TESIS

ANALISIS RISIKO SISTEMIK PADA IMPLEMENTASI SISTEM KESELAMATAN PERTAMBANGAN BERBASIS DIGITAL MENGGUNAKAN INTEGRASI FMEA-FTA

INE FEBRIYANTI

6032221179

Dosen Pembimbing:

Tri Joko Wahyu Adi, S.T., M.T., Ph.D

PROGRAM STUDI MAGISTER MANAJEMEN TEKNOLOGI

SEKOLAH INTERDISIPLIN MANAJEMEN DAN TEKNOLOGI

INSTITUT TEKNOLOGI SEPULUH NOPEMBER

2025

TESIS

ANALISIS RISIKO IMPLEMENTASI SISTEM KESELAMATAN PERTAMBANGAN BERBASIS DIGITAL: PENDEKATAN TERINTEGRASI FAILURE MODE AND EFFECTS ANALYSIS (FMEA) DAN FAULT TREE ANALYSIS (FTA)

INE FEBRIYANTI

6032221179

Dosen Pembimbing:
Tri Joko Wahyu Adi, S.T., M.T., Ph.D

PROGRAM STUDI MAGISTER MANAJEMEN TEKNOLOGI
SEKOLAH INTERDISIPLIN MANAJEMEN DAN TEKNOLOGI
INSTITUT TEKNOLOGI SEPULUH NOPEMBER
2025

LEMBAR PENGESAHAN TESIS

Tesis disusun untuk memenuhi salah satu syarat memperoleh gelar

Magister Manajemen Teknologi (M.MT)

di

Institut Teknologi Sepuluh Nopember

Oleh:

Ine Febriyanti

NRP: 6032221179

Tanggal Ujian: 13 Januari 2026

Periode Wisuda: Maret 2026

Disetujui oleh:

Pembimbing:

TRI JOKO WAHYU ADI, S.T., M.T., Ph.D.,
NIP. 197404202002121003 .....

Penguji:

1. **PROF. R. HARYO DWITO ARMONO, S.T., M.Eng., Ph.D.**
   NIP. 196808101995121001 .....

2. **PROF. RIDHO BAYUAJI, S.T., M.T., Ph.D.**
   NIP. 197307101998021002 .....

DEKAN SEKOLAH INTERDISIPLIN MANAJEMEN DAN TEKNOLOGI,

Prof. Dr. Tri Arief Sardjono, S.T., M.T
NIP: 197002121995121001

ANALISIS RISIKO SISTEMIK PADA IMPLEMENTASI SISTEM KESELAMATAN PERTAMBANGAN BERBASIS DIGITAL MENGGUNAKAN INTEGRASI FMEA–FTA

Nama : Ine Febriyanti
NRP : 6032221179
Dosen Pembimbing : Tri Joko Wahyu Adi, S.T., M.T., Ph.D.

ABSTRAK

Keselamatan kerja merupakan aspek fundamental dalam operasional pertambangan, terutama pada aktivitas dengan tingkat risiko tinggi dan cakupan area yang luas. Sesuai dengan Kepmen ESDM No. 1827 K/30/MEM/2018, setiap perusahaan pertambangan diwajibkan menerapkan sistem manajemen keselamatan yang efektif bagi seluruh kegiatan operasional. PT X mengelola area pertambangan seluas 33.887 hektar dengan jalur hauling sepanjang ±35 km yang melibatkan interaksi intensif antara alat berat, kendaraan angkut, dan pekerja. Kondisi tersebut menjadikan pengawasan keselamatan berbasis inspeksi manual dan pemantauan periodik kurang efektif dalam mendeteksi potensi bahaya secara tepat waktu. Untuk meningkatkan keandalan pemantauan, PT X mengimplementasikan sistem keselamatan berbasis Internet of Things (IoT) yang memungkinkan monitoring kondisi lapangan secara real-time. Namun, digitalisasi sistem keselamatan juga berpotensi menimbulkan risiko baru yang bersifat teknis, operasional, siber, dan sistemik, sehingga memerlukan analisis risiko yang komprehensif. Penelitian ini bertujuan menganalisis risiko sistemik pada implementasi sistem keselamatan pertambangan berbasis digital menggunakan integrasi metode Failure Mode and Effects Analysis (FMEA) dan Fault Tree Analysis (FTA). FMEA digunakan untuk mengidentifikasi mode kegagalan dan menentukan prioritas risiko melalui perhitungan Risk Priority Number (RPN) berdasarkan penilaian para ahli. Selanjutnya, FTA diterapkan untuk menelusuri hubungan kausal antar kegagalan dan mengidentifikasi akar penyebab risiko. Hasil analisis FMEA menunjukkan bahwa 32 dari 40 mode kegagalan berada pada kategori risiko sedang dengan distribusi RPN yang relatif merata, yang mengindikasikan karakter risiko bersifat sistemik dan saling bergantung. Kluster risiko operasional keselamatan menjadi penyumbang terbesar (40,77%), menunjukkan bahwa kelemahan utama sistem terletak pada fungsi deteksi bahaya, interpretasi data, dan penyampaian peringatan. Analisis FTA mengidentifikasi Top Event berupa kegagalan sistem dalam mendeteksi dan memberikan peringatan bahaya kritis secara real-time, serta jalur kegagalan paling kritis berdasarkan Minimal Cut Set (MCS), termasuk potensi *silent failure, blind operation*, dan kerentanan siber. Berdasarkan integrasi FMEA–FTA, ditetapkan lima risiko prioritas yang dimitigasi melalui strategi *risk avoidance, risk reduction, risk transfer, dan risk acceptance.* Evaluasi residual risk menunjukkan bahwa seluruh risiko prioritas berhasil diturunkan ke tingkat risiko rendah (RPN < 1,2), sehingga pendekatan ini mendukung pengambilan keputusan berbasis risiko, optimalisasi sumber daya, dan peningkatan keandalan sistem keselamatan digital dalam mencegah kecelakaan pertambangan.

Kata Kunci: Keselamatan pertambangan, Digitalisasi, IoT, FMEA, FTA, Risiko sistemik, Mitigasi keselamatan.

SYSTEMIC RISK ANALYSIS OF THE IMPLEMENTATION OF DIGITAL-BASED MINING SAFETY SYSTEMS USING AN INTEGRATED FMEA–FTA APPROACH APPROACH

Name : Ine Febriyanti
NRP : 6032221179
Lecturer : Tri Joko Wahyu Adi, S.T., M.T., Ph.D.

ABSTRACT

Occupational safety is a fundamental aspect of mining operations, particularly in activities characterized by high risk levels and extensive operational areas. In accordance with Decree of the Minister of Energy and Mineral Resources (Kepmen ESDM) No. 1827 K/30/MEM/2018, every mining company is required to implement an effective safety management system across all operational activities. PT X operates a mining area covering 33,887 hectares with a ±35 km hauling road, involving intensive interactions among heavy equipment, hauling vehicles, and workers. Under these conditions, safety supervision based on manual inspections and periodic monitoring becomes less effective in detecting potential hazards in a timely manner. To enhance monitoring reliability, PT X has implemented an Internet of Things (IoT)–based safety system that enables real-time monitoring of field conditions. However, the digitalization of safety systems may also introduce new risks of a technical, operational, cyber, and systemic nature, thereby necessitating a comprehensive risk analysis. This study aims to analyze systemic risks in the implementation of a digital-based mining safety system using an integrated Failure Mode and Effects Analysis (FMEA) and Fault Tree Analysis (FTA) approach. FMEA is employed to identify failure modes and determine risk priorities through the calculation of the Risk Priority Number (RPN) based on expert judgment. Subsequently, FTA is applied to trace causal relationships among failures and identify root causes. The FMEA results indicate that 32 out of 40 failure modes fall into the medium-risk category, with a relatively even distribution of RPN values, suggesting that the risks are systemic and interdependent in nature. The operational safety risk cluster contributes the largest proportion (40.77%), indicating that the primary system weaknesses lie in hazard detection, data interpretation, and warning delivery functions. The FTA identifies the Top Event as the failure of the system to detect and issue real-time warnings for critical hazards, along with the most critical failure paths based on Minimal Cut Sets (MCS), including the potential for silent failure, blind operation, and cyber vulnerabilities. Based on the integrated FMEA–FTA results, five priority risks are identified and mitigated using risk avoidance, risk reduction, risk transfer, and risk acceptance strategies. The residual risk evaluation shows that all priority risks are successfully reduced to a low-risk level (RPN < 1.2), demonstrating that this approach supports risk-informed decision-making, resource optimization, and enhanced reliability of digital safety systems in preventing mining accidents.

Keywords: mining safety, digitalization, IoT, FMEA, FTA, systemic risk, safety mitigation

KATA PENGANTAR

Puji dan syukur saya sampaikan ke hadirat Allah SWT atas segala rahmat dan karunia-Nya, sehingga saya dapat menyelesaikan tesis yang berjudul "Analisis Risiko Implementasi Proyek Digitalisasi Sistem Keselamatan Pertambangan, Berbasis FMEA dan FTA" sebagai salah satu syarat untuk memperoleh gelar Master pada **Magister Manajemen Teknologi Institut Teknologi Sepuluh Nopember**. Tesis ini disusun sebagai bentuk kontribusi ilmiah yang diharapkan dapat memberikan manfaat baik bagi praktisi maupun akademisi. Dalam proses penyusunan tesis ini, saya menyadari bahwa pencapaian ini tidak lepas dari bantuan, dukungan, dan bimbingan dari berbagai pihak. Oleh karena itu, penulis menyampaikan rasa terima kasih dan penghargaan yang sebesar-besarnya kepada:

1. Kedua orang tua Ibu dan Ayah, atas doa dan semangat yang selalu menguatkan saya dalam menyelesaikan studi ini.
2. Tri Joko Wahyu Adi, S.T., M.T., Ph.D., selaku dosen pembimbing utama, atas bimbingan, arahan, dan motivasi yang diberikan selama proses penyusunan tesis ini.
3. Seluruh staf pengajar di MMT ITS, atas ilmu dan wawasan yang telah diberikan selama masa studi.
4. PT. X yang telah memberikan support baik informasi maupun data yang diperlukan dalam penelitian ini.
5. Boy Parulian, teman seperjuangan di MMT ITS, atas kebersamaan, diskusi, dan semangat yang menguatkan selama masa studi.

Akhir kata, semoga tesis ini dapat memberikan manfaat bagi pengembangan ilmu pengetahuan serta menjadi referensi bagi penelitian selanjutnya.

Surabaya, 31 Mei 2025

Ine Febriyanti

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

BAB 1
PENDAHULUAN

1.1 Latar Belakang

Keselamatan kerja adalah aspek krusial yang memastikan operasional perusahaan berjalan dengan optimal dan efisien. Di setiap kegiatan operasional, terutama di industri dengan risiko tinggi seperti pertambangan, keselamatan kerja harus menjadi prioritas utama. Keselamatan kerja pada industri pertambangan merupakan aspek fundamental yang berisiko tinggi. Data global dan nasional menunjukkan bahwa sektor pertambangan masih menghadapi angka kecelakaan yang signifikan dan menuntut tindakan mitigasi yang serius. Menurut laporan dari (World Mining Data, 2023) aktivitas pertambangan tetap menjadi sektor kritikal yang memerlukan perhatian terhadap keselamatan kerja. Anggota *International Council on Mining and Metals* (ICMM) melaporkan *Fatality Frequency Rate* (FFR) rata-rata yaitu 0,013 fatalitas per juta jam kerja pada tahun 2023, dimana data ini digunakan sebagai tolak ukur performa keselamatan perusahaan tambang besar (ICMM, 2023).

Di tingkat nasional, data resmi menunjukkan kecenderungan yang perlu untuk diwaspadai. Kementerian Ketenagakerjaan melaporkan angka kasus kecelakaan kerja di seluruh sektor pada tahun 2023 sebesar 370.747 kasus (Kemnaker, 2023). Berdasarkan data dari Ditjen Minerba, jumlah kecelakaan kerja pada sektor pertambangan disajikan pada tabel berikut ini.

Tabel 1.1 Jumlah Kecelakaan Kerja pada Sektor Pertambangan

Tahun	**Total Kejadian**	**Rincian**
Keterangan	**Semua Kategori**	**Ringan / Berat / Fatal**
2022	378	Ringan: 219 Kasus Berat: 97 Kasus Fatal: 62 Kasus
2023	217	Ringan: 104 Kasus

		Berat: 65 Kasus Fatal: 48 Kasus
2024	140	Ringan: 11 Kasus Berat: 80 Kasus Fatal: 49 Kasus

Angka-angka tersebut menunjukkan bahwa masih adanya gap pada regulasi dan program keselamatan area pertambangan. Penerapan standar keselamatan yang baik tidak hanya melindungi pekerja dari kecelakaan, tetapi juga berdampak positif pada produktivitas perusahaan (Borys, 2020). Ketika kondisi kerja aman, karyawan cenderung melakukan tindakan yang lebih aman serta dapat meningkatkan efisiensi dan kualitas hasil kerja (Zohar & Luria, 2019). Selain itu, perusahaan yang konsisten dalam menjaga keselamatan kerja akan membangun reputasi yang baik di kalangan karyawan, mitra bisnis, dan masyarakat (Chen, 2019).

Penerapan sistem manajemen keselamatan menjadi keharusan untuk melindungi karyawan, aset perusahaan, dan lingkungan kerja. Di Indonesia, regulasi keselamatan pertambangan diatur melalui Kepmen ESDM No. 1827K/30/MEM/2018 tentang pedoman pelaksanaan Sistem Manajemen Keselamatan Pertambangan (SMKP). Regulasi ini memerintahkan identifikasi risiko, prosedur mitigasi, pelatihan karyawan, dan audit berkala untuk mengevaluasi efektivitas sistem keselamatan. Dengan menerapkan aturan ini, perusahaan tidak hanya memenuhi kewajiban hukum, tetapi juga membangun budaya keselamatan yang berkelanjutan dalam setiap kegiatan operasional. Keberhasilan Sistem Manajemen Keselamatan Pertambangan (SMKP) tidak hanya bergantung pada kebijakan perusahaan, tetapi juga pada kepatuhan dan partisipasi semua pihak yang terlibat, termasuk karyawan, kontraktor, dan subkontraktor sehingga pengelolaan keselamatan menjadi semakin kompleks. Pengawasan yang menyeluruh memastikan standar keselamatan diterapkan secara konsisten di setiap lini operasional.

PT. X merupakan perusahaan pertambangan batubara berskala besar yang mengelola area seluas 33.887 hektar dengan jalan hauling batubara sepanjang 35 km menggunakan sistem tambang terbuka (*open pit mining*) yang beroperasi pada area dengan karakteristik geologis dan geografis yang kompleks. Kondisi tanah pada area pertambangan PT X didominasi oleh lapisan tanah penutup (*overbuden*) yang tebal dengan sifat tanah lempun yang sensitif terhadap perubahan kadar air, serta batuan dengan tingkat kestabilan yang bervariasi. Dalam upaya pengambilan bahan galian, aktivitas pembongkaran dilakukan dengan metode peledakan, sehingga dapat meningkatkan potensi terjadinya longsor (*slope failure*), penurunan kestabilan lereng, serta perubahan kondisi geoteknik secara dinamis seiring dengan aktivitas penambangan. Karakteristik risiko geoteknik tersebut sejalan dengan temuan pada literature keselamatan pertambangan terbuka yang menyatakan bahwa kondisi tanah lempung, curah hujan tinggi, dan aktivitas peledakan merupakan faktor dominan penyebab ketidakstabilan lereng tambang (Kementerian ESDM, 2018) dan (Hoek & Bray, 2018).

Dari aspek topografi, area tambang pada PT X memiliki bentang alam yang luas dengan perbedaan elevasi yang signifikan dengan melibatkan aktivitas penggalian, penimbunan (*dumping*), serta pengangkutan material dalam skala besar dan intensitas tinggi. Kondisi ini meningkatkan risiko kecelakaan yang berkaitan dengan pergerakan alat berat, interaksi antar unit kerja, serta potensi terjadinya kecelakaan lalu lintas tambang, tergulirnya alat berat, dan tabrakan antar peralatan. Jenis kecelakaan tersebut secara statistik berkontribusi besar terhadap kecelakaan berat dan fatal di sektor pertambangan batubara, sebagaimana dilaporkan dalam publikasi keselamatan kerja pertambangan oleh (Kementerian ESDM, 2018). Selain itu, adanya pemukiman warga di sekitar area operasional PT X akan menambah kompleksitas pengelolaan keselamatan. Risiko keselamatan tidak hanya berdampak pada pekerja tambang, melainkan juga berpotensi menimbulkan dampak lingkungan dan sosial apabila terjadi kegagalan sistem keselamatan seperti longsor, debu berlebih, atau insiden alat berat. Faktor lingkungan lain yang dapat memperbesar tingkat ketidakpastian dan risiko operasional pertambangan seperti curah hujan tinggi, kondisi cuaca ekstrem, serta

perubahan lingkungan secara cepat, sebagaimana diidentifikasi dalam kajian keselamatan pertambangan terbuka oleh (ISO 45001, 2018).

Kombinasi kondisi tanah, topografi, skala operasi yang besar, serta faktor lingkungan tersebut menjadikan tingkat risiko keselamatan pada pertambangan PT X secara inheren lebih tinggi dibandingkan dengan industri lain yang beroperasi pada lingkungan yang lebih terkendali. Oleh karena itu, pendekatan keselamatan konvensional yang bersifat administratif dan berbasis inspeksi manual menjadi kurang memadai, sehingga diperlukan pendekatan keselamatan kerja yang lebih ketat, adaptif, dan berbasis teknologi untuk diterapkan pada PT X. Kondisi area pertambangan batubara pada PT X per tahun 2024 disajikan pada gambar 1.1 berikut ini.

Gambar 1.1 Kondisi Area Pertambangan Batubara pada PT X

Kondisi area pertambangan pada PT X menyebabkan proses pengawasan keselamatan kerja secara konvensional menjadi terbatas, baik dari sisi jangkauan area, frekuensi pemantauan, maupun kecepatan dalam merespons perubahan kondisi kerja. Keterbatasan ini akan berimplikasi pada meningkatnya potensi keterlambatan dalam mendeteksi kondisi berbahaya, khususnya pada aktivitas berisiko tinggi yang melibatkan alat berat dan pengangkutan material berskala besar. Berdasarkan data sekunder kecelakaan kerja PT X, jumlah insiden kecelakaan kerja selama tiga tahun terakhir menunjukkan tren penurunan, namun penurunan tersebut belum signifikan sehingga potensi risiko keselamatan kerja

masih relatif tinggi. Berikut ini disajikan data insiden kecelakaan kerja pada PT X selama 3 tahun terakhir.

Tabel 1.2 Jumlah Kecelakaan Kerja pada PT X

Tahun	Total Insiden	Rincian	
		Keterangan	**Jumlah**
2022	76	Ringan	73
		Berat	2
		Fatal	1
2023	67	Ringan	63
		Berat	2
		Fatal	2
2024	45	Ringan	45
		Berat	0
		Fatal	0

Data kecelakaan pertambangan PT X pada tabel 1.2 menunjukkan bahwa kecelakaan masih terjadi pada berbagai tingkat keparahan yang mengindikasikan bahwa risiko keselamatan kerja di PT X memiliki karakteristik risiko berlapis dan saling berkaitan dengan jenis aktivitas serta kondisi lingkungan kerja. Kecelakaan ringan umumnya terjadi pada aktivitas operasional rutin, seperti pekerjaan lapangan serta adanya interaksi langsung antara pekerja dengan peralatan dan lingkungan kerja pertambangan. Kecelakaan kerja ringan yang dominan berfungsi sebagai *leading indicator* adanya kondisi tidak aman atau potensi kegagalan sistem pengendalian keselamatan, sebagaimana dijelaskan dalam pendekatan keselamatan berbasis risiko oleh (Reason, 1997). Sementara itu, kecelakaan berat banyak berkaitan dengan aktivitas berisiko tinggi seperti pengoperasian alat berat, pengangkutan material dalam volume besar, serta pekerjaan pada area dengan kondisi geoteknik yang kompleks, yang dapat menyebabkan cedera serius dan kehilangan waktu kerja, serta berdampak langsung pada kelangsungan operasi tambang. Kecelakaan fatal seringkali merupakan hasil eskalasi risiko yang tidak terdeteksi atau tidak tertangani secara tepat waktu akibat kombinasi faktor

manusia, peralatan, lingkungan, dan sistem keselamatan. Hal ini menunjukkan bahwa kegagalan sistem keselamatan khususnya dalam mendeteksi dan memberikan peringatan terhadap kondisi bahaya kritis dapat berujung pada dampak keselamatan paling ekstrem.

Berdasarkan karakteristik spesifik pertambangan batubara dan data kecelakaan kerja PT X, dapat disimpulkan bahwa risiko keselamatan pertambangan bersifat dinamis dan sistemik. Oleh karena itu, pendekatan keselamatan konvensional yang bergantung pada inspeksi manual tidak lagi memadai untuk mengelola risiko dengan karakteristik tersebut. Sehingga pengembangan sistem keselamatan digital berbasis *Internet of Things* (IoT) menjadi kebutuhan yang mendesak untuk melakukan pemantauan kondisi kerja secara real-time, integrasi data sensor keselamatan, serta penyampaian peringatan dini secara cepat dan akurat. Dengan demikian, eskalasi risiko dari kecelakaan ringan menuju kecelakaan berat dan fatal dapat dicegah secara lebih efektif.

Studi tinjauan pada penerapan IoT dalam lingkungan konstruksi dan pertambangan menunjukkan bahwa pemanfaatan sensor dan sistem pemantauan *real-time* secara substansial meningkatkan kemampuan deteksi dini dan pengambilan keputusan responsif (Zhou, Liu, & Li, 2020). Teknologi *Internet of Things* (IoT) yang diadopsi seperti *mining eyes,* sensor lingkungan, *wearable device,* dan integrasi data warehouse dapat menawarkan potensi untuk mengurangi keterlambatan deteksi bahaya, memperluas jangkauan pemantauan, dan memperkuat bukti digital investigasi kecelakaan. Namun, adopsi IoT juga membawa risiko baru apabila tidak dikelola dengan baik. Beberapa literatur mencatat risiko utama impelementasi IoT di industri berat yaitu kegagalan perangkat/sensor, keterbatasan jaringan (*coverage & latency*), integrasi dengan sistem *legacy,* dan ancaman keamanan siber yang dapat mengganggu integritas data (Xu, Li, & Zhao, 2022). Dampak kegagalan sistem mencakup *downtime* operasional, penurunan keandalan pengambilan keputusan, kerugian finansial, dan potensi menurunnya kepercayaan pekerja terhadap sistem keselamatan (Kumar, Gupta, & Singh, 2021). Oleh karena itu perencanaan, pengujian, dan pemeliharaan sistem IoT yang matang sangat diperlukan agar teknologi ini

berfungsi optimal dan benar-benar meningkatkan keselamatan kerja di industri pertambangan (Sahanaa & Murugan, 2023).

Selain itu, laporan global dan kajian ilmiah menunjukkan bahwa meskipun banyak penelitian berfokus pada aspek teknis IoT (desain sensor, arsitektur jaringan, optimasi energi), namun kajian tentang analisis risiko implementasi IoT khususnya yang menggabungkan metode kuantitatif dan kualitatif menggunakan metode FMEA dan FTA masih terbatas dalam konteks keselamatan pertambangan (Xu, Li, & Zhao, 2022). Gap seperti ini yang menjadi fokus penelitian ini. Apabila perusahaan mampu mengidentifikasi dan melakukan mitigasi potensi risiko dengan baik, berbagai manfaat seperti efisiensi operasional, pengurangan biaya, bahkan peningkatan performa keselamatan kerja dapat tercapai. Oleh karena itu, diperlukan kajian lebih mendalam untuk memahami dan mengelola risiko yang terkait dengan penerapan IoT. Dengan pendekatan yang tepat, digitalisasi berbasis IoT dapat dioptimalkan untuk meningkatkan keselamatan pertambangan serta mendukung keberlanjutan operasional yang lebih aman dan efisien.

Dengan latar belakang tersebut, penelitian ini bertujuan untuk melakukan analisis risiko implementasi proyek digitalisasi sistem keselamatan pertambangan berbasis IoT di PT X dengan pendekatan kombinasi FMEA untuk prioritasi risiko dan FTA untuk identifikasi akar penyebab. Hasil penelitian diharapkan menghasilkan *risk register* dan rekomendasi mitigasi yang aplikatif untuk meningkatkan performa keselamatan di lapangan dan mengurangi potensi insiden sesuai benchmark nasional maupun internasional pada PT X.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah disebutkan maka rumusan masalah dalam penelitian ini adalah sebagai berikut:

a. Apa saja risiko yang mungkin terjadi saat implementasi proyek digitalisasi dengan penerapan teknologi IoT sistem monitoring keselamatan pertambangan pada PT X?
b. Apa sumber penyebab terjadinya risiko pada PT. X?

c. Bagaimana strategi mitigasi yang dapat diterapkan terhadap risiko yang mungkin terjadi?

1.3 Tujuan Penelitian

Adapun tujuan penelitian ini adalah sebagai berikut:

a. Mengidentifikasi dan menganalisis risiko yang mungkin terjadi saat implementasi proyek digitalisasi dengan penerapan teknologi IoT sistem monitoring keselamatan pertambangan di PT.X.
b. Mengidentifikasi dan menganalisis sumber penyebab terjadinya risiko
c. Menyusun rekomendasi mitigasi risiko untuk mereduksi risiko yang mungkin terjadi

1.4 Manfaat Penelitian

Penelitian ini memiliki dua manfaat utama, yaitu manfaat praktis dan manfaat teoritis yang diuraikan sebagai berikut:

1. Manfaat Praktis
   - Menyediakan *risk register* terukur dan rencana mitigasi yang dapat diadopsi oleh PT X untuk menurunkan angka insiden kecelakaan di area pertambangan.
   - Memberikan rekomendasi teknis-manajerial seperti kebijakan ataupun pelatihan secara berkala yang dapat mendukung implementasi IoT yang aman dan handal bagi PT X.
2. Manfaat Teoritis
   - Mengisi gap literatur terkait analisis risiko implementasi IoT di industri pertambangan serta aplikasi gabungan metode FMEA dan FTA dalam konteks digitalisasi keselamatan di area pertambangan.
   - Menyajikan literatur mengenai penerapan teknologi dalam industri risiko tinggi serta memberikan dasar bagi penelitian selanjutnya dalam bidang keselamatan pertambangan berbasis teknologi IoT.

1.5 Batasan Masalah

Batasan Masalah ditentukan dalam penelitian ini adalah sebagai berikut:

1. Penelitian ini hanya berfokus pada sistem digitalisasi keselamatan pertambangan berbasis *Internet of Things* (IoT) yang digunakan PT X, mencakup sensor keselamatan, perangkat pemantauan, jaringan komunikasi, sistem analitik, dashboard monitoring, dan mekanisme alarm. Sistem operasional non-digital atau sistem keselamatan konvensional tidak dianalisis secara mendalam. Analisis risiko dibatasi pada metode FMEA untuk penilaian dan prioritasi risiko dan FTA untuk mengidentifikasi akar penyebab.
2. Analisis risiko difokuskan pada risiko yang muncul selama implementasi dan operasional awal sistem IoT, bukan pada seluruh siklus hidup proyek (*lifecycle*). Risiko bisnis, risiko finansial makro, atau risiko eksternal (politik, regulasi nasional jangka panjang) tidak menjadi fokus utama penelitian.
3. Faktor ekonomi, perhitungan *cost–benefit*, penilaian investasi teknologi digital, maupun analisis dampak sosial (CSR, perizinan) tidak menjadi fokus penelitian ini, kecuali yang berhubungan langsung dengan penerapan IoT untuk keselamatan.
4. Penelitian tidak mencakup pengembangan prototipe, pengujian lapangan, atau validasi performa teknis perangkat IoT. Analisis bersifat evaluatif berdasarkan data lapangan yang tersedia dan persepsi pakar.

(Halaman ini sengaja dikosongkan)

BAB 2
KAJIAN PUSTAKA

2.1 Definisi dan terminologi

Analisis risiko implementasi proyek digitalisasi sistem keselamatan pertambangan adalah suatu pendekatan sistematis untuk menganalisis risiko yang dihadapi dalam operasional pertambangan pada implementasi teknologi digitalisasi. Tujuannya adalah untuk menganalisis risiko proyek digitalisasi dengan penerapan teknologi IoT yang digunakan untuk memonitor keselamatan pertambangan, menganalisis sumber penyebab terjadinya risiko, dan menentukan tindakan mitigasi risiko untuk mereduksi risiko yang mungkin terjadi. Berikut adalah istilah-istilah kunci yang digunakan dalam tesis ini:

Risiko

Menurut (ISO 31000, 2018) risiko merupakan efek dari ketidakpastian terhadap tujuan yang bisa berdampak terhadap pencapaian tujuan perusahaan, baik berdampak negatif maupun positif. Risiko juga diartikan sebagai kemungkinan terjadinya suatu peristiwa yang dapat menimbulkan dampak negatif terhadap pencapaian tujuan, baik dari operasional maupun finansial perusahaan.

Risiko Sistemik

Risiko sistemik adalah risiko yang muncul akibat ketergantungan dan interaksi antar komponen dalam suatu sistem, di mana kegagalan pada satu elemen dapat menyebar dan memicu kegagalan berantai, sehingga menyebabkan disfungsi sistem secara keseluruhan, meskipun setiap komponen secara individual memiliki tingkat risiko yang moderat (Helbing, 2013) dan (Leimester & Kolios, 2018). Dalam konteks sistem keselamatan digital berbasis IoT, risiko sistemik terjadi ketika kegagalan pada subsistem sensor, analitik, komunikasi, atau faktor manusia saling memperkuat, sehingga menurunkan kemampuan sistem untuk mendeteksi dan merespons kondisi bahaya secara efektif dan tepat waktu.

Implementasi Proyek Digitalisasi

Implementasi proyek digitalisasi mengacu pada proses penerapan teknologi digital pada sistem kerja atau operasional di perusahaan. Menurut (Deloitte, 2022), implementasi proyek digitalisasi pada perusahaan membantu meningkatkan produktivitas bahkan dapat mengurangi insiden kecelakaan kerja melalui pemantauan secara *real-time* dan analisis prediktif. Proyek digitalisasi pada perusahaan pertambangan bertujuan untuk meningkatkan efisiensi kegiatan operasional pertambangan dan keselamatan pertambangan secara menyeluruh di seluruh area pertambangan. Menurut (Bui, Nguyen, & Pham, 2022) menjelaskan bahwa proyek digitalisasi dalam industri pertambangan menciptakan sistem keselamatan yang lebih adaptif dan responsif terhadap risiko operasional meliputi penerapan sistem yang dikategorikan sebagai berikut.

1. *Internet of Things* (IoT)
   Jaringan perangkat fisik yang saling terhubung melalui internet dan mampu bertukar data secara otomatis.
2. Sensor
   Mendeteksi data lingkungan seperti gas beracun, suhu, kelembaban, getaran, posisi pekerja, dll.
3. Gateway
   Mengumpulkan, menyimpan, dan memproses data dari banyak perangkat.
4. Dashboard, dan lainnya.
   Menampilkan informasi secara visual kepada *Central Control Room*

Sistem Keselamatan Pertambangan

Sistem keselamatan pertambangan mencakup prosedur, kebijakan, dan teknologi yang bertujuan untuk melindungi tenaga kerja, peralatan maupun perlengkapan di area pertambangan. Sistem keselamatan pertambangan diatur oleh kementerian ESDM yang bertugas untuk mengatur, mengelola, dan mengawasi kebijakan nasional di bidang energi dan sumber daya mineral. Menurut Peraturan Menteri ESDM No. 26 Tahun 2018, sistem keselamatan pertambangan bertujuan untuk

mengurangi bahkan mencegah kecelakaan akibat kerja serta menjamin kelangsungan operasional perusahaan pertambangan.

