# CABARAN MIGRASI KE SENIBINA PATUH KESELAMATAN SIBER IEC62443 DALAM RANGKAIAN OT-IT SEKTOR MINYAK DAN GAS



UMAIR BIN BADROL

UNIVERSITI KEBANGSAAN MALAYSIA

# CABARAN MIGRASI KE SENIBINA PATUH KESELAMATAN SIBER IEC62443 DALAM RANGKAIAN OT-IT SEKTOR MINYAK DAN GAS

UMAIR BIN BADROL



PROJEK YANG DIKEMUKAKAN UNTUK MEMENUHI SEBAHAGIAN
SYARAT MEMPEROLEH IJAZAH SARJANA KESELAMATAN SIBER

FAKULTI TEKNOLOGI DAN SAINS MAKLUMAT
UNIVERSITI KEBANGSAAN MALAYSIA
BANGI

2023

**PENGAKUAN**

Saya akui karya ini adalah hasil kerja saya sendiri kecuali nukilan dan ringkasan yang tiap-tiap satunya telah saya jelaskan sumbernya.

24 Ogos 2023

UMAIR BIN BADROL
P103234

## PENGHARGAAN

Dengan nama Allah yang Maha Pengasih lagi Maha Penyayang. Saya panjatkan rasa syukur kepada Allah S.W.T, kerana dengan rahmat dan keizinanNya, saya berjaya menyiapkan kajian ini dalam tempoh yang ditetapkan untuk melengkapkan pembelajaran saya dalam bidang sarjana ini.

Saya ingin merakamkan rasa penghargaan dan ucapan terima kasih saya kepada Dr. Wan Fariza Paizi@Fauzi, sebagai penyelia projek yang telah memberikan petunjuk dan bimbingan yang berharga sepanjang proses pelaksanaan kajian ini. Saya juga ingin mengucapkan terima kasih kepada koordinator program, semua pensyarah dan staf Fakulti Teknologi dan Sains Maklumat (FTSM), Universiti Kebangsaan Malaysia yang telah banyak membantu saya, baik secara langsung mahupun tidak langsung dalam menyelesaikan kajian saya.

Penghargaan dan terima kasih juga saya sampaikan kepada ketua jabatan saya yang telah memberikan izin kepada saya untuk melanjutkan pelajaran dalam bidang sarjana ini.

Saya juga ingin merakamkan ucapan terima kasih kepada ibu bapa, isteri, dan keluarga yang saya sayangi atas dorongan dan pengorbanan masa yang telah diberikan dalam menyiapkan kajian ini. Segala jasa dan bakti anda akan dikenang hingga ke akhir hayat saya. Akhir sekali, saya berharap semoga projek ini dapat memberikan manfaat kepada industri dan juga kepada penyelidik-penyelidik lain yang akan menggunakan kajian ini sebagai rujukan pada masa depan.

**ABSTRAK**

Kajian ini memberi tumpuan kepada cabaran-cabaran yang dihadapi semasa proses integrasi rangkaian Teknologi Operasi (OT) dan Teknologi Maklumat (IT) dalam sektor Infrastruktur Kritikal Negara, khususnya dalam Loji Minyak dan Gas. Kajian ini berakar umbi daripada pengalaman dan pemerhatian langsung penyelidik semasa proses migrasi daripada seni bina sistem kawalan sedia ada kepada seni bina yang mematuhi piawaian IEC62443. Reka bentuk kajian melibatkan metodologi kajian kes, dengan momfokuskan kepada salah satu sektor Infrastruktur Kritikal Negara, iaitu industri Minyak dan Gas. Pengalaman langsung penyelidik dalam menganalisa, merancang, melaksana dan mengetuai proses integrasi dan migrasi telah didokumenkan dan dianalisis. Pengumpulan data melibatkan dokumentasi terperinci proses migrasi, termasuk cabaran-cabaran yang dihadapi, kerumitan teknikal dan kekangan sumber. Data yang dikumpul telah dianalisa secara menyeluruh menggunakan pendekatan kualitatif. Penyelidik menyemak dan meneliti cabaran yang didokumenkan dengan teliti untuk mengenal pasti tema, corak dan faktor berulang yang muncul semasa proses migrasi. Analisis tersebut memberikan pemahaman menyeluruh tentang cabaran yang terlibat ketika proses migrasi kepada seni bina yang mematuhi IEC62443 di Loji Minyak dan Gas. Empat cabaran utama telah dikenal pasti semasa kajian: objektif keselamatan IT (CIA) yang berbeza berbanding OT (AIC), kekurangan kompetensi, cabaran mengendali sistem OT legasi dan proprietari, dan kesukaran teknikal dalam melaksanakan keperluan piawaian. Penemuan kajian menyumbang kepada pemahaman tentang cabaran yang dihadapi dalam menyepadukan lapisan OT, berdasarkan model Purdue, dengan mematuhi piawaian IEC62443. Rumusan yang diperoleh akan membantu pihak berkepentingan industri, termasuk pembuat keputusan, profesional dan pengamal, dalam membangunkan strategi dan pendekatan yang berkesan untuk mengatasi cabaran ini dan mewujudkan seni bina rangkaian OT-IT yang selamat dalam sektor Infrastruktur Kritikal Negara. Kajian ini mempunyai implikasi yang lebih luas untuk keselamatan negara dan keselamatan awam, menyumbang kepada pengukuhan postur keselamatan siber keseluruhan Infrastruktur Kritikal Negara.

# CHALLENGES IN MIGRATING TO IEC62443 CYBER SECURITY COMPLIANT ARCHITECTURE FOR OPERATION TECHNOLOGY (OT) – INFORMATION TECHNOLOGY (IT) NETWORK IN OIL & GAS SECTOR

## ABSTRACT

This research focuses on the challenges encountered during the integration of Operational Technology (OT) and Information Technology (IT) networks in the Oil and Gas sector, particularly within national critical infrastructure plants. The study is rooted in the researcher's firsthand experience and observations during the migration process from existing control system architecture to an IEC62443 compliant architecture. The research design incorporates a case study methodology, focusing on a specific national critical infrastructure plant within the Oil and Gas sector. The researcher's firsthand experience in planning, implementing, and navigating the challenges of the migration has been documented and analyzed. The data collection involved detailed documentation of the migration process, including the encountered challenges, technical complexities, compatibility issues, and resource constraints. The collected data was subjected to a thorough analysis using a qualitative approach. The researcher carefully reviewed and examined the documented challenges to identify recurring themes, patterns, and factors that emerged during the migration process. The analysis provided a comprehensive understanding of the challenges involved in migrating to IEC62443 compliant architectures in national critical infrastructure plants. Four major challenges were identified during the research: different security objectives of IT (CIA) vs OT (AIC), skill gaps of personnel, managing legacy and proprietary systems, and technical issues in complying to IEC62443 requirements throughout the migration process. The different security objectives of IT and OT posed a significant challenge in implementing security measures that meet the needs of both IT and OT, while the skill gaps led to multiple misunderstandings. Managing legacy and proprietary systems was another major challenge, as these systems were not designed with cybersecurity in mind and were difficult to secure. Technical complexities in managing integration and migration of multiple different protocols add to the challenges faced. The research findings contribute to the understanding of the complexities involved in integrating OT layers, based on the Purdue model, in compliance with the IEC62443 Standards. The insights gained will assist industry stakeholders, including decision-makers, professionals, and practitioners, in developing effective strategies and approaches to overcome these challenges and establish secure OT-IT network architecture within national critical infrastructure plants. The research has broader implications for national security and public safety, contributing to strengthening the overall cybersecurity posture of the nation's critical infrastructure.

# KANDUNGAN

**Halaman**


| | | |
|---|---|---|
| **PENGAKUAN** | | **ii** |
| **PENGHARGAAN** | | **iii** |
| **ABSTRAK** | | **iv** |
| **ABSTRACT** | | **v** |
| **KANDUNGAN** | | **vi** |
| **SENARAI JADUAL** | | **x** |
| **SENARAI ILUSTRASI** | | **xi** |
| **SENARAI SINGKATAN** | | **xii** |
| **BAB I** | **PENGENALAN** | |
| 1.1 | Pendahuluan | 1 |
| 1.2 | Latar Belakang Kajian | 2 |
| 1.3 | Penyataan Masalah | 3 |
| 1.4 | Objektif Kajian | 4 |
| 1.5 | Persoalan Kajian | 4 |
| 1.6 | Kepentingan Kajian | 4 |
| 1.7 | Skop Kajian | 6 |
| 1.8 | Struktur Penulisan | 6 |
| | 1.8.1 Bab I Pengenalan | 7 |
| | 1.8.2 Bab II Kajian Kesusasteraan | 7 |
| | 1.8.3 Bab III Kaedah Kajian | 7 |
| | 1.8.4 Bab IV Hasil Kajian | 7 |
| | 1.8.5 Bab V Kesimpulan dan Cadangan | 7 |
| 1.9 | Kesimpulan | 7 |
| **BAB II** | **KAJIAN KESUSASTERAAN** | |
| 2.1 | Pengenalan Kepada Integrasi Teknologi Operasi (OT) – Teknologi Maklumat (IT) | 9 |
| | 2.1.1 Definisi dan Kepentingan Integrasi OT-IT | 9 |
| | 2.1.2 Evolusi Integrasi OT-IT | 10 |
| | 2.1.3 Trend Semasa dalam Integrasi OT-IT | 10 |
| 2.2 | Seni Bina Model Purdue Untuk Hierarki Kawalan | 11 |

| | | | |
|---|---|---|---|
| | 2.2.1 | Gambaran Keseluruhan Model Purdue | 11 |
| | 2.2.2 | Peranan Model Purdue dalam Integrasi OT-IT | 16 |
| | 2.2.3 | Aplikasi Model Purdue dalam Pelbagai Sektor | 17 |
| 2.3 | Piawaian IEC62443 Untuk Keselamatan Siber Rangkaian Komunikasi Industri | | 18 |
| | 2.3.1 | Piawaian IEC62443: CSMS yang Disesuaikan Untuk IACS | 19 |
| | 2.3.2 | Piawaian Berkaitan yang Lain | 22 |
| | 2.3.3 | Kepentingan IEC62443 dalam Integrasi OT-IT | 23 |
| 2.4 | Permasalahan Rintangan dalam Integrasi OT-IT | | 24 |
| | 2.4.1 | Kerumitan Teknikal dalam Integrasi OT-IT | 24 |
| | 2.4.2 | Isu Keserasian dalam Integrasi OT-IT | 24 |
| | 2.4.3 | Kekangan Sumber dalam Integrasi OT-IT | 25 |
| | 2.4.4 | Risiko Keselamatan dan Ancaman Siber | 25 |
| | 2.4.5 | Faktor Organisasi dan Budaya | 25 |
| | 2.4.6 | Permasalahan Kawal Selia | 26 |
| | 2.4.7 | Obsolesi Sistem Legasi | 26 |
| 2.5 | Peranan Kakitangan dalam Integrasi OT-IT | | 26 |
| | 2.5.1 | Perbezaan dalam Pengetahuan, Keutamaan dan Amalan antara OT dan Kakitangan IT | 27 |
| | 2.5.2 | Kesan Perbezaan Skil dan Keutamaan Kakitangan terhadap Integrasi OT-IT | 28 |
| 2.6 | Integrasi OT-IT dalam Sektor Minyak dan Gas | | 28 |
| | 2.6.1 | Gambaran Keseluruhan Integrasi OT-IT dalam Sektor Minyak dan Gas | 28 |
| | 2.6.2 | Integrasi OT-IT dalam Sektor Minyak dan Gas dan Sektor Infrastruktur Kritikal Lain | 29 |
| 2.7 | Keselamatan Siber dalam Integrasi OT-IT | | 30 |
| | 2.7.1 | Kepentingan Keselamatan Siber dalam Integrasi OT-IT | 31 |
| | 2.7.2 | Landskap Ancaman Siber dalam Integrasi OT-IT | 31 |
| 2.8 | Pematuhan Piawaian Industri dalam Integrasi OT-IT | | 32 |
| | 2.8.1 | Kepentingan Pematuhan Piawaian Industri | 32 |
| | 2.8.2 | Usaha dalam Pematuhan Piawaian Industri | 33 |
| | 2.8.3 | Pendekatan Untuk Memastikan Pematuhan Piawaian Industri | 33 |
| 2.9 | Trend Masa Depan dalam Integrasi OT-IT | | 34 |
| | 2.9.1 | Teknologi Terbaharu dalam Integrasi OT-IT | 34 |
| | 2.9.2 | Kesan Transformasi Digital Terhadap Integrasi OT-IT | 35 |
| | 2.9.3 | Cabaran dan Peluang Masa Depan dalam Integrasi OT-IT | 35 |
| 2.10 | Kesimpulan | | 36 |

