughan, D. (1996). *The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA*. University of Chicago Press.
- Wallace, J. C., & Ross, A. (2022). The utility of near-miss reporting: A systematic review. *Journal of Safety Research*, 81, 198-210. <https://doi.org/10.1016/j.jsr.2022.02.007>
- Weick, K. E. (1990). The vulnerable system: An analysis of the Tenerife air disaster. *Journal of Management*, 16(3), 571-593. <https://doi.org/10.1177/014920639001600304>
- Weick, K. E., & Sutcliffe, K. M. (2015). *Managing the Unexpected: Sustained Performance in a Complex World* (3rd ed.). Wiley.
- Wickens, C. D., & McCarley, J. S. (2008). *Applied Attention Theory*. CRC Press.
- Wickens, C. D., Hollands, J. G., Banbury, S., & Parasuraman, R. (2013). *Engineering Psychology and Human Performance* (4th ed.). Pearson.
- Wickens, C. D., Hollands, J. G., Banbury, S., & Parasuraman, R. (2013). *Engineering Psychology and Human Performance* (4th ed.). Pearson.
- Wickens, C. D., Hollands, J. G., Banbury, S., & Parasuraman, R. (2013). *Engineering Psychology and Human Performance* (4th ed.). Pearson.
- Wiegmann, D. A., & Shappell, S. A. (2017). *A Human Error Approach to Aviation Accident Analysis: The Human Factors Analysis and Classification System*. Routledge.
- Wiegmann, D. A., & Shappell, S. A. (2017). *A Human Error Approach to Aviation Accident Analysis: The Human Factors Analysis and Classification System*. Routledge.
- Woods, D. D., & Hollnagel, E. (2006). *Joint Cognitive Systems: Patterns in Cognitive Systems Engineering*. CRC Press.
- Yeow, J., Ng, P., Tai, H., & Chow, M. (2020). A Review On Human Error In Malaysia Manufacturing Industries. *Journal of Industrial and System-based Management*, 5(19), 01-13. <https://doi.org/10.35631/jistm.519001>

- Zanko, M., & Dawson, P. (2012). Occupational health and safety management in organizations: A review. *International Journal of Management Reviews*, 14(3), 328-344. <https://doi.org/10.1111/j.1468-2370.2011.00321.x>
- Zhang, T., Liu, Z., Zheng, S., Qu, X., & Tao, D. (2020). Predicting Errors, Violations, and Safety Participation Behavior at Nuclear Power Plants. *International Journal of Environmental Research and Public Health*, 17(15), 5613. <https://doi.org/10.3390/ijerph17155613>
- Zohar, D. (2002). The effects of leadership and climate on safety. *Journal of Applied Psychology*, 87(4), 587-596. <https://doi.org/10.1037/0021-9010.87.4.587>
- Zohar, D. (2010). Thirty years of safety climate research: Reflections and future directions. *Accident Analysis & Prevention*, 42(5), 1517-1522. <https://doi.org/10.1016/j.aap.2009.12.019>
- Zohar, D., & Hofmann, D. A. (2012). Organizational culture and climate. In S. W. J. Kozlowski (Ed.), *The Oxford Handbook of Organizational Psychology, Vol 1*. (pp. 643-666). Oxford University Press.

**DUMMYY**

# GLOSARIUM

- **Active Failure (Kegagalan Aktif):** Dalam konteks Model Keju Swiss, ini adalah lubang di lapisan pertahanan paling depan, yang mewakili tindakan tidak aman oleh orang di lini depan yang menjadi pemicu langsung insiden.
- **Active Failure (Kegagalan Aktif):** Tindakan tidak aman (kesalahan atau pelanggaran) yang dilakukan oleh orang di lini depan yang dampaknya langsung terasa. Dipandang sebagai gejala atau pemicu, bukan akar penyebab.
- **Akuntabilitas (Accountability):** Dalam konteks *Just Culture*, ini merujuk pada tanggung jawab bersama untuk belajar dari kegagalan dan memperbaiki sistem, bukan hanya tentang memberikan sanksi setelah insiden.
- **Beban Kerja Kognitif (Cognitive Workload):** Jumlah total sumber daya mental yang dibutuhkan untuk melakukan suatu tugas. Beban kerja yang terlalu tinggi atau terlalu rendah dapat menurunkan kinerja.
- **Bias Konfirmasi (Confirmation Bias):** Kecenderungan untuk mencari, menafsirkan, dan mengingat informasi yang mengkonfirmasi keyakinan yang sudah ada sebelumnya, sambil mengabaikan informasi yang bertentangan.
- **Blame Culture:** Budaya organisasi di mana individu atau kelompok secara rutin disalahkan atas kesalahan atau kegagalan, yang sering kali menghambat pelaporan dan pembelajaran.
- **Budaya Keselamatan (Safety Culture):** Produk dari nilai-nilai, sikap, dan pola perilaku individu dan kelompok yang menentukan komitmen dan gaya program K3 suatu organisasi. Ini adalah "cara kita melakukan sesuatu di sini" dalam hal keselamatan.