FMEA (*Failure Mode Effect Analysis*)

FMEA merupakan suatu metode untuk mengidentifikasi, menganalisis, dan melakukan evaluasi kemungkinan kegagalan dalam suatu sistem, menilai dampaknya, serta menentukan prioritas penanganan untuk mengendalikan suatu risiko (Stamatis, 2003). Metode FMEA diukur menggunakan tiga parameter utama yaitu *Severity* (tingkat keparahan)*, Occurance* (frekuensi kejadian)*,* dan *Detection* (kemungkinan deteksi) untuk menghasilkan nilai RPN (*Risk Priority Number*). Nilai RPN digunakan untuk menetapkan urgensitas dari tindakan mitigasi risiko yang dilakukan, dimana semakin tinggi nilai RPN maka semakin tinggi risiko yang mungkin terjadi (IEC, 2018).

FTA (*Fault Tree Analysis*)

FTA merupakan metode analisis risiko yang bersifat deduktif dan sistematis, dimana metode ini digunakan uintuk mengidentifikasi akar penyebab dari sebuah peristiwa kegagalan yang tidak diinginkan (*top event*) dalam suatu sistem (Vesely, Goldberg, Roberts, & Haasl, 1981). Metode FTA menghasilkan diagram pohon yang digunakan untuk menggambarkan hubungan logis antara berbagai penyebab dasar hingga peristiwa utama. Metode ini banyak diterapkan pada sistem yang memiliki risiko tinggi dan kompleks, termasuk industri pertambangan (IEC, 2006).

2.2 Dasar Teori

2.2.1 Manajemen Risiko

Manajemen Risiko adalah proses sistematis untuk mengidentifikasi, menganalisis, mengevaluasi, menangani, memantau, dan mengendalikan risiko yang berpotensi mempengaruhi pencapaian tujuan organisasi atau proyek. Proses ini bertujuan untuk meminimalkan dampak negatif dan/atau memaksimalkan peluang dalam setiap kegiatan (ISO 31000, 2018). Dalam industry risiko tinggi seperti pertambangan, manajemen risiko sangat penting untuk memastikan keselamatan

kerja dapat dikontrol melalui sistem yang efektif. Dengan manajemen risiko, perusahaan dapat melindungi aset yang ada di dalamya, baik manusia maupun peralatan dan meminimalisasi biaya tak terduga akibat kerugian.

Manajemen risiko harus diidentifikasi berdasarkan sumber dan data yang aktual. Risiko dapat berasal dari berbagai faktor, baik dari internal maupun eksternal perusahaan yang mencakup kondisi operasional perusaaan, teknologi yang digunakan, lingkungan, hingga peraturan pemerintah (PMBOK , 2021). Manajemen risiko merupakan proses terstruktur dari beberapa tahapan berkesinambungan, dimana setiap tahapan memiliki peran penting dalam memastikan risiko dapat berjalan dengan efektif. Berikut merupakan tahapan utama dalam manajemen risiko menurut (ISO 31000, 2018) yang diuraikan sebagai berikut:

1. Penetapan Konteks (*Establishing the Context*)

   Tahapan ini memiki tujuan untuk mengetahui dan memahami lingkungan internal beserta eksternal perusahaan, termasuk tujuan, kebijakan, bahkan batasan yang ada didalamnya (ISO 31000, 2018).
2. Identifikasi Risiko (*Risk Identification*)

   Tahapan ini merupakan suatu proses secara sistematis untuk menemukan, mengetahui, dan mendeskripsikan risiko yang mungkin akan mempengaruhi tercapainya tujuan perusahaan. Berdasarkan (PMBOK , 2021) metode yang umum digunakan saat tahapan ini yaitu observasi lapangan, diagram sebab akibat, maupun *Fault Tree Analysis* (FTA).
3. Analisis Risiko (*Risk Analysis*)

   Tahapan ini dilakukan untuk mengetahui tingkat kemungkinan terjadinya risiko, dampak risiko terhadap tujuan, serta faktor penyebab terjadinya risiko. Menurut (ISO 31010, 2019) pendekatan analisis bisa menggunakan pendekatan secara kualitatif menggunakan deskripsi maupun menggunakan pendekatan kuantitatif menggunakan data numerik dengan metode FMEA.
4. Evaluasi Risiko (*Risk Evaluation*)

   Tahapan selanjutnya bertujuan untuk membandingkan hasil analisis risiko dengan kriteria risiko yang telah ditentukan sebelumnya. Output dari evaluasi

risiko ini digunakan untuk menentukan prioritas risiko dan memutuskan apakah risiko dapat diterima atau harus segera ditangani.

5. Penanganan Risiko (*Risk Response*)

   Tahapan ini meliputi pemilihan dan pelaksanaan strategi yang akan digunakan oleh perusahaan. Strategi umum yang dapat digunakan diklasifikasikan menjadi empat bagian, yaitu *avoidance* yaitu menghindari kegiatan pemicu risiko, *reduction* yaitu mengurangi dampak risiko, *transfer* yaitu memindahkan risiko yang ada, ataupun *acceptance* yaitu menerima risiko dengan rencana kontinjensi.

   Setelah dilakukan penanganan risiko, kemudian dihasilkan "*residual risk*" yang harus dikendalikan agar perusahaan dapat menentukan apakah risiko yang tersisa masih dalam batas toleransi perusahaan khususnya di sektor industri berisiko tinggi seperti perusahaan pertambangan, minyak dan gas, ataupun manufaktur.

6. Monitoring dan Kontrol Risiko (*Risk Monitoring and Controlling*)

   Proses pada tahapan ini harus dilakukan secara berkala yang bertujuan untuk memastikan efektivitas tindakan mitigasi, menilai perubahan lingkungan, dan memperbarui dokumentasi risiko (COSO ERM , 2017).

7. Komunikasi dan Konsultasi (*Communication and Consultation*)

   Tahapan ini merupakan bagian akhir dari manajemen risiko, dimana komunikasi merupakan hal penting agar stakeholder perusahaan terkait dapat memastikan pemahaman risiko yang terjadi maupun yang akan terjadi, mendapatkan dukungan dari manajemen, serta membangun budaya sadar risiko dalam perusahaan.

2.2.2 Sistem Keselamatan Pertambangan

Menurut Peraturan Menteri ESDM No. 26 Tahun 2018, keselamatan pertambangan merupakan segala kegiatan untuk menjamin dan melindungi tenaga kerja, orang lain, dan lingkungan sekitar lokasi tambang agar terhindar dari potensi bahaya tambang. Sistem ini mencakup aspek manajemen risiko, kepatuhan hukum, penerapan teknologi keselamatan, dan budaya kerja yang aman di seluruh lini operasi tambang. Sistem keselamatan pertambangan didukung oleh

beberapa regulasi yang menjadi acuan untuk menerapkan manajemen keselamatan pertambangan yang semakin diperkuat dengan teknologi digital seperti pemantauan *real time,* automasi, dan integrasi sistem informasi keselamatan. Berikut beberapa regulasi yang disajikan pada tabel berikut ini.

Tabel 2.1 Regulasi Sistem Keselamatan Pertambangan

No	Regulasi	Keterangan
1	UU No. 4 Tahun 2009	Pertambangan mineral dan batubara
2	Permen ESDM No. 26 Tahun 2018	Pelaksanaan kaidah teknik pertambangan yang baik
3	Kepmen ESDM No. 1827 K/30/MEM/2018	Pedoman pelaksanaan SMKP Minerba
4	ISO 45001:2018	Sistem manajemen keselamatan dan kesehatan kerja

Sistem keselamatan pertambangan merujuk pada digitalisasi dalam pemanfaatan teknologi informasi dan komunikasi untuk meningkatkan efektivitas, efisiensi, dan akurasi dalam sistem keselamatan kerja. Teknologi digital memungkinkan sistem keselamatan tambang menjadi lebih prediktif dan adaptif terhadap perubahan kondisi operasional secara *real-time* (ICMM , 2021). Industri pertambangan menghadapi risiko tinggi terhadap keselamatan kerja sehingga untuk mengurangi risiko tersebut, digitalisasi berbasis *Internet of Things* diterapkan untuk meningkatkan kemampuan pemantauan, peringatan dini, dan pengendalian risiko secara *real-time.* IoT dalam industri pertambangan bisa meningkatkan keselamatan pertambangan secara *real-time*, analisis prediktif, dan respon yang lebih cepat.

2.2.3 Sistem Monitoring Keselamatan Kerja berbasis IoT

Konsep Monitoring Keselamatan Kerja berbasis IoT

Sistem monitoring keselamatan kerja berbasis *Internet of Things* (IoT) adalah solusi yang efektif untuk meningkatkan keselamatan kerja di lingkungan berisiko tinggi seperti pertambangan, dimana sistem ini dapat mengoptimalkan

keterbatasan supervisi dikarenakan cakupan area yang sangat luas. Sistem monitoring keselamatan kerja berbasis IoT memungkinkan manajemen risiko proaktif dengan memanfaatkan sensor data analitik *real-time* (Zhou, Liu, & Li, 2020). Adapun manfaat sistem monitoring keselamatan kerja berbasis IoT antara lain:

1. Deteksi dini bahaya: mencegah kecelakaan dengan memberikan peringatan sebelum bahaya terjadi.
2. Pemantauan *real-time*: Memungkinkan pengawasan terus-menerus dari Central Control Room.
3. Analisis data historis: Membantu evaluasi dan perencanaan keselamatan berbasis data.
4. Automatisasi respons: Sistem dapat mengambil tindakan otomatis (shutdown, alarm, dll).
5. Perlindungan pekerja: Melacak lokasi dan kondisi pekerja di area rawan (khususnya tambang bawah tanah).

Monitoring keselamatan pertambangan berbasis IoT menjadi elemen penting dalam penerapan keselamatan dan kesehatan kerja serta mendukung pelaksanaan SMKP (Sistem Manajemen Keselamatan Pertambangan). Sistem keselamatan kerja berbasis IoT telah menunjukkan kemampuan signifikan dalam mencegah kecelakaan kerja dengan memungkinkan deteksi bahaya secara *real-time* (Zhou, Liu, & Li, 2020).

IoT yang Digunakan dalam Monitoring Keselamatan Kerja

Fungsi IoT dalam monitoring keselamatan kerja pada industri pertambangan yaitu mengukur kondisi lingkungan kerja secara *real-time,* pemantauan aktivitas dan kondisi pekerja, pelacakan pekerja dan alat berat, memberikan sinyal otomatis ke *control room,* melakukan pencatatan dan penyimpanan data untuk analisis risiko. Selain itu, sistem IoT yang dapat digunakan dalam monitoring keselamatan kerja di industri pertambangan dikelompokkan sebagai berikut:

Tabel 2.2 IoT Monitoring Keselamatan Pertambangan

No.	Komponen IoT	Fungsi

1	Gas sensor	Deteksi gas beracun di tambang bawah tanah
2	Inclinometer & Accelerometer	Deteksi potensi longsor dan getaran abnormal pada struktur tambang
3	Wearable Device	Mendeteksi suhu tubuh, kelelahan, detak jantung pekerja
4	GPS & IMU	Melacak lokasi pekerja dan kendaraan, serta deteksi zona bahaya
5	Proximity Sensor	Mendeteksi keberadaan alat berat untuk mencegah tabrakan
6	Thermal Camera	Mengidentifikasi suhu tinggi dari peralatan atau tubuh pekerja

Sumber: (Singh & Rathore, 2021)

Selain itu, monitoring keselamatan kerja berbasis IoT juga memiliki komponen pendukung sistem yang diklasifikasikan sebagai berikut.

a. Gateway IoT
b. Jaringan Komunikasi
c. Cloud Server
d. Control Room / Dashboard

Pengambilan Keputusan dan Pengolahan Data berbasis IoT

Menurut (Bui & Zorzi, 2017) tahapan proses pengambilan keputusan berbasis IoT dapat mengubah data mentah menjadi keputusan melalui analisis *real-time* melalui proses yang diklasifikasikan sebagai berikut.

1. Akuisisi Data (*Data Acquisition*) dimana perangkat *wearable* ataupun sensor mengumpulkan data lingkungan, posisi, dan fisiologis.
2. Pengiriman Data (*Transmission*) melalui jaringan IoT ke gateway pusat.
3. Pemrosesan Data (*Data Processing*) secara lokal atau cloud untuk mendapatkan prediksi kondisi tidak aman berdasarkan tren historis.
4. Pengambilan Keputusan (*Decision Support*) dimana sistem memberikan sinyal otomatis apabila terjadi kondisi tidak normal.

5. Dokumentasi dan Logging , dimana semua kejadian dan data terekam dalam database untuk digunakan dalam evaluasi, investigasi, laporan, dan audit.

2.2.4 FMEA (*Failure Mode Effect Analysis*)

Setelah melakukan implementasi proyek, tahapan berikutnya penelitian ini menggunakan metode *Failure Modes Effects Analysis* (FMEA) yaitu metode analisis yang digunakan untuk mengidentifikasi potensi kegagalan dalam suatu sistem, produk, atau proses, serta mengevaluasi dampak dari kegagalan tersebut terhadap kinerja atau keselamatan. *Failure Modes Effects Analysis* (FMEA) adalah sebuah metode analisis yang digunakan untuk menganalisis potensi kegagalan dalam suatu proses atau produk dengan cara mengidentifikasi kegagalan (*failure modes*), penyebab (*failure causes),* dan dampak (*effects*). Metode ini digunakan untuk mengidentifikasi kegagalan yang paling kritis dan memberikan dasar bagi pengambilan keputusan untuk mengurangi atau menghindari risiko yang akan terjadi. Adapun langkah analisis *Failure Modes Effects Analysis* (FMEA) adalah sebagai berikut:

a. Mempelajari objek yang anak dianalisis.
b. Mengidentifikasi seluruh penyebab risiko potensial.
c. Merangkum dan mencatat seluruh konsekuensi dari risiko potensial untuk setiap *failure modes*.
d. Menetapkan nilai-nilai (melalui jalan observasi lapangan dan *brainstorming*) dalam skala 1 hingga 5, dengan menggunakan parameter pengukuran yang diklasifikasikan sebagai berikut.
    i. ***Severity* (S)** merupakan klasifikasi tingkat bahaya terhadap dampak yang ditimbulkan oleh risiko. Skala 1 (dampak kecil) hingga 5 (dampak sangat besar).
    ii. ***Occurrence* (O)** merupakan frekuensi terjadinya kegagalan berdasarkan satuan waktu tertentu. Skala 1 (sangat jarang terjadi) hingga 5 (terjadi sangat sering).
    iii. ***Detection* (D)** merupakan penilaian terhadap seberapa baik tingkat pengendalian dan pengawasan untuk mendeteksi risiko yang dapat terjadi sebelum efek tersebut dirasakan oleh konsumen. Skala 1 yang

mengindikasikan deteksi mudah hingga 5 yang mengindikasikan deteksi sangat sulit.

e. Menghitung *Risk Priority Number* (RPN) yang digunakan untuk menunjukan ranking atau prioritas setiap risiko yang terjadi.

Rumus *Risk Priority Number* (RPN) = S × O × D

f. Mengurutkan ranking kegagalan berdasarkan nilai RPN dari yang terbesar hingga terkecil.

Metode FMEA memiliki kelebihan serta kelemahan dalam implementasinya. Kelebihan metode FMEA antara lain:

- Proaktif dalam identifikasi risiko dengan membantu mengidentifikasi potensi kegagalan sejak awal dan memungkinkan tindakan perbaikan sebelum kegagalan nyata terjadi.
- Sistematis dan terstruktur yang memudahkan dalam identifikasi dan evaluasi potensi kegagalan secara menyeluruh.
- Pengambilan keputusan berdasarkan data dengan menggunakan RPN untuk pengambilan keputusan dalam menetapkan prioritas tindakan perbaikan.
- Meningkatkan Keandalan Produk dan Proses dengan mengidentifikasi dan mengurangi risiko sehingga dapat membantu meningkatkan keandalan dan keselamatan produk atau sistem.

Di sisi lain, kelemahan dari metode FMEA perlu dipertimbangkan antara lain:

- Memerlukan data yang akurat dikarenakan metode ini sangat bergantung pada data yang akurat untuk mengevaluasi kemungkinan dan dampak kegagalan. Tanpa data yang tepat, hasil analisis dapat menjadi tidak akurat atau bias.
- Analisis FMEA bisa memakan waktu dan memerlukan banyak sumber daya, terutama untuk sistem yang sangat kompleks.
- Tidak menggambarkan semua kemungkinan risiko dikarenakan hanya fokus pada risiko yang paling terlihat dengan tingkat urgensitas tinggi dan mungkin tidak mencakup semua potensi risiko yang ada dalam sistem.

2.2.5 *Fault Tree Analysis* (FTA)

Dalam melakukan penelitian, metode *Fault Tree Analysis* (FTA) atau biasa disebut analisis pohon kesalahan merupakan metode pencarian akar penyebab permasalahan (Leimester & Kolios, 2018). *Fault Tree Analysis* (FTA) adalah teknik analisis yang digunakan untuk mengidentifikasi dan menganalisis penyebab potensial dari suatu kegagalan dalam sistem yang lebih besar. FTA biasanya digunakan untuk mengevaluasi kemungkinan terjadinya kegagalan berdasarkan kombinasi berbagai faktor yang ada. Metode ini menyusun kejadian-kejadian atau kegagalan dalam sistem secara hierarkis menggunakan struktur pohon (*tree*) yang menggambarkan hubungan logis antara sebab akibat dari kegagalan tersebut. FTA merupakan teknik yang sangat berguna dalam mengevaluasi dan mengidentifikasi risiko serta penyebab kegagalan dalam suatu sistem. Dengan analisis menggunakan metode FTA, penulis dapat memberikan gambaran yang jelas mengenai hubungan sebab akibat antar kejadian dalam sebuah sistem. Meskipun ada tantangan dalam aplikasi FTA untuk sistem yang sangat kompleks, teknik ini tetap menjadi alat yang penting dalam analisis dan manajemen risiko di berbagai industri. Istilah dan symbol yang digunakan pada metode ini diuraikan sebagai berikut.

Tabel 2.3 Istilah dan Simbol Metode FTA

Istilah	Keterangan	Simbol
Basic Event	Simbol penyebab risiko atau akar penyebab risiko sehingga tidak perlu analisis lanjutan	
Intermediate Event	Penyebab tersebut memerlukan analisis lanjutan dimana simbol ini diikuti logic gates untuk menganalisis peristiwa selanjutnya.	
Undeveloped Event	Simbol yang menunjukkan bahwa peristiwa tersebut tidak dapat dianalisis lebih lanjut.	

Transfer Symbol	Simbol yang menunjukkan bahwa peristiwa tersebut memerlukan analisis lanjutan, diluar dari peristiwa risiko utama pada analisis yang sedang dikerjakan.	
AND *gate*	Kejadian risiko yang terjadi apabila seluruh inputnya terjadi.	
OR *gate*	Kejadian risiko yang terjadi pada salah satu inputnya terjadi atau lebih.	
Voting OR gate	Peristiwa yang terjadi jika jumlah peristiwa yang terjadi sesuai dengan kondisi yang dibutuhkan.	

Sumber: (Alijoyo, Wijaya, & Jacob, 2020)

Adapun metode FTA memiliki kelebihan diantaranya yaitu:

a. Identifikasi Penyebab Kegagalan

   Memungkinkan identifikasi penyebab utama yang dapat memicu kegagalan dalam sistem.

b. Penilaian Risiko

   Menilai risiko yang terkait dengan sistem/komponen serta membantu merencanakan strategi mitigasi.

c. Komunikasi yang Jelas

   Dengan menggunakan visualisasi pohon, hasil analisis FTA dapat dengan mudah dipahami oleh berbagai pihak, termasuk teknisi, manajer, dan pemangku kepentingan lainnya.

Di sisi lain, kelemahan dari FTA perlu dipertimbangkan pada saat pemilihan metode antara lain:

a. Kompleksitas dalam sistem besar

   FTA dapat menjadi kompleks ketika diterapkan pada sistem yang besar dan rumit, dengan banyak komponen yang saling berinteraksi.

b. Tidak Menyediakan Solusi Langsung

Walaupun FTA dapat membantu mengidentifikasi penyebab kegagalan, ia tidak selalu memberikan solusi praktis atau alternatif untuk mencegah kegagalan tersebut.

c. Keterbatasan Data

Keakuratan FTA sangat bergantung pada data yang akurat, terutama dalam hal probabilitas kegagalan komponen. Tanpa data yang tepat, hasil analisis bisa menjadi tidak akurat atau bias.

2.3 Penelitian Terdahulu

Kajian Penelitian Terdahulu dan Sintesis Risiko Implementasi IoT pada Keselamatan Pertambangan

Penelitian mengenai analisis risiko pada proyek digitalisasi telah berkembang pesat, terutama pada sektor energi, teknologi informasi, konstruksi, dan industri berbasis aset berisiko tinggi. Secara umum, studi-studi tersebut menempatkan digitalisasi sebagai upaya peningkatan efisiensi dan keselamatan, namun sekaligus mengubah profil risiko organisasi karena introduksi komponen baru sensor, jaringan, platform data, serta automasi berbasis perangkat lunak yang berpotensi menimbulkan kegagalan sistemik jika tidak dikelola secara memadai (ISO 31000, 2018). Dalam konteks ini, standar manajemen risiko menekankan pentingnya evaluasi risiko berdasarkan kemungkinan kegagalan dan dampak terhadap keselamatan manusia, aset, dan lingkungan, sehingga pendekatan pengelolaan risiko perlu bersifat prediktif, adaptif, dan terintegrasi. Sejalan dengan itu, kajian IoT juga menegaskan bahwa implementasi IoT bukan sekadar adopsi teknologi, melainkan transformasi sistem yang memperluas kompleksitas ekosistem digital melalui automasi, sensor, *big data, machine learning*, dan komunikasi nirkabel yang semuanya dapat memunculkan kelas risiko baru di luar risiko operasional konvensional (Atzori & Morabito, 2017).

Dominasi FMEA pada Analisis Risiko Proyek Digitalisasi

Sebagian besar penelitian analisis risiko proyek digitalisasi mengandalkan Failure Mode and Effects Analysis (FMEA) untuk mengidentifikasi mode kegagalan, mengukur tingkat prioritas, dan menyusun mitigasi yang fokus pada peningkatan

reliabilitas sistem. Temuan umum menunjukkan risiko dominan pada proyek digitalisasi berada pada ranah teknis misalnya kegagalan perangkat, ketidakandalan sensor, kesalahan integrasi sistem, serta kelemahan jaringan yang secara langsung dapat menurunkan efektivitas implementasi teknologi digital (Syahbana, Puspita, & Widyasthana, 2021). Namun, terdapat keterbatasan yang sering muncul pada studi berbasis FMEA. Pertama, sebagian penelitian cenderung menilai risiko setelah sistem digital berjalan, sehingga kurang menangkap risiko kritis pada tahap implementasi dan operasional awal. Kedua, beberapa studi belum mengevaluasi *residual risk* pasca mitigasi, sehingga efektivitas kontrol yang diusulkan belum dapat dinilai secara utuh. Ketiga, validasi risiko sering terbatas pada data dokumen atau observasi internal, tanpa penguatan melalui validasi ahli seperti *Focus Group Discussion* (FGD), padahal proyek digitalisasi berisiko tinggi umumnya memerlukan triangulasi perspektif lintas fungsi (ISO 31000, 2018).

Kontribusi FTA untuk Penelusuran Akar Penyebab, namun Minim Prioritisasi Kuantitatif

Di sisi lain, pendekatan Fault Tree Analysis (FTA) banyak digunakan untuk memahami struktur sebab-akibat dari suatu kejadian puncak (*top event*), khususnya dalam keselamatan kerja. FTA efektif untuk menelusuri akar penyebab secara logis dan sistematis, serta mengidentifikasi kombinasi faktor yang memicu kecelakaan atau kegagalan sistem. Dalam konteks proyek keselamatan kerja, FTA terbukti membantu organisasi menyusun mitigasi yang lebih terarah karena memperjelas jalur sebab-akibat dan keterkaitan antarkomponen risiko (Salim, Ratnaningsih, & Arifin , 2024). Akan tetapi, FTA juga memiliki keterbatasan yang sering muncul pada penelitian terdahulu, yaitu kecenderungan FTA digunakan secara berdiri sendiri, sehingga tidak menghasilkan prioritas risiko yang terukur sebagaimana FMEA (Salim, Ratnaningsih, & Arifin , 2024). Selain itu, beberapa penelitian FTA belum memperkuat akurasi struktur pohon kesalahan melalui triangulasi data (misalnya wawancara terstruktur, observasi, dan diskusi ahli), padahal kompleksitas faktor di lapangan tambang dapat memunculkan "*hidden causes*" yang tidak terdeteksi hanya dari data formal (ISO 31000, 2018).

Risiko Spesifik IoT pada Pertambangan: Perluasan dari Risiko Teknis ke Siber, Human, Lingkungan, dan Regulasi

Jika ditarik ke konteks pertambangan, adopsi IoT untuk sistem keselamatan membawa manfaat besar berupa *monitoring real-time*, peringatan dini, dan automasi respons. Namun literatur IoT menegaskan bahwa penerapan IoT memperkenalkan risiko baru yang harus dipetakan dan dikelola secara sistematis, terutama karena heterogenitas perangkat, ketergantungan jaringan, serta integrasi sistem data lintas platform (Atzori & Morabito, 2017). Hasil sintesis variabel risiko berdasarkan Tabel 2.4 menunjukkan bahwa risiko implementasi IoT pada keselamatan pertambangan tidak hanya bersifat teknis, tetapi terbagi ke enam kategori besar yaitu teknis; siber & privasi; operasional & keselamatan; human & organisasi; lingkungan & kalibrasi; serta regulasi.

Pada risiko teknis, lingkungan tambang yang ekstrem seperti debu, getaran, suhu, dan kelembapan diketahui sangat memengaruhi performa sensor dan sistem elektronik, sehingga risiko seperti kegagalan reliabilitas sensor, gangguan konektivitas/latensi, dan keterbatasan daya menjadi faktor kritis yang dapat mengganggu monitoring keselamatan (Khanna & Kaur, 2019). Selain itu, studi kasus IoT pada tambang bawah tanah menunjukkan tantangan jaringan dan implementasi sistem peringatan dini, yang mempertegas bahwa aspek konektivitas dan latency tidak dapat diperlakukan sebagai isu minor pada sistem keselamatan berbasis IoT (Nguyen & Nguyen, 2023).

Pada risiko siber & privasi, standar manajemen risiko keamanan informasi menegaskan bahwa ekosistem IoT rentan terhadap serangan karena banyaknya perangkat dan koneksi, sehingga kontrol akses, autentikasi, integritas data, serta perlindungan privasi menjadi pilar utama mitigasi (IEC, 2018). Literatur keamanan IoT juga menekankan variasi tingkat keamanan protokol nirkabel dan kompleksitas sistem terdistribusi sebagai sumber kerentanan yang signifikan (Roman, Zhou, & Lopez, 2013).

Pada risiko human & organisasi, adopsi IoT menuntut kesiapan kompetensi digital, budaya organisasi yang mendukung pembelajaran, dan pengelolaan

perubahan. Perspektif *human-centric* menegaskan bahwa automasi harus tetap menempatkan manusia sebagai pusat untuk menekan *human error* dan risiko resistensi adopsi (Tarafdar, Pullins, & Ragu-Nathan, 2019). Tanpa kesiapan operator dan pelatihan yang memadai, dashboard dan alarm berbasis IoT justru dapat memicu "*alarm fatigue*", salah interpretasi, dan penurunan kewaspadaan yang pada akhirnya berpotensi menurunkan performa keselamatan.

Pada risiko lingkungan & kalibrasi, isu kalibrasi sensor dan gangguan lingkungan seperti debu, kelembapan, dan suhu ekstrem menjadi sangat relevan karena dapat menghasilkan deviasi pengukuran yang berdampak langsung pada keputusan keselamatan (Zhang, Yang, & Chen, 2014).

Pada risiko regulasi, industri tambang dituntut memenuhi kewajiban audit keselamatan, retensi data, dan tata kelola pelaporan yang transparan, dimana ketidakpatuhan dapat memunculkan konsekuensi hukum dan gangguan operasional (ICMM , 2021).

Gap Penelitian yang Masih Terbuka

Berdasarkan gabungan kajian FMEA–FTA dan sintesis variabel risiko IoT pada keselamatan pertambangan, muncul beberapa gap penelitian yang jelas dan relevan untuk diselesaikan:

1. Keterbatasan integrasi metode: Penelitian terdahulu cenderung memisahkan FMEA (prioritisasi risiko) dan FTA (analisis akar penyebab). Akibatnya, banyak studi menghasilkan daftar prioritas tanpa pemahaman struktural penyebab, atau menghasilkan struktur penyebab tanpa prioritas kuantitatif yang operasional untuk pengambilan keputusan (Salim, Ratnaningsih, & Arifin , 2024) dan (Syahbana, Puspita, & Widyasthana, 2021).
2. Fokus temporal yang sempit: Sebagian studi digitalisasi lebih menekankan risiko pasca-implementasi, sementara risiko krusial pada tahap implementasi dan operasional awal, misalnya *reliability sensor* di *fase commissioning,* stabilitas jaringan di awal operasi, serta kesiapan operator sering belum dimodelkan secara memadai (Syahbana, Puspita, & Widyasthana, 2021); (Phong, Tuyen, & Osinski, 2024).

3. Ruang lingkup risiko belum komprehensif untuk IoT keselamatan tambang: Literatur digitalisasi sering berhenti pada risiko teknis, sementara implementasi IoT untuk keselamatan pertambangan menuntut cakupan lebih luas yang mencakup siber privasi (ISO 27005, 2018), human–organisasi, kalibrasi–lingkungan, dan kepatuhan regulasi/retensi data (ISO 31000, 2018); (Roman, Zhou, & Lopez, 2013); (Tarafdar, Cooper, & Stich, 2019); (Zhang, Yang, & Chen, 2014).
4. Validasi lapangan dan *residual risk*: Banyak penelitian belum menutup siklus analisis sampai evaluasi *residual risk* dan validasi pakar lintas fungsi. Padahal, untuk sistem keselamatan pertambangan, mitigasi yang kredibel perlu diuji melalui triangulasi, misalnya FGD dengan praktisi safety, operasional, maintenance, dan IT/OT security agar rekomendasi tidak bias dan relevan terhadap kondisi operasional PT X (ISO 31000, 2018).

Dengan demikian, gap tersebut menguatkan urgensi penelitian ini untuk membangun kerangka analisis risiko yang terpadu dengan menggabungkan FMEA (prioritisasi kuantitatif) dan FTA (penelusuran akar penyebab) pada konteks implementasi sistem keselamatan pertambangan berbasis IoT, dengan ruang lingkup risiko yang komprehensif (teknis, siber, operasional, human, lingkungan, regulasi) serta divalidasi melalui pendekatan ahli dan lapangan. Kerangka terpadu ini diharapkan menghasilkan keluaran yang lebih menyeluruh, terukur, dan aplikatif untuk penguatan keselamatan dan keandalan operasional di PT X.