**BAB III KAEDAH KAJIAN**

3.1 Pengenalan 37

3.2 Reka Bentuk Kajian 37

3.3 Kaedah Kajian Kesusasteraan 38

3.3.1 Mengenalpasti Penyataan Masalah 39
3.3.2 Carian Hasil Kajian dan Sumber Rujukan 39

3.4 Pelaksanaan Kajian Secara Praktikal Di Lapangan 39

3.4.1 Reka Bentuk Kajian Lapangan 40
3.4.2 Kaedah Pengumpulan Data 41
3.4.3 Kaedah Analisis Data 42

3.5 Kesimpulan 44

**BAB IV HASIL KAJIAN**

4.1 Pengenalan 46

4.2 Keutamaan Berbeza OT dan IT 47

4.2.1 Gambaran Keseluruhan Keutamaan OT dan IT 48
4.2.2 Perbezaan Keutamaan dan Kesannya Terhadap Proses Integrasi 49
4.2.3 Kajian Kes yang Menggambarkan Keutamaan Berbeza OT dan IT 51

4.3 Kekurangan Kompetensi dan Set Kemahiran Komprehensif oleh Kakitangan Keselamatan Siber OT-IT 55

4.3.1 Jurang Kemahiran Antara OT dan Kakitangan IT: Pemerhatian dan Kesan 56
4.3.2 Pengkhususan dalam Disiplin IT dan Cabarannya 57
4.3.3 Contoh Kes yang Menggambarkan Jurang Kemahiran dan Cabaran Pengkhususan 58

4.4 Cabaran Dengan OT Legasi dan Sistem Proprietari 62

4.4.1 Gambaran Keseluruhan Cabaran dengan Sistem Legasi dan Proprietari 63
4.4.2 Kesan Sistem Legasi Terhadap Proses Integrasi OT-IT 64
4.4.3 Contoh Kes yang Menggambarkan Cabaran dengan Sistem Legasi 65

4.5 Kesukaran Teknikal dalam Melaksanakan Keperluan Piawaian 68

4.5.1 Gambaran Keseluruhan Kesukaran Teknikal 68
4.5.2 Impak Kesukaran Teknikal Terhadap Proses Integrasi 69
4.5.3 Contoh Kes yang Menggambarkan Kesukaran Teknikal 69

| | | |
|---|---|---|
| 4.6 | Hasil Soalan Kaji Selidik – Mengurangkan Bias Melalui Maklum Balas Ahli Pasukan Projek | 72 |
| | 4.6.1 Kaji Selidik dan Metodologi | 72 |
| | 4.6.2 Dapatan Kaji Selidik | 73 |
| | 4.6.3 Analisa dan Penyelarasan Dengan Dapatan Kajian | 74 |
| 4.7 | Kesimpulan | 75 |
| **BAB V** | **KESIMPULAN DAN CADANGAN** | |
| 5.1 | Pengenalan | 76 |
| 5.2 | Rumusan dan Hasil Kajian | 76 |
| 5.3 | Kekangan Kaedah Kajian | 78 |
| 5.4 | Perluasan Skop Kajian | 79 |
| 5.5 | Cadangan Kajian Lanjutan | 80 |
| **RUJUKAN** | | **81** |
| **LAMPIRAN** | | |
| Lampiran A | Borang Soalan Kaji Selidik | 86 |
| Lampiran A.1 | Borang Jawapan 1 Soalan Kaji Selidik | 87 |
| Lampiran A.2 | Borang Jawapan 2 Soalan Kaji Selidik | 88 |
| Lampiran A.3 | Borang Jawapan 3 Soalan Kaji Selidik | 89 |

## SENARAI JADUAL

**No. Jadual** **Halaman**

Jadual 3.1 Reka Bentuk Kajian Daripada Penyataan Masalah Sehinggalah Hasil Kajian 38

## SENARAI ILUSTRASI


| No. Rajah | | Halaman |
|---|---|---|
| Rajah 2.1 | Model Purdue | 16 |
| Rajah 2.2 | Kategori Terangkum Dalam IEC62443 | 20 |
| Rajah 2.3 | Konsep Zon dan Konduit Pada Seni Bina Rujukan | 21 |
| Rajah 3.1 | Carta Alir Proses Kajian Kesusasteraan | 38 |
| Rajah 4.1 | Perbezaan Keutamaan Objektif Keselamatan Siber OT dan IT | 48 |
| Rajah 4.2 | Perbezaan Keutamaan OT dan IT, Kesan, dan Contoh Kes | 55 |
| Rajah 4.3 | Jurang Kompetensi Kakitangan OT dan IT Beserta Contoh Kes | 62 |
| Rajah 4.4 | Cabaran Sistem Legasi dan Proprietari | 68 |
| Rajah 4.5 | Cabaran Teknikal | 72 |

**SENARAI SINGKATAN**

| | |
|---|---|
| AI | *Artificial Intelligence* |
| AIC | *Availability, Integrity, Confidentiality* |
| CIA | *Confidentiality, Integrity, Availability* |
| CSMS | *Cyber Security Management Systems* |
| DCS | *Distributed Control System* |
| DMZ | *De-Militarized Zone* |
| HSE | *Health, Safety, and Environment* |
| IACS | *Industrial Automation Control System* |
| ICS | *Industrial Control System* |
| IEC | *International Electrotechnical Commission* |
| IoT | *Internet of Things* |
| ISA | *International Society of Automation* |
| IT | *Information Technology* |
| ML | *Machine Learning* |
| NIST | *National Institute of Standards and Technology* |
| OPC | *Open Platform Communications* |
| OT | *Operation Technology* |
| PLC | *Programmable Logic Controller* |

# BAB I

# PENGENALAN

## 1.1 PENDAHULUAN

Kemunculan Revolusi Perindustrian 4.0 memerlukan syarikat perindustrian merentasi pelbagai sektor, termasuk Penjanaan Kuasa dan Minyak & Gas, untuk memulakan perjalanan transformasi digital. Sebagai sebahagian daripada transformasi ini, integrasi rangkaian Teknologi Operasi (OT) dan Teknologi Maklumat (IT) telah menjadi penting untuk memanfaatkan data daripada aset fizikal, jentera dan proses untuk meningkatkan kecekapan, penyelenggaraan ramalan dan keuntungan yang dipertingkatkan. Walau bagaimanapun, integrasi rangkaian OT dan IT mendedahkan persekitaran OT kepada landskap ancaman siber yang meluas dan maju.

Untuk menangani kebimbangan ini, Suruhanjaya Elektroteknikal Antarabangsa (IEC) telah membangunkan piawaian IEC62443, menggariskan keperluan untuk seni bina rangkaian OT-IT yang selamat. Pematuhan piawaian ini adalah penting untuk melindungi infrastruktur kritikal, mengurangkan ancaman siber dan memastikan keselamatan, kebolehpercayaan dan ketersediaan sistem perindustrian. Akibatnya, banyak syarikat perindustrian kini berhadapan dengan tugas yang kompleks untuk proses migrasi daripada seni bina sistem kawalan sedia ada mereka kepada seni bina yang mematuhi IEC62443.

Kajian ini bertujuan untuk mengenal pasti cabaran yang dihadapi dalam proses migrasi ini. Dengan mendokumentasikan dan berkongsi pengalaman kami, pihak berkepentingan industri lain boleh mendapatkan pandangan tentang kesukaran dan halangan yang terlibat apabila beralih daripada rangkaian OT-IT legasi kepada seni bina baharu yang mematuhi keperluan IEC62443. Penemuan ini akan menyumbang kepada

pemahaman kolektif tentang cabaran, membuka jalan untuk kajian masa depan untuk mencadangkan penyelesaian dan strategi yang berkesan untuk mengatasinya.

## 1.2 LATAR BELAKANG KAJIAN

Sektor Minyak dan Gas, memberikan penekanan yang kuat untuk mencapai tahap produktiviti dan kebolehpercayaan peralatan yang tinggi. Untuk mencapai objektif ini, industri semakin menggunakan alat perisian analitik dan perisian pemantauan termaju. Alat ini bergantung pada data yang diekstrak daripada Sistem Kawalan Perindustrian (ICS), terutamanya melalui Sistem Kawalan Teragih (DCS), yang membentuk domain Teknologi Operasi (OT). Walau bagaimanapun, akses kepada rangkaian OT sangat terhad kepada kakitangan yang berautoriti. Oleh itu, usaha perlu dilakukan untukmelaksanakan pemindahan data OT kepada alat analisis yang berada dalam rangkaian pada peringkat Perusahaan (Enterprise Level network) ataupun lebih dikenali sebagai rangkaian IT.

Permintaan yang semakin meningkat untuk transformasi digital dalam sektor Minyak dan Gas memerlukan integrasi Teknologi Operasi (OT) dan rangkaian Teknologi Maklumat (IT) untuk meningkatkan produktiviti dan kebolehpercayaan peralatan. Walau bagaimanapun, integrasi ini mendedahkan persekitaran OT kepada landskap ancaman siber yang luas dan canggih. Untuk mengurangkan risiko ini, piawaian industri, seperti IEC62443, telah diwujudkan untuk memastikan seni bina rangkaian OT-IT yang selamat.

Proses migrasi daripada seni bina sistem kawalan sedia ada kepada seni bina yang mematuhi IEC62443 menimbulkan cabaran yang ketara, terutamanya dalam sektor Infrastruktur Kritikal Negara. Cabaran ini termasuk kerumitan teknikal, isu keserasian, kekangan sumber dan halangan lain yang menghalang kejayaan pelaksanaan seni bina yang mematuhi IEC62443. Selain itu, proses migrasi perlu menangani perbezaan dalam pengetahuan, keutamaan dan amalan antara kakitangan OT dan IT.