- **Budaya Menyalahkan (*Blame Culture*):** Lingkungan organisasi di mana kesalahan atau kegagalan secara rutin diatribusikan pada individu, yang kemudian dihukum atau disalahkan, sehingga menekan pelaporan dan pembelajaran.
- **Crew Resource Management (CRM):** Sebuah set prosedur pelatihan untuk digunakan dalam lingkungan di mana *human error* dapat memiliki efek yang menghancurkan. CRM berfokus pada peningkatan keterampilan non-teknis seperti komunikasi, kerja tim, kepemimpinan, dan pengambilan keputusan.
- **Defenses in Depth (Pertahanan Berlapis):** Filosofi keselamatan di mana sistem dilindungi oleh beberapa lapisan penghalang yang tumpang tindih dan beragam (teknis, prosedural, manusiawi), dengan asumsi bahwa tidak ada satu lapisan pun yang sempurna.
- **Environment (Lingkungan):** Komponen dalam Model SHELL yang merujuk pada konteks fisik dan organisasi di mana sistem beroperasi, termasuk pencahayaan, kebisingan, suhu, budaya, dan tekanan produksi.
- **Ergonomi:** Ilmu terapan yang berfokus pada perancangan sistem, tugas, dan lingkungan agar sesuai dengan kapabilitas, keterbatasan, dan kebutuhan manusia.
- **Error Tolerance:** Prinsip desain di mana sistem dirancang untuk mendeteksi dan menahan konsekuensi dari kesalahan manusia, dengan asumsi bahwa kesalahan tidak dapat dihilangkan sepenuhnya.
- **Fatigue Risk Management System (FRMS):** Seperangkat praktik manajemen berbasis data yang terstruktur untuk mengidentifikasi, menilai, memitigasi, dan memantau risiko yang terkait dengan kelelahan pekerja.
- **Feedback Loop (Putaran Umpan Balik):** Mekanisme dalam sistem di mana output dari suatu tindakan kembali menjadi input, memengaruhi perilaku di masa depan. Bisa bersifat menyeimbangkan (negatif) atau menguatkan (positif).

- **Hardware (Perangkat Keras):** Komponen dalam Model SHELL yang merujuk pada elemen-elemen fisik dari sistem, seperti mesin, alat, dan stasiun kerja.
- **Heuristik:** Jalan pintas mental atau “aturan praktis” yang digunakan otak untuk membuat penilaian dan keputusan dengan cepat dan efisien.
- **Human Error:** Tindakan atau keputusan manusia yang menyimpang dari niat, ekspektasi, atau standar yang ada, yang mengakibatkan hasil yang tidak diinginkan. Dalam pendekatan sistemik, ini dipandang sebagai gejala, bukan penyebab utama.
- **Iklm Keselamatan (Safety Climate):** Persepsi bersama karyawan tentang kebijakan, prosedur, dan praktik keselamatan di organisasi mereka pada waktu tertentu. Merupakan manifestasi yang dapat diukur dari budaya keselamatan.
- **Just Culture:** Budaya yang menyeimbangkan antara akuntabilitas dan tidak menyalahkan. Ia menciptakan lingkungan yang aman untuk melaporkan kesalahan, sambil tetap mempertahankan standar perilaku profesional dan tidak menoleransi pelanggaran yang sembrono.
- **Keamanan Psikologis (Psychological Safety):** Keyakinan bersama di antara anggota tim bahwa lingkungan aman untuk mengambil risiko interpersonal, seperti mengajukan pertanyaan, menyuarakan keprihatinan, atau mengakui kesalahan, tanpa takut akan hukuman atau penghinaan.
- **Kelelahan (Fatigue):** Keadaan penurunan kapasitas mental atau fisik akibat kurang tidur atau pengerahan tenaga yang berkepanjangan, yang secara signifikan mengganggu kinerja kognitif.
- **Kepemimpinan Transaksional:** Gaya kepemimpinan yang berfokus pada pertukaran antara pemimpin dan pengikut, di mana kinerja yang baik diberi imbalan dan kinerja yang buruk diberi sanksi.
- **Kepemimpinan Transformasional:** Gaya kepemimpinan yang menginspirasi dan memotivasi pengikut untuk melampaui kepentingan