2.4 Sintesis Variabel Risiko

Pertambangan merupakan suatu industri dengan risiko keselamatan kerja yang cukup tinggi, sehingga sistem manajemen keselamatan pertambangan harus diimplementasikan secara lebih prediktif, adaptif, efektif dan efisien guna meminimalisir potensi munculnya risiko di area pertambangan. (ISO 31000, 2018) menekankan bahwa setiap sistem harus di evaluasi berdasarkan kemungkinan kegagalan dan dampaknya terhadap keselamatan, aset, dan lingkungan. Pada industri pertambangan, risiko yang muncul umumnya berasal

dari kondisi geoteknik, kegiatan operasional, peralatan mekanik, cuaca, hingga faktor manusia.

Proyek digitalisasi sistem keselamatan pertambangan dengan teknologi IoT akan membawa perubahan yang signifikan terhadap struktur risiko operasional. Implementasi IoT pada perusahaan pertambangan dapat meningkatkan integrasi teknologi digital seperti automasi, sensor IoT, bi data, machine learning, serta penggunaan jaringan komunikasi nirkabel. Implementasi teknologi IoT pada industri pertambangan tentunya membawa berbagai manfaat seperti meningkatkan efisiensi operasional, automasi proses, dan peningkatan keselamatan kerja. Penelitian oleh (Atzori & Morabito, 2017) menekankan bahwa implementasi IoT memperkenalkan risiko baru yang perlu dipetakan dan dikelola secara sistematis. Berdasarkan hasil kajian dari beberapa literature dan regulasi keselamatan pertambangan, risiko impelementasi IoT dapat dikategorikan sebagai berikut.

Risiko Teknis

Risiko ini berakibat pada terjadinya kegagalan fungsi atau penurunan kinerja komponen teknis IoT yang menyebabkan gangguan operasional, kesalahan pengukuran, maupun ancaman keselamatan. Lingkungan pertambangan yang ekstrem sangat mempengaruhi performa sensor dan sistem elektronik (Khanna & Kaur, 2019).

- ***Reliability Sensor***

  Kegagalan sensor yang menyebabkan data tidak akurat atau data tidak tesedia. IoT *risk analysis* menyebutkan bahwa faktor perangkat (*device*) yang berkontribusi sebagai sumber utama kegagalan berdasarkan hasil penelitian oleh jurnal (Andrade, Ortiz-Garces, Tintin, & Lluminquinga, 2022).

- ***Connectivity & Network Latency***

  Latensi tinggi, packet loss, maupun gangguan komunikasi yang berdampak ke sistem monitoring *real-time*. Sistem peringatan dini berbasis IoT di tambang bawah tanah menghadapi tantangan jaringan menurut penelitian yang dilakukan oleh (Phong, Tuyen, & Osinski, 2024).

- ***Power & Energy Availability***

Ketersediaan daya listrik/baterai untuk perangkat IoT di lingkungan yang ekstrem sering menjadi masalah.

Risiko Siber & Privasi

Sesuai (ISO 27005), perangkat IoT merupakan target rentan terhadap serangan siber. Penelitian oleh (Zhang, Wang, & Li, 2023) menemukan bahwa lebih dari 70% sistem IoT industri pernah mengalami percobaan intrusi. Sistem IoT di pertambangan menggunakan protokol nirkabel yang memiliki tingkat keamanan bervariasi sehingga dapat meningkatkan risiko keamanan (Roman, Zhou, & Lopez, 2013). Risiko siber dan privasi menjadi isu dominan dikarenakan beberapa hal sebagai berikut:

- ***Weak Authentication / Access Control***

  Sistem IoT yang tidak memiliki autentifikasi kuat, *mis-use credential*, serta menjadi ventor serangan siber.
- ***Intrusion / Malware Attack Surface***

  Implementasi sistem IoT mengakibatkan jumlah perangkat dan koneksi meningkat sehingga permukaan serangan (*attack surface*) IoT menjadi sangat besar (Andrade & et al, 2022).
- ***Data Integrity & Private Breach***

  Manipulasi data sensor atau pencurian data pekerja dapat mengganggu keputusan operasional dan keselamatan. Studi keamanan IoT menyebutkan bahwa integritas data sebagai salah satu elemen kunci yang sangat krusial (Karim, Kabir , Lei, Lefticaru, & Baset, 2025).

Risiko Operasional & Keselamatan

Risiko operasional dan keselamatan muncul ketika sistem IoT gagal mendeteksi bahaya atau memberikan aksi automasi yang salah. Meta-review IoT safety menunjukkan rata-rata 18% alarm otomatis menunjukkan *inaccurate reading* (Al-Masri, Thangavel, & Kaddoum, 2023). Risiko operasional dan keselamatan bisa muncul dikarenakan beberapa hal berikut ini:

- ***False Negative Hazard Detection***

Sensor gagal untuk mendeteksi kondisi berbahaya sehingga tindakan preventif terlambat atau tidak dilakukan. Penelitian oleh (Phong, Tuyen, & Osinski, 2024) menunjukkan bahwa sensor IoT dapat membantu namun faktor kesalahan tetap ada.

- ***Automation-Induced Hazard / Faulty Actuation***

  Apabila sistem otomasi atau aktuasi remote bekerja secara otomatis namun tanpa mempertimbangkan kondisi lapangan dengan baik maka dapat memunculkan hazard baru. Literatur IoT mining menyebutkan bahwa automasi tanpa pendekatan *human-centric* bisa menjadi risiko (GlobalData, 2025).

- ***Dashboard Error / Alarm Fatigue***

  Sistem monitoring dengan banyak alarm bisa mengakibatkan fatigue operator atau misinterpretasi yang menurunkan efektivitas keselamatan.

Risiko Human & Organisasi

Penelitian yang dilakukan oleh (You, Lou, Mao, Xu, & et al, 2023) menyebutkan bahwa industri 5.0 menenkankan jika otomatisasi harus tetap menempatkan manusia sebagai pusat (*human-centric*) agar risiko *human error* dapat diminimalkan. Menurut (Tarafdar, Pullins, & Ragu-Nathan, 2019) keberhasilan integrasi IoT sangat dipengaruhi oleh kesiapan SDM dan budaya organisasi. Tantangan pada risiko ini berupa:

- ***Digital Literacy & Operator Readiness***

  Operator dengan literasi digital rendah atau pelatihan yang terbatas akan kesulitan untuk memanfaatkan sistem IoT dan interpretasi hasil monitoring. Laporan industri memaparkan bahwa kekurangan kemampuan yang selaras menjadi hambatan utama adopsi IoT di tambang.

- ***Technostress & Resistance to Change***

  Adopsi teknologi baru menimbulkan stress, resistensi, dan potensi kesalahan pengguna sehingga *human-centric* industry 5.0 menekankan pentingnya aspek manusia dan otomatisasi.

- ***Training Adequacy & Organizational Culture***

Kultur organisasi yang tidak mendukung pelatihan bahkan adanya pelatihan yang tidak memadai akan memperbesar timbulnya risiko operasional.

Risiko Lingkungan & Kalibrasi

Sensor IoT sangat sensitif terhadap lingkungan ekstrem seperti debu, getaran, suhu tinggi, dan kelembaban. Penelitian oleh (Zhang, Yang, & Chen, 2014) menyebutkan bahwa perubahan lingkungan signifikan dapat menyebabkan deviasi pengukuran bahkan kegagalan total sensor.

- ***Sensor Calibration & Environmental Interference***

  Kondisi pada area pertambangan seperti debu, kelembapan, dan suhu ekstrem dapat menurunkan akurasi sensor atau mempercepat degradasi perangkat. Penelitian yang dilakukan oleh (Boopathy & et al, 2024) menyebutkan bahwa kondisi lingkungan menjadi tantangan utama dalam implementasi sistem IoT.

- ***Environmental Impact Risk***

  Implementasi digitalisasi dan otomatisasi pada area pertambangan mungkin akan menyebabkan dampak lingkungan baru karena penggunaan energi yang jauh lebih tinggi dari sebelumnya (GlobalData, 2025).

Risiko Regulasi

Regulasi pertambangan mengharuskan organisasi memenuhi persyaratan audit keselamatan, retensi data, dan standar perlindungan data digital. Ketidakpatuhan dapat menyebabkan sanksi hukum dan gangguan operasional yang signifikan (ICMM, 2020).

- ***Compliance & Data Retention Risk***

  Sistem IoT menghasilkan volume data yang besar dimana regulasi perusahaan pertambangan mensyaratkan untuk melakukan pencatatan, pelaporan, dan audit. Apabila terjadi kegagalan dalam hal tersebut maka akan berdampak pada hukum/operasional.

Tabel 2.4 menyajikan sintesis risiko yang dirumuskan berdasarkan kajian sistematis terhadap penelitian terdahulu dan regulasi terkait, yang menggambarkan kategori serta karakteristik risiko utama dalam implementasi sistem keselamatan pertambangan berbasis *Internet of Things* (IoT).

Tabel 2.4 Sintesis Variabel Risiko Implementasi IoT pada Sistem Keselamatan Pertambangan

No.	Kategori Risiko	Variabel Risiko	Deskripsi	Referensi
1	Risiko Teknis	*Reliability Sensor*	Kegagalan atau degradasi sensor IoT yang menyebabkan data tidak akurat atau tidak tersedia sehingga mengganggu monitoring keselamatan dan operasi tambang.	(ISO 31000, 2018); (Khanna & Kaur, 2019); (Andrade & et al, 2022).
		Connectivity & Network Latency	Gangguan jaringan, latensi tinggi, dan packet loss yang berdampak pada keterlambatan sistem peringatan dini dan monitoring real-time.	(Atzori & Morabito, 2017); (Phong, Tuyen, & Osinski, 2024).
		Power & Energy Availability	Keterbatasan pasokan listrik atau daya baterai perangkat IoT di lingkungan pertambangan ekstrem.	(Khanna & Kaur, 2019); (GlobalData, 2025).
2	Risiko Siber & Privasi	*Weak Authentication / Access Control*	Lemahnya mekanisme autentikasi dan kontrol akses yang membuka peluang akses tidak sah.	(ISO 27005, 2018); (Roman, Zhou, & Lopez, 2013); (Zhang, Wang, & Li, 2023)

No.	Kategori Risiko	Variabel Risiko	Deskripsi	Referensi
		Intrusion / Malware Attack Surface	Meningkatnya permukaan serangan siber akibat bertambahnya jumlah perangkat IoT.	(Andrade & et al, 2022); (Zhang, Wang, & Li, 2023).
		Data Integrity & Privacy Breach	Risiko manipulasi data sensor dan kebocoran data pribadi pekerja.	(Karim, Kabir , Lei, Lefticaru, & Baset, 2025); (ISO 27005, 2018).
3	Risiko Operasional & Keselamatan	*False Negative Hazard Detection*	Kegagalan sistem IoT mendeteksi kondisi berbahaya sehingga tindakan preventif terlambat.	(Al-Masri, Thangavel, & Kaddoum, 2023); (Phong, Tuyen, & Osinski, 2024).
		Automation-Induced Hazard / Faulty Actuation	Kesalahan aktuasi otomatis yang menciptakan hazard baru karena tidak mempertimbangkan kondisi lapangan.	(GlobalData, 2025); (You, Lou, Mao, Xu, & et al, 2023).
		Dashboard Error / Alarm Fatigue	Kelelahan operator akibat banyaknya alarm dan informasi yang menurunkan efektivitas keputusan.	(Al-Masri, Thangavel, & Kaddoum, 2023).

No.	Kategori Risiko	Variabel Risiko	Deskripsi	Referensi
4	Risiko Human & Organisasi	*Digital Literacy & Operator Readiness*	Rendahnya literasi digital dan kesiapan operator dalam menggunakan sistem IoT.	(Tarafdar, Cooper, & Stich, 2019); (You, Lou, Mao, Xu, & et al, 2023).
		Technostress & Resistance to Change	Stres teknologi dan resistensi terhadap adopsi sistem IoT.	(Tarafdar, Cooper, & Stich, 2019); (You, Lou, Mao, Xu, & et al, 2023).
		Training Adequacy & Organizational Culture	Budaya organisasi dan pelatihan yang tidak memadai dalam mendukung implementasi IoT.	(Tarafdar, Cooper, & Stich, 2019); (ICMM, 2020).
5	Risiko Lingkungan & Kalibrasi	*Sensor Calibration & Environmental Interference*	Gangguan lingkungan ekstrem yang menyebabkan deviasi pengukuran atau kegagalan sensor.	(Zhang, Yang, & Chen, 2014); (Boopathy & et al, 2024).
		Environmental Impact Risk	Dampak lingkungan baru akibat peningkatan konsumsi energi sistem digital dan otomasi.	(GlobalData, 2025).
6	Risiko Regulasi	*Compliance & Data Retention Risk*	Ketidakpatuhan terhadap regulasi keselamatan, audit, dan	(ISO 31000, 2018); (ICMM,

No.	Kategori Risiko	Variabel Risiko	Deskripsi	Referensi
			retensi data digital.	2020).

2.5 Posisi Penelitian

Penelitian ini diposisikan pada kajian manajemen risiko implementasi sistem keselamatan pertambangan berbasis *Internet of Things* (IoT) pada lingkungan operasional berisiko tinggi. Berbeda dengan penelitian terdahulu yang umumnya menggunakan pendekatan tunggal seperti *Failure Mode and Effects Analysis* (FMEA) atau *Fault Tree Analysis* (FTA) secara terpisah, penelitian ini mengintegrasikan FMEA dan FTA dalam satu kerangka analisis terpadu. Integrasi tersebut memungkinkan penilaian risiko yang tidak hanya bersifat kuantitatif dan prioritatif, tetapi juga mampu menelusuri akar penyebab risiko secara sistematis.

Selain itu, penelitian ini secara khusus memfokuskan analisis pada tahap implementasi dan operasional awal sistem IoT, yang selama ini relatif kurang mendapat perhatian dibandingkan fase pasca-implementasi. Ruang lingkup risiko yang dikaji bersifat komprehensif, mencakup aspek teknis, siber dan privasi, operasional dan keselamatan, human dan organisasi, lingkungan dan kalibrasi, serta regulasi. Dengan dukungan validasi lapangan melalui keterlibatan praktisi dan pakar keselamatan pertambangan, penelitian ini diharapkan menghasilkan temuan yang lebih menyeluruh, terukur, dan aplikatif bagi pengambilan keputusan keselamatan di PT X.

(Halaman ini sengaja dikosongkan)

BAB 3
METODOLOGI PENELITIAN

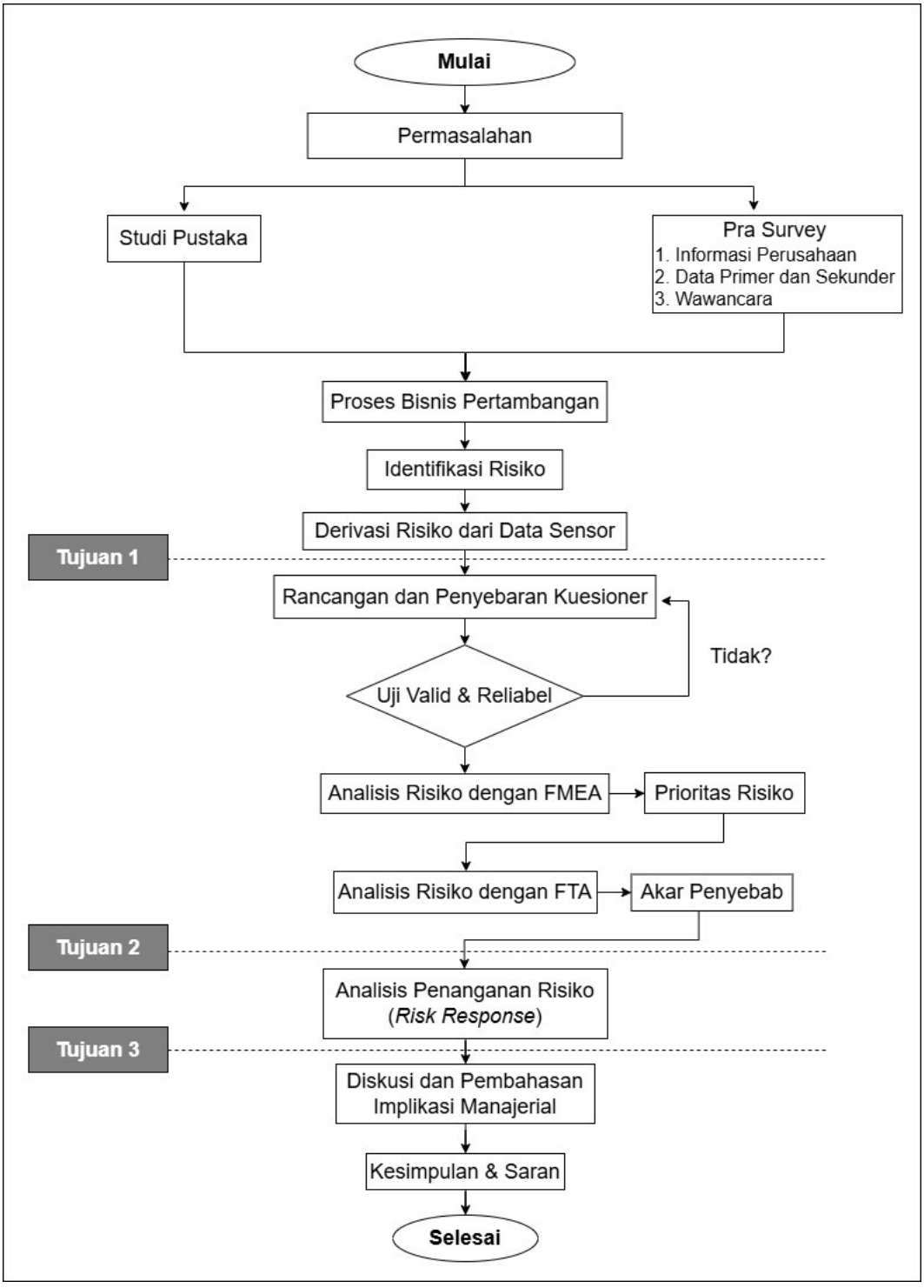
3.1 Jenis Penelitian

Penelitian ini merupakan penelitian terapan (*applied research*) dengan pendekatan kualitatif–kuantitatif (*mixed methods*) yang bertujuan untuk menganalisis dan memitigasi risiko implementasi sistem keselamatan pertambangan berbasis *Internet of Things* (IoT). Pendekatan kualitatif digunakan untuk mengidentifikasi dan memetakan risiko melalui kajian literatur, regulasi keselamatan pertambangan, observasi lapangan, serta diskusi kelompok terarah (FGD) dengan praktisi dan pakar. Sementara itu, pendekatan kuantitatif diterapkan untuk menilai dan memprioritaskan risiko menggunakan metode *Failure Mode and Effects Analysis* (FMEA), serta menelusuri akar penyebab risiko secara sistematis melalui *Fault Tree Analysis* (FTA).

Berdasarkan tingkat analisisnya, penelitian ini bersifat deskriptif–analitis, karena tidak hanya mendeskripsikan karakteristik risiko, tetapi juga menganalisis hubungan sebab-akibat dan tingkat keparahan risiko pada tahap implementasi dan operasional awal sistem IoT. Dengan demikian, hasil penelitian diharapkan mampu memberikan rekomendasi mitigasi risiko yang terukur, komprehensif, dan aplikatif bagi peningkatan keselamatan pertambangan di PT X.

3.2 Tahapan Penelitian

Penelitian ini dilaksanakan melalui serangkaian tahapan yang disusun secara sistematis sebagaimana ditunjukkan pada Gambar 3.1 Bagan Alir Penelitian, untuk memastikan proses analisis risiko berjalan terstruktur, komprehensif, dan dapat dipertanggungjawabkan secara ilmiah. Setiap tahapan dirancang saling terkait, dimulai dari identifikasi risiko hingga perumusan rekomendasi mitigasi, dengan mengintegrasikan pendekatan kualitatif dan kuantitatif sehingga alur penelitian dapat menggambarkan proses analisis risiko implementasi sistem keselamatan pertambangan berbasis Internet of Things (IoT) secara menyeluruh.



Gambar 3.1 Diagram Alir Penelitian

3.2.1 Studi Pustaka

Studi pustaka dalam penelitian ini dilakukan untuk membangun landasan konseptual dan metodologis terkait manajemen risiko pertambangan serta implementasi sistem keselamatan berbasis *Internet of Things* (IoT). Kajian literatur mencakup standar dan regulasi yang relevan, seperti ISO 31000 dan ISO/IEC 27005, serta publikasi ilmiah yang membahas risiko teknis, siber, operasional, human, lingkungan, dan regulasi dalam penerapan IoT di industri berisiko tinggi. Hasil studi pustaka digunakan untuk menyusun sintesis variabel risiko, menentukan kategori dan definisi operasional risiko, serta memilih metode analisis yang tepat, khususnya *Failure Mode and Effects Analysis* (FMEA) dan *Fault Tree Analysis* (FTA), sebagai dasar dalam perancangan kerangka analisis risiko pada tahap implementasi dan operasional awal sistem keselamatan pertambangan berbasis IoT.

3.2.2 Pra Survey

Pra-survei dilakukan untuk memperoleh gambaran umum mengenai kondisi perusahaan atau proyek yang menjadi objek penelitian, serta karakteristik pelaksanaan kegiatan. Tahap ini juga bertujuan mengidentifikasi dan mengumpulkan data sekunder terkait aspek-aspek risiko yang telah terdokumentasi sebelumnya, seperti laporan proyek, catatan insiden, maupun dokumen manajemen risiko internal. Selain itu, pra-survei menjadi sarana awal untuk memperoleh data primer melalui diskusi dan wawancara dengan praktisi yang memahami konteks operasional proyek, sehingga peneliti dapat memastikan bahwa variabel penelitian yang disusun benar-benar relevan, akurat, dan dapat mendukung analisis pada tahap berikutnya.

Data Primer

Data ini diperoleh melalui kuesioner yang disebarkan kepada unit/divisi yang relevan di PT X, yaitu divisi *mining innovation and digitalization*, divisi *mining operation*, dan divisi *safety health and environment.* Teknik sampling yang digunakan adalah *purposive sampling* (*non-probability*) untuk memilih responden yang memiliki peran dan kompetensi dalam sistem digitalisasi pertambangan.

Penelitian ini mengunakan Skala FMEA 1-5 untuk menilai parameter FMEA. Selain kuesioner, penelitian ini juga melakukan *Focus Group Discussion* (FGD) dengan *stakeholders* terkait untuk menggali akar penyebab risiko, persepsi terhadap implementasi IoT, serta strategi mitigasi risiko yang akan diimplementasikan.

Data Sekunder

Data ini didapatkan melalui dokumen internal perusahaan berupa IBPR (Identifikasi Bahaya dan Penilaian Risiko) untuk mengetahui potensi bahaya ataupun potensi risiko pada kegiatan operasional perusahaan pertambangan. Data historis operasional perusahaan selama satu tahun terakhir atau lebih (apabila tersedia) yang meliputi catatan insiden kecelakaan pertambangan, downtime peralatan, maupun pelaporan sistem pengawasan digital atau manual. Selain itu, peneliti juga mendapatkan data pendukung dari berbagai literatur dan jurnal ilmiah yang relevan dengan konsep penelitian ini untuk mendukung kerangka teoritik dan metodologis penelitian.

3.2.3 Variabel Risiko

Variabel risiko bertujuan untuk mengetahui dan memahami secara sistematis seluruh potensi kejadian yang dapat mengganggu keberhasilan dari tujuan penelitian yang mengacu pada hasil sintesis variabel pada bab sebelumnya. Seluruh variabel risiko yang telah di identifikasi kemudian diterjemahkan menjadi definisi operasional, indikator, dan *failure mode* sesuai dengan pendekatan FMEA. Variabel tersebut selanjutnya digunakan sebagai dasar penyusunan instrumen penilaian risiko yang terdiri dari tiga parameter pengukuran yaitu *severity, occurance,* dan *detection* serta memetakan hubungan sebab-akibat dalam metode FTA. Dengan demikian seluruh konsep dari kajian teori dapat diukur secara kuantitatif dalam bentuk kuesioner terstruktur yang akan diklasifikasikan pada tabel berikut ini.

Tabel 3.1 Variabel Risiko Penelitian

Kategori Risiko	Kode	Variabel Risiko	Definisi Operasional	Kode	Failure Mode
Teknik & Sistem	X_1	*Reliability sensor*	Tingkat kemampuan sensor menghasilkan data yang akurat, stabil, dan dapat dipercaya secara konsisten selama periode operasi, tanpa terjadi drift, noise berlebih, atau hilangnya fungsi sensor. Sumber: (IEC, 2010); (ISO, 2003)	$X_{1.1}$	Sensor gagal membaca parameter keselamatan secara akurat
				$X_{1.2}$	Sensor mengalami downtime atau putus koneksi berulang
				$X_{1.3}$	Sensor menghasilkan data fluktuatif tanpa korelasi
				$X_{1.4}$	Sensor mengalami drift performa seiring waktu
	X_2	*Network latency & packet loss*	Keandalan jaringan IoT dalam mengirimkan data secara tepat waktu tanpa delay signifikan maupun kehilangan paket data. Sumber: (NIST, 2020)	$X_{2.1}$	Data keselamatan terlambat dikirim (*high latency*)
				$X_{2.2}$	Paket data hilang selama transmisi
				$X_{2.3}$	Sistem monitoring berhenti menampilkan data *real-time*
	X_3	*Power & energy availability*	Ketersediaan eneergi/sumber daya (listrik atau baterai) yang memadai	$X_{3.1}$	Perangkat IoT mati mendadak karena suplai daya terputus

Kategori Risiko	Kode	Variabel Risiko	Definisi Operasional	Kode	Failure Mode
			untuk perangkat IoT agar dapat terus beroperasi di lingkungan pertambangan.	$X_{3.2}$	Baterai cadangan tidak mampu menopang perangkat saat pemadaman
				$X_{3.3}$	Sistem IoT gagal reboot setelah gangguan listrik
			Sumber: (Hossain, Ahmad, Habibi, & Waqas, 2024)		
Siber & Privasi	X_4	*Weak authentication /access control*	Tingkat kelemahan mekanisme autentikasi, kontrol akses perangkat, dan user.	$X_{4.1}$	Pengguna tidak sah dapat mengakses dashboard karena autentikasi lemah
			Sumber: (ISO, 2008)	$X_{4.2}$	Kredensial tidak terenkripsi sehingga mudah dicuri
				$X_{4.3}$	Pengaturan hak akses tidak sesuai (*over-privilege*)
	X_5	*Intrusion / malware attack*	Insiden dimana perangkat atau jaringan IoT menjadi target serangan (intrusi, malware) yang mempengaruhi fungsi operasional atau keselamatan.	$X_{5.1}$	Sistem mengalami intrusi yang memodifikasi konfigurasi atau log
				$X_{5.2}$	Ra Malware menghambat pengiriman data sensor *real-time*

Kategori Risiko	Kode	Variabel Risiko	Definisi Operasional	Kode	Failure Mode
			Sumber: (ENISA, 2019)	$X_{5.3}$	Serangan siber mengakibatkan shutdown pada sistem monitoring
	X_6	*Data integrity & privacy breach*	Manipulasi atau bocornya data sensor/pengguna yang mempengaruhi pengambilan keputusan operasional.	$X_{6.1}$	Data keselamatan termodifikasi atau korup selama transmisi
				$X_{6.2}$	Data sensitif bocor karena pelanggaran privasi
			Sumber: (ISO, 2013)	$X_{6.3}$	Sistem gagal menjaga konsistensi data antara perangkat dan server
Operasional dan Keselamatan	X_7	*False negative hazard detection*	Sistem IoT gagal mendeteksi kondisi bahaya sehingga tindakan pencegahan tidak dilakukan.	$X_{7.1}$	Sistem tidak mendeteksi gas berbahaya meskipun konsentrasi meningkat
			Sumber: (Reason, J. , 2016); (IEC, 2010)	$X_{7.2}$	Algoritma mendeteksi area aman padahal ada potensi longsor/kecelakaan
				$X_{7.3}$	Sensor bahaya tidak mengeluarkan alarm meskipun kondisi tidak normal

Kategori Risiko	Kode	Variabel Risiko	Definisi Operasional	Kode	Failure Mode
	X_8	*Faulty actuation/automation-induced hazard*	Risiko yang muncul akibat mekanisme aktuasi atau otomasi sistem IoT yang melakukan tindakam otomatis tanpa oversight manusia yang memadai dan mungkin tidak sesuai dengan kondisi lapangan. Sumber: (IEC, 2010)	$X_{8.1}$	Aktuator gagal mengaktifkan fungsi keselamatan saat dibutuhkan
				$X_{8.2}$	Aktuator memberikan respons berlebihan atau salah parameter
				$X_{8.3}$	Aktuator terlambat bekerja hingga kondisi menjadi kritis
	X_9	*Interface / Dashboard Error & Alarm Fatigue*	Antarmuka monitoring yang kurang user friendly atau jumlah alarm yang berlebihan (*alarm fatigue*) sehingga operator salah menginterpretasi atau menunda respons. Sumber: (Cvach, 2012)	$X_{9.1}$	Dashboard menampilkan data tidak sinkron dengan kondisi lapangan
				$X_{9.2}$	Alarm terlalu sering sehingga operator mengabaikan peringatan penting (*alarm fatigue*)
				$X_{9.3}$	Antarmuka tidak menampilkan pesan error jelas saat gangguan
				$X_{9.4}$	Informasi visual tidak terbaca jelas di lingkungan tambang

Kategori Risiko	Kode	Variabel Risiko	Definisi Operasional	Kode	Failure Mode
Human & Organisasi	X_{10}	*Digital Literacy & Operator Readiness*	Kemampuan operator atau teknisi untuk memahami, menggunakan, dan menanggapi sistem IoT. Sumber: (Bosch, de Menezes, & Pees, 2022)	$X_{10.1}$	Operator tidak memahami fungsi/logika sistem digital
				$X_{10.2}$	Operator salah menafsirkan indikator risiko pada dashboard
				$X_{10.3}$	Operator lambat merespons karena belum mahir mengoperasikan perangkat digital
	X_{11}	*Technostress & Resistance to Change*	Tekanan psikologis atau resistensi pekerja terhadap penggunaan teknologi baru IoT, termasuk kekhawatiran kehilangan kontrol, adaptasi sistem baru, atau sikap negative terhadap perubahan. Sumber: (Tarafdar, Cooper, & Stich, 2019)	$X_{11.1}$	Operator menolak penggunaan sistem digital (*resistance*)
				$X_{11.2}$	Stres akibat teknologi menurunkan konsentrasi dan kepatuhan
				$X_{11.3}$	Operator merasa terbebani oleh frekuensi penggunaan perangkat digital
	X_{12}	*Training Adequacy & Organisational*	Pelatihan dan budaya keselamatan digital organisasi yang memadai.	$X_{12.1}$	Pelatihan tidak mencakup skenario kegagalan sistem kritis

Kategori Risiko	Kode	Variabel Risiko	Definisi Operasional	Kode	Failure Mode
		Culture	Sumber: (Reason, J. , 2016); (ISO 45001, 2018)	$X_{12.2}$	Operator tidak mendapatkan pelatihan berkelanjutan
				$X_{12.3}$	Budaya organisasi kurang mendukung penggunaan teknologi digital
				$X_{12.4}$	SOP digitalisasi tidak tersosialisasi atau tidak konsisten diterapkan
Lingkungan & Kalibrasi	X_{13}	*Sensor Calibration Error / Environmental Interference*	Penurunan akurasi atau kerusakan sensor akibat kondisi lingkungan tambang (debu, kelembaban, suhu ekstrem, getaran) atau kurangnya kalibrasi tepat waktu. Sumber: (Hosain, Ahmad, Habibi, & Wagas, 2024)	$X_{13.1}$	Kalibrasi sensor tidak tepat sehingga output bias
				$X_{13.2}$	Debu, kelembapan, getaran, atau suhu ekstrem mengganggu sensor
				$X_{13.3}$	Sensor mengalami offset karena akumulasi interferensi
	X_{14}	*Environmental Impact Risk of IoT*	Dampak lingkungan dari implementasi IoT yang mempengaruhi keberlanjutan	$X_{14.1}$	Perangkat IoT menghasilkan limbah elektronik tidak terkelola

Kategori Risiko	Kode	Variabel Risiko	Definisi Operasional	Kode	Failure Mode
		Deployment	operasional dan kepatuhan regulasi. Sumber: (Wu & et al, 2023)	$X_{14.2}$	Instalasi perangkat mengganggu flora/fauna sekitar tambang
				$X_{14.3}$	Frekuensi radio perangkat berpotensi mengganggu ekosistem lokal
Regulasi	X_{15}	*Compliance & Data Retention Risk*	Kegagalan dalam memenuhi persyaratan regulasi tambang terkait pelaporan, pencatatan data IoT, audit, atau retensi data pekerja. Sumber: (Leveson, 2016)	$X_{15.1}$	Sistem tidak memenuhi standar keselamatan pertambangan yang berlaku
				$X_{15.2}$	Data tidak disimpan sesuai periode retensi regulasi
				$X_{15.3}$	Penyimpanan dan pemrosesan data tidak sesuai pedoman privasi
				$X_{15.4}$	Audit kepatuhan gagal karena dokumentasi digital tidak lengkap/valid

3.2.4 Rancangan dan Penyebaran Kuesioner

Pengumpulan data dalam penelitian ini dilakukan menggunakan instrumen kuesioner berbasis *Failure Mode and Effects Analysis* (FMEA) dengan skala penilaian 1–5 pada tiga parameter utama, yaitu *Severity* (S), *Occurrence* (O), dan *Detection* (D). Rancangan kuesioner disusun berdasarkan hasil studi pustaka dan sintesis variabel risiko implementasi sistem keselamatan pertambangan berbasis *Internet of Things* (IoT), sehingga setiap butir pertanyaan merepresentasikan risiko yang relevan pada tahap implementasi dan operasional awal sistem. Penggunaan FMEA menuntut penilaian yang bersifat *expert judgment*, sehingga validitas hasil sangat bergantung pada kompetensi dan pengalaman responden.