Projek kajian ini dimulakan untuk mengenal pasti cabaran yang dihadapi dalam proses migrasi ke seni bina yang mematuhi IEC62443 dalam sektor Infrastruktur

Kritikal Negara. Penyelidik, yang terlibat secara langsung dalam projek migrasi, berkhidmat sebagai sumber data utama. Reka bentuk kajian menggabungkan metodologi kajian kes, memfokuskan pada sektor Infrastruktur Kritikal Negara khususnya dalam sektor Minyak dan Gas. Pengalaman langsung penyelidik dalam menganalisa, merancang, melaksana dan mengetuai proses migrasi telah didokumenkan dan dianalisis. Penemuan kajian ini bertujuan untuk membimbing pembuat keputusan, meningkatkan postur keselamatan siber infrastruktur kritikal, dan memastikan kesinambungan perkhidmatan penting.

## 1.3 PENYATAAN MASALAH

Permintaan yang semakin meningkat untuk transformasi digital dalam sektor Minyak dan Gas memerlukan integrasi Teknologi Operasi (OT) dan rangkaian Teknologi Maklumat (IT) untuk meningkatkan produktiviti dan kebolehpercayaan peralatan. Walau bagaimanapun, integrasi ini mendedahkan persekitaran OT kepada landskap ancaman siber yang luas dan canggih. Untuk mengurangkan risiko ini, piawaian industri, seperti IEC62443, telah diwujudkan untuk memastikan seni bina rangkaian OT-IT yang selamat. Berhijrah daripada seni bina sistem kawalan sedia ada kepada seni bina yang mematuhi IEC62443 menimbulkan cabaran yang ketara, terutamanya dalam sektor Infrastruktur Kritikal Negara. Cabaran ini termasuk kerumitan teknikal, isu keserasian, kekangan sumber dan halangan lain yang menghalang kejayaan pelaksanaan seni bina yang mematuhi IEC62443. Selain itu, proses migrasi memerlukan mengangani perbezaan dalam pengetahuan, keutamaan dan amalan antara kakitangan OT dan IT. Dengan menangani cabaran ini, industri boleh mewujudkan rangkaian OT-IT yang teguh dan selamat yang melindungi infrastruktur kritikal sambil membolehkan manfaat transformasi digital. Oleh itu, objektif kajian ini adalah untuk mengenal pasti cabaran yang dihadapi dalam proses migrasi kepada seni bina yang mematuhi IEC62443 dalam sektor Infrastruktur Kritikal Negara. Melalui penerokaan proses migrasi dan analisis mendalam, kajian ini bertujuan untuk memberikan pandangan berharga tentang cabaran-cabaran dan halangan unik yang dihadapi, bertujuan menyumbang kepada pengetahuan industri dan membantu pihak berkepentingan dalam menangani dan mengatasi cabaran ini dengan berkesan semasa migrasi kepada seni bina yang mematuhi IEC62443 pada masa akan datang.

## 1.4 OBJEKTIF KAJIAN

Objektif utama kajian ini adalah:

i) Meneliti pendekatan dan amalan semasa OT-IT yang digunakan dalam sektor Infrastruktur Kritikal Negara, dengan tumpuan khusus pada sektor Minyak dan Gas, untuk mengenal pasti cabaran yang dihadapi semasa proses migrasi.

ii) Mengenal pasti kerumitan teknikal tertentu, isu keserasian, kekangan sumber dan halangan lain yang menghalang kejayaan pelaksanaan seni bina yang mematuhi IEC62443 dalam rangkaian OT-IT sektor Infrastruktur Kritikal Negara.

## 1.5 PERSOALAN KAJIAN

Melalui isu-isu yang dihuraikan dalam penyataan masalah di atas, persoalan kajian dapat dihasilkan iaitu:

i) Apakah cabaran dan halangan utama yang dihadapi dalam proses migrasi daripada seni bina sistem kawalan sedia ada kepada seni bina yang mematuhi IEC62443 dalam sektor Infrastruktur Kritikal Negara?

ii) Apakah cabaran teknikal khusus dan isu keserasian teknikal OT-IT yang dihadapi semasa migrasi kepada seni bina yang mematuhi IEC62443 dalam rangkaian OT-IT sektor Infrastruktur Kritikal Negara?



## 1.6 KEPENTINGAN KAJIAN

Kajian dalam mengenal pasti cabaran ketika proses migrasi kepada seni bina yang mematuhi IEC62443 dalam sektor Infrastruktur Kritikal Negara mempunyai beberapa kepentingan dan manfaat kepada pelbagai pihak.

Pertama, kajian ini menangani keperluan penting dalam sektor Minyak dan Gas, juga dalam konteks Infrastruktur Kritikal Negara. Memandangkan transformasi digital menjadi satu keperluan, integrasi rangkaian OT dan IT membawa pelbagai cabaran. Memahami dan mengenal pasti cabaran-cabaran ini adalah penting bagi organisasi yang

ingin melakukan proses migrasi dan dalam masa sama meningkatkan postur keselamatan siber mereka sambil mengekalkan kecekapan operasi.

Kedua, kajian ini memberikan pandangan tentang cabaran khusus yang dihadapi semasa proses migrasi. Dengan mendokumentasikan dan menganalisa cabaran yang dihadapi, kajian ini menyumbang kepada pengetahuan kolektif pengamal industri, pembuat keputusan dan profesional yang terlibat dalam integrasi OT-IT. Hasil kajian ini boleh menjadi rujukan untuk projek migrasi masa hadapan, membolehkan pihak berkepentingan menjangka dan menangani potensi halangan secara proaktif.

Ketiga, kajian ini memberi penerangan tentang kerumitan yang berkaitan dengan perpindahan kepada seni bina yang mematuhi IEC62443. Loji Infrastruktur Kritikal Negara memerlukan seni bina rangkaian OT-IT yang teguh dan selamat untuk melindungi aset dan operasi kritikal. Dengan mengenal pasti cabaran yang berkaitan dengan kerumitan teknikal, isu keserasian, kekangan sumber, dan perbezaan antara amalan OT dan IT, kajian ini membantu industri dalam membangunkan strategi yang berkesan untuk mengatasi halangan ini.

Selain itu, kajian ini mempunyai implikasi yang lebih luas untuk keselamatan negara dan keselamatan awam. Loji Infrastruktur Kritikal Negara memainkan peranan penting dalam memastikan kelancaran fungsi perkhidmatan penting. Seni bina rangkaian OT-IT yang selamat dan berdaya tahan adalah penting dalam melindungi infrastruktur kritikal ini daripada ancaman siber. Dengan menangani cabaran dalam migrasi, kajian itu menyumbang kepada pengukuhan postur keselamatan siber keseluruhan Infrastruktur Kritikal Negara.

Kajian ini juga menyerlahkan kepentingan pematuhan dengan piawaian IEC62443. Memandangkan industri semakin mengguna pakai piawaian ini untuk meningkatkan keselamatan siber, memahami cabaran dalam melaksanakan seni bina yang mematuhi menjadi penting. Kajian ini memberikan pandangan berharga tentang cabaran khusus untuk sektor Infrastruktur Kritikal Negara, membolehkan organisasi menyelaraskan usaha migrasi mereka dengan amalan terbaik industri dan keperluan kawal selia.

Secara keseluruhannya, kajian ini mempunyai kepentingan yang signifikan untuk sektor Minyak dan Gas dan Infrastruktur Kritikal Negara. Dengan mengenal pasti cabaran dalam proses migrasi kepada seni bina yang mematuhi IEC62443, kajian ini menyumbang kepada pengetahuan kolektif pengamal industri, membantu dalam pembangunan strategi yang berkesan, mengukuhkan keselamatan negara dan menggalakkan pematuhan piawaian industri. Penemuan kajian ini bertujuan untuk membimbing pembuat keputusan dan seterusnya meningkatkan postur keselamatan siber infrastruktur kritikal.

## 1.7 SKOP KAJIAN

Kajian ini memfokuskan pada integrasi lapisan Teknologi Operasi (OT), berdasarkan model Purdue, dan mematuhi piawaian IEC62443 dalam sektor Infrastruktur Kritikal Negara, khususnya dalam Loji Minyak dan Gas. Kajian ini bertujuan untuk mengkaji cabaran yang dihadapi semasa proses integrasi Tahap OT yang berbeza, termasuk Tahap OT 0 (Proses), Tahap OT 1 (Kawalan), Tahap OT 2 (Penyeliaan), Tahap OT 3 (Pengurusan Operasi), dan Zon Demiliterisasi (DMZ) dan seterusnya bersambung dengan Rangkaian Perusahaan dan Internet. Skop ini merangkumi analisis menyeluruh tentang cabaran yang dihadapi, kerumitan teknikal, kekangan sumber dan keperluan pematuhan yang dinyatakan dalam piawaian IEC62443. Dengan memfokuskan pada cabaran integrasi dalam konteks khusus ini, kajian bertujuan memberikan pandangan berharga tentang selok-belok integrasi lapisan OT dan DMZ dengan mematuhi piawaian IEC62443, mengikut Model Purdue, dalam sektor Infrastruktur Kritikal Negara di Loji Minyak dan Gas. Penemuan kajian ini akan membantu pihak berkepentingan industri memahami dengan lebih baik cabaran yang berkaitan dengan integrasi ini, memudahkan pembangunan strategi dan pendekatan untuk mengatasi cabaran ini dengan berkesan, dan juga memastikan seni bina rangkaian OT-IT yang selamat.



## 1.8 STRUKTUR PENULISAN

Kajian ini dibahagikan kepada lima (5) bab iaitu Pengenalan, Kajian Kesusasteraan, Kaedah Kajian, Hasil Kajian, dan Kesimpulan dan Cadangan.

### 1.8.1 Bab I Pengenalan

Bab I menerangkan latar belakang kajian, penyataan masalah, objektif kajian, persoalan kajian, kepentingan kajian, skop kajian, dan kesimpulan.

### 1.8.2 Bab II Kajian Kesusasteraan

Bab II merupakan Kajian Kesusasteraan yang dimulai dengan pengenalan kepada OT-IT, Model Purdue, dan juga piawaian IEC62443. Bab ini seterusnya membincangkan cabaran umum serta peranan kakitangan dalam integrasi OT-IT, pelaksanaannya dalm sektor Minyak dan Gas. Ia turut membincangkan aspek keselamatan siber dalam integrasi OT-IT dan pematuhan piawaian industri dalam pelaksanaannya. Ia diakhiri dengan trend masa depan dalam integrasi OT-IT dan kesimpulan.

### 1.8.3 Bab III Kaedah Kajian

Bab III menerangkan kaedah kajian yang digunakan dalam menghasilkan kajian ini. Ie menerangkan reka bentuk, metodologi kajian termasuk kaedah pelaksanaan kajian di lapangan.

### 1.8.4 Bab IV Hasil Kajian

Bab IV membincangkan dapatan kajian hasil daripada kajian yang dilaksanakan di lapangan. Ia membincangkan cabaran-cabaran yang dikenalpasti melalui kajian dalam pelaksanaan proses integrasi OT-IT.