pribadi demi tujuan bersama, melalui karisma, inspirasi, stimulasi intelektual, dan pertimbangan individual.

- **Kesadaran Situasi (*Situation Awareness - SA*):** Persepsi elemen-elemen di lingkungan, pemahaman maknanya, dan proyeksi status mereka di masa depan. Terdiri dari tiga tingkatan: persepsi, pemahaman, dan proyeksi.
- **Kondisi Laten (*Latent Conditions*):** Kegagalan atau kelemahan tersembunyi dalam sistem (misalnya, prosedur yang buruk, pelatihan yang tidak memadai, keputusan manajemen yang keliru) yang mungkin tidak aktif selama beberapa waktu tetapi menciptakan prasyarat untuk terjadinya kegagalan aktif.
- **Lapisan Pertahanan (*Defensive Layers*):** Direpresentasikan sebagai irisan keju; merupakan penghalang, penjaga, atau pertahanan (teknis, prosedural, manusiawi) yang dirancang untuk melindungi sistem dari bahaya.
- **Lapse:** Jenis kesalahan eksekusi berbasis keterampilan yang disebabkan oleh kegagalan memori, seperti lupa melakukan langkah yang dimaksudkan dalam suatu tugas.
- **Latent Condition (Kondisi Laten):** Dalam konteks Model Keju Swiss, ini adalah lubang di lapisan-lapisan pertahanan di belakang (organisasi, pengawasan, desain), yang merupakan kelemahan tersembunyi yang diciptakan oleh keputusan sebelumnya.
- **Latent Condition (Kondisi Laten):** Kelemahan atau "jebakan" tersembunyi di dalam sistem (misalnya, desain buruk, prosedur tidak praktis, pelatihan tidak memadai) yang merupakan hasil dari keputusan manajerial atau organisasi dan dapat tetap tidak aktif untuk waktu yang lama.
- **Leading Indicators (Indikator Utama):** Metrik proaktif yang mengukur kesehatan proses keselamatan dan kekuatan pertahanan sistem, berbeda dengan *lagging indicators* yang mengukur hasil kegagalan (misalnya, jumlah kecelakaan).

- **Lintasan Peluang Kecelakaan (*Trajectory of Accident Opportunity*):** Jalur lurus imajiner yang tercipta ketika lubang-lubang di semua lapisan pertahanan secara sesaat sejajar, memungkinkan bahaya untuk menyebabkan kerugian.
- ***Liveware* (Manusia):** Komponen dalam Model SHELL yang merujuk pada individu manusia di dalam sistem, dengan semua kapabilitas dan keterbatasannya. *Liveware* pusat adalah fokus analisis, sementara *Liveware* lain adalah orang lain yang berinteraksi dengannya.
- **Memori Kerja (*Working Memory*):** Sistem memori berkapasitas terbatas untuk penyimpanan dan manipulasi informasi sementara untuk tugas-tugas kompleks seperti pemahaman, pembelajaran, dan penalaran.
- ***Mismatch* (Ketidakcocokan):** Istilah kunci dalam analisis SHELL yang merujuk pada kesesuaian yang buruk antara dua komponen sistem pada antarmuka mereka (misalnya, antara manusia dan desain mesin).
- ***Mistake*:** Jenis kesalahan perencanaan di mana tindakan dieksekusi sesuai rencana, tetapi rencana itu sendiri salah atau tidak memadai untuk mencapai tujuan. Dibagi menjadi *rule-based* dan *knowledge-based mistakes*.
- **Model Domino:** Model sebab-akibat kecelakaan linear yang dipopulerkan oleh H.W. Heinrich, yang menggambarkan kecelakaan sebagai hasil dari serangkaian peristiwa berurutan.
- **Model Keju Swiss (*Swiss Cheese Model*):** Sebuah model konseptual yang dikembangkan oleh James Reason untuk menggambarkan bagaimana kecelakaan di sistem kompleks terjadi melalui penembusan beberapa lapisan pertahanan yang tidak sempurna.
- **Model SHELL:** Sebuah kerangka kerja konseptual dalam *human factors* yang digunakan untuk menganalisis interaksi antara manusia (*Liveware*) dan komponen sistem lainnya: *Software*, *Hardware*, dan *Environment*.
- **Niat (*Intention*):** Tujuan atau rencana mental yang dimiliki seseorang sebelum melakukan suatu tindakan. Menjadi dasar untuk membedakan