Populasi penelitian ini mencakup praktisi yang terlibat langsung dalam pengelolaan keselamatan, operasional pertambangan, serta pengembangan dan pemanfaatan sistem digital berbasis IoT di PT X. Teknik pengambilan sampel yang digunakan adalah *purposive sampling*, yaitu pemilihan responden secara sengaja berdasarkan kriteria keahlian, pengalaman kerja, dan keterlibatan dalam implementasi digitalisasi keselamatan pertambangan. Berdasarkan kriteria tersebut, diperoleh 20 responden yang memenuhi kualifikasi sebagai *Subject Matter Experts* (SME) dan dinilai memadai untuk memberikan penilaian risiko yang valid dan representatif dalam analisis FMEA.

Tabel 3.2 Responden Penelitian

Aspek Karakteristik	Kategori	Jumlah (n)	Persentase	Relevansi terhadap Penilaian Risiko
Divisi / Departemen	*Mining Innovation & Digitalization*	6	30%	Aspek teknis IoT, integrasi sistem, monitoring dan troubleshooting digital
	Mining Operation	5	25%	Perspektif operasional lapangan dan penggunaan

Aspek Karakteristik	Kategori	Jumlah (n)	Persentase	Relevansi terhadap Penilaian Risiko
				sistem IoT
	Safety, Health, & Environment	9	45%	Aspek keselamatan, manajemen risiko, dan kepatuhan K3
Jabatan / Level	Direksi / Eksekutif Senior	1	5%	Perspektif strategis dan kebijakan keselamatan
	Manajerial Tinggi	4	20%	Pengawasan risiko dan pengambilan keputusan manajerial
	Manajer Menengah / Supervisi	6	30%	Pengendalian lapangan dan implikasi keselamatan
	Staf Operasional / Spesialis	4	20%	Penilaian risiko berbasis kondisi teknis aktual
	Tim Pendukung & Administrasi	5	25%	Integrasi sistem, data, dan keandalan operasional

3.2.5 Uji Validitas dan Reliabilitas

Uji Validitas menggunakan *Correlation Product Moment*

Uji validitas dalam penelitian ini bertujuan untuk memastikan bahwa setiap butir pertanyaan pada kuesioner mampu mengukur konstruk penelitian secara akurat dan relevan. Instrumen yang valid merepresentasikan konsep yang diteliti secara

tepat dan tidak menyimpang dari konstruk yang diukur (Arikunto, 2013). Metode uji validitas yang digunakan adalah *Correlation Product Moment* (Pearson), dengan cara mengorelasikan skor setiap item dengan total skor variabel.

Metode *Correlation Product Moment* dipilih karena sesuai untuk kuesioner dengan skala interval dan efektif digunakan pada penelitian dengan jumlah responden kecil hingga sedang. Selain itu, metode ini memberikan informasi mengenai kontribusi masing-masing item terhadap konstruk yang diukur sehingga dapat digunakan sebagai dasar untuk mempertahankan, melakukan revisi, atau mengeliminasi item pertanyaan (Sugiyono, 2017).

Pengambilan keputusan validitas dilakukan dengan membandingkan nilai r_hitung dengan r_tabel pada tingkat signifikansi $\alpha = 0{,}05$ dan derajat kebebasan $df = n - 2$. Suatu item dinyatakan valid apabila r_hitung > r_tabel, sedangkan item dengan r_hitung ≤ r_tabel dinyatakan tidak valid dan dipertimbangkan untuk direvisi atau dihapus dari instrumen penelitian. Untuk memperkuat interpretasi, tingkat kekuatan hubungan antar variabel juga dianalisis berdasarkan kriteria koefisien korelasi Pearson sebagaimana dikemukakan oleh (Sugiyono, 2022).

Tabel 3.3 Interpretasi Nilai Uji Validitas menggunakan Pearson

Nilai *r*	Keterangan
0,00 – 0,199	Sangat lemah
0,20 – 0,399	Lemah
0,40 – 0,599	Cukup
0,60 – 0,799	Kuat
0,80 – 1,000	Sangat kuat

Uji Reliabilitas menggunakan *Cronbach's Alpha*

Uji reliabilitas dilakukan untuk menilai tingkat konsistensi dan keandalan instrumen penelitian dalam mengukur konstruk secara stabil. Instrumen yang reliabel akan menghasilkan data yang konsisten apabila digunakan berulang kali pada kondisi yang relatif sama (Arikunto, 2013). Dalam penelitian ini, uji reliabilitas dilakukan menggunakan koefisien *Cronbach's Alpha*, yang umum

digunakan untuk mengukur konsistensi internal instrumen kuesioner berbasis skala interval.

Metode *Cronbach's Alpha* dipilih karena sesuai untuk kuesioner dengan banyak item yang mengukur satu konstruk atau beberapa konstruk yang saling terkait, serta efektif digunakan pada jumlah sampel kecil hingga sedang. Nilai *Cronbach's Alpha* mencerminkan sejauh mana item-item dalam satu variabel memiliki keterkaitan dan mengukur konsep yang sama (Sugiyono, 2017). Pengambilan keputusan reliabilitas dilakukan dengan membandingkan nilai *Cronbach's Alpha* (α) terhadap nilai batas minimal yang direkomendasikan. Suatu variabel dinyatakan reliabel apabila memiliki nilai *Cronbach's Alpha* ≥ 0,70, sedangkan nilai 0,60 ≤ α < 0,70 masih dapat diterima untuk penelitian eksploratif. Variabel dengan nilai α < 0,60 dinyatakan tidak reliabel dan memerlukan perbaikan atau penghapusan item pertanyaan (Sugiyono, 2022).

Tabel 3.4 Interpretasi Nilai Uji Reliabilitas dengan *Cronbach's Alpha*

Nilai Alpha (α)	Interpretasi Reliabilitas
≥ 0,90	Sangat tinggi
0,80 – 0,89	Tinggi
0,70 – 0,79	Cukup
0,60 – 0,69	Kurang
0,50 – 0,59	Rendah
< 0,50	Tidak reliable

3.2.6 Analisis Risiko

Untuk menilai, memetakan, dan memprioritaskan risiko implementasi IoT di area pertambangan, penelitian ini menggunakan kombinasi dua metode utama, yaitu FMEA untuk penilaian risiko dan FTA untuk identifikasi sumber risiko. Pendekatan dengan metode ganda ini selaras dengan rekomendasi (ISO 31010, 2019) yang menyatakan bahwa penggunaan lebih dari satu teknik analisis risiko akan memberikan gambaran risiko yang lebih komprehensif dan meningkatkan akurasi pengambilan keputusan.

Penilaian Risiko menggunakan FMEA

Metode FMEA merupakan pendekatan sistematis yang digunakan untuk mengidentifikasi mode kegagalan, penyebab, serta konsekuensi yang dapat timbul sehingga strategi mitigasi risiko dapat dirancang secara proaktif sebelum kegagalan terjadi (Stamatis, 2003). Di sektor pertambangan, metode ini dinilai relevan dikarenakan aktivitas operasional perusahaan memiliki potensi risiko tinggi seperti kecelakaan alat berat, insiden peledakan, paparan gas berbahaya, hingga kegagalan sensor IoT pada sistem keselamatan. Sehingga metode FMEA diterapkan pada penelitian ini karena mampu untuk memberikan penilaian objektif terhadap risiko yang memungkinkan manajemen untuk melakukan prioritas tindakan mitigasi secara terukur.

Penilaian FMEA secara kuantitatif mengacu pada standar internasional (IEC, 2018) yang mendefinisikan tiga parameter utamayaitu *Severity* (S)*, Occurance* (O)*,* dan *Detection* (D) yang masing-masing parameter diberi skor 1-5 sehingga didapatkan perhitungan *Risk Priority Number* (RPN). Skor untuk parameter FMEA ditentukan melalui *Focus Group Discussion* (FGD) dengan stakeholder internal perusahaan maupun data sekunder perusahaan, kemudian dilakukan penilaian menggunakan Skala FMEA 1 hingga 5 yang diolah secara statistik sehingga menghasilkan perhitungan RPN untuk mengkategorikan setiap risiko. Nilai RPN digunakan untuk menentukan prioritas mitigasi, dimana RPN $\geq$ 30 dikategorikan sebagai risiko signifikan yang harus segera ditangani (Hadipuro, Yulianto, & Rachman, 2023).

Identifikasi Sumber Risiko menggunakan FTA

Metode FTA merupakan metode deduktif yang berawal dari *top event* (kegagalan puncak) dan menurunkan penyebabnya menjadi *basic event* melalui logika gate (OR, AND). Pendekatan ini sesuai dengan teori *Fault Tree Classic* seperti yang dijelaskan di *Fault Tree Handbook* (Vesely, 1981). Dalam penelitian ini, proses FTA meliputi:

a. Menentukan *top event* berdasarkan hasil FMEA sebelumnya dan frekuensi kejadian tertinggi berdasarkan data kecelakaan tahunan milik perusahaan.

b. Menyusun pohon kesalahan (*fault tree*) dengan logic gate (OR, AND) dan *hierarki basic event*.
c. Identifikasi *basic event*s yang bisa didapatkan dari data perusahaan tahun sebelumnya.
d. Menilai probabilitas *basic event*s menggunakan 2 pendekatan. Pendekatan pertama yaitu data historis perusahaan apabila catatan data tersebut tersedia di perusahaan. Namun apabila data tidak tersedia, peneliti bisa menggunakan pendekatan kedua dengan skala interval.
e. Menghitung probabilitas *top event* untuk menunjukkan risiko kumulatif dan prioritas mitigasi.

3.2.7 Respon Risiko

Respon risiko merupakan tahapan akhir dalam proses manajemen risiko setelah kegiatan identifikasi dan analisis risiko selesai, yang bertujuan untuk menurunkan probabilitas terjadinya risiko maupun mengurangi dampak yang ditimbulkan. Pada tahap ini, setiap risiko yang telah dianalisis dirumuskan strategi mitigasinya melalui dua pendekatan utama, yaitu *Focus Group Discussion* (FGD) dengan para pemangku kepentingan serta penyusunan tabulasi rencana mitigasi dan *residual risk*. Respon risiko yang dihasilkan selanjutnya diklasifikasikan ke dalam empat kategori utama, yaitu *risk avoidance, risk reduction, risk transfer, dan risk acceptance,* sesuai dengan karakteristik dan tingkat risiko yang dihadapi. Pengelompokan respon risiko ini bertujuan untuk memastikan bahwa setiap risiko ditangani secara sistematis, proporsional, serta selaras dengan kapasitas pengendalian dan toleransi risiko organisasi, sehingga strategi mitigasi yang diterapkan dapat berjalan efektif, efisien, dan berkelanjutan.

Focus Group Discussion (FGD) dalam Manajemen Risiko

FGD merupakan metode diskusi yang terstruktur dengan melibatkan sekelompok individu dengan latar belakang dan keahlian yang berbeda untuk membahas mengenai isu tertentu secara lebih detail dan mendalam yang ditujukan pada PIC (*Person in Charge*) yang terlibat langsung pada proses bisnis penerapan IoT yang disajikan pada tabel berikut ini.

Tabel 3.5 Stakeholder PT X dalam FGD Mitigasi Risiko

No	Divisi	Jumlah
1	Mining Innovation & Digitalization	3
2	Mining Operation & Technical Services	2
3	Healt & Safety	2

Dengan dilakukannya FGD bersama PIC PT X, diharapkan menghasilkan *Output* berupa rencana mitigasi risiko keselamatan pertambangan yang datanya mengacu pada hasil analisis FMEA dan FTA yang menghasilkan nilai RPN. Selanjutnya disusun rencana mitigasi yang akan diterapkan lengkap dengan PIC dan waktu implementasi. Teknik FGD dipilih sebagai metode partisipatif yang sangat direkomendasikan dalam standar manajemen risiko seperti (ISO 31010, 2019) tentang *risk assessment techniques* karena meningkatkan keterlibatan stakeholder dan validitas keputusan mitigasi.

Tabulasi Rencana Mitigasi dan *Residual Risk*

Setelah melakukan identifikasi dan evaluasi risiko, langkah selanjutnya yaitu menyusun rencana mitigasi risiko yang sistematis dan efektif. Proses mitigasi risiko melibatkan beberapa hal yang dijelaskan sebagai berikut.

- **Penetapan tindakan mitigasi**

  Menentukan langkah konkret yang diambil untuk mengurangi atau menghilangkan risiko yang mungkin terjadi secara preventif.
- **Penunjukan tanggung jawab**

  Menetapkan individu ataupun tim yang bertanggung jawab atas pelaksanaan setiap tindakan mitigasi.
- **Penentuan waktu pelaksanaan**

  Menetapkan jadwal atau *timeline* untuk implementasi setiap tindakan mitigasi.
- **Penilaian residual risk**

  Setelah proses mitigasi, nilai risiko akan dihitung ulang untuk mengetahui nilai RPN akan turun secara signifikan atau sebaliknya. *Residual risk* juga bertujuan untuk menentukan mitigasi risiko dapat diterima atau memerlukan tindakan tambahan. Menurut (Kurniawan & Hasan, 2022) penurunan nilai RPN > 70% menunjukkan bahwa tindakan mitigasi yang dirancang melalui

FGD diperkirakan efektif secara signifikan. Evaluasi re*sidual risk* dilakukan secara berkala, misalnya dalam kurun waktu minimal 3 bulan untuk memastikan mitigasi tetap efektif dan menyesuaikan rencana jika diperlukan.

3.2.8 Diskusi, Pembahasan dan Implikasi manajerial

Subbab ini menjelaskan kerangka analisis dan fokus pembahasan yang akan dilakukan setelah seluruh tahapan pengolahan data selesai. Diskusi akan difokuskan pada interpretasi hasil analisis risiko yang diperoleh dari integrasi *Failure Mode and Effects Analysis* (FMEA) dan *Fault Tree Analysis* (FTA), khususnya dalam mengkaji pola risiko, keterkaitan antar failure mode, serta karakteristik risiko sistemik pada implementasi sistem keselamatan pertambangan berbasis digital. Pada tahap ini, hasil perhitungan RPN dan struktur pohon kesalahan akan dianalisis untuk mengidentifikasi risiko prioritas dan jalur kegagalan kritis yang berpotensi mengganggu fungsi keselamatan.

Selanjutnya, pembahasan akan mengaitkan temuan analisis tersebut dengan teori, standar, dan hasil penelitian terdahulu yang relevan, guna menilai kesesuaian, perbedaan, serta kontribusi penelitian terhadap pengembangan manajemen risiko pertambangan berbasis digital. Pembahasan juga akan mencakup evaluasi efektivitas respon risiko yang dirumuskan melalui *Focus Group Discussion* (FGD), termasuk analisis penurunan tingkat risiko berdasarkan perhitungan residual risk, sebagai indikator keberhasilan strategi mitigasi yang diusulkan.

Sementara itu, implikasi manajerial akan membahas bagaimana hasil analisis dan pembahasan dapat diterjemahkan ke dalam pengambilan keputusan praktis di tingkat manajemen. Implikasi ini akan difokuskan pada pemanfaatan prioritas risiko sebagai dasar perencanaan mitigasi, penguatan sistem keselamatan pertambangan, optimalisasi alokasi sumber daya, peningkatan monitoring dan pengendalian risiko, serta dukungan terhadap kepatuhan regulasi keselamatan pertambangan. Dengan demikian, subbab ini berfungsi sebagai penghubung antara hasil analisis teknis dan penerapannya dalam konteks operasional dan manajerial PT X.

(Halaman ini sengaja dikosongkan)

BAB 4
ANALISIS DATA & PEMBAHASAN

4.1 Gambaran Umum Obyek Penelitian

Penelitian ini dilakukan pada proyek digitalisasi sistem keselamatan pertambangan berbasis IoT di PT X, sebuah perusahaan pertambangan batubara berskala besar dengan luas area operasional sekitar 33.887 hektar dan jalur hauling utama sepanjang ±35 km yang menghubungkan pit aktif, area disposal, fasilitas pengolahan, hingga pelabuhan pengiriman. Proses penambangan yang berlangsung secara terus-menerus, melibatkan aktivitas penggalian, pemuatan, dan pengangkutan material dengan intensitas tinggi, dikombinasikan dengan kondisi geoteknik yang dinamis, cuaca ekstrem, serta interaksi simultan antara alat berat, kendaraan hauling, dan pekerja, menjadikan keselamatan kerja sebagai aspek yang sangat kritis dalam seluruh rantai operasi pertambangan.

Kompleksitas operasi tersebut, ditambah dengan keterlibatan berbagai kontraktor dan penyebaran area kerja yang luas, menyebabkan keterbatasan sistem keselamatan konvensional yang masih bergantung pada inspeksi manual dan pemantauan periodic yang berpotensi menimbulkan keterlambatan dalam mendeteksi bahaya seperti paparan gas berbahaya, potensi longsor lereng, tabrakan alat berat, maupun kondisi tidak aman pada jalur hauling. Untuk mengatasi tantangan tersebut, PT X mengimplementasikan digitalisasi sistem keselamatan berbasis IoT dengan memanfaatkan sensor gas, sensor geoteknik, sensor kondisi alat, serta sistem pemantauan kendaraan, yang terintegrasi melalui jaringan komunikasi nirkabel dan pusat kendali keselamatan.

Kondisi operasional pertambangan di PT X menunjukkan bahwa setiap tahapan proses penambangan memiliki karakteristik aktivitas dan potensi bahaya yang berbeda, sehingga memerlukan pendekatan keselamatan yang spesifik dan terintegrasi. Keterkaitan antara proses penambangan, aktivitas utama, potensi bahaya, serta kebutuhan sensor dan teknologi IoT dirangkum secara sistematis pada Tabel 4.1 berikut.

Tabel 4.1 Proses Penambangan, Bahaya, Implementasi Sensor/IoT, dan Derivasi Risiko dari Data Sensor

No	Proses Penambangan	Aktivitas Utama	Potensi Bahaya	Jenis Sensor / Teknologi IoT	Data yang Dihasilkan Sensor	Derivasi Risiko dari Data Sensor
1	Pembukaan & Penggalian Pit	Excavation, drilling, blasting	Longsor lereng, runtuhan batu, paparan gas	Inclinometer, piezometer, sensor gas	Pergerakan lereng, tekanan air pori, konsentrasi gas	• Data tidak terbaca/bias à *false negative hazard detection* • Keterlambatan transmisi data à *late warning hazard*
2	Pemuatan Material	Loading dengan excavator/shovel	Tertimpa material, tabrakan alat berat	Proximity sensor, LiDAR, camera-based AI	Memonitor jarak aman antara alat berat dan pekerja, *blind spot detection*	• Kegagalan deteksi objek à*collision risk* • Kesalahan AI à *unsafe operation*
3	Pengangkutan (Hauling)	Hauling pada jalur utama ±35 km	Tabrakan kendaraan,	GPS, accelerometer,	Memantau kecepatan, perilaku	• Data GPS tidak akurat à *loss of*

No	Proses Penambangan	Aktivitas Utama	Potensi Bahaya	Jenis Sensor / Teknologi IoT	Data yang Dihasilkan Sensor	Derivasi Risiko dari Data Sensor
			kelelahan operator	*fatigue monitoring camera*	operator, kondisi kendaraan, rute	*situational awareness* • Fatigue tidak terdeteksi à *human factor risk*
4	Disposal & Dumping Area	Pembuangan material overbuden	Runtuhan dump, ketidakstabilan tanah	Tilt sensor, soil pressure sensor	Sudut kemiringan, tekanan tanah	• Sensor drift à *instability undetected* • Alarm tidak aktif à *dump collapse risk*
5	Pemantauan Lingkungan Tambang	Operasi 24 jam	Paparan debu, gas, cuaca ekstrem	Dust sensor, weather station IoT	Kualitas udara, hujan, angin	• Data lingkungan bias à *environmental exposure risk* • Integrasi data gagal à *decision error*
6	Operasi Alat	Operasi dozer,	Mechanical failure,	Sensor kondisi	Getaran, suhu	• Kegagalan deteksi

No	Proses Penambangan	Aktivitas Utama	Potensi Bahaya	Jenis Sensor / Teknologi IoT	Data yang Dihasilkan Sensor	Derivasi Risiko dari Data Sensor
	Berat	excavator, dump truck	blind spot	mesin, vibration sensor	mesin, performa	dini à *equipment breakdown* • Data tidak tervalidasi à *unsafe operation*
7	Akuisisi Data Sensor	Pengumpulan data lapangan	Data hilang, data tidak lengkap	IoT node, embedded sensor	Raw sensor data	• Data tidak terkumpul à *moniroting gap*
8	Transmisi Data & Jaringan	Pengiriman data ke server	Latency, packet loss, jaringan terputus	Gateway IoT, jaringan nirkabel	Status koneksi, latency	• Keterlambatan data à delayed alarm • Packet loss à data integrity risk
9	Analitik & Pemrosesan Data	Hazard detection & analytics	Salah interpretasi bahaya	Edge computing, AI analytics	Hazard classification, risk score	• Algoritma salah à *false alarm/false negative*
10	Sistem Peringatan &	Warning & actuation	Bahaya tidak diinformasikan	Alarm system, wearable alert	Visual/audio warning	• Alarm gagal aktif à *failure to warn*

No	Proses Penambangan	Aktivitas Utama	Potensi Bahaya	Jenis Sensor / Teknologi IoT	Data yang Dihasilkan Sensor	Derivasi Risiko dari Data Sensor
	Alarm					*critical hazard*
11	Control Room & Monitoring	Pemantauan keselamatan terpusat	Keterlambatan respon, salah interpretasi	Dashboard IoT, alarm system DSS	Visualisasi risiko real-time	• Human error à decision making risk
12	Tanggap Darurat	Evakuasi dan shutdown	Respon terlambat, komunikasi gagal, evakuasi terlambat	Alarm otomatis, aktuator, komunikasi nirkabel	Tindakan proteksi, perintah evakuasi	• Komunikasi gagal à *emergency response failure*
13	Pemeliharaan & Kalibrasi	*Maintenance* sensor dan sistem	Sensor drift, data bias	Sistem kalibrasi digital, health monitoring IoT	Status sensor, drift data	• Sensor tidak terkalibrasi à *systemic detection failure*
14	Manajemen Data & Kepatuhan	Pelaporan dan audit K3	Data tidak valid, gagal audit	Cloud platform, data logging, cybersecurity tools	Log data, audit trail	• Data hilang/bocor à *compliance & cyber risk*

4.2 Analisis Deskriptif Responden

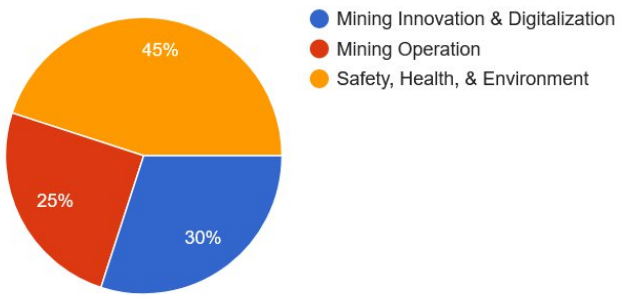
Pengumpulan data menggunakan instrumen kuesioner berbasis skala FMEA 1-5 pada tiga parameter utama yaitu *Severity* (S), *Occurance* (O), dan *Detection* (D). Penilaian risiko menggunakan metode FMEA menuntut pemahaman teknis yang kuat dan pengalaman operasional yang relevan sehingga diperlukan validasi bahwa responden memiliki kompetensi dan kredibilitas sebagai *Subject Matter Experts* (SME) sebelum hasil penilaian digunakan pada analisis berikutnya. Analisis deskriptif responden bertujuan untuk menilai kelayakan, kompetensi, dan relevansi pengalaman para responden dalam memberikan penilaian risiko pada konteks digitalisasi keselamatan pertambangan berbasis IoT di PT X.

Penelitian ini menggunakan metode *purposive sampling*, yaitu teknik pemilihan responden secara sengaja berdasarkan kriteria tertentu, terutama terkait tingkat keahlian dan keterlibatan dalam implementasi sistem digitalisasi keselamatan berbasis IoT dan pengalaman kerja di area operasional pertambangan. Berdasarkan kriteria tersebut, diperoleh 20 responden yang memenuhi kualifikasi untuk memberikan penilaian risiko penelitian ini sehingga dapat merepresentasikan kondisi aktual implementasi IoT pada sistem keselamatan pertambangan di PT X.

Profil Responden

Profil responden mencakup beberapa karakteristik utama yang mencerminkan kompetensi, pengalaman, dan relevansi responden dalam implementasi digitalisasi keselamatan pertambangan yang diklasifikasikan sebagai berikut:

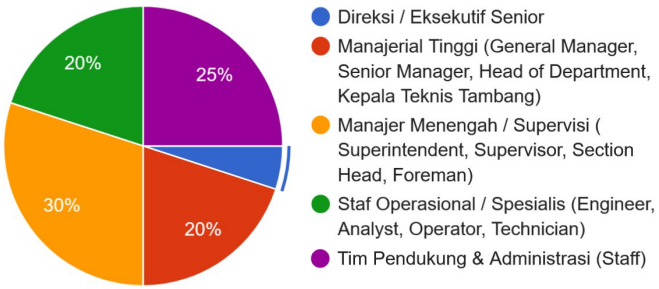
- **Divisi / Departemen**



Gambar 4.1 Profil Responden berdasarkan Divisi/Departemen Kerja

Berdasarkan diagram pada gambar di atas, responden berasal dari beberapa unit kerja di PT X diantaranya yaitu 30% responden berasal dari Divisi *Mining Innovation & Digitalization* yang memiliki kompetensi teknis terkait instalasi, konfigurasi, *troubleshooting*, dan *monitoring* sistem IoT; 25% responden dari Divisi *Mining Operation* yang memahami alur kerja lapangan, kondisi peralatan, dan bagaimana sensor IoT digunakan pada aktivitas operasional; serta 45% responden berasal dari Divisi *Safety, Health, & Environment* yang berperan dalam validasi dampak keselamatan, manajemen risiko, serta kepatuhan terhadap standar K3.

- **Jabatan / Level**



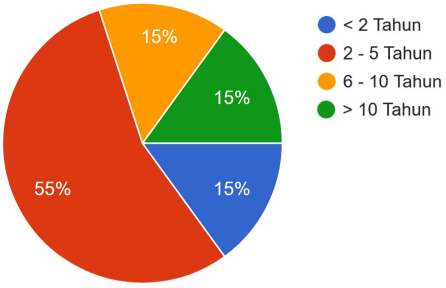
Gambar 4.2 Profil Responden berdasarkan Jabatan

Analisis jabatan responden mencakup 5 tingkatan manajerial dengan persentase tertinggi sebesar 30% pada posisi manajer menengah/supervisi, dimana responden dengan jabatan ini dapat melihat risiko dari perspektif prosedural, pengawasan, dan implikasi keselamatan pertambangan di PT X. Responden dengan persentase sebesar 25% yaitu tim pendukung & administrasi (staff) yang memberikan penilaian berdasarkan aspek teknik, integrasi sistem, dan keandalan sensor. Selain itu posisi jabatan pada staff operasional dan manajerial tinggi, masing-masing memiliki persentase sebesar 20%. Responden pada posisi direksi/eksekutif senior memiliki persentase terendah yaitu 5% dari total keseluruhan responden.

Variasi dari jabatan tersebut menjamin representasi dari level pengambil keputusan strategis hingga pelaksana operasional di lapangan. Responden pada level manajerial memberikan perspektif pengawasan risiko secara makro, sementara staff operasional memberikan penilaian risiko berdasarkan kondisi

aktual di lapangan. Kombinasi dari jabatan ini dinilai dapat meningkatkan reliabilitas penilaian FMEA dari tiga parameter utama yaitu S, O, dan D karena mencakup persepsi risiko dari berbagai tingkatan organisasi.

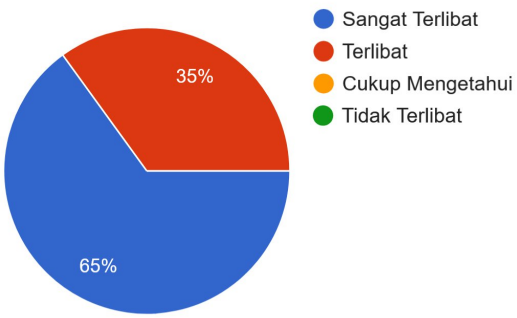
- **Lama Pengalaman Kerja**



Gambar 4.3 Profil Responden berdasarkan Lama Pengalaman Kerja

Pengalaman kerja responden menjadi indikator penting dalam menilai tingkat kedalaman pemahaman terhadap proses digitalisasi operasional pertambangan. Berdasarkan grafik di atas, mayoritas responden memiliki pengalaman kerja lebih dari 2 tahun dengan persentase sebesar 55% dan lebih dari 30% telah bekerja minimal 6 tahun. Durasi pengalaman kerja berpengaruh langsung terhadap pemahaman terhadap operasi tambang, sensitivitas terhadap potensi kegagalan sistem, serta kemampuan menilai efektivitas deteksi berbasis teknologi IoT. Semakin lama pengalaman kerja, semakin tinggi dan konsisten penilaian terhadap risiko operasional yang kompleks sehingga dapat memperkuat asumsi bahwa responden memiliki validitas kompetensi untuk memberikan penilaian FMEA.