### 1.8.5 Bab V Kesimpulan dan Cadangan

Bab V merupakan perbincangan dan rumusan terhadap pelaksanaan aktiviti kajian yang dijalankan, serta cadangan penambahbaikan kajian pada masa akan datang

## 1.9 KESIMPULAN

Kajian ini menyumbang kepada pengetahuan mengenai integrasi rangkaian OT-IT dan menjelaskan cabaran-cabaran yang dihadapai apabila melaksnakan integrasi lapisan OT-IT dengan mematuhi piawaian IEC62443. Dengan menangani cabaran ini,

organisasi boleh mengukuhkan pertahanan keselamatan siber mereka, meningkatkan kecekapan operasi dan memastikan kebolehpercayaan dan daya tahan sistem infrastruktur kritikal. Secara keseluruhannya, kajian ini menekankan kepentingan memahami dan menangani cabaran yang dihadapi semasa integrasi lapisan OT, mengikut model Purdue, dan mematuhi piawaian IEC62443. Maklumat yang diperoleh daripada kajian ini boleh membantu dalam memacu kemajuan dalam seni bina rangkaian OT-IT yang selamat dan patuh, akhirnya melindungi sektor Infrastruktur Kritikal Negara dan memupuk persekitaran operasi yang berdaya tahan dan terjamin.

# BAB II

# KAJIAN KESUSASTERAAN

## 2.1 PENGENALAN KEPADA INTEGRASI TEKNOLOGI OPERASI (OT) – TEKNOLOGI MAKLUMAT (IT)

Bidang integrasi OT-IT telah mendapat perhatian yang ketara sejak beberapa tahun kebelakangan ini disebabkan oleh peningkatan keperluan untuk ketersambungan dan kerjasama antara domain Teknologi Operasi (OT) dan Teknologi Maklumat (IT) (David Hough 2016).

Bab ini memberikan gambaran keseluruhan integrasi OT-IT, definisi, kepentingan, evolusi dan aliran semasanya.

### 2.1.1 Definisi dan Kepentingan Integrasi OT-IT

Integrasi OT-IT merujuk kepada integrasi domain tradisional yang berasingan, iaitu Teknologi Operasi (OT) dan Teknologi Maklumat (IT), dalam sistem perindustrian. OT merangkumi sistem perkakasan dan perisian yang memantau dan mengawal proses fizikal, manakala IT memfokuskan pada pemprosesan data, penyimpanan dan komunikasi. Integrasi OT dan IT membolehkan organisasi mencapai kecekapan operasi yang lebih besar, membuat keputusan yang lebih baik dan keterlihatan yang dipertingkatkan ke dalam proses industri.

Kepentingan integrasi OT-IT terletak pada keupayaannya untuk merapatkan jurang antara alam fizikal dan digital. Dengan menyepadukan sistem OT dan IT, organisasi boleh memanfaatkan data masa nyata daripada proses industri, membolehkan penyelenggaraan ramalan, pengoptimuman proses dan pemantauan jarak jauh. Integrasi ini juga memudahkan pertukaran maklumat antara peringkat organisasi yang berbeza. Di dalam konteks industri Minyak dan Gas, ini bermaksud integrasi

kawalan proses di loji dan perkongsian data di peringkat perusahaan dan eksekutif. Ini membolehkan kerjasama yang lebih baik dan memberi maklumat yang terkini kepada golongan eksekutif untuk membuat keputusan yang lebih tepat (Yong-Lip 2019).

### 2.1.2 Evolusi Integrasi OT-IT

Evolusi integrasi OT-IT boleh dikesan kembali ke zaman awal sistem kawalan industri (ICS). Pada mulanya, sistem perindustrian bergantung pada proprietari, penyelesaian terpencil yang beroperasi secara bebas daripada rangkaian IT. Walau bagaimanapun, apabila teknologi maju dan permintaan untuk ketersambungan berkembang, integrasi OT dan IT tidak dapat dielakkan.

Dari masa ke masa, evolusi integrasi OT-IT telah didorong oleh beberapa faktor. Penggunaan piawaian dan protokol terbuka, seperti OPC (Komunikasi Platform Terbuka), memudahkan kesalingoperasian antara sistem OT dan IT. Peningkatan ketersediaan dan kemampuan infrastruktur rangkaian juga memainkan peranan penting dalam membolehkan komunikasi lancar dan pertukaran data antara domain OT dan IT. Selain itu, kemunculan teknologi IoT (Internet of Things) telah mempercepatkan integrasi OT dan IT, yang membolehkan integrasi peranti fizikal dan sensor dengan rangkaian IT (M.Felser et al. 2019).

### 2.1.3 Trend Semasa dalam Integrasi OT-IT

Pada masa kini, bidang integrasi OT-IT menyaksikan pelbagai trend yang membentuk masa depan sistem perindustrian. Industri 4.0, yang sering dirujuk sebagai revolusi perindustrian keempat. Ia menekankan pendigitalan proses perindustrian melalui penggunaan teknologi canggih seperti automasi, robotik dan analisis data. Aliran ini menyerlahkan kepentingan integrasi OT-IT dalam mendayakan operasi industri yang pintar, bersambung dan dipacu data.

Percambahan peranti IoT adalah satu lagi trend penting yang memacu integrasi OT-IT. Peranti IoT yang dibenamkan dalam aset dan jentera perindustrian membolehkan pemantauan masa nyata, penyelenggaraan ramalan dan peningkatan kecekapan. Peranti ini menjana sejumlah besar data yang boleh dianalisis dan

digunakan oleh kedua-dua sistem OT dan IT. Ia memudahkan proses membuat keputusan dan mengoptimumkan operasi (Wang et al. 2016).

Integrasi rangkaian OT dan IT dalam sektor infrastruktur kritikal, seperti tenaga, Minyak dan Gas, semakin mendapat momentum. Trend ini bertujuan untuk meningkatkan daya tahan, kebolehpercayaan dan keselamatan sistem infrastruktur kritikal dengan menyepadukan domain OT dan IT, dengan itu membolehkan pemantauan berpusat, pengurusan jauh dan langkah keselamatan siber yang proaktif.

## 2.2 SENI BINA MODEL PURDUE UNTUK HIERARKI KAWALAN

Model Purdue, juga dikenali sebagai Seni Bina Rujukan Perusahaan Purdue, ialah rangka kerja hierarki yang menyediakan pendekatan berstruktur untuk mengatur dan menyepadukan sistem kawalan dalam persekitaran industri. Ia dibangunkan pada tahun 1990-an sebagai tindak balas kepada keperluan piawai seni bina untuk menangani kerumitan sistem kawalan industri (ICS) dan memudahkan integrasi domain Teknologi Operasi (OT) dan Teknologi Maklumat (IT). Model ini terdiri daripada beberapa tahap hierarki yang mewakili lapisan berfungsi yang berbeza dalam sistem kawalan, setiap satunya bertanggungjawab untuk tugas dan operasi tertentu (W Xu 2022).



### 2.2.1 Gambaran Keseluruhan Model Purdue

Model Purdue adalah berdasarkan model rujukan seni bina yang diperkenalkan untuk sistem kawalan *(Control Systems)*. Model Purdue ini menyediakan rangka kerja untuk mensegmentasikan rangkaian sistem kawalan industri daripada rangkaian perusahaan korporat dan internet. Model ini digunakan sebagai seni bina dasar untuk semua rangka kerja kawalan industri seperti IEC 62443, ISA99, dan NIST 800-82, dan API 1164. Ia merupakan model konsep bagi pembahagian atau segmentasi rangkaian bagi sistem kawalan industri ataupun OT. Sumbangan paling penting model seni bina ini ialah tahap perincian dan cadangan praktikal untuk asimilisasikan dan menyatupadukan perusahaan dalam proses perindustrian standard.

Dinamakan sempena Universiti Purdue, di mana ia pada mulanya dibangunkan, model ini membahagikan sistem perindustrian kepada tahap hierarki, masing-masing

menjalankan fungsi tertentu dan mengekalkan keperluan keselamatan yang berbeza. Model ini terdiri daripada enam (6) Tahap *(Layer)* bermula Tahap 0 sehingga Tahap 5.

Tahap 0 ialah Proses. Tahap ini merangkumi komponen fizikal proses industri, seperti penderia *(sensor),* penggerak *(actuator)*, dan sistem kawalan. Sistem ini bertanggungjawab untuk mengumpul dan menghantar data daripada persekitaran operasi. Memandangkan tahap ini berkaitan dengan kawalan proses kritikal, langkah keselamatan tertumpu pada memastikan integriti dan kebolehpercayaan mekanisme pemerolehan dan kawalan data.

Tahap 1 ialah Kawalan. Tahap ini terdiri daripada sistem yang menerima data daripada Tahap 0 (Proses) dan menghantar arahan kawalan. Ia merangkumi sistem kawalan seperti Pengawal Logic Boleh Aturcara (PLC), Peranti Elektronik Pintar, dan Unit Terminal Jauh. Keselamatan di Tahap 1 adalah amat penting, kerana sebarang capaian, manipulasi atau gangguan yang tidak dibenarkan boleh memberi kesan secara langsung kepada proses fizikal yang dipandu oleh Tahap 0. Langkah keselamatan yang dilaksanakan di sini direka bentuk untuk melindungi saluran komunikasi antara peranti kawalan dan menghalang sebarang capaian yang tidak dibenarkan atau mengusik. Dengan mendapatkan Tahap 1, industri memastikan pelaksanaan perintah operasi yang boleh dipercayai dan tepat, mengekalkan integriti proses yang memacu operasi mereka. Lapisan keselamatan asas ini penting untuk matlamat yang lebih luas untuk mewujudkan pertahanan yang teguh terhadap ancaman siber merentas keseluruhan hierarki Model Purdue.



Tahap 2 ialah Penyeliaan *(Supervisory)*. Tahap ini berfungsi sebagai pengatur landskap perindustrian, mengawasi dan menyelaraskan berbilang sistem kawalan daripada Tahap 1. Di sini, konsep seperti penjadualan pengeluaran, pengoptimuman dan penyelarasan antara segmen berlainan proses perindustrian diutamakan. Pada Tahap 2, sistem seperti Sistem Perlaksanaan Pembuatan (MES) atau Sistem Kawalan Teragih (DCS) memainkan peranan penting dalam mengharmonikan aktiviti pelbagai elemen kawalan. Pertimbangan keselamatan di Tahap 2 berkembang melangkaui sistem kawalan individu untuk merangkumi penyelarasan dan pengoptimuman proses yang lebih luas. Matlamatnya adalah untuk melindungi daripada pelanggaran data yang boleh

menjejaskan jadual pengeluaran, mengganggu aliran kerja, atau bahkan membawa kepada ketidakcekapan dalam keseluruhan proses. Dengan memastikan keselamatan pertukaran data dan komunikasi pada tahap ini, industri memastikan proses industri mereka beroperasi dengan cara yang disegerakkan dan dioptimumkan, menyumbang kepada kecemerlangan operasi keseluruhan. Mengekalkan keselamatan di Tahap 2 bukan sahaja melindungi kecekapan proses perindustrian tetapi juga menyumbang kepada matlamat yang lebih besar untuk mengekalkan integriti keseluruhan hierarki Model Purdue. Tahap keselamatan ini, apabila digabungkan dengan langkah-langkah yang dilaksanakan pada Tahap 0 dan 1, membentuk strategi padu yang memperkukuh seni bina perindustrian daripada potensi ancaman siber.