kesalahan (penyimpangan tidak disengaja dari niat) dari pelanggaran (penyimpangan disengaja dari aturan).

- **Pelanggaran (*Violation*):** Penyimpangan yang disengaja dari prosedur, aturan, atau praktik yang aman. Berbeda dari kesalahan, pelanggaran bersifat motivasional.
- **Pendekatan Sistemik (*Systems Approach*):** Kerangka kerja untuk memahami dan menganalisis fenomena (seperti kecelakaan) dengan memandangnya sebagai hasil dari interaksi dinamis antara semua komponen dalam sebuah sistem yang terintegrasi, bukan sebagai hasil dari kegagalan komponen tunggal.
- ***Performance Shaping Factors (PSFs)*:** Faktor-faktor internal, eksternal, dan stresor dalam lingkungan kerja yang memengaruhi kemungkinan terjadinya kesalahan. Juga dikenal sebagai *Error Producing Conditions*.
- **Perhatian (*Attention*):** Mekanisme kognitif yang memungkinkan pemrosesan informasi yang relevan secara selektif sambil mengabaikan informasi lain.
- ***Person-Model*:** Paradigma keselamatan yang memandang kesalahan manusia sebagai penyebab utama kegagalan, yang berasal dari kekurangan individu seperti kelalaian, kurangnya motivasi, atau kecerobohan.
- ***Pre-Mortem*:** Sebuah teknik analisis risiko proaktif di mana tim membayangkan kegagalan sebuah proyek atau operasi di masa depan dan bekerja mundur untuk mengidentifikasi kemungkinan penyebab sistemiknya.
- **Prinsip Rasionalitas Lokal (*Principle of Local Rationality*):** Gagasan bahwa tindakan orang masuk akal bagi mereka pada saat mereka melakukannya, berdasarkan tujuan, pengetahuan, dan konteks situasional mereka.
- **Ritme Sirkadian:** Jam biologis internal sekitar 24 jam yang mengatur siklus tidur-bangun dan fungsi fisiologis lainnya.

- **Safety-I:** Paradigma keselamatan yang mendefinisikan keselamatan sebagai ketiadaan hasil negatif (kecelakaan) dan berfokus pada analisis reaktif terhadap apa yang salah.
- **Safety-II:** Paradigma keselamatan yang mendefinisikan keselamatan sebagai kemampuan sistem untuk berhasil dalam kondisi yang bervariasi dan berfokus pada pemahaman proaktif tentang mengapa hal-hal biasanya berjalan dengan baik.
- **Sistem Manajemen K3 (K3MS):** Kerangka kerja formal (seperti ISO 45001) yang digunakan organisasi untuk mengelola risiko K3 secara sistematis melalui siklus perencanaan, implementasi, evaluasi, dan perbaikan.
- **Sistem Manajemen K3 (SMK3):** Bagian dari sistem manajemen organisasi secara keseluruhan yang digunakan untuk mengembangkan dan menerapkan kebijakan K3 dan mengelola risiko K3. Contohnya adalah standar ISO 45001.
- **Sistem:** Kumpulan komponen yang saling berinteraksi (misalnya, manusia, teknologi, organisasi) yang bekerja bersama untuk mencapai tujuan tertentu.
- **Slip:** Jenis kesalahan eksekusi berbasis keterampilan yang disebabkan oleh kegagalan perhatian, di mana tindakan yang dimaksudkan dilakukan dengan cara yang salah atau pada objek yang salah.
- **Software (Perangkat Lunak):** Komponen dalam Model SHELL yang merujuk pada aspek-aspek non-fisik dan prosedural dari sistem, seperti prosedur, aturan, *checklists*, dan manual.
- **System-Model:** Paradigma keselamatan yang memandang kesalahan manusia sebagai gejala dari masalah yang lebih dalam di dalam sistem. Ia berfokus pada analisis kondisi laten dan desain sistem untuk mencegah kegagalan.
- **Taksonomi:** Ilmu atau praktik klasifikasi. Dalam konteks ini, merujuk pada pengelompokan sistematis berbagai jenis *human error*.