- **Tingkat pemahaman atau keterlibatan terhadap digitalisasi keselamatan**



Gambar 4.4 Profil Responden berdasarkan Tingkat Pemahaman/Keterlibatan terhadap Digitalisasi Keselamatan

Berdasarkan grafik di atas, 65% responden terlibat secara intens dalam pengoperasian, pengembangan, ataupun evaluasi sistem digitalisasi keselamatan pertambangan secara *real-time* pada PT X. Selain itu, 35% lainnya memiliki keterlibatan yang cukup signifikan terutama dalam penggunaan data IoT dalam pengambilan keputusan operasional dan keselamatan pertambangan. Tingkat keterlibatan responden terhadap digitalisasi berpengaruh pada kemampuan responden dalam menilai parameter FMEA dengan akurat sehingga penilaian risiko akan mencerminkan pengalaman empiris dan bukan asumsi subjektif.

Karakteristik Responden

Tabel 4.2 Karakteristik Responden

	Kategori	**Jumlah (n)**	**Persentase**
Divisi/Departemen	*Mining Innovation & Digitalization*	6	30%
	Mining Operation	5	25%
	Safety, Health, & Environment	9	45%
Jabatan/Level	Direksi / Eksekutif Senior	1	5%
	Manajerial Tinggi (General Manager, Senior Manager , Head of Departement, Kepala Teknis Tambang)	4	20%
	Manajer Menengah / Supervisi (Superintendent, Seupervisor, Section Head, Foreman)	6	30%
	Staf Operasional / Spesialis (Engineer, Analyst, Operator, Technician)	4	20%
	Tim Pendukung & Administrasi (Staff)	5	25%
Pengalaman Kerja	< 2 Tahun	3	15%

	Kategori	Jumlah (n)	Persentase
	2 – 5 Tahun	11	55%
	6 – 10 Tahun	3	15%
	> 10 Tahun	3	15%
Tingkat Keterlibatan Digitalisasi	Sangat Terlibat	13	65%
	Terlibat	7	35%
	Cukup Terlibat	0	0
	Tidak Terlibat	0	0

Berdasarkan tabel di atas, terlihat bahwa responden pada penelitian ini memiliki latar belakang yang relevan dengan penilaian risiko digitalisasi sistem keselamatan pertambangan. Selain itu, sebagian besar responden memiliki pengalaman kerja lebih dari 2 tahun yang mengindikasikan bahwa responden pada penelitian ini telah memiliki kompetensi dan pemahaman yang matang terhadap proses operasional serta potensi risiko digitalisasi sistem keselamatan pertambangan. Selain itu, tingkat pemahaman responden terhadap digitalisasi juga tergolong baik, dimana semua responden memiliki tingkat persentase keterlibatan yang tinggi dalam implementasi digitalisasi keselamatan pertambangan. Dengan demikian, karakteristik pada tabel di atas mendukung kelayakan responden sebagai *Subject Matter Experts* (SME) untuk memberikan penilaian FMEA yang valid dan dapat dipercaya.

4.3 Identifikasi (Derivasi) Risiko Sistem Digitalisasi Keselamatan Pertambangan

Risiko-risiko yang diidentifikasi pada penelitian ini diturunkan (derivasi) secara langsung dari karakteristik proses penambangan terbuka (*open-pit mining*) dan alur operasional keselamatan yang berlangsung di PT X. Proses penambangan melibatkan aktivitas berisiko tinggi seperti penggalian di pit aktif, pengangkutan material melalui jalur hauling jarak jauh, pengoperasian alat berat secara simultan, serta keberadaan pekerja di area dengan kondisi geoteknik dan lingkungan yang dinamis. Dalam konteks ini, sistem keselamatan berbasis IoT berfungsi sebagai

critical safety layer yang bertugas melakukan deteksi bahaya, pemrosesan data, pemberian peringatan, dan aktivasi tindakan pengendalian secara *real-time*. Oleh karena itu, setiap tahapan dalam rantai fungsi keselamatan digital, mulai dari akuisisi data sensor, transmisi jaringan, pemrosesan dan penyajian informasi, hingga respons manusia dan actuator secara inheren berpotensi menimbulkan kegagalan yang berdampak langsung terhadap keselamatan operasional.

Kategori risiko *Reliability Sensor* (X_1) dan *Sensor Calibration Error / Environmental Interference* (X_{13}) diturunkan dari kondisi fisik lingkungan tambang yang ekstrem, seperti debu, getaran, suhu tinggi, dan kelembapan, yang dapat menurunkan akurasi sensor gas, getaran, dan geoteknik. Kegagalan pada tahap ini berimplikasi langsung pada *false negative hazard detection*, di mana kondisi berbahaya tidak terdeteksi meskipun telah melampaui ambang batas keselamatan. Selanjutnya, risiko *Network Latency & Packet Loss* (X_2) serta *Power & Energy Availability* (X_3) berkaitan dengan karakteristik area tambang yang luas dan terpencil, yang sangat bergantung pada jaringan komunikasi nirkabel dan suplai daya tidak stabil. Gangguan pada lapisan ini dapat menciptakan *blind spot monitoring* dan keterlambatan respons darurat, khususnya pada jalur hauling dan area pit yang jauh dari pusat kontrol.

Risiko pada lapisan keamanan siber dan integritas data meliputi *Weak Authentication & Access Control* (X_4), *Intrusion/Malware Attack* (X_5), serta *Data Integrity & Privacy Breach* (X_6) diturunkan dari integrasi sistem keselamatan IoT dengan infrastruktur jaringan perusahaan dan sistem kontrol terpusat. Dalam operasi pertambangan modern, gangguan siber tidak hanya berdampak pada aspek data, tetapi dapat secara langsung memanipulasi parameter keselamatan, menonaktifkan alarm, atau menyebabkan shutdown sistem monitoring, sehingga meningkatkan potensi kegagalan sistemik pada fungsi keselamatan.

Pada tahap hilir dari sistem digital, risiko *False Negative Hazard Detection* (X_7) dan *Faulty Actuation Hazard* (X_8) merepresentasikan kegagalan fungsi keselamatan inti, di mana sistem gagal mendeteksi bahaya atau gagal mengeksekusi tindakan proteksi yang diperlukan. Risiko ini sangat kritis dalam konteks pertambangan karena dapat menyebabkan keterlambatan evakuasi,

kegagalan shutdown alat berat, atau eskalasi kejadian berbahaya. Selanjutnya, risiko *Interface/Dashboard Error & Alarm Fatigue* (X_9) diturunkan dari kondisi operasional ruang kendali (*control room*) yang menuntut pengambilan keputusan cepat berdasarkan visualisasi data, sehingga desain antarmuka dan manajemen alarm menjadi faktor penentu efektivitas respons keselamatan.

Aspek manusia dan organisasi direpresentasikan melalui risiko *Digital Literacy & Operator Readiness* (X_{10}), *Technostress & Resistance to Change* (X_{11}), serta *Training Adequacy & Organisational Culture* (X_{12}), yang diturunkan dari realitas bahwa sistem keselamatan digital tetap bergantung pada interpretasi dan tindakan operator. Keterbatasan kompetensi digital, resistensi terhadap teknologi baru, serta pelatihan yang tidak memadai dapat menyebabkan kesalahan interpretasi, keterlambatan respons, atau pengabaian peringatan keselamatan, meskipun sistem teknologi telah berfungsi secara teknis.

Terakhir, risiko *Environmental Impact Risk of IoT Deployment* (X_{14}) dan *Compliance & Data Retention Risk* (X_{15}) diturunkan dari kewajiban perusahaan pertambangan untuk memastikan bahwa implementasi teknologi digital tidak menimbulkan dampak lingkungan baru dan tetap memenuhi regulasi keselamatan, lingkungan, serta perlindungan data. Kegagalan pada aspek ini dapat berdampak pada sanksi hukum, penghentian operasi, dan kerugian reputasi perusahaan. Dengan demikian, keseluruhan failure modes yang diidentifikasi dalam penelitian ini merupakan representasi sistematis dari interaksi antara proses penambangan, teknologi digital, dan faktor manusia, yang secara bersama-sama membentuk profil risiko sistemik pada implementasi sistem keselamatan pertambangan berbasis IoT. Detail rincian risiko dan potensi kegagalan (*Failure Mode*) dapat dilihat pada Tabel 4.3 berikut.

Identifikasi Kegagalan (*Failure Modes*)

Tabel 4.3 *Failure Modes*

Variabel	Kode	*Failure Mode*	Penyebab (*Cause*)	Dampak (*Effect*)
X_1 **Reliability Sensor**	$X_{1.1}$	Sensor gagal membaca parameter keselamatan secara akurat.	Sensitivitas sensor rendah, desain sensor tidak sesuai lingkungan tambang, deteksi terganggu oleh kondisi fisik ekstrem, kerusakan komponen internal.	Parameter keselamatan tidak terdeteksi à potensi *false negative* risiko kecelakaan meningkat.
	$X_{1.2}$	Sensor mengalami *downtime* atau putus koneksi berulang.	Konektor lepas, gangguan komunikasi RF, modul transmisi rusak, prosedur instalasi buruk.	Hilangnya data *real-time* à *blind spot monitoring* à keterlambatan respon darurat.
	$X_{1.3}$	Sensor menghasilkan data fluktuatif tanpa korelasi.	Fluktuasi daya *grounding* buruk, noise lingkungan tinggi, degradasi sensor.	Signal noise à sistem membaca kondisi palsu à *false alarms* / pengabaian alarm / keputusan salah.
	$X_{1.4}$	Sensor mengalami drift performa seiring waktu.	Penuaan komponen, tidak ada kalibrasi berkala, degradasi performa material.	Output bias bertahap à ambang batas alarm tidak valid à *missed detection.*

Variabel	Kode	*Failure Mode*	Penyebab (*Cause*)	Dampak (*Effect*)
X_2 Network Latency & Packet Loss	$X_{2.1}$	Data keselamatan terlambat dikirim (*high latency*).	Bandwidth terbatas, jaringan padat, interferensi komunikasi.	Delay informasi à keputusan terlambat à respons mitigasi tertunda.
	$X_{2.2}$	Paket data hilang selama transmisi.	*Noise/packet collision*, sinyal lemah, *buffer overflow,* protokol tidak *reliable.*	Data tidak lengkap àinterpretasi risiko salah àpotensi *false negative*.
	$X_{2.3}$	Sistem monitoring berhenti menampilkan data *real-time*.	*Server overload, gateway crash, buffer saturation.*	Operator kehilangan visibilitas à peningkatan risiko operasional yang fatal.
X_3 Power & Energy Availability	$X_{3.1}$	Perangkat IoT mati mendadak karena suplai daya terputus.	*Power cut*, kabel putus, modul *power supply* rusak.	Hilangnya monitoring lokal à *blind spot* keselamatan.
	$X_{3.2}$	Baterai cadangan tidak mampu menopang perangkat saat pemadaman.	Kapasitas baterai menurun; tidak ada *maintenance*; suhu ekstrem menurunkan performa.	Perangkat tidak aktif saat *power outage* à potensi kecelakaan tak terdeteksi.
	$X_{3.3}$	Sistem IoT gagal reboot setelah gangguan listrik.	*Firmware crash,* restart otomatis tidak stabil.	Perangkat tetap offline sampai intervensi manual à downtime

Variabel	Kode	*Failure Mode*	Penyebab (*Cause*)	Dampak (*Effect*)
				berkepanjangan.
X_4 Weak Authentication /Access Control	$X_{4.1}$	Pengguna tidak sah dapat mengakses dashboard karena autentikasi lemah.	Default password, password lemah, *brute-force attack.*	Data dimanipulasi*, anauthorized actions, data exposure, misconfiguration.*
	$X_{4.2}$	Kredensial tidak terenkripsi sehingga mudah dicuri.	*Plaintext storage, insecure transport protocols.*	*Credential theft* à *account takeover* à *manipulation of system.*
	$X_{4.3}$	Pengaturan hak akses tidak sesuai (*over-privilege*).	Kesalahan konfigurasi, *lack of least privilege policy.*	Penghapusan atau perubahan data.
X_5 Intrusion/ Malware Attack	$X_{5.1}$	Sistem mengalami intrusi yang memodifikasi konfigurasi atau log.	*Unpatched vulnerabilities,* segmentasi jaringan lemah, layanan sistem terekspos ke jaringan publik.	Integritas konfigurasi sistem hilang à parameter keselamatan dimanipulasi à *false readings / hidden attacks.*
	$X_{5.2}$	Malware menghambat pengiriman data sensor *real-time.*	Infeksi malware yang memblokir kanal komunikasi, botnet, DoS bot (serangan DoS pada jaringan IoT).	Gangguan atau keterlambatan pengiriman *critical safety data* à kegagalan aktivasi tindakan mitigasi secara tepat waktu.

Variabel	Kode	*Failure Mode*	Penyebab (*Cause*)	Dampak (*Effect*)
	$X_{5.3}$	Serangan siber mengakibatkan *shutdown* pada sistem monitoring.	Serangan ransomware pada server kontrol, serangan terarah terhadap ICS/SCADA, *credential compromise.*	Sistem monitoring tidak berfungsi sepenuhnya à area tambang tanpa pemantauan risiko à potensi bahaya tidak terdeteksi.
X_6 Data Integrity & Privacy Breach	$X_{6.1}$	Data keselamatan termodifikasi atau korup selama transmisi.	Serangan MITM (*Man in the Middle*), tidak adanya mekanisme verifikasi data (CRC/checksum), kerusakan penyimpanan.	Data keselamatan tidak valid dan menyesatkan à keputusan operasional salah dan beresiko
	$X_{6.2}$	Data sensitif bocor karena pelanggaran privasi.	Kontrol akses lemah, pencurian atau ekstraksi data, penyimpanan cadangan tidak terenkripsi.	*Legal exposure, loss of trust, regulatory penalties*.
	$X_{6.3}$	Sistem gagal menjaga konsistensi data antara perangkat dan server.	Kesalahan sinkronisasi waktu, ketidakandalan protokol komunikasi, unreliable messaging.	*Inconsistent state* à kesalahan penilaian situasi keamanan pertambangan.
X_7 False Negative Hazard Detection	$X_{7.1}$	Sistem tidak mendeteksi gas berbahaya meskipun konsentrasi meningkat.	Kegagalan fungsi sensor gas (*sensor failure*), kesalahan penetapan nilai ambang batas alarm (*threshold*),	Paparan gas beracun atau ledakan tidak terdeteksi à potensi fatal bagi pekerja.

Variabel	Kode	*Failure Mode*	Penyebab (*Cause*)	Dampak (*Effect*)
			area tanpa cakupan sensor (*blind spots*).	
	$X_{7.2}$	Algoritma mendeteksi area aman padahal ada potensi longsor/kecelakaan.	Training data tidak memadai, algoritma overfitting, jumlah sensor lapangan tidak mencukupi.	*Slope failure undetected* à pekerja terjebak atau peralatan rusak.
	$X_{7.3}$	Sensor bahaya tidak mengeluarkan alarm meskipun kondisi tidak normal.	*Alarm routing failure*, gangguan komunikasi antar modul alarm, *software* bug.	Evakuasi tidak dilakukan à peringatan tidak muncul à *near-miss or fatal incident.*
X_8 Faulty Actuation Hazard	$X_{8.1}$	Aktuator gagal mengaktifkan fungsi keselamatan saat dibutuhkan.	Keausan mekanis, gangguan pada kabel kontrol, kehilangan perintah aktivasi.	Sistem proteksi tidak bekerja saat kondisi darurat à eskalasi bahaya.
	$X_{8.2}$	Aktuator memberikan respons berlebihan atau salah parameter.	*Control logic error*, kesalahan input sensor.	Respon mekanik berbahaya yang menyebabkan kerusakan asset dan potensi cedera operator.
	$X_{8.3}$	Aktuator terlambat bekerja hingga kondisi menjadi	*Network latency*, antrean proses kontrol.	Mitigasi bahaya terlambat dilakukan à kecelakaan

Variabel	Kode	*Failure Mode*	Penyebab (*Cause*)	Dampak (*Effect*)
		kritis.		membesar.
X_9 Interface / Dashboard Error & Alarm Fatigue	$X_{9.1}$	Dashboard menampilkan data tidak sinkron dengan kondisi lapangan.	*Latency*, ketidaksesuaian interval pembaruan data, data *coaching* lama.	Operator menerima informasi tidak akurat à kesalahan pengambilan keputusan.
	$X_{9.2}$	Alarm terlalu sering sehingga operator mengabaikan peringatan penting (alarm fatigue).	Frekuensi alarm berlebihan akibat false alarm, sensitivitas sensor terlalu tinggi, konfigurasi alarm tidak optimal.	Alarm kritis diabaikan kegagalan respons terhadap kondisi berbahaya.
	$X_{9.3}$	Antarmuka tidak menampilkan pesan error jelas saat gangguan.	Perancangan UI tidak mengikuti standar, kurangnya kode diagnostik.	Operator tidak dapat mendiagnosis masalah dengan cepat à waktu respons meningkat.
	$X_{9.4}$	Informasi visual tidak terbaca jelas di lingkungan tambang.	Kontras rendah, ukuran huruf kecil, refleksi cahaya.	Pesan keselamatan terlambat dipahami à risiko eskalasi kondisi kritis.
X_{10} Digital Literacy &	$X_{10.1}$	Operator tidak memahami fungsi/logika sistem digital.	Pelatihan tidak memadai, antarmuka sistem sulit dipahami, complex UI,	Kesalahan penggunakan sistem digital meningkatkan probabilitas

Variabel	Kode	*Failure Mode*	Penyebab (*Cause*)	Dampak (*Effect*)
Operator Readiness			tidak adanya SOP operasional berbasis sistem digital.	human error dalam keputusan keselamatan.
	$X_{10.2}$	Operator salah menafsirkan indikator risiko pada dashboard.	Indikator dan symbol risiko tidak jelas, kurangnya guideline, kurangnya pemahaman terhadap parameter kritis keselamatan.	Interpretasi salah à tindakan mitigasi tidak sesuai kebutuhan.
	$X_{10.3}$	Operator lambat merespons karena belum mahir mengoperasikan perangkat digital.	Minim pengalaman operasional, kurangnya simulasi darurat, hands-on training terbatas.	Tanggap darurat lambat à mitigasi bahaya terlambat à potensi kecelakaan meningkat.
X_{11} Technostress & Resistance to Change	$X_{11.1}$	Operator menolak penggunaan sistem digital (*resistance*).	Resistensi budaya organisasi, ketakutan akan kehilangan pekerjaan akibat otomasi.	Sistem keselamatan tidak dioperasikan sesuai desain à aktivitas manual beresiko dipertahankan.
	$X_{11.2}$	Stres akibat teknologi menurunkan konsentrasi dan kepatuhan.	Beban kognitif tinggi, antarmuka tidak ramah pengguna, notifikasi berlebihan.	Penurunan fokus kerja à meningkatnya kesalahan procedural dan potensi insiden.

Variabel	Kode	*Failure Mode*	Penyebab (*Cause*)	Dampak (*Effect*)
	$X_{11.3}$	Operator merasa terbebani oleh frekuensi penggunaan perangkat digital.	Frekuensi alarm tinggi, *workflow* digital tidak efisien.	Kepatuhan operasional menurun à operator berpotensi mem-bypas prosedur keselamatan.
X_{12} Training Adequacy & Organisational Culture	$X_{12.1}$	Pelatihan tidak mencakup skenario kegagalan sistem kritis.	Struktur kurikulum pelatihan tidak lengkap, keterbatasan anggaran dan waktu.	Operator tidak siap menghadapi kondisi abnormal à penanganan darurat tidak efektif.
	$X_{12.2}$	Operator tidak mendapatkan pelatihan berkelanjutan.	Tidak ada program berkelanjutan, keterbatasan shift operasional.	Penurunan kompetensi seiring waktu à pengambilan keputusan kurang akurat.
	$X_{12.3}$	Budaya organisasi kurang mendukung penggunaan teknologi digital.	Manajemen tidak memberikan contoh implementasi teknologi, kurangnya penghargaan internal.	Adopsi sistem digital rendah à manfaat sistem keselamatan tidak optimal.
	$X_{12.4}$	SOP digitalisasi tidak tersosialisasi atau tidak konsisten diterapkan.	Komunikasi internal buruk, dokumen SOP tidak diperbarui.	Ketidakkonsistenan operasi à kegagalan audit keselamatan dan risiko hukum.
X_{13} Sensor Calibration	$X_{13.1}$	Kalibrasi sensor tidak tepat sehingga *output* bias.	Kesalahan kalibrasi manual, tidak adanya sistem kalibrasi otomatis,	Data pengukuran tidak akurat à alarn aktif atau pasif tidak sesuai

Variabel	Kode	*Failure Mode*	Penyebab (*Cause*)	Dampak (*Effect*)
Error / Environmental Interference			referensi standar tidak digunakan.	kondisi nyata.
	$X_{13.2}$	Debu, kelembapan, getaran, atau suhu ekstrem mengganggu sensor.	Paparan lingkungan tambang yang agresif, pelindung sensor tidak memadai.	*Intermittent failures* à keandalan sensor menurun drastis.
	$X_{13.3}$	Sensor mengalami offset karena akumulasi interferensi.	Kontaminasi material, efek magnetisasi, pelapisan kotoran.	Kesalahan pengukuran progresif à deviasi tidak terdeteksi à risiko false negative meningkat.
X_{14} Environmental Impact Risk of IoT Deployment	$X_{14.1}$	Perangkat IoT menghasilkan limbah elektronik tidak terkelola.	Tidak adanya kebijakan *e-waste management*, siklus perangkat tidak direncanakan.	Kontaminasi lingkungan tambang à sanksi regulasi lingkungan.
	$X_{14.2}$	Instalasi perangkat mengganggu flora/fauna sekitar tambang.	Penilaian lokasi instalasi tidak tepat, pemasangan dilakukan tanpa analisis dampak.	Konflik sosial dan penolakan izin operasional.
	$X_{14.3}$	Frekuensi radio perangkat berpotensi mengganggu ekosistem lokal.	Kepadatan emisi RF terlalu tinggi, frekuensi tidak sesuai zona regulasi.	Gangguan ekologis dan pengaduan masyarakat lokal.
X_{15}	$X_{15.1}$	Sistem tidak memenuhi	Tidak mengikuti standar K3, SMKP,	Penangguhan izin operasi dan

Variabel	Kode	*Failure Mode*	Penyebab (*Cause*)	Dampak (*Effect*)
Compliance & Data Retention Risk		standar keselamatan pertambangan yang berlaku.	ISO/IEC, sertifikasi tidak dilakukan.	implikasi hukum.
	$X_{15.2}$	Data tidak disimpan sesuai periode retensi regulasi.	Kebijakan penyimpanan tidak memadai, kesalahan konfigurasi retensi otomatis.	Kegagalan audit keselamatan dan risiko litigasi.
	$X_{15.3}$	Penyimpanan dan pemrosesan data tidak sesuai pedoman privasi.	Tidak mengikuti UU PDP/GDPR, enkripsi data tidak diterapkan.	Tuntutan hukum dan kerugian reputasi perusahaan.
	$X_{15.4}$	Audit kepatuhan gagal karena dokumentasi digital tidak lengkap/valid.	Tidak ada arsip terstruktur, logging tidak memadai.	Ketidaksesuaian laporan audit à tindakan regulatori.

4.4 Uji Validitas dan Reliabilitas Instrumen FMEA

Uji validitas dan reliabilitas menggunakan instrumen FMEA berupa daftar indikator risiko yang mencakup berbagai *failure mode* atau potensi kegagalan implementasi proyek digitalisasi sistem keselamatan pertambangan. Uji validitas digunakan untuk memastikan bahwa setiap butir pertanyaan dapat mengukur apa yang seharusnya diukur serta uji reliabilitas digunakan untuk memastikan bahwa item pertanyaan mampu memberikan hasil yang konsisten.

Uji Validitas

Uji validitas dilakukan untuk menguji kemampuan suatu instrumen dalam mengukur suatu variabel penelitian. Uji validitas pada bagian ini dilakukan menggunakan korelasi *product moment* (r) dengan signifikasi 5%. Apabila nilai signifikan < 0,05 atau nilai $r_{hitung} > r_{table}$ maka data tersebut dinyatakan valid. Nilai r_{table} didapatkan dari tabel r dengan df = N-2, dimana N adalah jumlah sampel penelitian sebanyak 20 orang. Maka diperoleh nilai df = 18 dengan nilai r_{table} = 0,444.

Tabel 4.4 Hasil Uji Validitas

Kode	Indikator	r hitung	Sig	Keterangan
$X_{1.1}$	Sensor gagal membaca parameter keselamatan secara akurat.	-0,181	0,445	Tidak Valid
$X_{1.2}$	Sensor mengalami *downtime* atau putus koneksi berulang.	-0,260	0,268	Tidak Valid
$X_{1.3}$	Sensor menghasilkan data fluktuatif tanpa korelasi.	0,658	0,002	Valid
$X_{1.4}$	Sensor mengalami *drift* performa seiring waktu.	0,676	0,001	Valid
$X_{2.1}$	Data keselamatan terlambat dikirim (*high latency*).	0,081	0,735	Tidak Valid
$X_{2.2}$	Paket data hilang selama transmisi.	0,606	0,005	Valid
$X_{2.3}$	Sistem monitoring berhenti	0,664	0,001	Valid

Kode	Indikator	r hitung	Sig	Keterangan
	menampilkan data *real-time*.			
$X_{3.1}$	Perangkat IoT mati mendadak karena suplai daya terputus.	0,248	0,291	Tidak Valid
$X_{3.2}$	Baterai cadangan tidak mampu menopang perangkat saat pemadaman.	0,606	0,005	Valid
$X_{3.3}$	Sistem IoT gagal reboot setelah gangguan listrik.	0,664	0,001	Valid
$X_{4.1}$	Pengguna tidak sah dapat mengakses dashboard karena autentikasi lemah.	0,788	0,000	Valid
$X_{4.2}$	Kredensial tidak terenkripsi sehingga mudah dicuri.	0,812	0,000	Valid
$X_{4.3}$	Pengaturan hak akses tidak sesuai (*over-privilege*).	0,800	0,000	Valid
$X_{5.1}$	Sistem mengalami intrusi yang memodifikasi konfigurasi atau log.	0,715	0,000	Valid
$X_{5.2}$	Malware menghambat pengiriman data sensor *real-time.*	0,796	0,000	Valid
$X_{5.3}$	Serangan siber mengakibatkan *shutdown* pada sistem monitoring.	0,640	0,002	Valid
$X_{6.1}$	Data keselamatan termodifikasi atau korup selama transmisi.	0,807	0,000	Valid
$X_{6.2}$	Data sensitif bocor karena pelanggaran privasi.	0,903	0,000	Valid
$X_{6.3}$	Sistem gagal menjaga konsistensi data antara perangkat dan server.	0,903	0,000	Valid
$X_{7.1}$	Sistem tidak mendeteksi gas berbahaya meskipun konsentrasi meningkat.	0,816	0,000	Valid

Kode	Indikator	r hitung	Sig	Keterangan
$X_{7.2}$	Algoritma mendeteksi area aman padahal ada potensi longsor/kecelakaan.	0,903	0,000	Valid
$X_{7.3}$	Sensor bahaya tidak mengeluarkan alarm meskipun kondisi tidak normal.	0,867	0,000	Valid
$X_{8.1}$	Aktuator gagal mengaktifkan fungsi keselamatan saat dibutuhkan.	0,785	0,000	Valid
$X_{8.2}$	Aktuator memberikan respons berlebihan atau salah parameter.	0,796	0,000	Valid
$X_{8.3}$	Aktuator terlambat bekerja hingga kondisi menjadi kritis.	0,816	0,000	Valid
$X_{9.1}$	Dashboard menampilkan data tidak sinkron dengan kondisi lapangan.	0,177	0,455	Tidak Valid
$X_{9.2}$	Alarm terlalu sering sehingga operator mengabaikan peringatan penting (*alarm fatigue*).	0,794	0,000	Valid
$X_{9.3}$	Antarmuka tidak menampilkan pesan error jelas saat gangguan.	0,405	0,076	Valid
$X_{9.4}$	Informasi visual tidak terbaca jelas di lingkungan tambang.	0,544	0,013	Valid
$X_{10.1}$	Operator tidak memahami fungsi/logika sistem digital.	0,903	0,000	Valid
$X_{10.2}$	Operator salah menafsirkan indikator risiko pada dashboard.	0,807	0,000	Valid
$X_{10.3}$	Operator lambat merespons karena belum mahir mengoperasikan perangkat digital.	0,763	0,000	Valid
$X_{11.1}$	Operator menolak penggunaan	0,198	0,402	Tidak Valid

Kode	Indikator	r hitung	Sig	Keterangan
	sistem digital (*resistance*).			
$X_{11.2}$	Stres akibat teknologi menurunkan konsentrasi dan kepatuhan.	0,715	0,000	Valid
$X_{11.3}$	Operator merasa terbebani oleh frekuensi penggunaan perangkat digital.	0,715	0,000	Valid
$X_{12.1}$	Pelatihan tidak mencakup skenario kegagalan sistem kritis.	0,806	0,000	Valid
$X_{12.2}$	Operator tidak mendapatkan pelatihan berkelanjutan.	0,903	0,000	Valid
$X_{12.3}$	Budaya organisasi kurang mendukung penggunaan teknologi digital.	0,755	0,000	Valid
$X_{12.4}$	SOP digitalisasi tidak tersosialisasi atau tidak konsisten diterapkan.	0,818	0,000	Valid
$X_{13.1}$	Kalibrasi sensor tidak tepat sehingga output bias.	0,762	0,000	Valid
$X_{13.2}$	Debu, kelembapan, getaran, atau suhu ekstrem mengganggu sensor.	-0,181	0,445	Tidak Valid
$X_{13.3}$	Sensor mengalami offset karena akumulasi interferensi.	0,669	0,001	Valid
$X_{14.1}$	Perangkat IoT menghasilkan limbah elektronik tidak terkelola.	0,715	0,000	Valid
$X_{14.2}$	Instalasi perangkat mengganggu flora/fauna sekitar tambang.	0,198	0,402	Tidak Valid
$X_{14.3}$	Frekuensi radio perangkat berpotensi mengganggu ekosistem lokal.	0,257	0,273	Tidak Valid
$X_{15.1}$	Sistem tidak memenuhi standar keselamatan pertambangan yang	0,755	0,000	Valid

Kode	Indikator	r hitung	Sig	Keterangan
	berlaku.			
$X_{15.2}$	Data tidak disimpan sesuai periode retensi regulasi.	0,755	0,000	Valid
$X_{15.3}$	Penyimpanan dan pemrosesan data tidak sesuai pedoman privasi.	0,765	0,000	Valid
$X_{15.4}$	Audit kepatuhan gagal karena dokumentasi digital tidak lengkap/valid.	0,692	0,001	Valid

Hasil uji validitas pada tabel di atas yang diperoleh melalui SPSS dapat disimpulkan bahwa terdapat beberapa *failure mode* yang tidak valid pada penelitian ini yang memiliki nilai $r_{hitung} < r_{tabel}$ (0,444) atau nilai Sig > 0,05 pada taraf signifikan 5%. Maka dapat disimpulkan bahwa *failure mode* tersebut tidak dapat mewakili variabel yang diteliti, sehingga perlu dikeluarkan dari penelitian ini. Sedangkan *failure mode* dengan $r_{hitung} > r_{tabel}$ (0,444) atau nilai Sig < 0,05 pada taraf signifikan 5% dapat dinyatakan telah valid dan dapat digunakan pada penelitian ini. Secara keseluruhan sebanyak 80% *failure mode* memiliki validitas tinggi dengan detail 40 item valid dari total keseluruhan sebanyak 49 item *failure mode* yang diukur pada kuesioner.