Tahap 3 ialah Pengurusan Operasi *(Operations Management)*. Tahap ini merangkumi fungsi yang menguruskan aliran kerja untuk menghasilkan produk akhir yang diingini. Contoh fungsi di tahap ini ialah pengumpulan data dan analisis, pengumpulan data lalu, stesen kerja kejuruteraan, dan pengurusan aset. Tahap ini adalah tahap terakhir di OT sebelum bersambung ke tahap IT. Oleh itu, pertimbangan keselamatan di tahap ini lebih kepada memastikan pertimbangan keselamatan di tahap ini lebih kepada mengawal akses dan mewujudkan seni bina rangkaian yang selamat.

Tahap 0 hingga 3 turut dikenali sebagai rangkaian Teknologi Operasi (OT). Tahap 4 dan 5 ialah rangkaian Teknologi Maklumat (IT). Untuk menyambungkan OT dan IT, Tahap 3.5 diwujudkan dan dikenali sebagai Zon Demilitarisasi (DMZ)

Tahap 3.5 dikenali sebagai Zon Demilitarisasi *(Demilitarized Zone* atau *DMZ)*. DMZ berfungsi sebagai zon penampan antara OT (Tahap 0 hingga 3) dan IT, biasanya disambungkan ke internet atau sistem IT korporat. Tujuannya adalah dua: untuk meningkatkan keselamatan dengan mengasingkan sistem dalaman yang kritikal daripada ancaman luar dan untuk memudahkan komunikasi terkawal antara kedua-dua domain. Dalam konteks integrasi OT-IT, DMZ ialah titik kritikal di mana pertukaran data dan komunikasi berlaku. Ia direka untuk memastikan bahawa sebarang maklumat yang mengalir masuk dan keluar dari rangkaian OT menjalani pemeriksaan keselamatan yang ketat. Di sini, tembok api, sistem pengesanan pencerobohan dan mekanisme keselamatan lain digunakan untuk meneliti trafik data dan melindungi daripada akses

yang tidak dibenarkan atau aktiviti berniat jahat. DMZ memainkan peranan penting dalam menguatkuasakan prinsip seni bina pertahanan yang mendalam dan kepercayaan sifar. Dengan meneliti dan menapis trafik pada persimpangan ini, potensi ancaman dipintas sebelum ia boleh menembusi lebih dalam ke dalam rangkaian OT. Ini membantu mengekalkan integriti sistem Tahap 0 hingga Tahap 3 dan menghalang aktor luaran daripada mengakses secara langsung proses dan data kritikal.

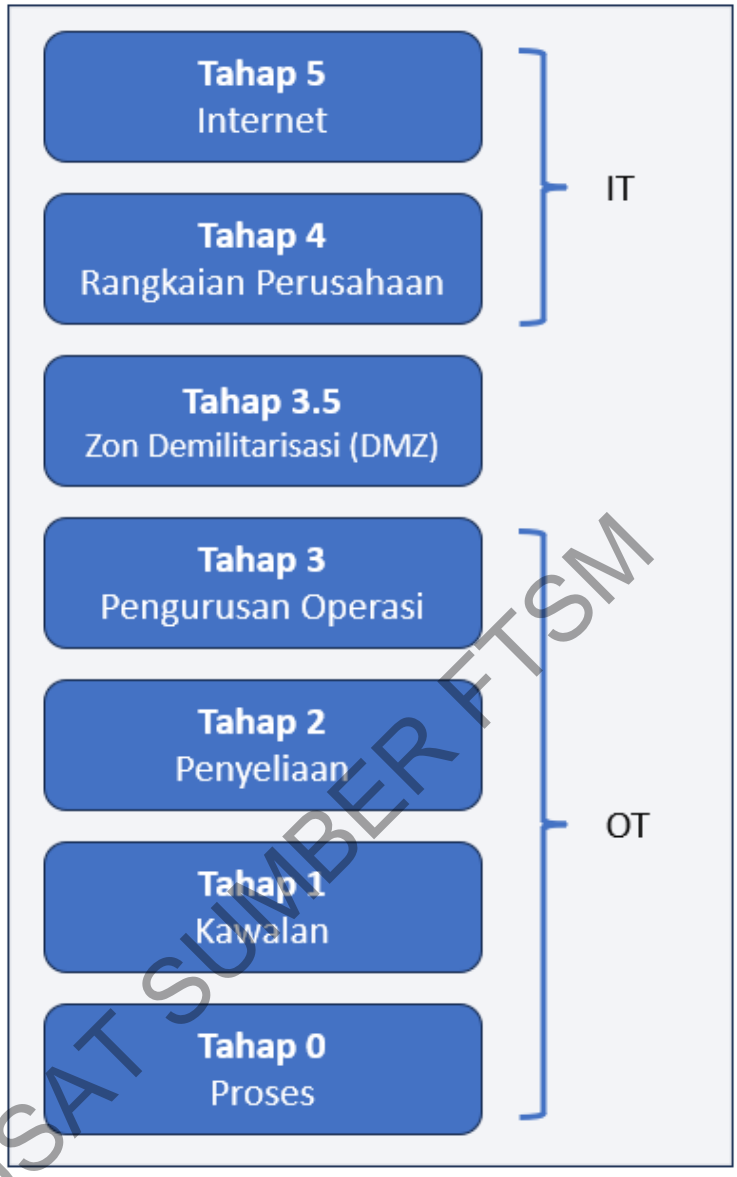
Tahap 4 ialah Rangkaian Perusahaan *(Enterprise network)*. Tahap ini merangkumi spektrum sistem IT yang mengurus aspek perniagaan teras termasuklah operasi kewangan, sumber manusia, pemerolehan, perancangan strategik, dan segala hubungan komunikasi sesama pekerja. Di sini juga, data yang dijana di rangkaian OT boleh dianalisis dengan lebih lanjut melalui cerapan yang boleh diambil tindakan, dan seterusnya membolehkan pembuatan keputusan yang pantas dan lebih berinformatif. Dari sudut keselamatan, tahap 4 memperkenalkan beberapa pertimbangan kritikal yang memudahkan integrasi lancar proses perniagaan dalam rangka kerja Model Purdue. Walaupun kerahsiaan data mungkin bukan tumpuan utama, integriti dan ketepatan data kekal diutamakan. Kawalan capaian yang teguh, kaedah pengesahan yang ketat dan jejak audit yang komprehensif adalah penting untuk melindungi ketepatan data kewangan, strategik dan kawal selia. Keselamatan rangkaian diutamakan, memastikan komunikasi yang diperkukuh antara Tahap 4 dan lapisan lain melalui penyulitan dan sistem pemantauan lanjutan. Kemas kini perisian yang konsisten dan penilaian kerentanan adalah penting untuk mengurangkan potensi titik eksploitasi. Keselamatan fizikal kawasan Tahap 4 mengehadkan akses tanpa kebenaran, dan keselamatan akses daripada rangkaian luar dan internet diutamakan.



Tahap 5 ialah tahap Internet dan rangkaian luar. Ini termasuklah rangkaian bagi bantuan daripda vendor dan juga perkhidmatan awan. Walaupun tidak digariskan secara eksplisit dalam Model Purdue konvensional, Tahap 5 memainkan peranan penting dalam seni bina industri moden, terutamanya dalam konteks menyelaraskan OT dengan landskap digital yang lebih luas. Tujuannya memenuhi dua objektif utama: mengukuhkan keselamatan dengan memisahkan sistem dalaman daripada ancaman luaran, dan membolehkan komunikasi terkawal antara kedua-dua domain. Dalam landskap integrasi OT dengan IT, Tahap 5 berdiri sebagai persimpangan penting di

mana pertukaran data dan interaksi berlaku. Ia memastikan bahawa data yang memasuki atau meninggalkan rangkaian perusahaan menjalani pemeriksaan keselamatan yang ketat. Di sini, spektrum langkah keselamatan, termasuk tembok api dan sistem pengesanan pencerobohan, meneliti trafik data untuk menghalang akses tanpa kebenaran dan aktiviti berniat jahat. Tahap 5 memainkan peranan penting dalam menegakkan prinsip seni bina pertahanan yang mendalam dan kepercayaan sifar. Dengan memeriksa dan menapis aliran data dengan teliti di persimpangan ini, potensi risiko dipintas sebelum ia boleh menyusup lebih dalam ke dalam rangkaian dalaman. Perlindungan ini memelihara integriti sistem Tahap 0 hingga Tahap 4, sambil pada masa yang sama menghalang entiti luar daripada menyusup terus ke proses dan data sensitif.

Ilustrasi Tahap 0 ke Tahap 5 Model Purdue adalah seperti yang ditunjukkan dalam Rajah 2.1 di bawah.




Rajah 2.1 Model Purdue



### 2.2.2 Peranan Model Purdue dalam Integrasi OT-IT

Model Purdue memainkan peranan penting dalam memudahkan integrasi domain OT dan IT dalam sistem perindustrian. Ia menyediakan seni bina rujukan biasa yang membolehkan komunikasi lancar, kebolehoperasian dan pertukaran data antara tahap hierarki sistem kawalan yang berbeza. Dengan mewujudkan rangka kerja berstruktur, Model Purdue membantu organisasi merapatkan jurang antara sistem OT dan IT yang secara tradisinya berasingan, memudahkan kerjasama, kecekapan dan membuat keputusan yang lebih baik.

Salah satu faedah utama Model Purdue ialah keupayaannya untuk memudahkan kebolehoperasian dan penyeragaman. Dengan menyediakan struktur yang jelas dan antara muka yang jelas antara tahap yang berbeza, model ini memastikan keserasian dan komunikasi yang cekap antara pelbagai komponen sistem kawalan. Ini menggalakkan kesalingoperasian antara sistem vendor yang berbeza dan membolehkan integrasi teknologi dan komponen baharu ke dalam infrastruktur sedia ada.

Selain itu, Model Purdue menyokong pelaksanaan langkah keselamatan siber dalam integrasi OT-IT. Dengan mentakrifkan dengan jelas sempadan dan laluan komunikasi antara tahap yang berbeza, model ini membantu mengenal pasti potensi kelemahan keselamatan dan membolehkan pelaksanaan kawalan keselamatan pada setiap peringkat. Pendekatan berlapis kepada keselamatan ini, seperti yang ditakrifkan oleh Model Purdue, membolehkan pelaksanaan strategi pertahanan mendalam untuk melindungi sistem infrastruktur kritikal daripada ancaman siber (A Srivastava 2021).



### 2.2.3 Aplikasi Model Purdue dalam Pelbagai Sektor

Dalam sektor pembuatan, Model Purdue telah dilaksanakan secara meluas untuk mewujudkan hierarki sistem kawalan berstruktur. Dengan mengguna pakai model, syarikat pembuatan boleh mencapai keterlihatan dan kawalan yang lebih baik ke atas proses pengeluaran mereka. Struktur hierarki membolehkan pertukaran data yang cekap, pemantauan masa nyata, dan penyelarasan antara tahap sistem kawalan yang berbeza. Cara Model Purdue telah meningkatkan kecekapan pengeluaran, meningkatkan kawalan kualiti dan membolehkan pengurusan inventori yang berkesan dalam sektor pembuatan.