- **Visi Terowongan (*Tunnel Vision*):** Penyempitan perhatian yang terjadi di bawah stres atau beban kerja tinggi, di mana seseorang hanya fokus pada sumber informasi pusat dan mengabaikan isyarat di periferal.
- ***Work-as-Done*:** Cara pekerjaan sebenarnya dilakukan di lapangan, dengan segala adaptasi, improvisasi, dan penyesuaian terhadap kondisi nyata.
- ***Work-as-Imagined*:** Cara pekerjaan diasumsikan atau direncanakan untuk dilakukan, seperti yang dijelaskan dalam prosedur atau manual resmi.

DUMMMY

# BIODATA PENULIS



**ANDI TENRIOLA FITRI KESSI** tertarik pada bidang K3 berawal dari kesadaran bahwa keselamatan kerja adalah fondasi produktivitas dan kemanusiaan di industri atau tempat kerja. Lulusan bidang ilmu kesehatan masyarakat Universitas Hasanuddin tahun 1997. Kemudian melanjutkan pendidikan program Pascasarjana Kesehatan Masyarakat Universitas Indonesia dan selesai 2001. Penulis berkarir sebagai dosen sejak 2001 dan menjadi dosen di Lembaga Layanan Pendidikan Tinggi Wilayah IX dan dipekerjakan pada Sekolah Tinggi Ilmu Kesehatan Makassar Program Studi Hiperkes dan Keselamatan Kerja sejak 2005. Penulis aktif sebagai peneliti dibidang Keselamatan dan Kesehatan Kerja yang telah dipublish ditingkat nasional serta melakukan Pengabdian Kepada Masyarakat.

Email penulis : [atenriolafky@gmail.com](mailto:atenriolafky@gmail.com)

# MEMITIGASI HUMAN ERROR

## DALAM SISTEM MANAJEMEN K3

Mengapa kesalahan manusia terus menjadi penyebab dominan kecelakaan kerja, bahkan dalam organisasi yang telah memiliki Sistem Manajemen K3?

Buku *Memitigasi Human Error dalam Sistem Manajemen K3 – Jilid 1* mengajak pembaca meninggalkan cara pandang lama yang menyederhanakan kecelakaan sebagai akibat kelalaian individu. Melalui pendekatan keselamatan berbasis sistem, buku ini menunjukkan bahwa human error lebih tepat dipahami sebagai gejala dari dinamika sistem kerja yang kompleks: desain yang tidak ramah manusia, budaya menyalahkan, tekanan produksi, hingga kepemimpinan yang keliru arah.

Jilid pertama ini membangun fondasi konseptual dan filosofis untuk memahami human error dalam konteks K3 modern. Pembaca diajak menelusuri evolusi paradigma keselamatan, mengkritisi model sebab-akibat tradisional, serta memahami peran krusial sistem, budaya, dan organisasi dalam menciptakan atau mencegah kegagalan.

Bukan sekadar buku teknis, karya ini menawarkan lensa baru: keselamatan sebagai hasil dari sistem yang dirancang dengan kesadaran terhadap manusia. Sebuah pengantar penting bagi siapa pun yang ingin melangkah lebih jauh menuju praktik K3 yang matang, reflektif, dan berkelanjutan—serta pintu awal menuju pembahasan lanjutan pada jilid berikutnya.