Uji Reliabilitas

Uji reliabilitas pada penelitian ini digunakan untuk mengukur sejauh mana hasil pengukuran dengan objek yang sama menghasilkan data yang konsisten dan stabil yang di analisis menggunakan nilai *Cronbach's Alpha.* Data penelitian dinyatakan *reliable* atau handal apabila nilai koefisien *Cronbach's Alpha* > 0,7. Berikut ini merupakan hasil uji reliabilitas yang disajikan pada tabel berikut ini:

Tabel 4.5 Hasil Uji Reliabilitas

Variabel	*Cronbach's Alpha*	N of Items	Keterangan
X_1	0,720	7	Reliabel
X_2	0,732	7	Reliabel
X_3	0,701	7	Reliabel

X_4	0,762	5	Reliabel
X_5	0,729	6	Reliabel
X_6	0,745	8	Reliabel
X_7	0,743	9	Reliabel
X_8	0,729	7	Reliabel
X_9	0,818	9	Reliabel
X_{10}	0,804	9	Reliabel
X_{11}	0,708	7	Reliabel
X_{12}	0,793	9	Reliabel
X_{13}	0,710	8	Reliabel
X_{14}	0,816	8	Reliabel
X_{15}	0,733	9	Reliabel

Hasil uji reliabilitas pada tabel di atas menunjukkan bahwa setiap indikator yang digunakan pada penelitian ini dalam mengukur variabel X_1- X_{15} telah memiliki nilai *Cronbach Alpha* > 0,70 sehingga disimpulkan bahwa semua indikator pada penelitian ini dapat dinyatakan memiliki reliabilitas yang tinggi dan hasilnya dapat dipercaya.

4.5 Analisis FMEA (*Failure Mode and Effect Analysis*)

Analisis FMEA pada penelitian kuantitatif dilakukan dengan menghitung nilai RPN (*Risk Priority Number*) pada setiap *failure mode* untuk menetapkan prioritas risiko berdasarkan tiga parameter yaitu S (*Severity*), O (*Occurance*), dan D (*Detection*) yang diukur pada skala penilaian 1 sampai 5 pada kuesioner. Nilai RPN kemudian digunakan untuk menentukan peringkat prioritas risiko dari item *failure mode* sehingga fokus mitigasi dapat diarahkan pada risiko yang paling kritis.

Perhitungan RPN (*Risk Priority Number*)

Perhitungan nilai RPN didapatkan dari nilai rata-rata parameter S, O, dan D yang hanya melibatkan item *failure mode* yang sudah dinyatakan valid pada uji validitas hasil kuesioner yang telah di isi oleh 20 responden.

Tabel 4.6 Hasil Nilai RPN

Variabel	*Failure Mode*	S	O	D	RPN	Level Risiko
X_1	$X_{1.3}$	3.25	2.80	3.00	27.30	Sedang
	$X_{1.4}$	3.25	2.45	2.85	22.69	Sedang
X_2	$X_{2.2}$	3.30	2.35	3.10	24.04	Sedang
	$X_{2.3}$	3.30	2.45	3.05	24.66	Sedang
X_3	$X_{3.2}$	3.30	2.65	3.05	26.67	Sedang
	$X_{3.3}$	3.30	2.30	3.05	23.15	Sedang
X_4	$X_{4.1}$	3.75	2.00	3.00	22.50	Sedang
	$X_{4.2}$	3.30	2.20	2.95	21.42	Sedang
	$X_{4.3}$	3.30	1.90	3.05	19.12	Rendah
X_5	$X_{5.1}$	4.05	1.95	3.00	23.69	Sedang
	$X_{5.2}$	3.35	2.10	3.00	21.11	Sedang
	$X_{5.3}$	4.35	1.95	3.05	25.87	Sedang
X_6	$X_{6.1}$	3.75	2.15	3.15	25.40	Sedang
	$X_{6.2}$	3.50	2.30	3.05	24.55	Sedang
	$X_{6.3}$	3.10	2.65	3.05	25.06	Sedang
X_7	$X_{7.1}$	4.30	2.10	3.05	27.54	Sedang
	$X_{7.2}$	4.30	2.10	2.95	26.64	Sedang
	$X_{7.3}$	4.25	2.10	2.95	26.33	Sedang
X_8	$X_{8.1}$	3.95	2.20	2.80	24.33	Sedang
	$X_{8.2}$	3.35	2.30	2.95	22.73	Sedang
	$X_{8.3}$	3.30	2.15	2.95	20.93	Sedang
X_9	$X_{9.2}$	3.35	2.75	2.90	26.72	Sedang
	$X_{9.3}$	3.00	2.30	2.95	20.36	Rendah
	$X_{9.4}$	2.95	2.50	3.05	22.49	Sedang
X_{10}	$X_{10.1}$	3.30	2.40	3.00	23.76	Sedang
	$X_{10.2}$	3.30	2.25	3.15	23.39	Sedang
	$X_{10.3}$	3.05	2.50	2.90	22.11	Sedang
X_{11}	$X_{11.2}$	2.90	2.10	2.95	17.97	Rendah

	$X_{11.3}$	2.75	2.10	2.60	15.02	Rendah
$\boldsymbol{X_{12}}$	$X_{12.1}$	3.80	2.10	2.95	23.54	Sedang
	$X_{12.2}$	3.30	2.10	2.90	20.10	Rendah
	$X_{12.3}$	3.30	1.95	3.05	19.63	Rendah
	$X_{12.4}$	3.70	2.10	3.10	24.09	Sedang
$\boldsymbol{X_{13}}$	$X_{13.1}$	4.15	2.10	2.95	25.71	Sedang
	$X_{13.3}$	3.20	2.10	2.95	19.82	Rendah
$\boldsymbol{X_{14}}$	$X_{14.1}$	2.90	1.95	2.95	16.68	Rendah
$\boldsymbol{X_{15}}$	$X_{15.1}$	4.10	1.95	3.05	24.38	Sedang
	$X_{15.2}$	3.30	1.95	3.05	19.63	Sedang
	$X_{15.3}$	3.55	1.95	3.05	21.11	Sedang
	$X_{15.4}$	3.55	1.95	2.95	20.42	Sedang

Dari hasil penilaian kuantitatif perhitungan RPN terhadap seluruh *failure mode* yang valid, diperoleh nilai RPN dengan rentang risiko rendah sebanyak 8 *failure mode* serta 32 *failure mode* memiliki rentang risiko sedang. Hal ini mengindikasikan bahwa mayoritas risiko bersifat *moderate*, namun tetap memerlukan mitigasi karena dalam konteks keselamatan pertambangan akan berimplikasi fatal apabila terjadi *failure cascade.*

Analisis Prioritas Risiko (*Risk Interpretation*)

Berdasarkan hasil perhitungan nilai RPN, didapatkan 10 prioritas tertinggi dari item *failure mode* yang perlu menjadi fokus mitigasi dalam penguatan digitalisasi keselamatan pertambangan pada PT X yang diklasifikasikan pada tabel berikut ini.

Tabel 4.7 Prioritas Risiko berdasarkan Nilai RPN

Fokus Risiko	Kode	Failure Mode	RPN	Persentase (%)	Persentase Kumulatif (%)
Operasional & Keselamatan	$X_{7.1}$	Sistem tidak mendeteksi gas berbahaya meskipun konsentrasi	27.54	10.47%	10.47%

		meningkat.			
Teknik & Sistem	$X_{1.3}$	Sensor menghasilkan data fluktuatif tanpa korelasi.	27.30	10.38%	20.86%
Operasional & Keselamatan	$X_{9.2}$	Alarm terlalu sering sehingga operator mengabaikan peringatan penting (*alarm fatigue*).	26.72	10.16%	31.02%
Teknik & Sistem	$X_{3.2}$	Baterai cadangan tidak mampu menopang perangkat saat pemadaman.	26.67	10.14%	41.16%
Operasional & Keselamatan	$X_{7.2}$	Algoritma mendeteksi area aman padahal ada potensi longsor/kecelakaan.	26.64	10.13%	51.30%
Operasional & Keselamatan	$X_{7.3}$	Sensor bahaya tidak mengeluarkan alarm meskipun kondisi tidak normal.	26.33	10.01%	61.31%
Siber & Privasi	$X_{5.3}$	Serangan siber mengakibatkan *shutdown* pada sistem monitoring.	25.87	9.84%	71.15%
Lingkungan & Kalibrasi	$X_{13.1}$	Kalibrasi sensor tidak tepat sehingga *output* bias.	25.71	9.78%	80.93%
Siber & Privasi	$X_{6.1}$	Data keselamatan termodifikasi atau	25.49	9.69%	90.62%

		korup selama transmisi.			
Teknik & Sistem	$X_{2.3}$	Sistem monitoring berhenti menampilkan data *real-time.*	24.66	9.38%	100%

Berdasarkan tabel di atas, 10 risiko prioritas tertinggi memiliki distribusi dampak yang hampir merata, dengan kontribusi masing-masing berada pada rentang 9.38% - 10.47% dari keseluruhan. Distribusi risiko berbentuk kurva merata (*flat/ uniform distribution*) bukan kurva dominan tunggal, yang mengindikasikan bahwa hal ini bersifat ***systemic risk pattern*** **yang saling berkaitan dan saling bergantung**, bukan berasal dari salah satu item *failure mode* yang paling dominan. Karakter risiko bersifat *cascading,* seperti berikut ini:

faulty data à faulty interpretation à no alarm à no response à fatal incident

Berdasarkan distribusi nilai risiko yang relatif merata, pola risiko yang terbentuk menunjukkan karakteristik systemic risk yang berasal dari beberapa kluster utama, yang selanjutnya diklasifikasikan sebagai berikut.

1. ***Operational Safety Cluster*** **(Risiko Operasional dan Keselamatan)**

Bagian ini memiliki kontribusi 40.77% dari total risiko yang mengindikasikan bahwa fungsi dasar keselamatan pertambangan (*hazard detection*) sedang mengalami tekanan paling berat. Sistem keselamatan pertambangan bergantung pada tiga lapisan yaitu sensor, analitik, dan alarm/actuator. Sehingga apabila salah satu dari ketiga lapisan tersebut gagal maka keseluruhan fungsi penyelamatan gagal di implementasikan.

2. ***System Reliability Cluster*** **(Risiko Teknik dan Sistem)**

Bagian ini memiliki kontribusi 29.90% dari total risiko yang mengindikasikan bahwa ketersediaan sistem (*availability*) merupakan salah satu *root systematic driver* terbesar. Ketidakandalan perangkat keras dan infrastruktur pendukung tidak hanya meningkatkan RPN pada masing-masing *failure mode* tetapi juga menciptakan efek domino pada *operational safety cluster*.

3. *Cyber-Physical Risk Cluster* (Risiko Siber dan Privasi)

Bagian ini memiliki kontribusi sebesar 19.53% yang berperan sebagai *common cause*, yaitu penyebab yang bisa memengaruhi banyak *failure mode* sekaligus. Risiko ini menjadi pemicu (*trigger*) dan *risk amplifier* yang dapat menyebabkan kegagalan simultan pada sensor, deteksi, dan alarm/actuator.

4. *Environmental Drift Cluster* (Risiko Lingkungan dan Kalibrasi)

Bagian ini memiliki kontribusi sebesar 9.78% yang memiliki kontribusi signifikan karena sifatnya memengaruhi akurasi seluruh sensor sehingga berpengaruh pada failure mode $X_{1.3}$, $X_{7.2}$, dan $X_{7.1}$. Kalibrasi yang salah berpotensi menciptakan *systematic bias* pada sistem keselamatan, dimana hal ini lebih berbahaya dibanding kegagalan acak.

Rangkuman dari mekanisme *systemic risk* dapat dilihat pada Tabel 4.8 berikut ini.

Tabel 4.8 Mekanisme Risiko Sistemik pada Sistem Keselamatan Pertambangan Berbasis Digital

Kluster Risiko	**Kontribusi Risiko (%)**	**Mekanisme Sistemik**	**Cara Risiko Menyebar (*Systemic Interaction*)**	**Dampak terhadap Sistem Keselamatan**
Operational Safety Cluster (Risiko Operasional & Keselamatan)	40,77%	Kegagalan fungsi inti keselamatan (hazard detection & response).	Kegagalan pada salah satu lapisan sensor, analitik, atau alarm/aktuator memutus rantai keselamatan.	Loss of safety function dan potensi insiden fatal.
System Reliability Cluster (Risiko Teknik & Sistem)	29,90%	Rendahnya keandalan dan ketersediaan sistem	Gangguan daya, jaringan, atau perangkat keras menciptakan efek domino.	Blind spot monitoring dan keterlambatan respons

		pendukung.		darurat.
Cyber-Physical Risk Cluster (Risiko Siber & Privasi)	19,53%	Common cause failure dan risk amplifier lintas sistem.	Gangguan siber memengaruhi banyak failure mode secara simultan.	Kegagalan sistemik serentak pada sistem keselamatan digital.
Environmental Drift Cluster (Risiko Lingkungan & Kalibrasi)	9,78%	Bias sistemik akibat degradasi dan interferensi lingkungan.	Drift kalibrasi memengaruhi seluruh sensor secara konsisten.	False negative sistemik pada deteksi bahaya.

4.6 Analisis FTA (*Fault Tree Analysis*)

Analisis FTA (*Fault Tree Analysis*) dilakukan untuk mengidentifikasi struktur penyebab (*causal structure*) dari kejadian puncak (*Top Event*) yang berpotensi mengakibatkan kecelakaan fatal di area pertambangan. FTA dilakukan setelah tahap FMEA menghasilkan prioritas risiko melalui nilai RPN, sehingga FTA berfungsi untuk menelusuri hubungan logis antar penyebab, *interdependency,* serta *common cause failure* yang tidak dapat dijelaskan secara komprehensif oleh analisis FMEA. Pada konteks penelitian ini, FTA dilakukan secara kualitatif yang divalidasi melalui hasil FGD (*Focus Group Discussion*) bersama perwakilan *stakeholder* PT X, sehingga struktur *Fault Tree* yang dihasilkan secara akurat dapat mencerminkan kondisi nyata sistem digitalisasi keselamatan pertambangan.

Penentuan *Top Event* (TE)

Penentuan *Top Event* (TE) merupakan tahapan kunci dalam *Fault Tree Analysis* (FTA) yang merepresentasikan kejadian paling kritis dan tidak diinginkan dalam sistem. Berdasarkan hasil *Failure Mode and Effects Analysis* (FMEA), sepuluh *failure mode* dengan nilai RPN tertinggi menunjukkan pola *systemic risk cascade*, di mana risiko tidak muncul secara terpisah, tetapi berasal dari kegagalan berantai

pada fungsi deteksi dan peringatan keselamatan. Temuan ini mengindikasikan bahwa risiko paling kritis dalam sistem keselamatan pertambangan adalah kegagalan sistem dalam mendeteksi bahaya dan menyampaikan peringatan secara tepat waktu.

Temuan tersebut diperkuat melalui *Focus Group Discussion* (FGD) dengan para pemangku kepentingan PT X, yang menyepakati bahwa konsekuensi paling fatal di lapangan adalah ketidakmampuan sistem digital dalam memberikan peringatan keselamatan yang andal dan *real-time*, sehingga tindakan mitigasi tidak dapat dilakukan secara cepat. Kesepakatan ini selaras dengan prioritas manajemen PT X dalam melindungi keselamatan pekerja dan menjaga kontinuitas operasional. Oleh karena itu, *Top Event* (TE) dalam penelitian ini dirumuskan sebagai **"Kegagalan Sistem Keselamatan Digital untuk Mendeteksi dan Memberikan Peringatan Kondisi Bahaya Kritis secara *Real-Time*** (*Failure to Detect and Warn Critical Hazard* – FTCH)". *Top Event* ini terjadi ketika sistem keselamatan digital gagal menghasilkan atau menyampaikan peringatan secara akurat dan tepat waktu saat parameter bahaya melampaui ambang batas aman, sehingga meningkatkan potensi terjadinya *near-miss* hingga *fatality.*

Identifikasi *Intermediante Events* (IE)

Intermediate Event (IE) merupakan kelompok penyebab tingkat menengah yang berkontribusi terhadap *Top Event* (TE). TE terjadi apabila salah satu IE terjadi. Berdasarkan pemetaan risiko pada analisis FMEA yang menghasilkan 10 priorotas risiko dan hasil validasi melalui FGD, struktur FTA disusun dalam 4 *Intermediate Events* (IE) sebagai kelompok penyebab utama yang diuraikan pada tabel berikut ini.

Tabel 4.9 *Intermediate Event (IE)*

Kode	***Intermediate Event* (IE)**	**Deskripsi**
IE_1	Kegagalan Sistem Deteksi Bahaya	Ketidakmampuan sensor dalam menghasilkan data yang valid (*sensor failure*).
IE_2	Kegagalan Sistem Analitik &	Kesalahan dalam pengolahan atau

	Interpretasi	interpretasi data sensor (*algorithmic/logic failure*).
$\overline{IE_3}$	Kegagalan Sistem Notifikasi Alarm	Alarm tidak berbunyi atau tidak diteruskan (*alarm failure*).
$\overline{IE_4}$	Kegagalan Infrastruktur Pendukung & *Cyber-Physical System*	Jaringan, daya, dan keamanan siber gagal atau tidak berfungsi (*system support failure*)

Identifikasi *Basic Events* (BE)

Basic Event (BE) adalah penyebab paling dasar yang bersifat spesifik dan terukur serta BE merupakan akar kegagalan (*root cause*) yang tidak dapat diuraikan lebih lanjut dalam struktur FTA. *Basic Event* (BE) merupakan unit paling kecil dari kegagalan sistem yang langsung berakibat pada terjadinya *fault*.

Tabel 4.10 Identifikasi *Basic Event* (BE) pada *Fault Tree Analysis* Sistem Keselamatan Pertambangan Digital

Kode	*Basic Event*	Deskripsi
IE_1	**Kegagalan Sistem Deteksi Bahaya (*Sensor Failure*)**	**Kegagalan pada tahap akuisisi data lapangan yang menyebabkan kondisi bahaya tidak terdeteksi secara akurat.**
$BE_{1.1}$	Gas berbahaya tidak terdeteksi	Sensor gagal mendeteksi peningkatan konsentrasi gas meskipun telah melampaui ambang batas keselamatan.
$BE_{1.2}$	Kalibrasi sensor tidak tepat	Proses kalibrasi tidak akurat menyebabkan output sensor bias dan menyimpang dari kondisi aktual.
$BE_{1.3}$	Data sensor fluktuatif	Sensor menghasilkan sinyal tidak stabil akibat noise atau degradasi komponen sehingga data tidak andal.
$BE_{1.4}$	Kerusakan sensor akibat lingkungan ekstrem	Paparan suhu tinggi, kelembaban, dan vibrasi menurunkan stabilitas dan performa sensor.

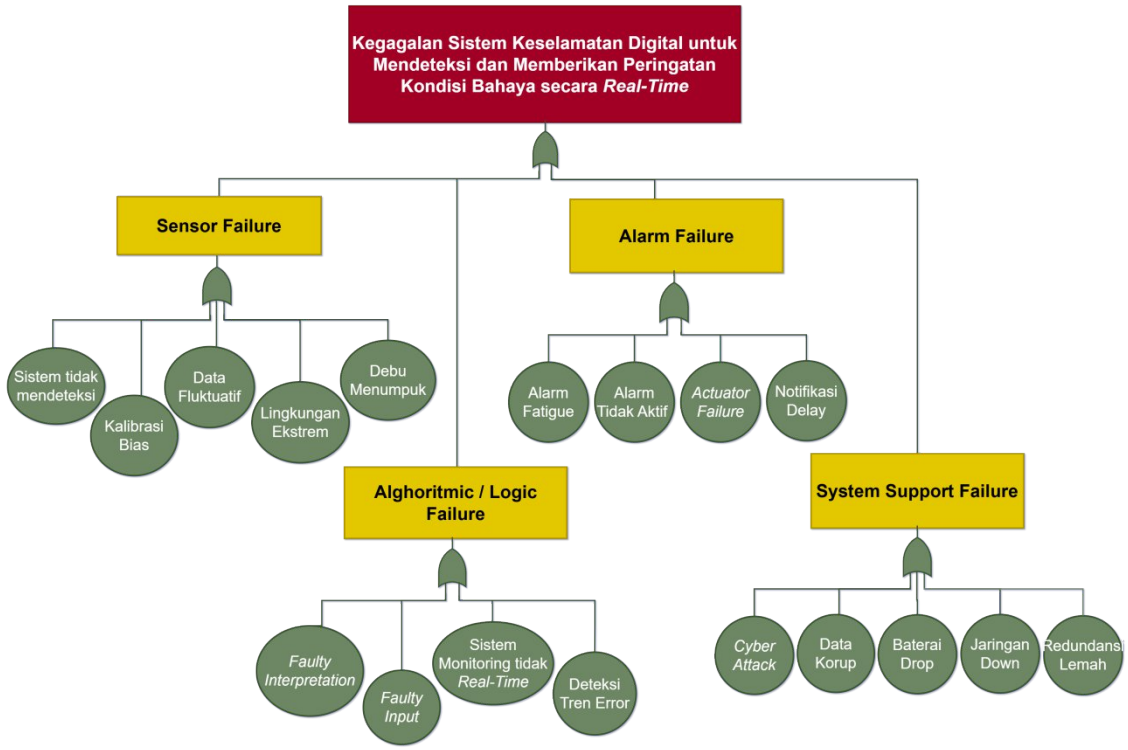
Kode	*Basic Event*	Deskripsi
$BE_{1.5}$	Penumpukan debu pada sensor	Akumulasi debu/partikulat menurunkan sensitivitas sensor dan meningkatkan risiko false negative.
IE_2	**Kegagalan Sistem Analitik & Interpretasi (Algorithmic/Logic Failure)**	**Kegagalan pemrosesan dan interpretasi data keselamatan oleh sistem analitik.**
$BE_{2.1}$	Algoritma salah klasifikasi kondisi aman	Sistem mengklasifikasikan area sebagai aman meskipun terdapat potensi kecelakaan atau longsor.
$BE_{2.2}$	Faulty interpretation akibat input tidak akurat	Data sensor yang tidak valid menyebabkan kesalahan interpretasi algoritma.
$BE_{2.3}$	Monitoring tidak real-time	Keterlambatan pembaruan data menyebabkan kondisi lapangan tidak terpantau aktual.
$BE_{2.4}$	Deteksi tren bahaya gagal	Kesalahan analitik menyebabkan sistem tidak mampu mengenali tren peningkatan risiko.
IE_3	**Kegagalan Sistem Notifikasi Alarm (Alarm Failure)**	**Kegagalan pada penyampaian peringatan dan aktivasi respons keselamatan.**
$BE_{3.1}$	Alarm fatigue	Frekuensi alarm berlebihan menyebabkan operator mengabaikan peringatan kritis.
$BE_{3.2}$	Alarm tidak aktif saat kondisi bahaya	Sistem gagal memicu alarm meskipun parameter keselamatan telah melampaui batas aman.
$BE_{3.3}$	Actuator failure	Aktuator gagal menjalankan fungsi keselamatan sehingga alarm atau proteksi tidak aktif.

Kode	*Basic Event*	Deskripsi
$BE_{3.4}$	Keterlambatan notifikasi	Notifikasi tidak tersampaikan tepat waktu ke control room atau supervisor.
$\boldsymbol{IE_4}$	**Kegagalan Infrastruktur Pendukung & Cyber-Physical System**	**Kegagalan infrastruktur dan sistem pendukung yang memengaruhi operasi keselamatan digital.**
$BE_{4.1}$	Serangan siber	Intrusi atau malware menyebabkan shutdown sistem monitoring keselamatan.
$BE_{4.2}$	Data keselamatan korup	Data rusak atau dimodifikasi selama transmisi sehingga informasi keselamatan tidak valid.
$BE_{4.3}$	Kegagalan baterai cadangan	Baterai tidak mampu menopang perangkat IoT saat terjadi pemadaman listrik.
$BE_{4.4}$	Gangguan jaringan	Jaringan komunikasi down menyebabkan sistem berhenti menampilkan data real-time.
$BE_{3.4}$	Kelemahan redundansi server dan backup	Tidak tersedianya failover memadai menyebabkan downtime sistem secara menyeluruh.

Diagram Struktur FTA (*Fault Tree Analysis*)

Diagram *Fault Tree Analysis* (FTA) pada penelitian ini menggambarkan struktur hubungan sebab–akibat yang menjelaskan bagaimana berbagai kegagalan pada sistem keselamatan digital dapat memicu terjadinya *Top Event* (TE). Diagram disusun menggunakan kombinasi gerbang logika OR dan AND, di mana gerbang OR menunjukkan bahwa kegagalan pada salah satu sub-sistem sudah cukup untuk menyebabkan *Top Event*, sedangkan gerbang AND digunakan pada kondisi tertentu ketika beberapa penyebab harus terjadi secara bersamaan.

Top Event diuraikan ke dalam beberapa *Intermediate Event* (IE) yang merepresentasikan kegagalan pada fungsi utama sistem, yaitu deteksi bahaya, pemrosesan analitik, penyampaian alarm, dan infrastruktur pendukung. Setiap *Intermediate Event* selanjutnya dijabarkan menjadi *Basic Event* (BE) sebagai akar penyebab paling dasar. Struktur hierarkis ini, sebagaimana ditunjukkan pada Gambar 4.5, memperlihatkan bahwa kegagalan sistem keselamatan bersifat sistemik dan berantai, sehingga kehilangan fungsi keselamatan tidak disebabkan oleh satu kegagalan tunggal, melainkan oleh interaksi antar komponen sistem.



Gambar 4.5 *Struktur FTA*

Analisis Jalur Kritis (*Minimal Cut Set*)

Minimal Cut Set (MCS) adalah kombinasi paling sederhana dari *Basic Event* (BE) yang secara kolektif cukup untuk memicu terjadinya *Top Event* (TE). Pada sistem IoT pertambangan di PT X, MCS menjadi penting karena kegagalan deteksi atau alarm tidak hanya berasal dari satu komponen tetapi merupakan interaksi berlapis yang diuraikan pada tabel 4.11 berikut ini.

Tabel 4.11 *Minimal Cut Sets (MOCUS)*

Kode	*Critical Path*	Interpretasi	Temuan FGD PT X	Dampak
MCS_1	$BE_{1.1}$à$BE_{2.2}$ à$BE_{3.2}$	Sistem deteksi gagalàinterpretasi gagal à alarm tidak aktif	• Kalibrasi tidak dilakukan sesuai rencana karena kebutuhan alat di lapangan yang sangat tinggi • Area pit tertentu memiliki zona *blind spot* jaringan. • Operator menyebut "alarm sering terlambat muncul" saat sinyal lemah.	Fatal tanpa peringatan
MCS_2	$BE_{1.3}$à$BE_{2.1}$	Data noiseà interpretasi salah	Sensor sering terkena debu/lumpur/grease terutama pada alat bergerak seperti DT/Excavator.	Keputusan tidak tepat
MCS_3	$BE_{4.1}$OR $BE_{4.2}$	*Cyber attack* à *shutdown* sistem *monitoring*	Kekhawatiran terhadap potensi serangan siber ke IoT meningkat.	*Blind operation*

MCS_4	$BE_{3.1}$	*Over alarm*à *alarm fatigue*	Terjadi alarm spam dari sensor kecepatan unit dan kestabilan lereng.	Alarm kritis diabaikan
MCS_5	$BE_{3.3}$à$BE_{4.4}$	*Actuator failure + loss telemetri* à *blind condition.*	Telemetri sering hilang intermiten di area hauling karena beban jaringan.	Dampak paling berbahaya

Berdasarkan tabel di atas, didapatkan prioritas mitigasi berdasarkan hasil MCS yang diklasifikasikan sebagai berikut:

1. MCS_1 dan MCS_5 (Dampak Fatal - *Immediate Action*)

Jalur pada MCS_1 menghasilkan *silent failure* yang mengakibatkan bahaya muncul tanpa alarm sehingga hal ini merupakan skenario paling fatal karena pekerja tidak memiliki waktu untuk melakukan mitigasi. Sedangkan jalur pada MCS_5 termasuk yang paling berbahaya karena sistem tidak mampu membaca kondisi lapangan maupun mengaktifkan aktuasi untuk mitigasi. Sehingga harus dilakukan langkah mitigasi sebagai berikut: (1) Kalibrasi sensor secara berkala (2) Penambahan *edge computing* agar tidak bergantung pada jaringan (3) *Upgrade* server ETL & *network load balancing*

2. MCS_3 (*Cybersecurity Enhancement*)

Jalur pada MCS_3 menghasilkan *blind operation* yang berakibat pada operator kehilangan visibilitas kondisi tambang secara total. Jalur ini harus di mitigasi dengan aman dan benar yang diklasifikasikan sebagai berikut: (1) Instalasi *secondary network local buzzer* berbasis *microcontroller* (2) *Update firmware* rutin seluruh perangkat lapangan (3) *Zero-trust access control*

3. MCS_2 (*Data Quality Improvement*)

Jalur pada MCS_2 menyebabkan keputusan operasional yang tidak tepat misalnya bahaya nyata yang tidak terbaca oleh sistem sehingga harus dilakukan tindakan mitigasi sebagai berikut: (1) Pembersihan sensor secara periodik. (2) Pengecekan peralatan termasuk didalamnya sensor sebelum mengoperasikan unit.

4. MCS_4 (*Alarm Fatigue Management*)

Jalur pada MCS_4 menyebabkan alarm kritis diabaikan sehingga menyebabkan *near-miss* hingga kecelakaan. Hal ini harus di mitigasi dengan klasifikasi sebagai berikut: (1) Penerapan *graded alarm priority* (2) *Training* operator terkait *alert acuity*

Interpretasi Hasil FTA

Interpretasi hasil *Fault Tree Analysis* (FTA) memberikan gambaran yang jelas mengenai bagaimana kegagalan pada komponen, subsistem, proses digital, serta faktor manusia dapat saling berinteraksi hingga memicu terjadinya *Top Event*. Berdasarkan struktur *fault tree*, hasil *Focus Group Discussion* (FGD), serta analisis *Minimal Cut Set* (MCS), diperoleh pemahaman bahwa risiko pada sistem keselamatan pertambangan berbasis IoT tidak berdiri sendiri, melainkan terbentuk dari hubungan yang saling bergantung antar elemen sistem.

Secara umum, interpretasi hasil FTA mengarah pada tiga temuan utama. Pertama, **risiko yang dihadapi bersifat sistemik dan interdependen**, sehingga upaya mitigasi tidak cukup difokuskan pada perbaikan komponen individual, tetapi harus menargetkan node kritis dalam arsitektur IoT. Kedua, terdapat **dua jalur kegagalan utama yang berpotensi memicu dampak fatal, yaitu jalur degradasi sensor dan jalur kegagalan infrastruktur serta siber**. Kedua jalur ini dapat memutus fungsi deteksi dan peringatan secara menyeluruh, sehingga sistem kehilangan kemampuan memberikan respons keselamatan yang tepat waktu. Ketiga, **faktor manusia tidak dapat dipandang sebagai penyebab tunggal, namun berperan sebagai penguat risiko ketika sistem teknis mulai mengalami gangguan**. Oleh karena itu, aspek SOP, desain alarm, dan program pelatihan harus menjadi bagian integral dari strategi mitigasi.