Sektor tenaga juga telah menggunakan Model Purdue untuk menyepadukan sistem penjanaan, penghantaran dan pengedaran. Integrasi ini memastikan penyelarasan yang berkesan, pengesanan kerosakan dan penyelenggaraan merentas pelbagai peringkat hierarki sistem kawalan. Model Purdue membantu menyelaraskan operasi sistem kawalan, meningkatkan kesedaran situasi dan membolehkan pengurusan tenaga yang cekap. Model Purdue menunjukkan manfaat dalam mengurangkan masa henti, mengoptimumkan pengagihan tenaga dan meningkatkan kebolehpercayaan sistem secara keseluruhan dalam sektor tenaga.

Industri lain, seperti rawatan air dan air sisa, farmaseutikal dan pengangkutan, telah memanfaatkan Model Purdue untuk mengoptimumkan seni bina sistem kawalan mereka dan meningkatkan kesalingoperasian antara domain OT dan IT. Ini menunjukkan bagaimana Model Purdue memudahkan integrasi yang lancar, pertukaran data yang cekap dan kawalan yang lebih baik ke atas proses kritikal dalam pelbagai sektor perindustrian (K Perrett 2023).

## 2.3 PIAWAIAN IEC62443 UNTUK KESELAMATAN SIBER RANGKAIAN KOMUNIKASI INDUSTRI

Dalam era digital kontemporari, keselamatan siber telah muncul sebagai kebimbangan utama bagi organisasi. Dari segi sejarah, entiti yang beroperasi dalam bidang Teknologi Maklumat (IT) dan perniagaan telah menyedari ancaman keselamatan siber. Mereka sering melaksanakan sistem pengurusan keselamatan siber (CSMS) yang teguh seperti yang digariskan oleh piawaian global seperti ISO/IEC 17799 dan ISO/IEC 27001. Sistem ini menawarkan metodologi berstruktur untuk melindungi aset organisasi daripada ancaman siber.

Walau bagaimanapun, landskap mula berubah dengan kemunculan Sistem Automasi dan Kawalan Perindustrian (IACS). Sistem ini mula menggabungkan teknologi komersial di luar rak, yang asalnya direka untuk operasi perniagaan. Penyepaduan ini mendedahkan IACS kepada kelemahan siber yang semakin meningkat. Memandangkan sistem ini tidak direka bentuk secara semulajadi dengan langkah keselamatan siber yang teguh, sistem ini terdedah kepada ancaman yang berpotensi membawa kepada kesan kesihatan, keselamatan dan alam sekitar (HSE) yang ketara.

Dalam industri Minyak dan Gas, memastikan integrasi yang selamat bagi Teknologi Operasi (OT) dan sistem Teknologi Maklumat (IT) adalah penting untuk mengekalkan kecekapan operasi dan melindungi infrastruktur kritikal. Piawaian IEC62443 untuk rangkaian komunikasi industri memainkan peranan penting dalam membimbing sektor Minyak dan Gas ke arah amalan keselamatan siber yang teguh dan integrasi OT-IT yang selamat. Bab ini menyediakan semakan meluas piawaian

IEC62443, termasuk gambaran keseluruhannya dan kepentingan dalam integrasi OT-IT dalam sektor Minyak dan Gas.

### 2.3.1 Piawaian IEC62443: CSMS yang Disesuaikan Untuk IACS

IEC62443 ialah set piawaian yang diiktiraf secara global yang direka khusus untuk memastikan keselamatan siber Sistem Automasi dan Kawalan Perindustrian (IACS). Asal-usulnya dikesan kembali kepada Persatuan Automasi Antarabangsa (*International Society of Automation*, ISA), yang pada mulanya membangunkan piawaian sebagai ISA-99. Piawaian ini dibina berpandukan ISO/IEC 17799 dan ISO/IEC 27001 dengan menangani perbezaan antara IACS (OT) dan sistem IT. Menyedari kepentingannya dan keperluan mendesak untuk piawaian global yang bersatu, Suruhanjaya Elektroteknik Antarabangsa (IEC) kemudiannya menerima pakainya, memberikannya gelaran IEC62443.

Sistem Automasi dan Kawalan Perindustrian memainkan peranan penting dalam pelbagai industri, daripada penjanaan kuasa dan pengedaran kepada pembuatan dan pengangkutan. Dari segi sejarah, sistem ini beroperasi secara berasingan. Walau bagaimanapun, dengan kemunculan transformasi digital dan penumpuan IT tradisional (Teknologi Maklumat) dan OT (Teknologi Operasi), mereka menjadi lebih saling berkaitan dan bersepadu dengan sistem IT yang lain. Integrasi ini, walaupun bermanfaat dalam banyak cara, juga mendedahkan mereka kepada pelbagai ancaman siber yang lebih luas.



IEC62443 bukan sahaja menangani komponen teknikal keselamatan siber, seperti penyulitan atau sistem pengesanan pencerobohan. Ia menggunakan pendekatan holistik, meliputi kedua-dua aspek teknikal dan berorientasikan proses keselamatan siber. Perspektif komprehensif ini memastikan bahawa walaupun piawaian menyediakan panduan tentang langkah perlindungan untuk sistem, ia juga menekankan dasar, prosedur dan amalan organisasi yang menyokong keselamatan berterusan.

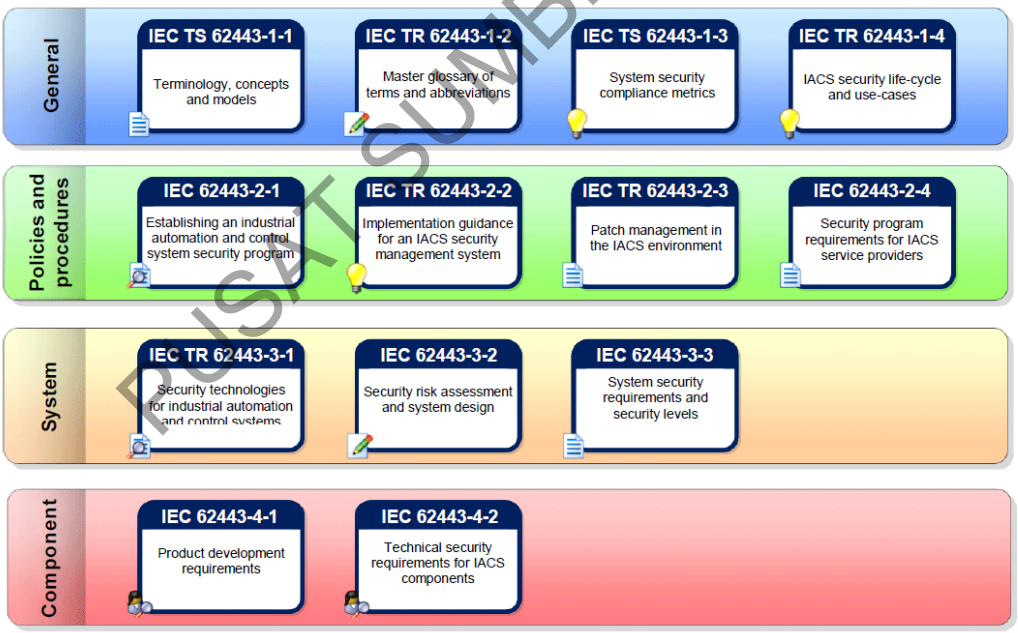
Ciri yang membezakan piawaian IEC62443 ialah fleksibiliti yang wujud. Memahami bahawa setiap operasi perindustrian mempunyai cabaran dan ciri uniknya, piawaian ini direka bentuk untuk disesuaikan. Kebolehsuaian ini membolehkan

organisasi menyesuaikan strategi keselamatan siber mereka berdasarkan persekitaran operasi khusus, profil risiko dan matlamat perniagaan mereka.

IEC62443 berfungsi sebagai panduan menyeluruh untuk organisasi, mengemudi mereka melalui domain keselamatan siber industri yang rumit. Sama ada syarikat utiliti yang bertujuan untuk melindungi sistem kawalannya atau entiti pembuatan yang berusaha untuk melindungi proses automatiknya, IEC62443 menawarkan rangka kerja dan cerapan yang diperlukan untuk mewujudkan pendirian keselamatan siber yang berdaya tahan.

IEC62433 merangkumi keseluruhan kitar hidup IACS dari aspek keselamatan siber termasuklah ketika peringkat penilaian, mereka bentuk & pelaksanaan, dan penyelenggaraan. Kategori terangkum dalm IEC62443 adalah seperti Rajah 2.2 di bawah.



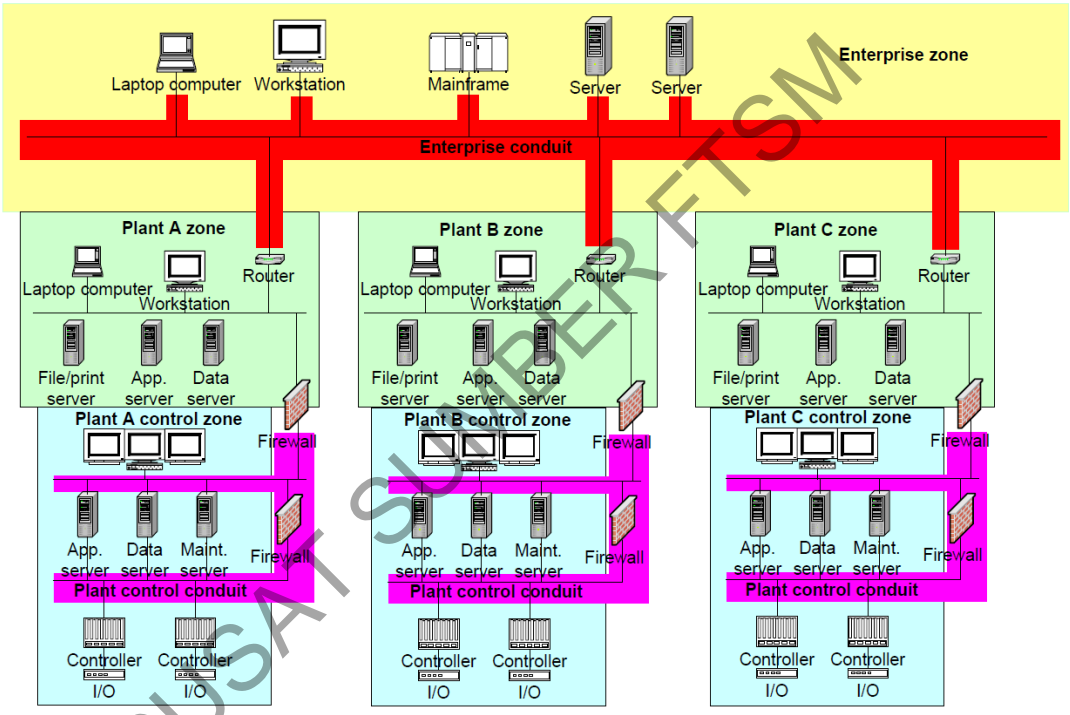



Rajah 2.2 Kategori Terangkum Dalam IEC62443

Sumber: IEC62443

Salah satu komponen penting piawaian IEC62443 ialah penekanannya pada seni bina rujukan (Reference Architecture), khususnya konsep "zon dan konduit". Rangka kerja ini menggambarkan bagaimana pelbagai komponen dalam Sistem Automasi dan

Kawalan Perindustrian (IACS) harus dibahagikan dan saling berkaitan. Dengan mewujudkan zon yang berbeza dan memastikan konduit selamat untuk komunikasi antara mereka, piawaian ini menyediakan pendekatan berstruktur untuk melindungi komponen sistem daripada potensi ancaman siber. Pelan tindakan seni bina ini bukan sahaja meningkatkan keselamatan siber tetapi juga menyelaraskan integrasi dan pengurusan sistem. Contoh yang ditunjukkan di dalam IEC62443 adalah seperti dalam Rajah 2.3 di bawah.






Rajah 2.3 Konsep Zon dan Konduit Pada Seni Bina Rujukan

Sumber: IEC62443

Dari aspek seni bina, IEC62443 menekankan pendekatan yang komprehensif dan berkaedah untuk memastikan keselamatan siber yang teguh. Langkah-langkah ini ialah pembahagian sistem, yang melibatkan pengkategorian rangkaian ke dalam zon yang berbeza, masing-masing dicirikan oleh keperluan keselamatan yang serupa, dan konduit, yang berfungsi sebagai laluan komunikasi antara zon ini. Setiap zon dan konduit mesti mempunyai tahap keselamatan sasaran yang ditentukan, ditentukan melalui penilaian risiko yang teliti. Selain itu, pengerasan peranti adalah penting,

memastikan peranti dikonfigurasikan dengan selamat dengan menghapuskan perkhidmatan yang berlebihan dan menutup port yang tidak diperlukan. Sama pentingnya ialah pelaksanaan mekanisme pengesahan pengguna yang teguh, menjamin bahawa pengguna hanya boleh mengakses sumber yang penting untuk peranan mereka. Untuk mengatasi landskap ancaman siber yang sentiasa berkembang, adalah penting untuk mengekalkan rejimen kemas kini perisian dan perisian tegar biasa, menampal sebarang kelemahan yang diketahui. Selain itu, seni bina harus dilengkapi dengan sistem pengesanan pencerobohan, dilengkapi dengan strategi tindak balas insiden yang jelas. Kesemua ini adalah diperlukan bagi memastikan seni bina OT dan integrasi OT-IT mematuhi piawaian yang diperlukan oleh IEC62443.

### 2.3.2 Piawaian Berkaitan yang Lain

#### a. ISO/IEC 17799 dan ISO/IEC 27001

Piawaian IEC62443 disesuaikan secara khusus untuk Sistem Automasi dan Kawalan Perindustrian (IACS), memfokuskan pada memastikan keselamatan siber sistem ini dalam sektor perindustrian. Ia menekankan pembahagian sistem, menentukan tahap keselamatan untuk zon dan konduit, dan langkah khusus lain yang berkaitan dengan persekitaran industri. Sebaliknya, ISO/IEC 17799, yang kemudiannya menjadi ISO/IEC 27002, dan piawaian pengiringnya ISO/IEC 27001, bersifat lebih umum. Mereka menyediakan rangka kerja untuk pengurusan keselamatan maklumat dalam organisasi, meliputi rangkaian luas sistem IT. Walaupun IEC62443 lebih khusus, memfokuskan pada cabaran unik IACS, ISO/IEC 17799 dan 27001 menawarkan pendekatan holistik kepada keselamatan maklumat, yang boleh digunakan untuk rangkaian organisasi dan sektor yang lebih luas.

#### b. ISA99

IEC62443 dan ISA 99 pada dasarnya, adalah sama. Piawaian IEC62443 pada mulanya dibangunkan oleh Persatuan Automasi Antarabangsa (ISA) sebagai ISA 99. Ia kemudiannya diterima pakai oleh Suruhanjaya Elektroteknikal Antarabangsa (IEC), menjadi IEC62443. Kedua-dua piawaian menangani keselamatan siber IACS, menekankan keperluan untuk pendekatan yang disesuaikan untuk melindungi sistem

perindustrian daripada ancaman siber. Penjajaran mereka mempamerkan pengiktirafan global tentang kepentingan mendapatkan IACS.

**c. NIST SP 800-82**

Penerbitan Khas (SP) 800-82 Institut Piawaian dan Teknologi Kebangsaan (NIST) ialah satu lagi piawaian yang menangani keselamatan siber IACS. Seperti IEC62443, ia direka untuk memenuhi keperluan unik sistem perindustrian. Walau bagaimanapun, walaupun IEC62443 ialah piawaian antarabangsa dengan perspektif global, NIST SP 800-82 ialah piawaian Amerika Syarikat, selalunya sejajar dengan peraturan Amerika Syarikat dan kebimbangan negara yang khusus. Kedua-dua piawaian ini menekankan kepentingan pembahagian sistem, tampalan biasa dan pengesahan pengguna. Walau bagaimanapun, NIST SP 800-82 sering menggunakan panduan yang lebih terperinci tentang ancaman dan kelemahan tertentu, terutamanya yang berkaitan dengan infrastruktur kritikal Amerika Syarikat. Sebagai perbandingan, IEC62443 menyediakan rangka kerja yang lebih tinggi, membolehkan fleksibiliti dalam aplikasinya merentas konteks global yang berbeza.

Walaupun semua piawaian ini bertujuan untuk meningkatkan keselamatan siber, skop, kedalaman dan tumpuannya berbeza-beza. Kekuatan IEC62443 terletak pada tumpuan khususnya pada cabaran unik IACS, manakala piawaian lain seperti ISO/IEC 17799 dan 27001 menawarkan garis panduan keselamatan maklumat yang lebih luas. NIST SP 800-82, sebaliknya, menyediakan panduan terperinci yang disesuaikan dengan kebimbangan infrastruktur kritikal Amerika Syarikat.



### 2.3.3 Kepentingan IEC62443 dalam Integrasi OT-IT

Integrasi sistem OT dan IT dalam industri Minyak dan Gas membawa banyak faedah, seperti peningkatan kecekapan operasi, analisis data masa nyata dan membuat keputusan secara pantas. Bagaimanapun, integrasi ini turut mendedahkan sektor Minyak dan Gas kepada risiko ancaman siber yang tinggi. Piawaian IEC62443 memainkan peranan penting dalam mengurangkan risiko ini dan memastikan integrasi OT-IT yang selamat.

Dengan mengguna pakai piawaian IEC62443, syarikat Minyak dan Gas boleh menyelaraskan amalan keselamatan siber mereka dengan amalan terbaik industri dan piawaian antarabangsa. Piawaian ini menawarkan pendekatan holistik terhadap keselamatan siber, menangani bukan sahaja aspek teknologi tetapi juga faktor organisasi dan prosedur. Ia menekankan kepentingan pengurusan risiko, pemantauan berterusan, dan perancangan tindak balas insiden. Melaksanakan piawaian IEC62443 membolehkan syarikat Minyak dan Gas mewujudkan rangka kerja keselamatan siber yang teguh, melindungi aset kritikal, melindungi daripada akses tanpa kebenaran dan mengekalkan kerahsiaan, integriti dan ketersediaan sistem mereka (U Gentile et al. 2019).

## 2.4 PERMASALAHAN RINTANGAN DALAM INTEGRASI OT-IT

Dalam proses mengintegrasikan sistem Teknologi Operasi (OT) dan Teknologi Maklumat (IT), beberapa permasalahan akan dihadapi dan mesti ditangani untuk memastikan integrasi OT-IT berjaya. Bab ini mengkaji permasalahan penting yang dihadapi oleh organisasi dalam industri Minyak dan Gas semasa proses integrasi ini. Memahami dan mengurangkan permasalahan ini adalah penting untuk mewujudkan persekitaran OT-IT yang berdaya tahan dan selamat (Alahmari 2023).

### 2.4.1 Kerumitan Teknikal dalam Integrasi OT-IT

Integrasi sistem OT dan IT membawa pelbagai kerumitan teknikal. Kerumitan ini timbul daripada perbezaan dalam teknologi, protokol komunikasi dan seni bina antara domain OT dan IT. Mengintegrasikan sistem OT lama dengan infrastruktur IT moden boleh mengemukakan isu keserasian, variasi dalam format data dan cabaran dalam seni bina rangkaian. Organisasi perlu menangani kerumitan teknikal ini untuk memudahkan pertukaran data dan aliran maklumat yang lancar antara sistem OT dan IT (Berardi et al. 2023).

### 2.4.2 Isu Keserasian dalam Integrasi OT-IT

Isu keserasian adalah cabaran biasa apabila menyepadukan sistem OT dan IT. Sistem OT legasi, yang mungkin telah dibangunkan tanpa mengambil kira integrasi IT, selalunya tidak mempunyai keserasian dengan teknologi dan protokol IT moden. Ini

boleh mengakibatkan kesukaran dalam perkongsian data, integrasi aplikasi dan mencapai kesalingoperasian antara sistem OT dan IT. Organisasi dalam industri Minyak dan Gas mesti menangani isu keserasian ini untuk memastikan integrasi yang lancar dan kerjasama yang berkesan antara domain OT dan IT (Berardi et al. 2023).

### 2.4.3 Kekangan Sumber dalam Integrasi OT-IT

Melaksanakan integrasi OT-IT memerlukan sumber yang besar, termasuk pelaburan kewangan, kakitangan mahir dan masa. Banyak organisasi dalam industri Minyak dan Gas menghadapi kekangan sumber yang boleh menghalang proses integrasi. Belanjawan terhad, kekurangan profesional mahir dengan kepakaran dalam kedua-dua domain OT dan IT, dan keutamaan operasi boleh mewujudkan halangan kepada integrasi yang berjaya. Organisasi mesti mengenal pasti strategi untuk mengatasi kekangan sumber ini dan memperuntukkan sumber yang mencukupi untuk memastikan kelancaran pelaksanaan inisiatif integrasi OT-IT (A Sobol et al. 2020).

### 2.4.4 Risiko Keselamatan dan Ancaman Siber

Mengintegrasikan sistem OT dengan rangkaian IT meningkatkan pendedahan kepada risiko keselamatan dan ancaman siber. Sifat saling berkaitan sistem OT-IT mendedahkan potensi kelemahan yang boleh dieksploitasi oleh pihak yang berniat jahat. Risiko keselamatan siber termasuklah akses tanpa kebenaran, pelanggaran data dan potensi gangguan kepada operasi kritikal. Organisasi dalam industri Minyak dan Gas mesti mengutamakan langkah keselamatan siber untuk mengurangkan risiko ini dan memastikan kerahsiaan, integriti dan ketersediaan sistem OT-IT mereka (Ocaka et al. 2022).

### 2.4.5 Faktor Organisasi dan Budaya

Integrasi OT-IT bukan sahaja melibatkan cabaran teknikal tetapi juga faktor organisasi dan budaya. Perbezaan dalam struktur organisasi, proses dan keutamaan antara jabatan OT dan IT boleh menghalang kerjasama dan penyelarasan yang berkesan. Selain itu, jurang budaya antara domain operasi dan teknologi maklumat boleh membawa kepada penentangan terhadap perubahan dan kekurangan pemahaman tentang perspektif masing-masing. Organisasi mesti menangani faktor organisasi dan budaya ini untuk

memupuk persekitaran kolaboratif dan kohesif yang kondusif untuk integrasi OT-IT yang berjaya (Abbatemarco et al. 2022).