Hasil analisis FTA juga menunjukkan bahwa **kegagalan sistem keselamatan IoT di PT X dipengaruhi oleh empat node utama, yaitu deteksi, interpretasi, alarm, dan infrastruktur pendukung.** Kegagalan pada node-node tersebut **membentuk pola *systematic cascading risk***, yang konsisten dengan temuan FMEA. Jalur kegagalan paling kritis teridentifikasi pada rangkaian $IE_1 \rightarrow IE_2 \rightarrow$

IE_3, sementara gangguan pada aspek *cyber-physical* dan jaringan lapangan berperan sebagai pemicu utama terjadinya cascade failure. Temuan ini menegaskan bahwa risiko tidak terletak pada satu komponen tertentu, melainkan pada interaksi dan ketergantungan antar subsistem.

Dengan demikian, penerapan FTA memperkuat rekomendasi bahwa strategi **mitigasi risiko harus diarahkan pada stabilisasi sistem secara menyeluruh, bukan hanya pada peningkatan kinerja komponen secara parsial**. Pendekatan ini memastikan bahwa fungsi keselamatan tetap andal meskipun terjadi gangguan pada salah satu bagian sistem.

4.7 Analisis Penanganan Risiko (*Risk Response*)

Analisis *risk response* dilakukan untuk menentukan strategi pengendalian risiko yang paling efektif berdasarkan hasil analisis FMEA dan FTA pada implementasi sistem digitalisasi keselamatan pertambangan berbasis IoT pada PT X. Tujuan *risk response* yaitu mengurangi peluang dan dampak risiko, menghilangkan atau mereduksi *Basic Event* (BE) yang menjadi akar penyebab *critical path* dalam MCS, menurunkan nilai RPN hingga mencapai tingkat *residual risk* yang dapat diterima perusahaan, serta menentukan strategi dan tindakan mitigasi sesuai **kategori *risk response*** seperti ***avoidance, reduction, transfer,* atau *acceptance***. Selain itu, *risk response* diarahkan untuk memutus *critical path* pada MCS sehingga kombinasi *Basic Event* tidak lagi memenuhi struktur logis dalam *Fault Tree* dan *Top Event* tidak dapat muncul. Analisis *risk response* pada penelitian ini difokuskan pada lima risiko prioritas tertinggi berdasarkan nilai RPN serta *critical path* pada MCS yang berkontribusi langsung terhadap *Top Event* yaitu *Failure to Detect and Warn Critical Hazard* (FTCH).

Prioritas Risiko berdasarkan RPN Tertinggi

Berdasarkan hasil FMEA, lima *failure mode* prioritas dengan nilai RPN tertinggi ditunjukkan pada tabel berikut ini.

Tabel 4.12 Prioritas Risiko berdasarkan 5 Nilai RPN Tertinggi

Prioritas	Kode	*Failure Mode*	RPN	BE
1	$X_{7.1}$	Sistem tidak mendeteksi gas berbahaya	27.54	$BE_{1.1}$
2	$X_{1.3}$	Sensor menghasilkan data fluktuatif/noise	27.30	$BE_{1.3}$
3	$X_{9.2}$	Alarm fatigue akibat alarm berlebih	26.72	$BE_{3.1}$
4	$X_{3.2}$	Baterai cadangan tidak menopang perangkat IoT	26.67	$BE_{4.3}$
5	$X_{7.2}$	Algoritma salah mengklasifikasi area aman padahal berbahaya	26.64	$BE_{2.1}$

Lima *failure mode* pada tabel di atas, memiliki pengaruh dominan terhadap risiko keseluruhan dan berkontribusi membentuk *critical path* pada MCS penyebab *Top Event*. BE pada prioritas 1, 2, dan 5 berada pada MCS_1 dan MCS_2 yaitu *interdependent systemic failure*. $BE_{3.1}$ adalah *single-point human-factor failure* berada dalam MCS_4. Terakhir $BE_{4.3}$ memiliki nilai RPN tinggi walaupun tidak muncul pada lima MCS utama.

Critical Path* berdasarkan *Minimal Cut Set

Untuk menentukan strategi mitigasi yang tepat, *failure mode* prioritas dipetakan terhadap MCS yang telah dihasilkan melalui analisis FTA. MCS menunjukkan kombinasi dari BE yang menyebabkan terjadinya *Top Event*.

Tabel 4.13 *Critical Path* berdasarkan *Minimal Cut Set*

BE Prioritas	MCS	*Critical Path*	Jenis Kegagalan	Dampak	Kategori
$\boldsymbol{BE_{1.1}}$	MCS_1	$BE_{1.1}$ à $BE_{2.2}$ à $BE_{3.2}$	*Interdependent Systemic*	Fatal tanpa peringatan	*Avoidance + Reduction*

$\boldsymbol{BE_{1.3}}$, $\boldsymbol{BE_{2.1}}$	MCS_2	$BE_{1.3}$ à $BE_{2.1}$		Keputusan tidak tepat	*Reduction* dan *transfer*
$\boldsymbol{BE_{3.1}}$	MCS_4	$BE_{3.1}$	*Human Factor*	Alarm fatigue	*Reduction* + *Acceptance*
$\boldsymbol{BE_{4.3}}$	-	-	Infrastruktur	*Blind condition*	*Reduction*

Berdasarkan pemetaan BE terhadap *critical path* MCS, strategi *risk response* diklasifikasikan menjadi *risk avoidance, risk reduction, risk transfer,* dan *risk acceptance* yang ditetapkan secara berbeda untuk setiap *critical path*. $BE_{1.1}$ berada pada *critical path* MCS_1, diklasifikan sebagai risiko yang tidak dapat ditoleransi karena memiliki dampak paling fatal pada bahaya yang muncul tanpa alarm (*silent failure*) sehingga pekerja tidak memiliki waktu untuk melakukan mitigasi. Risiko ini membutuhkan kombinasi ***risk avoidance*** dan ***risk reduction*** dalam penanganannya. *Risk avoidance* digunakan untuk menghilangkan pola ketergantungan sistem deteksi à interpretasi à alarm yang menyebabkan *silent failure*. Pada PT X, kondisi lapangan seperti *blind spot* jaringan, delay telemetri, dan tidak adanya backup alarm lokal dapat memperbesar risiko *silent failure*. Tindakan mitigasi yang dapat dilakukan untuk menghilangkan pola berbahaya (*risk avoidance*) yaitu memutus ketergantungan alarm pada jaringan sehingga alarm harus tetap berbunyi di lokasi alat walaupun jaringan down dengan menggunakan *local buzzer* berbasis *microcontroller*; serta mendesain ulang arsitektur alarm dengan mengganti model *cloud-triggered alarm* dengan *edge-triggered alarm*. Selain itu harus dilakukan *risk reduction* untuk memperbaiki atau menurunkan probabilitas komponen BE dengan melakukan tindakan seperti kalibrasi sensor secara terjadwal, sensor redundancy (*dual sensing system*), *self-diagnostic* sensor yang melakukan *auto-check* setiap 1 menit, penambahan repeater jaringan di pit untuk mengurangi *blind spot*, serta *preventive maintenance* berbasis *runtime* karena lebih cocok pada PT X yang banyak menggunakan unit bergerak seperti DT & Excavator.

Selanjutnya, *critical path* pada MCS_2 yaitu $BE_{1.3}$ menyebabkan $BE_{2.1}$ sehingga memicu *Top Event* terjadi. Kedua BE pada jalur ini termasuk pada BE prioritas

yang harus segera dilakukan mitigasi karena berdampak pada pengambilan keputusan yang tidak tepat sehingga diperlukan ***risk reduction*** berbasis peningkatan kualitas data dan algoritma. Penyebab dari $BE_{1.3}$ berasal dari lingkungan seperti debu, lumpur, atau grease sehingga *root cause* dapat dikurangi dengan melakukan pembersihan sensor secara periodik. Untuk memastikan mitigasi berjalan secara efektif dilakukan peraturan yang mewajibkan seluruh operator alat berat untuk melakukan inspeksi sebelum mengoperasikan unit. Selain itu, ***risk transfer*** pada $BE_{2.1}$ dilakukan dengan melakukan kalibrasi alat sensor yang dikelola oleh pihak ketiga yang *reliable*.

Selanjutnya yaitu $BE_{3.1}$ yang merupakan *critical path* dari MCS_4, berdampak pada *alarm fatigue*. Tindakan mitigasi pada risiko ini yaitu kombinasi dari *risk reduction* dan *risk acceptance* karena *human factor risk* tidak dapat dihilangkan sepenuhnya (*avoidance*) dan tidak dapat ditransfer pada pihak ketiga karena tanggung jawab tetap pada operator. ***Risk reduction*** pada risiko ini dapat dilakukan dengan tindakan seperti penerapan *graded alarm priority,* integrasi alarm audio pada kabin operator alat berat dan alarm visual pada *central control room*, serta penyesuaian alarm berdasarkan cuaca dan kondisi pit sehingga tidak menghasilkan sensor getaran *false* saat hujan. *Risk acceptance* dapat dilakukan dengan memberikan pelatihan operator shift secara berkala agar memahami *alert acuity* dan adanya *dashboard alarm summary* untuk mencegah kelelahan kognitif operator di *central control room*.

Terakhir pada $BE_{4.3}$ yang tidak termasuk dalam MCS utama namun RPN pada risiko ini tinggi yang berdampak pada *blind condition* sehingga menyebabkan unit IoT mati total sehingga diperlukan tindakan mitigasi ***risk reduction***. *Failure* dapat dikurangi dengan melakukan penggandaan jalur kelistrikan sensor ke *engine unit* sehingga IoT tetap berfungsi walaupun baterai tidak terisi atau kosong selama *engine unit* beroperasi. Risiko ini tidak dapat dihilangkan secara total (*avoidance*) dikarenakan *battery-dependent system* tetap diperlukan.

Perhitungan Residual Risk

Perhitungan *residual risk* dilakukan berdasarkan FGD yang dilakukan secara *online* dengan perwakilan dari tiga divisi PT X yaitu divisi *mining innovation & digitalization*, divisi *mining operation,* dan divisi *safety, health, & environment*. Setiap parameter RPN yaitu S, O, dan D disepakati dengan mempertimbangkan efektivitas mitigasi yang dapat dicapai secara realistis di lingkungan pertambangan PT X, keterbatasan infrastruktur jaringan dan kondisi pit, kemampuan operator, serta karakteristik sensor yang digunakan pada PT X. Tujuan perhitungan *residual risk* adalah memastikan bahwa mitigasi yang diusulkan pada penelitian ini efektif untuk menurunkan risiko serta memutus *critical path* sehingga tidak lagi menjadi pemicu terjadinya *Top Event* yang akan diuraikan pada tabel berikut ini:

***Residual Risk* pada $BE_{1.1}$**

Parameter *Severity* berkurang 80% karena dengan adanya sistem *detector* berbasis lokal maka kondisi dan tindakan berbahaya dapat di antisipasi walaupun kondisi sinyal terbatas. Parameter *Occurrence* tidak berkurang karena *residual risk* ini tidak mempengaruhi probabilitas kegagalan terjadi. Parameter *Detection* berkurang 80% karena dengan adanya sistem *detector* berbasis lokal maka sistem atau kontrol yang ada saat ini menjadi lebih efektif untuk mendeteksi kegagalan.

Tabel 4.14 *Residual Risk* pada $BE_{1.1}$

Parameter	Sebelum Mitigasi	Setelah Mitigasi
Severity (S)	4.30	0.86
Occurance (O)	2.10	2.10
Detection (D)	3.05	0.61
RPN	27.54	1.10

***Residual Risk* pada $BE_{1.3}$**

Parameter *Severity* berkurang 80% karena dengan adanya pembersihan dan inspeksi sensor secara periodik maka kondisi dan tindakan berbahaya dapat di antisipasi dengan menghilangkan kendala *data error*. Parameter *Occurrence* berkurang 60% karena *risk response* ini memungkinkan frekuensi kegagalan

menurun. Parameter *Detection* berkurang 60% karena dengan adanya pembersihan dan inspeksi sensor secara periodik maka data yang dihasilkan lebih valid karena sensor dilakukan inspeksi secara periodik.

Tabel 4.15 *Residual Risk* pada $BE_{1.3}$

Parameter	Sebelum Mitigasi	Setelah Mitigasi
Severity (S)	3.25	0.65
Occurance (O)	2.80	1.12
Detection (D)	3.00	1.20
RPN	27.30	0.87

***Residual Risk* pada $BE_{3.1}$**

Parameter *Severity* tidak berkurang karena walaupun dilakukan respon terhadap risiko tetap tidak mengurangi keparahan jika kegagalan terjadi. Parameter *Occurrance* berkurang 80% karena *graded alarm priority* ini memungkinkan frekuensi kegagalan menurun. Parameter *Detection* berkurang 80% karena dengan *graded alarm priority* maka sistem atau kontrol yang ada saat ini dapat lebih efektif dalam mendeteksi kegagalan.

Tabel 4.16 *Residual Risk* pada $BE_{3.1}$

Parameter	Sebelum Mitigasi	Setelah Mitigasi
Severity (S)	3.35	3.35
Occurance (O)	2.75	0.55
Detection (D)	2.90	0.58
RPN	26.72	1.07

***Residual Risk* pada $BE_{4.3}$**

Parameter *Severity* tidak berkurang karena walaupun dilakukan respon terhadap risiko tetap tidak mengurangi keparahan jika kegagalan terjadi. Parameter *Occurrance* berkurang 80% karena penggandaan jalur kelistrikan sensor ke *engine unit* dapat mengurangi potensi kegagalan sensor IoT walaupun baterai tidak terisi atau kosong selama engine unit beroperasi. Parameter *Detection* berkurang 80% karena dengan penggandaan jalur kelistrikan sensor ke *engine unit* maka sistem

atau kontrol yang ada saat ini dapat lebih efektif dalam mendeteksi kegagalan sensor.

Tabel 4.17 *Residual Risk* pada $BE_{4.3}$

Parameter	Sebelum Mitigasi	Setelah Mitigasi
Severity (S)	3.30	3.30
Occurance (O)	2.65	0.53
Detection (D)	3.05	0.61
RPN	26.67	1.07

***Residual Risk* pada $BE_{2.1}$**

Parameter *Severity* berkurang 80% karena dengan adanya kalibrasi sensor maka kondisi dan tindakan berbahaya dapat terantisipasi lebih dini dengan menghilangkan kendala data tidak valid. Parameter *Occurrence* berkurang 80% karena *risk response* ini memungkinkan frekuensi kegagalan menurun. Parameter *Detection* berkurang 80% karena dengan *risk response* ini maka data yang dihasilkan lebih valid karena sensor dikalibrasi secara periodik.

Tabel 4.18 *Residual Risk* pada $BE_{2.1}$

Parameter	Sebelum Mitigasi	Setelah Mitigasi
Severity (S)	4.30	0.86
Occurance (O)	2.10	0.42
Detection (D)	2.95	0.59
RPN	26.64	0.21

Dari lima prioritas risiko yang dianalisis, didapatkan nilai RPN residual setelah dilakukan langkah mitigasi yang kemudian divalidasi melalui *Focus Group Discussion* dengan PT X. Tabel *residual risk* setelah dilakukan mitigasi disajikan sebagai berikut.

Tabel 4.19 *Residual Risk* berbasis FGD dengan PT X

BE	MCS	RPN Awal	RPN Residual	Level Risiko	Evaluasi FGD
$\boldsymbol{BE_{1.1}}$	MCS_1	27.54	1.10	Rendah	Hasil mitigasi dapat memutus jalur fatal yaitu *silent failure* karena alarm tetap aktif walaupun jaringan down, sehingga risiko ini dapat dikendalikan tapi belum bisa terdampak signifikan karena masih terdapat area yang tidak bisa tercover dengan jaringan lokal.
$\overline{\boldsymbol{BE_{1.3}}}$	MCS_2	27.30	0.87	Rendah	Risiko turun secara signifikan sehingga validitas input sensor stabil dan risiko salah interpretasi hampir hilang.
$\boldsymbol{BE_{2.1}}$	MCS_2	26.64	0.21	Rendah	Kombinasi mitigasi yang dilakukan dapat memutus jalur IE2 sehingga tidak salah dalam interpretasi.
$\overline{\boldsymbol{BE_{3.1}}}$	MCS_4	26.72	1.07	Rendah	Dari semua mitigasi yang dilakukan, risiko human factor masih ada namun masih dalam batas toleransi sehingga kalibrasi sensor harus terjadwal dengan baik.
$\overline{\boldsymbol{BE_{4.3}}}$	-	26.67	1.07	Rendah	Risiko turun signifikan walaupun masih bergantung pada *engine uptime*.

4.8 Diskusi dan Pembahasan

Pola Risiko Sistemik pada Sistem Keselamatan Digital

Hasil analisis FMEA menunjukkan bahwa profil risiko pada sistem digitalisasi keselamatan pertambangan PT X didominasi oleh kategori risiko sedang, yaitu 32 dari 40 failure mode yang valid. Dominasi risiko sedang ini tidak mengindikasikan bahwa sistem berada pada kondisi aman, melainkan mencerminkan akumulasi risiko berintensitas moderat yang saling berinteraksi dan berpotensi menghasilkan konsekuensi yang serius. Hal ini tercermin dari distribusi sepuluh nilai RPN tertinggi yang relatif merata pada rentang 9,38%–10,47%, yang menandakan tidak adanya satu sumber risiko tunggal yang dominan. Pola tersebut konsisten dengan karakteristik systemic risk pada sistem digital kompleks, di mana kegagalan muncul sebagai hasil interaksi simultan antar subsistem, bukan dari satu titik kegagalan terisolasi (Leimester & Kolios, 2018). Dalam konteks PT X, mekanisme ini tampak pada urutan kegagalan berantai mulai dari data sensor yang tidak andal, kesalahan interpretasi, alarm yang tidak aktif, hingga ketiadaan respons terhadap kondisi berbahaya yang dapat berujung pada insiden fatal.

Struktur Tekanan Risiko Berdasarkan Kluster

Pengelompokan failure mode ke dalam empat kluster risiko memberikan gambaran yang lebih jelas mengenai struktur tekanan risiko pada sistem keselamatan digital. Operational Safety Cluster menyumbang kontribusi terbesar sebesar 40,77%, yang menegaskan bahwa titik kelemahan utama sistem berada pada fungsi inti keselamatan, yaitu deteksi bahaya, interpretasi kondisi, dan penyampaian peringatan. Temuan ini sejalan dengan literatur IoT keselamatan kerja yang menekankan bahwa akurasi deteksi dan keandalan alarm merupakan determinan paling kritis dalam lingkungan berisiko tinggi (Zhou, Liu, & Li, 2020).

Di sisi lain, System Reliability Cluster (29,90%) dan Cyber-Physical Risk Cluster (19,53%) berperan sebagai risk amplifier. Gangguan pada jaringan komunikasi, suplai daya, atau serangan siber tidak hanya meningkatkan risiko pada subsistem tertentu, tetapi juga berpotensi melumpuhkan keseluruhan rantai keselamatan. Sementara itu, Environmental Drift Cluster meskipun memiliki kontribusi paling kecil (9,78%), bersifat sangat strategis karena dapat menimbulkan systematic bias,

seperti kondisi ketika sensor secara konsisten membaca parameter bahaya di bawah ambang batas aman. Kondisi ini, sebagaimana dijelaskan dalam IEC 60812, jauh lebih berbahaya dibandingkan kegagalan acak karena sulit terdeteksi dan berlangsung dalam jangka waktu panjang.

Pendalaman Kausal Risiko melalui Fault Tree Analysis

Analisis FTA memberikan kedalaman yang lebih tinggi dalam memahami struktur penyebab kegagalan sistem keselamatan digital. Penetapan Top Event berupa Failure to Detect and Warn Critical Hazard (FTCH) selaras dengan prioritas risiko hasil FMEA dan merepresentasikan bentuk kehilangan fungsi keselamatan yang paling fatal. Struktur Fault Tree menunjukkan bahwa FTCH dapat dipicu oleh kombinasi kegagalan pada sistem deteksi sensor, kesalahan analitik dan interpretasi, kegagalan sistem alarm, serta gangguan infrastruktur dan siber. Temuan ini konsisten dengan studi di bidang pertambangan digital yang menyatakan bahwa kegagalan sistem IoT keselamatan umumnya bersifat multi-layered dan tidak berdiri sendiri (Kurniawan & Hasan, 2022).

Jalur Kegagalan Kritis dan Interdependensi Sistem

Analisis Minimal Cut Set (MCS) semakin memperjelas jalur kegagalan paling kritis dalam sistem. Beberapa MCS menunjukkan potensi silent failure dan blind operation, yaitu kondisi ketika sistem gagal mendeteksi bahaya sekaligus gagal memberikan peringatan, sehingga pekerja tidak memiliki kesempatan untuk melakukan tindakan mitigasi. Jalur kegagalan lain menyoroti kerentanan siber sebagai pemicu system-wide collapse, yang semakin relevan dalam implementasi Industrial IoT. Selain itu, kualitas data sensor dan fenomena alarm fatigue muncul sebagai faktor penting yang dapat menyebabkan salah interpretasi atau pengabaian peringatan kritis. Temuan ini menegaskan bahwa risiko menjadi sangat berbahaya ketika beberapa komponen gagal secara bersamaan dan saling memperlemah fungsi satu sama lain, sejalan dengan konsep interdependensi risiko pada sistem cyber-physical.

Implikasi Strategi Mitigasi Berbasis Sistem Terintegrasi

Kombinasi FMEA dan FTA tidak hanya menghasilkan daftar risiko, tetapi juga memberikan diagnosis menyeluruh terhadap struktur penyebab dan titik lemah sistem keselamatan digital. Hasil ini menunjukkan bahwa strategi mitigasi tidak cukup dilakukan melalui tindakan teknis yang bersifat lokal, seperti penggantian sensor atau peningkatan kapasitas jaringan semata, melainkan harus diarahkan pada stabilisasi sistem secara terintegrasi. Oleh karena itu, pendekatan mitigasi dirumuskan berdasarkan empat kategori utama, yaitu risk avoidance, risk reduction, risk transfer, dan risk acceptance.

Lima failure mode prioritas selanjutnya dimitigasi melalui FGD bersama stakeholder PT X. Risiko yang berpotensi menimbulkan silent failure ditangani melalui risk avoidance dan risk reduction dengan penerapan kalibrasi sensor berkala, penambahan edge computing, serta peningkatan kapasitas server dan jaringan. Risiko operasional akibat kesalahan pengambilan keputusan ditangani melalui kombinasi risk reduction dan risk transfer, termasuk pembersihan sensor secara periodik dan kalibrasi oleh pihak ketiga yang kompeten. Risiko yang masih dapat ditoleransi ditangani melalui risk acceptance yang disertai pengawasan terstruktur dan peningkatan pelatihan operator. Sementara itu, risiko infrastruktur yang menyebabkan kondisi blind spot dimitigasi melalui penguatan redundansi daya dan sistem pendukung.

Evaluasi Residual Risk dan Kontribusi Penelitian

Efektivitas tindakan mitigasi dievaluasi melalui perhitungan residual risk untuk memastikan bahwa nilai RPN dapat diturunkan ke tingkat yang dapat diterima. Hasil evaluasi menunjukkan bahwa lima risiko prioritas memiliki nilai RPN residual di bawah 1,2 berdasarkan validasi FGD, yang mengindikasikan bahwa strategi mitigasi yang dirumuskan efektif. Pendekatan ini sejalan dengan prinsip Critical Control Management (ICMM, 2021), yang menekankan bahwa keandalan keselamatan hanya dapat dicapai apabila seluruh elemen kritis—sensor, algoritma, alarm, jaringan, daya, keamanan siber, dan kesiapan operator—berfungsi secara konsisten dan terverifikasi.

Secara keseluruhan, penelitian ini memberikan kontribusi akademik dan praktis berupa pemahaman empiris mengenai pola risiko sistemik pada sistem keselamatan pertambangan berbasis IoT. Temuan ini menjadi landasan bagi PT X dalam merancang intervensi mitigasi yang tidak hanya menurunkan risiko individual, tetapi juga mengurangi potensi cascade failure yang dapat memicu insiden besar dalam operasi pertambangan. Tabel berikut merupakan sintesis dari diskusi dan pembahasan diatas.

Tabel 4.20 Sintesis Diskusi dan Pembahasan Hasil Analisis Risiko

Aspek Analisis	**Temuan Utama**	**Interpretasi dan Implikasi**
Profil Risiko FMEA	32 dari 40 failure mode berada pada kategori risiko sedang; distribusi 10 RPN tertinggi relatif merata (9,38%–10,47%).	Risiko tidak didominasi satu kegagalan tunggal, tetapi terbentuk dari akumulasi risiko moderat yang saling berinteraksi dan berpotensi memicu dampak serius.
Pola Risiko Sistemik	Teridentifikasi urutan kegagalan berantai: data tidak andal → interpretasi salah → alarm tidak aktif → tidak ada respons.	Menunjukkan karakter systemic risk pada sistem keselamatan digital, di mana kegagalan bersifat interdependen dan berpotensi menghasilkan cascade failure.
Kluster Risiko (FMEA)	Operational Safety (40,77%), System Reliability (29,90%), Cyber-Physical (19,53%), Environmental Drift (9,78%).	Fungsi inti keselamatan menjadi titik tekanan utama, sementara keandalan sistem dan risiko siber berperan

Aspek Analisis	Temuan Utama	Interpretasi dan Implikasi
		sebagai risk amplifier yang memperbesar dampak kegagalan.
Top Event (FTA)	Failure to Detect and Warn Critical Hazard (FTCH).	Merepresentasikan kehilangan fungsi keselamatan paling kritis pada sistem digital berbasis IoT.
Intermediate Events (FTA)	Kegagalan deteksi sensor, kesalahan analitik, kegagalan alarm, serta gangguan infrastruktur dan siber.	Menegaskan bahwa kegagalan keselamatan muncul dari interaksi multi-layer antar subsistem, bukan kegagalan tunggal.
Minimal Cut Set (MCS)	Silent failure, blind operation, kerentanan siber, dan alarm fatigue.	Risiko menjadi sangat kritis ketika beberapa komponen gagal secara simultan dan saling melemahkan fungsi keselamatan.
Karakter Risiko Utama	Interdependensi antar subsistem deteksi–interpretasi–alarm–infrastruktur.	Menguatkan kebutuhan mitigasi berbasis stabilisasi sistem, bukan sekadar perbaikan komponen individual.
Strategi Respon Risiko	Risk avoidance, risk reduction, risk transfer, dan risk acceptance.	Respon risiko harus dipilih secara kontekstual sesuai karakter failure mode

Aspek Analisis	Temuan Utama	Interpretasi dan Implikasi
		dan dampaknya terhadap keselamatan.
Prioritas Mitigasi	Lima failure mode prioritas ditetapkan dan divalidasi melalui FGD.	Validasi ahli memastikan mitigasi relevan secara teknis dan operasional.
Tindakan Mitigasi Kunci	Kalibrasi sensor berkala, edge computing, peningkatan kapasitas jaringan, graded alarm priority, dan redundansi daya.	Mengurangi potensi cascade failure dan meningkatkan keandalan sistem keselamatan secara menyeluruh.
Residual Risk	Nilai RPN residual < 1,2 untuk lima risiko prioritas.	Menunjukkan efektivitas mitigasi dengan risiko diturunkan ke tingkat rendah dan dapat diterima.
Keselarasan Best Practice	Pendekatan sejalan dengan prinsip Critical Control Management (CCM).	Keandalan keselamatan hanya tercapai jika seluruh elemen kritis terverifikasi dan berfungsi konsisten.

4.9 Implikasi Manajerial

Penerapan metodologi FMEA dan FTA dalam penelitian ini memberikan implikasi manajerial yang signifikan bagi keberhasilan implementasi proyek digitalisasi sistem keselamatan pertambangan. Melalui pemanfaatan nilai *Risk Priority Number* (RPN), manajemen dapat mengambil keputusan secara lebih objektif dan terarah dengan memfokuskan mitigasi pada risiko yang paling kritis, sehingga sumber daya tidak terbuang pada area yang kurang berdampak. Identifikasi akar penyebab kegagalan (*root causes*) sistem digital melalui analisis

FTA juga meningkatkan kualitas perencanaan implementasi, karena manajemen dapat mengantisipasi potensi hambatan sejak tahap awal dan merancang langkah pencegahan yang lebih matang. Selain itu, hasil keterpaduan FMEA–FTA membantu merumuskan strategi mitigasi yang lebih spesifik dan terukur, dengan tindakan yang langsung menyasar titik kegagalan utama baik dari sisi teknologi maupun proses operasional. Dari perspektif keselamatan, metodologi ini memperkuat sistem keselamatan pertambangan dengan memastikan bahwa teknologi digital yang diterapkan telah melalui evaluasi risiko menyeluruh sehingga aman, andal, dan sesuai dengan kebutuhan lapangan. Implikasi lainnya adalah optimalisasi alokasi sumber daya proyek, meliputi anggaran, tenaga ahli, dan waktu karena prioritas risiko yang jelas membantu manajemen menentukan kebutuhan investasi mitigasi secara lebih efisien. Penelitian ini juga mendukung peningkatan monitoring dan kontrol proyek melalui pengembangan *risk register*, indikator kinerja risiko (KRI), dan mekanisme peringatan dini yang memungkinkan deteksi cepat terhadap potensi kegagalan sistem digital. Secara keseluruhan, metode ini memberikan kontribusi pada peningkatan kepatuhan terhadap regulasi keselamatan pertambangan, termasuk SMKP Minerba dan standar K3 lain yang relevan, sehingga implementasi proyek digitalisasi tidak hanya efektif secara teknis, tetapi juga selaras dengan kewajiban hukum dan standar industri yang berlaku.

(Halaman ini sengaja dikosongkan)

BAB 5

KESIMPULAN DAN SARAN

5.1 Kesimpulan

1. Berdasarkan hasil identifikasi, analisis risiko, dan pemetaan proses bisnis terhadap implementasi teknologi *Internet of Things* (IoT) pada sistem monitoring keselamatan pertambangan di PT X penelitian ini menyimpulkan bahwa proyek digitalisasi keselamatan pertambangan menghadapi berbagai risiko yang bersifat teknis, operasional, infrastruktur, siber, serta risiko yang berkaitan dengan faktor manusia dan organisasi. Risiko-risiko tersebut mencakup kegagalan fungsi sensor dalam mendeteksi bahaya, fluktuasi dan ketidakandalan data, gangguan jaringan dan daya listrik, kegagalan alarm dan aktuator, serangan siber yang berpotensi menyebabkan sistem shutdown, keterbatasan kesiapan operator dalam memahami dan mengoperasikan sistem digital secara optimal, serta kegagalan sistem peringatan dini dalam mendeteksi dan menyampaikan kondisi bahaya secara real-time. Melalui penerapan metode FMEA, risiko tersebut dapat di analisis dan diprioritaskan secara sistematis berdasarkan tiga parameter utama yaitu *Severity, Occurance,* dan *Detection* untuk mengukur nilai RPN (*Risk Priority Number*) sehingga memberikan output berupa prioritas risiko tertinggi yang memerlukan analisis lanjutan dan penanganan khusus. Dengan demikian, FMEA terbukti efektif sebagai metode untuk mengidentifikasi dan prioritasi risiko pada implementasi sistem keselamatan pertambangan berbasis IoT di PT X.
2. Sumber penyebab risiko teridentifikasi berasal dari empat kelompok utama, yaitu pertama kegagalan fungsi deteksi sensor yang dipengaruhi kondisi lingkungan ekstrem; kedua yaitu kesalahan analitik dan interpretasi data keselamatan; ketiga yaitu kegagalan sistem alarm dan aktuator dalam menyampaikan peringatan kritis; serta terakhir yaitu gangguan infrastruktur pendukung, keamanan siber, dan kesiapan organisasi. Pola hubungan antar

penyebab menunjukkan bahwa risiko dalam sistem keselamatan digital bersifat interdependen dan sistemik, di mana kegagalan tidak berasal dari satu titik kelemahan tunggal, melainkan dari interaksi kompleks antar subsistem deteksi, interpretasi, peringatan, dan infrastruktur pendukung. Temuan ini menegaskan bahwa risiko tidak terletak pada satu komponen tertentu, melainkan pada interaksi dan ketergantungan antar subsistem sehingga strategi mitigasi risiko harus disusun secara terintegrasi berdasarkan empat kategori *risk response*, yaitu *risk avoidance, risk reduction, risk transfer,* dan *risk acceptance.*

3. Fokus utama mitigasi risiko diarahkan pada *risk avoidance* dan *risk reduction*, terutama melalui kalibrasi sensor secara berkala, penerapan *edge computing* untuk mengurangi ketergantungan pada jaringan, peningkatan kapasitas server dan *network load balancing* guna mencegah *silent failure*, penerapan *graded alarm priority,* integrasi alarm audio pada kabin operator alat berat dan alarm visual pada *central control room*, serta penyesuaian konfigurasi alarm berdasarkan kondisi cuaca di area pit untuk menghindari *alarm fatigue*. Untuk risiko yang tidak dapat dihilangkan sepenuhnya, pendekatan *risk transfer* dan *risk reduction* diterapkan melalui kalibrasi sensor oleh pihak ketiga yang kompeten, pembersihan sensor secara periodik, serta inspeksi perangkat sebelum operasi. Risiko non-kritis yang masih berada dalam batas toleransi operasional dikelola melalui *risk acceptance* dengan pengawasan ketat dan penguatan kompetensi operator melalui pelatihan berkala agar mampu memahami tingkat urgensi peringatan (*alert acuity*).

   Efektivitas tindakan mitigasi dievaluasi melalui perhitungan *residual risk* untuk memastikan bahwa nilai risiko pasca-mitigasi berada pada tingkat yang dapat diterima. Hasil penelitian menunjukkan bahwa lima risiko prioritas memiliki nilai RPN residual di bawah 1,2 yang mengindikasikan bahwa strategi mitigasi yang diusulkan efektif dan layak diimplementasikan secara operasional. Dengan demikian, penelitian ini tidak hanya memetakan risiko dan akar penyebabnya, tetapi juga memberikan kerangka mitigasi yang komprehensif, terukur, dan berbasis evaluasi untuk mendukung penerapan

sistem keselamatan digital yang lebih andal di lingkungan pertambangan PT X.

Secara keseluruhan hasil penelitian ini memberikan implikasi manajerial yang signifikan bagi sistem pengelolaan keselamatan pertambangan berbasis digital. **Pertama**, manajemen dapat menggunakan hasil FMEA dan FTA sebagai dasar pengambilan keputusan berbasis prioritas risiko, sehingga sumber daya proyek dapat difokuskan pada titik kegagalan yang paling kritis. **Kedua**, temuan penelitian mendukung peningkatan kualitas perencanaan dan implementasi proyek digitalisasi keselamatan dengan menekankan pentingnya keandalan sistem secara menyeluruh, bukan hanya pada aspek teknologi individual. **Ketiga**, penelitian ini mendorong penguatan tata kelola keselamatan melalui integrasi aspek teknis, manusia, dan organisasi, termasuk penyempurnaan SOP, desain alarm yang lebih *human-centric*, serta program pelatihan berkelanjutan. **Keempat**, pendekatan mitigasi berbasis *Critical Control Management* memungkinkan perusahaan meningkatkan kepatuhan terhadap regulasi keselamatan pertambangan dan meminimalkan potensi *cascade failure* yang dapat mengganggu keselamatan pekerja dan kontinuitas operasional.

Penelitian ini memiliki beberapa keterbatasan yang perlu dicermati dalam interpretasi hasil. **Pertama**, studi ini difokuskan pada satu kasus implementasi sistem keselamatan pertambangan berbasis IoT di PT X, sehingga penerapan temuan pada konteks pertambangan lain perlu mempertimbangkan perbedaan karakteristik operasi dan lingkungan. **Kedua**, penilaian risiko dan validasi mitigasi dilakukan berdasarkan expert judgment melalui FGD, yang meskipun telah melibatkan lintas fungsi dan mekanisme konsensus, tetap merefleksikan kondisi operasional pada periode penelitian. **Ketiga,** analisis yang dilakukan bersifat statis dan belum menangkap dinamika risiko jangka panjang, seperti degradasi sistem atau perubahan pola ancaman siber. Meskipun demikian, pendekatan FMEA–FTA yang digunakan tetap memberikan kerangka analisis yang kuat, terstruktur, dan relevan untuk memahami serta mengelola risiko sistemik pada sistem keselamatan digital pertambangan.

5.2 Saran

Berdasarkan hasil temuan dan pembahasan, penelitian ini memberikan gambaran komprehensif mengenai risiko, akar penyebab, dan strategi mitigasi pada implementasi sistem digitalisasi keselamatan pertambangan berbasis IoT. Meskipun demikian, masih terdapat ruang pengembangan yang dapat memperkaya pemahaman dan meningkatkan efektivitas sistem keselamatan digital di masa mendatang. Oleh karena itu, penelitian lanjutan perlu diarahkan untuk memperdalam aspek implementatif dan faktor manusia yang sangat memengaruhi keberhasilan sistem. Dua arah penelitian berikut direkomendasikan sebagai tindak lanjut.

1. **Evaluasi Efektivitas Mitigasi melalui Implementasi *Pilot Project* Sistem IoT**

   Penelitian lanjutan dapat difokuskan pada pengujian langsung efektivitas rekomendasi mitigasi dalam skala pilot project atau testbed di area tambang nyata. Pendekatan ini memungkinkan peneliti untuk menilai kinerja sensor, algoritma deteksi, rangkaian alarm, serta stabilitas jaringan dalam kondisi lapangan yang dinamis. Evaluasi berbasis praktik ini dapat menghasilkan pembaruan strategi mitigasi yang lebih adaptif dan kontekstual, sekaligus memberikan pemahaman yang lebih baik mengenai performa sistem digital keselamatan secara real-time.

2. **Kajian Mendalam Mengenai Faktor Manusia, Literasi Digital, dan Ergonomi Kognitif**

   Penelitian selanjutnya juga perlu menyoroti aspek manusia sebagai komponen kritis dalam keberhasilan implementasi sistem keselamatan digital. Fokus dapat diarahkan pada analisis kesiapan digital operator, beban kognitif, persepsi risiko, dan fenomena seperti alarm fatigue yang mempengaruhi akurasi respons operator. Metode seperti *Human Reliability Analysis* (HRA), *Cognitive Task Analysis* (CTA), atau asesmen ergonomi kognitif dapat digunakan untuk memahami pola interaksi manusia dan mesin lebih mendalam. Hasil penelitian ini akan mendukung pengembangan desain

antarmuka, SOP operasional, serta program pelatihan yang lebih intuitif, efektif, dan berpusat pada pengguna.

DAFTAR PUSTAKA

Adiraja. (2024). *Internet of Things (IoT) dalam Keselamatan Pertambangan*. Retrieved from dari https://adiraja-integrasi.com/internet-of-things-iot-dalam-keselamatan-pertambangan/

Agstyawardhana, P. P., Puspita, I. A., & Yasa, P. (2024). Perancangan Risk Register dan Risk Treatment Berbasis ISO 31000:2011 pada Proyek Join Planning Program (JPP) Tahap 2 pada PT XYZ menggunakan FMEA.

Agusti , J. R., Harahap, U. N., & Hasibuan, Y. M. (2025). Implementation of Failure Mode and Effect Analysis for Minimizing Defects. *Jurnal Teknik Industri*.

Alijoyo, A., Wijaya, B., & Jacob, I. (2020). *Fault Tree Analysis (Analisis Pohon Kesalahan)*. CRMS.

Al-Masri, E., Thangavel, T., & Kaddoum, G. (2023). Investigating Messaging Protocols for the Internet of Things (IoT). *IEEE Access*, 10850-10862.

Andrade, R., & et al. (2022). Factors of Risk Analysis for IoT Systems . *MDPI*, 162.

Andrade, R., Ortiz-Garces, I., Tintin, X., & Lluminquinga, G. (2022). Factors of Risk Analysis for IoT Systems . *MDPI*, 162.

Arikunto, S. (2013). *Prosedur Penelitian: Suatu Pendekatan Praktik.* Jakarta: Rineka Cipta.

Atzori, L. L., & Morabito, G. (2017). The Internet of Things: A survey. Computer Networks.

Barnett, W. D. (1995). Application of QFD to The Software Development Process. *International Journal of Quality & Reliability Managament, Vol. 12*.

Basyaib, F. (2007). *Manajemen resiko.* Grasindo.

Boopathy, V., & et al. (2024). Lorawan based Coalminers Rescue and Health Monitoring System Using IoT. *Technical Science* .

Borys, D. (2020). The Impact of Safety Management Systems on Organizational Performance in the Mining Industry. *Journal of Safety Research*, 123-130.

Bosch, S., de Menezes, R., & Pees, S. (2022). Electronic nose sensor drift affects diagnostic reliability in respiratory disease screening. *MDPI*.

Bui, N. Q., Nguyen, D. T., & Pham, H. Q. (2022). Digital Transformation in Mining Industry: Challenges and Solutions through IoT. *Journal of Mining Science and Technology*, 102-112.

Bui, N., & Zorzi, M. (2022). Health and Safety Monitoring in Mines using IoT: Challenges and Opportunities. *IEEE Internet of Things Journal* .

Bui, T. T., & Zorzi, M. (2017). The Role of IoT in Industrial Safety: Real Time Data and Decision Support Systems. *IEEE Internet of Things Journal*, 547-556.

Chen, C. (2019). Safety Culture and Its Impact on Safety Performance in the Mining Industry . *Journal Safety Science*, 1-9.

COSO ERM . (2017). *Enterprise Risk Management: Integrating with Strategy and Performance.* Committee of Sponsoring Organizations of the Treadway Commision .

Cronbach, L. J. (1951). Coefficient Alpha and the Internal Structure of Tests. *Psychometrika*, 297-334.

Cvach, M. (2012). Monitor alarm fatigue: An integrative review. *Biomedical Instrumentation & Technology*, 268-277.

Deloitte. (2022). *The Future of Mining: Digitally Enabled Workforce in the Age of Automation*. Retrieved from Deloitte Insights: https://www2.deloitte.com

El-Awady, S. M. (2023). Overview of Failure Mode and Effects Analysis (FMEA): A Patient Safety Tool. *National Center for Biotechnology Information*, 24-26.

ENISA. (2019). Good Practices for Security of IoT – Secure Software Development Lifecycle. . *European Union Agency for Cybersecurity*.

Fauzi, M. A., Setiawan, W., & Duha, T. (2024). Implementasi Teknologi Big Data di Era Digital. . *Jurnal Ilmiah Ilmu Pendidikan*, 22-30.

Fauzi, M. A., Setiawan, W., Dewi, E., & Duha, T. (2024). Implementasi Teknologi Big Data di Era Digital. *Jurnal Ilmiah Ilmu Pendidikan*, 22-30.

George, D., & Mallery, P. (2003). *SPSS for Windows Step by Step: A Simple Guide and Reference, 11.0 Update.* Boston: Allyn & Bacon.

GlobalData. (2025). IoT enhances productivity, safety, and ESG compliance for the mining sector. *Mine*.

Gupta, S., Bose, I., & Kaur, R. (2024). IoT and AI-driven Safety Monitoring in Mining Operations: An Industry 4.0 Approach. *International Journal of Mining Science and Technology*.

Hadipuro, A., Yulianto, F., & Rachman, A. (2023). Evaluasi Risiko Kecelakaan Tambang menggunakan FMEA dan FTA. *Jurnal Keselamatan Kerja Indonesia*, 25-34.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2014). *Multivariate Data Analysis (7th Edition)*. Pearson Education Limited .

Helbing, D. (2013). Globally Networked Risk and How to Respond. *Nature*, 51-59.

Hidayat, M. (2019). Pengoperasian Alat Berat Tambang dan Keselamatan Kerja. *Jurnal Teknik Mesin* , 153-158.

Hidayat, M. (2019). Pengoperasian Alat Berat Tambang dan Keselamatan Kerja. *Jurnal Teknik Mesin*, 153-158.

Hindustan Zinc Limited (HZL). (n.d.). *Emerging Risk and Strategic Response*. Retrieved from UAT Environment: rdxuat.com

Hosain, M., Ahmad, I., Habibi, D., & Wagas, M. (2024). Enhancing IoT sensors precision through sensor drift calibration with variational autoencoder. *IEEE Internet of Things Journal*.

Hossain, M., Ahmad, I., Habibi, D., & Waqas, M. (2024). Enhancing IoT sensors precision through sensor drift calibration with variational autoencoder. *IEEE Internet of Things Journal*.

Hutchins, G. (2018). *ISO 31000: 2018 enterprise risk management.* Greg Hutchins.

ICMM . (2021). *Critical Control Management: Good Practice Guide.* London: International Council on Mining and Metals.

ICMM. (2020). Good Practice Guidance on Health and Safety in Mining.

ICMM. (2023). Safety Performance Report . *International Council Mining and Metals*.

IEC. (2006). *Fault Tree Analysis (FTA).* International Electrotechnical Commision, IEC 61025.

IEC. (2010). IEC 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems. *International Electrotechnical Commission*.

IEC. (2018). *Analysis Techniques for System Reliability - Procedure for Failure Mode and Effects Analysis (FMEA).* International Electrotechnical Commision 60812.

ISO. (2003). ISO 13374-1: Condition Monitoring and Diagnostics of Machines - Part 1: General Guidelines. *International Organization for Standardization.*

ISO. (2008). ISO/IEC 27005: Information Security Risk Management. *International Organization for Standardization*.

ISO. (2013). ISO 27701: Security Techniques — Privacy Information Management. ISO. *International Organization for Standardization*.

ISO 27005. (2018). Information Security Risk Management.

ISO 31000. (2018). *Risk Management - Guidelines.* International Organization for Standardization.

ISO 31010. (2019). *Risk Management - Risk Assessment Techniques.* International Organization for Standardization.

ISO 45001. (2018). *Occupational Health and Safety Management Systems - Requirements with Guidance for Use.* Geneva: International Organization for Standardization.

James, B. A., Putri, E. L., Zalianti, N. R., & Wijonarko, P. (2023). Perancagan Sistem Smart Mining untuk Industri Pertambangan Batu Bara. *Jurnal Kajian Teknik Elektro*, 116-124.

Karim, M. R., Kabir , S., Lei, C., Lefticaru, R., & Baset, M. A. (2025). A Combined Approach to Safety and Security of IoT by Applying Fault Tree Analysis and Attack Trees with Minimal Cut Sets . *AVITEC*.

Kemnaker. (2023). Laporan Kecelakaan Kerja Tahun 2023. *Kementerian Ketenagakerjaan RI*.

Khanna, A., & Kaur, S. (2019). IoT-based monitoring in hazardous industrial environments. *IEEE Access*.

Kumar, R., Gupta, V., & Singh, P. (2021). Impact of system failures on operational reliability, financial performance, and worker trust in digital safety systems. *International Journal of Industrial Safety Engineering*, 45-59.

Kurniawan, A., & Hasan, R. (2022). Integrasi FMEA dan FGD untuk Pengendalian Risiko Industri Tambang. *Jurnal Keselamatan Tambang*, 12-26.

Lai-Kow, C. &.-L. (2002). *Quality function deployment: A literature review.* European Journal of Operational Research.

Leimester, J. M., & Kolios, A. (2018). Digital Infrastructure Risks in Industriak IoT Applications. *Journal of Risk Analysis and Management*, 78-89.

Leimester, J. M., & Kolios, A. (2018). Digital Transformation and the Future of Work: Impact and Challenges. *Business & Information Systems Engineering*, 275-278.

Leveson, N. (2016). *Engineering a Safer World: Systems Thinking Applied to Safety.* MIT Press.

Longyu, L., Jianxin, Y., & Tao, X. (2025). Risk Analysis of Digital Twin Project Operation Based on Improved FMEA Method. *MDPI*, 48.

Medina, F., Ruiz, H., Espindola, J., & Avendano, E. (2024). Deploying IIoT Systems for Long-Term Planning in Underground Mining: A Focus on the Monitoring of Explosive Atmospheres. *MDPI*.

Nguyen, V. T., & Nguyen, C. T. (2023). The Effect of Structural Equation Modeling on Chatbot Usage: An Investigation of Dialogflow. *International Journal of Applied Information Technology*.

NIST. (2020). NISTIR 8259: Foundational Cybersecurity Activities for IoT Device Manufacturers. *National Institute of Standards and Technology*.

NS, M. A. (2022). Pemanfaatan Teknologi Digitalisasi Dalam Aktivitas Konservasi Batubara Di Area Kerja PT. Berau Coal dan PT. Pamapersada Nusantara. *Prosiding Temu Profesi Tahunan PERHAPI*, 45-56.

Phong, N. D., Tuyen, U. Q., & Osinski, P. (2024). Risk Warning Systems for Underground Mining Using IoT Solutions: A Case Study . *International Journal of GEOMATE*, 119.

PMBOK . (2021). *A Guide to the Project Management Body of Knowledge (7th ed)*. Project Management Institute.

PMI. (2000). *A Guide to the Project Management Body of Knowledge (PMBOK Guide)*. Project Management Institute.

Polit, D. F., & Beck, C. T. (2012). *Nursing Research: Generating and Assessing Evidence for Nursing Practice (9th Edition)*. Lippincott Williams & Wilkins.

Prawiyogi, A. G. (2023). Perkembangan Internet of Things (IoT) pada Sektor Energi: Sistematik Literatur Review. *Jurnal MENTARI: Manajemen, Pendidikan dan Teknologi Informasi*, 187-197.

Purnomo, A. (2023). Studi Strategi Implementasi Teknologi IoT di Pertambangan Terpencil. *Jurnal Teknologi dan Industri*, 101-110.

Rahman, M., Zhang, R., Gladstone, D., Williams, B., Chen, E., Dexter, C., et al. (2021). Failure Mode and Effects Analysis (FMEA) for Experimental Use of FLASH on a Clinical Accelerator. *arXiv*.

Reason, J. . (2016). Organizational accidents revisited. *Safety Science*.

Ridwan, M., Frinaldi, A., Rembrandt, & Lanin, D. (2024). Evaluasi Efektivitas Kebijakan Publik dalam Penanggulangan Risiko Kebakaran di Industri Smelter. Studi Kasus Smelter Morowali. *Jurnal Ilmiah Innovative*, 43-55.

Ridwan, M., Frinaldi, A., Rembrandt, & Lanin, D. (2024). Evaluasi Efektivitas Kebijakan Publik dalam Penanggulangan Risiko Kebakaran di Industri Smelter: Studi Kasus Smelter Morowali. *Jurnal Ilmiah Innovative*, 43-55.

Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed IoT. *Computer Networks*.

Sahanaa, S., & Murugan, M. (2023). Analisis Risiko Keselamatan pada Aktivitas Penambangan Batu Bara. *Jurnal Ilmiah Permas*, 1235-1245.

Sahanaa, S., & Murugan, M. (2023). Analisis Risiko Keselamatan pada Aktivitas Penambangan Batu Bara. *Jurnal Ilmiah Permas*, 1235-1245.

Salim, B. S., Ratnaningsih, A., & Arifin , S. (2024). Analisis Akar Penyebab Risiko K3 Pelaksanaan Pekerjaan Abuntment dan Pemasangan Girder Metode FTA Proyek Tol Solo – NYIA Kulon Progo.

Saxena, N., Tiwari, A., & Chatterjee, R. (2023). Recent Advancements in IoT Implementation for Environmental Safety and Production Monitoring in Underground Mines. *Journal of Cleaner Production*.

Singh, R., & Rathore, A. (2021). Sensor Calibration and Data Accuracy in Industrial IoT: A Practical Guide. *Industrial Journal of Industrial Informatics* , 45-57.

Singh, S., & Rathore, V. S. (2021). A Review on IoT based Safety Monitoring Systems in Mining: Technology, Application, and Challenges. *International Journal of Mining Science and Technology*, 201-212.

Stamatis, D. H. (2003). *Failure Mode and Effect Analysis: FMEA from Theory to Execution.* ASQ Quality Press.

Stamatis, D. H. (2003). *Failure Mode and Effect Analysis: FMEA from Theory to Execution (2nd edition).* ASQ Quality Press.

Sugiyono. (2017). *Metode Penelitian Kuantitatif, Kualitatif, dan R&D.* Bandung: Alfabeta .

Sugiyono. (2022). *Metode Penelitian Kuantitatif, Kualitatif, R&D.* Bandung: Alfabeta.

Surya, M. R. (2019). Perencanaan Strategis Sistem Informasi dan Teknologi Informasi pada Perusahaan Jasa Event Organizer PT. X. *Institut Teknologi Sepuluh*.

Syahbana, G., Puspita, I. A., & Widyasthana, S. (2021). Perancangan risk responses untuk menghadapi risiko yang terjadi pada proyek digitalisasi SPBU Pertamina menggunakan metode FMEA di PT Telkom.

Tarafdar, M., Cooper, C., & Stich, J. (2019). The technostress trifecta—Techno-eustress, techno-distress, and design: Theoretical directions and an agenda for research. *Journal of Management Information Systems*, 6-42.

Tarafdar, M., Pullins, E., & Ragu-Nathan, T. (2019). Technostress and job outcomes. *Journal of Management Information Systems*.

Vesely, W. E. (1981). *Fault Tree Handbook.* U.S: Nuclear Regulatory Commision.

Vesely, W. E., Goldberg, F. F., Roberts, N. H., & Haasl, D. F. (1981). *Fault Tree Handbook.* US: Nuclear Regulatory Commision.

Ward, J. G. (2002). *Strategic planning for information systems (Vol. 3).* Chichester: Wiley.

World Mining Data. (2023). *World Mining Data 2023.* Austrian Federal Ministry of Finance.

Wu, T., & et al. (2023). Data quality challenges in IoT-based environmental monitoring systems: A systematic survey. *Water, Air, & Soil Pollution*.

Xu, Y., Li, H., & Zhao, X. (2022). Challenges and risks of IoT adoption in heavy industry: Device reliability, network constraints, legacy system integration, and cybersecurity threats. *Journal of Industrial Information Integration*, 100-118.

Yani, H. (2012). *Design For Six Sigma untuk Perancangan Layanan Online Melalui Media Fan Page Facebook.* Indonesia: Universitas Katolik Parahyangan.

You, J., Lou, S., Mao, R., Xu, T., & et al. (2023). An improved FMEA quality risk assessment framework for enterprise data assets. *Information Processing & Management*.

Zhang, A., Wang, B., & Li, C. (2023). A Hybrid STPA-FMEA Approach for Industrial IoT System Risk Analysis. *Sensors*, 4664-4678'.

Zhang, Y., Yang, Q., & Chen, L. (2014). Environmental effects on industrial sensor accuracy. *IEEE Sensors Journal*.

Zhou, C., Liu, D., & Li, Y. (2020). Real Time Safety Monitoring in Underground Mining using IoTand Data Analytics . *Journal of Safety Research*, 135-145.

Zhou, Q., Ding, L., & Luo, H. (2020). Application of IoT in Underground Mining: A Review. *Automation in Construction* , 112.

Zohar, D., & Luria, G. (2019). The Effect of Safety Climate on Safety Performance: A Meta-Analysis. *Journal of Occupational Health Psychology*, 1-15.

LAMPIRAN

Lampiran 1 Kuesioner Penelitian

KUESIONER PENELITIAN TESIS

Your email will be recorded when you submit this form

* Indicates required question

BAGIAN I. PROFIL RESPONDEN

Nama Responden *

Your answer

Divisi / Departemen *

- Mining Innovation & Digitalization
- Mining Operation
- Safety, Health, & Environment

Jabatan *

- Direksi / Eksekutif Senior
- Manajerial Tinggi (General Manager, Senior Manager, Head of Department, Kepala Teknis Tambang)
- Manajer Menengah / Supervisi (Superintendent, Supervisor, Section Head, Foreman)
- Staf Operasional / Spesialis (Engineer, Analyst, Operator, Technician)
- Tim Pendukung & Administrasi (Staff)

Pengalaman Kerja di Pertambangan *

- < 2 Tahun
- 2 - 5 Tahun
- 6 - 10 Tahun
- > 10 Tahun

Keterlibatan dalam Implementasi IoT *

- Sangat Terlibat
- Terlibat
- Cukup Mengetahui
- Tidak Terlibat

BAGIAN II. PETUNJUK PENGISIAN SKALA FMEA 1-5

Parameter Severity (S) yaitu keparahan dari suatu dampak yang ditimbulkan oleh risiko.

Parameter	Skor	Skala Pengukuran	Deskripsi
S (*Severity*) Tingkat keparahan dampak	1	**Dampak Sangat Rendah**	Tidak ada dampak yang terukur pada fungsi, keselamatan, atau operasional (tidak ada cedera / hanya *near miss (first aid case)*.
	2	**Dampak Rendah / Minor**	Dampak kecil, dapat diperbaiki dengan cepat, tidak mempengaruhi fungsi keselamatan utama. Misalnya hanya cedera ringan (MTC - *Medical Treatment Case*) atau perbaikan kecil pada sistem IoT.
	3	**Dampak Sedang / Moderate**	Fungsi keselamatan terganggu sementara atau sebagian seperti cedera sedang (RWC - *Restricted Work Case*), gangguan operasional, atau mengalami potensi kerugian.
	4	**Dampak Tinggi / Serius**	Dampak signifikan yang mempengaruhi fungsi keselamatan utama seperti risiko cedera permanen (LTI - *Lost Time Injury*), kerugian asset, atau downtime.
	5	**Dampak Sangat Tinggi / Kritis**	Risiko fatal (kegiatan operasional dihentikan / adanya kecelakaan serius / kematian).

Parameter Occurance (O) yaitu frekuensi terjadinya kegagalan berdasarkan satuan waktu tertentu.

Parameter	Skor	Skala Pengukuran	Deskripsi
O (*Occurance*) Frekuensi kejadian	1	**Sangat rendah**	Kemungkinan terjadi sangat kecil atau belum pernah terjadi dalam sejarah.
	2	**Rendah**	Kegagalan jarang terjadi dalam frekuensi tahunan.
	3	**Sedang**	Kegagalan mungkin terjadi secara berkala dalam frekuensi triwulan.
	4	**Tinggi**	Kegagalan sering terjadi atau sangat mungkin terjadi pada setiap bulan.
	5	**Sangat Tinggi**	Kegagalan hampir pasti terjadi atau terjadi secara terus menerus setiap minggu.

Parameter Detection (D) yaitu penilaian terhadap seberapa baik tingkat pengendalian dan pengawasan untuk mendeteksi risiko yang dapat terjadi sebelum efek tersebut dirasakan oleh konsumen.

Parameter	Skor	Skala Pengukuran	Deskripsi
D (*Detection*) Kemungkinan deteksi kontrol	1	**Sangat Tinggi** (Sangat mudah terdeteksi)	Deteksi kegagalan otomatis dengan sistem *fail-safe* dengan kontrol kualitas yang ketat dan deteksi real-time yang teruji.
	2	**Tinggi** (Mudah terdeteksi)	Deteksi cukup baik dan andal, dimana kontrol otomatis atau prosedur checklist harian sangat disiplin.
	3	**Sedang**	Deteksi memerlukan usaha / deteksi tidak otomatis atau mungkin terlambat.
	4	**Rendah** (Sulit dideteksi)	Deteksi sangat sulit sehingga butuh pengawasan / test khusus.
	5	**Sangat Rendah** (Hampir tidak bisa terdeteksi)	Kegagalan tidak mungkin terdeteksi/terkontrol karena tidak ada sistem/prosedur deteksi yang relevan atau kontrol yang sudah ada tidak berfungsi.

Back Next Clear form

Lampiran 2 Pertanyaan pada Kuesioner Penelitian

BAGIAN III. TABEL PENILAIAN RISIKO IMPLEMENTASI PROYEK DIGITALISASI SISTEM KESELAMATAN PERTAMBANGAN PADA PT. X

X1: Reliability Sensor

X1.1 Sensor gagal membaca parameter keselamatan secara akurat *

	1	2	3	4	5
S: Jika sensor memberikan pembacaan tidak akurat, seberapa serius dampak pada keselamatan operasional?	○	○	○	○	○
O: Seberapa sering sensor memberikan pembacaan tidak akurat?	○	○	○	○	○
D: Seberapa mudah ketidaktepatan pembacaan terdeteksi sebelum menyebabkan insiden?)	○	○	○	○	○

X1.2 Sensor mengalami downtime atau putus koneksi berulang *

	1	2	3	4	5
S: Apabila sensor offline, seberapa serius konsekuensi terhadap sistem keselamatan?	○	○	○	○	○
O: Seberapa sering sensor mengalami downtime/ putus koneksi?	○	○	○	○	○
D: Seberapa mudah terdeteksi bahwa sensor sedang offline	○	○	○	○	○

X1.3 Sensor menghasilkan data fluktuatif tanpa korelasi *

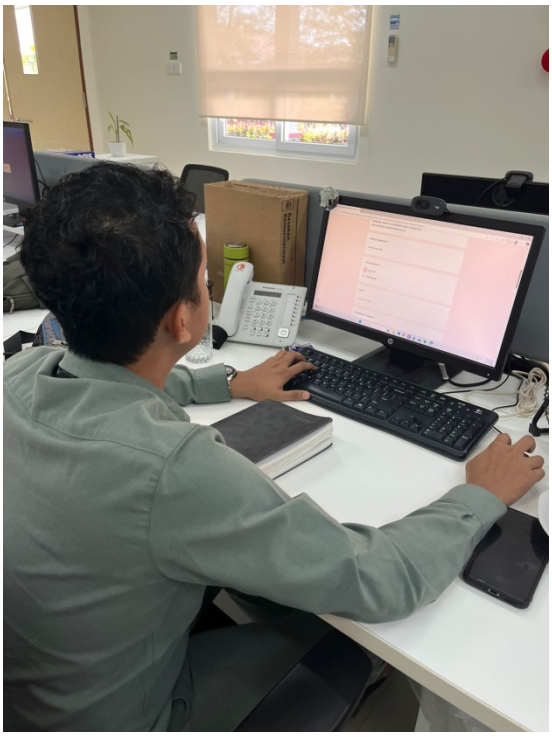
	1	2	3	4	5
S: Jika data sensor fluktuatif, seberapa besar akibatnya terhadap pengambilan keputusan keselamatan?	○	○	○	○	○
O: Seberapa sering terjadi fluktuasi data yang tidak sesuai kondisi nyata?	○	○	○	○	○
D: Seberapa mudah operator/ algoritma mendeteksi fluktuasi palsu sebelum mengambil tindakan?	○	○	○	○	○

X1.4 Sensor mengalami drift performa seiring waktu *

	1	2	3	4	5
S: Jika sensor mengalami drift, seberapa besar dampaknya terhadap akurasi pengawasan?	○	○	○	○	○
O: Seberapa sering terjadi drift performa pada sensor di lapangan?	○	○	○	○	○
D: Seberapa mudah drift teridentifikasi melalui prosedur kalibrasi atau pemeriksaan rutin?	○	○	○	○	○

Lampiran 3 Dokumentasi Pengisian Kuesioner pada PT X


SOLUSI
KIDECO



Lampiran 4 Dokumentasi FGD dengan PT X secara Online