### 2.4.6 Permasalahan Kawal Selia

Industri Minyak dan Gas beroperasi dalam persekitaran yang sangat terkawal dengan keperluan khusus untuk keselamatan, perlindungan alam sekitar dan keselamatan siber. Pematuhan dengan piawaian dan peraturan industri adalah penting semasa integrasi OT-IT. Walau bagaimanapun, menangani landskap kompleks keperluan kawal selia dan memastikan pematuhan merentas kedua-dua domain OT dan IT adalah sangat mencabar. Organisasi mesti secara proaktif menangani cabaran kawal selia dan pematuhan untuk memastikan pematuhan kepada piawaian dan peraturan yang berkaitan (Filkins et al. 2019).

### 2.4.7 Obsolesi Sistem Legasi

Banyak organisasi dalam industri Minyak dan Gas bergantung pada sistem OT legasi yang mungkin menghadapi isu obsolesi. Sistem legasi ini mungkin tidak menerima kemas kini atau sokongan biasa daripada vendor, menjadikannya mudah terdedah kepada kelemahan keselamatan dan isu keserasian dengan infrastruktur IT moden. Adalah penting bagi organisasi untuk membangunkan strategi untuk mengurus obsolesi sistem legasi, termasuk rancangan pemodenan dan strategi migrasi yang selamat, untuk memastikan proses integrasi OT-IT yang lancar dan selamat (Berardi et al. 2023).



## 2.5 PERANAN KAKITANGAN DALAM INTEGRASI OT-IT

Integrasi sistem Teknologi Operasi (OT) dan Teknologi Maklumat (IT) memerlukan kerjasama dan penyelarasan yang berkesan di kalangan kakitangan dari kedua-dua domain. Bab ini meneroka peranan penting kakitangan dalam integrasi OT-IT dalam konteks industri Minyak dan Gas. Ia menyelidiki perbezaan dalam pengetahuan, keutamaan dan amalan antara kakitangan OT dan IT, menganalisis kesan perbezaan ini pada proses integrasi, dan membentangkan strategi untuk merapatkan jurang dan memupuk kerjasama yang berjaya.

### 2.5.1 Perbezaan dalam Pengetahuan, Keutamaan dan Amalan antara OT dan Kakitangan IT

Kakitangan OT dan kakitangan IT membawa bidang kepakaran yang berbeza, yang sering membawa kepada perbezaan dalam pengetahuan, keutamaan dan amalan. Kakitangan OT biasanya mempunyai pengetahuan yang mendalam tentang proses industri, keperluan keselamatan, dan kebolehpercayaan operasi. Kepakaran mereka terletak pada mengekalkan ketersediaan dan kefungsian sistem industri kritikal. Sebaliknya, kakitangan IT pakar dalam infrastruktur rangkaian, keselamatan siber, pengurusan data dan integrasi sistem. Mereka menumpukan pada memastikan kerahsiaan, integriti dan ketersediaan data dan sistem maklumat. Bidang kepakaran yang berbeza ini boleh mewujudkan jurang komunikasi dan menghalang kerjasama yang berkesan antara kakitangan OT dan IT semasa proses integrasi.

Selain itu, kakitangan OT dan IT sering mempunyai keutamaan yang berbeza disebabkan oleh perspektif dan tanggungjawab mereka yang unik. Kakitangan OT mengutamakan keselamatan, kebolehpercayaan dan kesinambungan operasi, kerana sebarang gangguan dalam bidang ini boleh membawa kesan yang teruk ke atas proses industri dan keselamatan kakitangan. Sebaliknya, kakitangan IT mengutamakan keselamatan data, integriti rangkaian dan prestasi sistem. Keutamaan yang berbeza ini kadangkala boleh membawa kepada konflik dan cabaran apabila cuba menyelaraskan objektif dan mereka bentuk sistem bersepadu.

Selain itu, perbezaan dalam amalan dan metodologi antara kakitangan OT dan IT boleh menambahkan lagi cabaran kerjasama. Kakitangan OT sering mengikut prosedur, amalan dan piawaian yang ditetapkan khusus untuk industri mereka. Sebaliknya, kakitangan IT mematuhi amalan terbaik industri, rangka kerja keselamatan siber dan rangka kerja tadbir urus IT. Perbezaan dalam amalan ini boleh menimbulkan kesukaran dalam menjajarkan proses dan aliran kerja semasa integrasi sistem OT dan IT (A Sobol et al. 2020).

### 2.5.2 Kesan Perbezaan Skil dan Keutamaan Kakitangan terhadap Integrasi OT-IT

Perbezaan dalam pengetahuan, keutamaan dan amalan antara kakitangan OT dan IT boleh memberi kesan ketara kepada proses integrasi OT-IT. Ketidakselarian objektif dan keutamaan boleh berlaku disebabkan oleh perspektif yang berbeza tentang keperluan operasi berbanding pertimbangan keselamatan siber. Ini boleh membawa kepada cabaran dalam mereka bentuk dan melaksanakan sistem bersepadu yang memenuhi keperluan kedua-dua domain dengan berkesan. Jurang komunikasi yang disebabkan oleh perbezaan dalam istilah, jargon dan pemahaman teknikal boleh mengakibatkan salah komunikasi, salah faham dan ralat semasa proses integrasi.

Kesan perbezaan kakitangan melangkaui aspek teknikal kepada budaya organisasi dan kerjasama. Jurang budaya antara domain operasi dan teknologi maklumat boleh menghalang kerja berpasukan dan komunikasi yang berkesan. Penentangan terhadap perubahan, kekurangan persefahaman bersama dan ketidakpercayaan antara kakitangan OT dan IT boleh menghalang proses integrasi dan mengakibatkan hasil yang tidak optimum (G Murino 2021).



## 2.6 INTEGRASI OT-IT DALAM SEKTOR MINYAK DAN GAS

Integrasi Teknologi Operasi (OT) dan Teknologi Maklumat (IT) merupakan aspek kritikal dalam perjalanan transformasi digital dalam sektor Minyak dan Gas. Bab ini mendalami penerokaan pelbagai kajian kes yang menonjolkan pelaksanaan integrasi OT-IT dalam sektor Minyak dan Gas. Ia memberikan pemahaman yang mendalam tentang aspek praktikal, cabaran dan kisah kejayaan yang dikaitkan dengan integrasi OT-IT dalam sektor ini. Bab ini dibahagikan kepada tiga bahagian utama.

### 2.6.1 Gambaran Keseluruhan Integrasi OT-IT dalam Sektor Minyak dan Gas

Sektor Minyak dan Gas telah menjadi asas ekonomi global selama beberapa dekad, menyediakan tenaga yang diperlukan untuk menggerakkan industri, memanaskan rumah dan pengangkutan bahan api. Dalam beberapa tahun kebelakangan ini, sektor ini telah mengalami transformasi digital yang ketara, dengan integrasi Teknologi Operasi (OT) dan Teknologi Maklumat (IT) memainkan peranan penting dalam proses ini.

Integrasi OT-IT dalam sektor Minyak dan Gas melibatkan integrasi sistem IT tradisional, yang mengurus data dan proses maklumat, dengan sistem kawalan industri (ICS) dan sistem OT lain yang memantau dan mengawal proses fizikal dalam operasi Minyak dan Gas. Integrasi ini didorong oleh keperluan untuk meningkatkan kecekapan operasi, meningkatkan pembuatan keputusan dan memastikan keselamatan infrastruktur kritikal.

Proses integrasi melibatkan beberapa langkah utama, termasuk penjajaran strategi IT dan OT, penggunaan piawaian dan protokol biasa, dan pelaksanaan langkah keselamatan siber yang teguh untuk melindungi daripada potensi ancaman. Matlamat utama adalah untuk mewujudkan infrastruktur digital yang bersatu, selamat dan cekap yang boleh menyokong operasi kompleks sektor Minyak dan Gas (M Ghadrdan et al. 2022).

### 2.6.2 Integrasi OT-IT dalam Sektor Minyak dan Gas dan Sektor Infrastruktur Kritikal Lain

Integrasi OT dan IT adalah elemen asas dalam pemodenan dan perlindungan infrastruktur kritikal. Setiap sektor dalam infrastruktur ini, sama ada Air, Tenaga, Komunikasi atau Pengangkutan, mempunyai cabaran dan keperluan yang berbeza apabila ia berkaitan dengan integrasi ini.

Sektor Air, misalnya, berkisar pada pemantauan berterusan dan pengurusan rawatan, pengagihan dan kualiti air. Memastikan bekalan air yang konsisten dan mengekalkan data masa nyata daripada pelbagai penderia adalah penting. Aspek fizikal, seperti aliran air dan tekanan, memainkan peranan penting, menambah lapisan kerumitan kepada proses integrasi.

Dalam sektor Tenaga, tumpuan adalah pada penjanaan kuasa, pengagihan, dan pemantauan penggunaan. Sektor ini ditugaskan untuk mengurus sistem grid yang luas, melindungi loji penjanaan kuasa, dan memastikan keseimbangan antara permintaan kuasa dan bekalan dalam masa nyata. Sektor Komunikasi berdiri sebagai tulang belakang dunia kita yang saling berkaitan. Ia direka bentuk sekitar penghantaran data, penerimaan dan penyimpanan. Memastikan perkhidmatan komunikasi tanpa gangguan

dan menyepadukan banyak saluran komunikasi, masing-masing dengan protokol dan piawaiannya yang unik, adalah cabaran utama. Privasi data, memandangkan sejumlah besar data yang dihantar, adalah kebimbangan yang ketara.

Sektor Pengangkutan menekankan kawalan lalu lintas, pemantauan kenderaan, dan pengoptimuman laluan. Dengan kenderaan sentiasa bergerak dan laluan yang kerap berubah, pengurusan data trafik masa nyata menjadi penting. Keselamatan kekal menjadi keutamaan, memastikan aliran trafik lancar dan mencegah kemungkinan kemalangan.

Sektor Minyak dan Gas menampilkan landskap yang agak berbeza. Tidak seperti sektor lain, industri Minyak dan Gas beroperasi dalam persekitaran yang sering terpencil dan ekstrem, daripada platform penggerudian laut dalam kepada medan minyak padang pasir yang luas. Keperluan untuk data masa nyata bukan hanya mengenai kecekapan operasi tetapi sangat terikat dengan aspek keselamatan. Gangguan atau salah komunikasi boleh membawa kepada akibat ekonomi, alam sekitar dan manusia yang teruk. Tambahan pula, sektor Minyak dan Gas berurusan dengan pengekstrakan, pengangkutan, dan penapisan hidrokarbon, menguruskan bahan meruap dalam keadaan yang melampau. Ini menjadikan integrasi sistem OT dan IT bukan sahaja mencabar tetapi juga kritikal. Talian paip, lori tangki dan loji penapisan membentuk jaringan kompleks yang mesti berfungsi dengan lancar, di mana kepentingannya sangat tinggi. Selain itu, persekitaran kawal selia untuk sektor Minyak dan Gas adalah sangat ketat. Potensi implikasi alam sekitar dan ekonomi daripada sebarang kemalangan bermakna peraturan adalah ketat, dan pematuhan adalah yang terpenting. Ini seterusnya membezakan sektor Minyak dan Gas daripada yang lain, menuntut pendekatan khusus untuk integrasi OT-IT yang mempertimbangkan cabaran unik dan kepentingannya yang tinggi.



## 2.7 KESELAMATAN SIBER DALAM INTEGRASI OT-IT

Integrasi rangkaian Teknologi Operasi (OT) dan Teknologi Maklumat (IT) dalam sektor Minyak dan Gas telah membuka ruang baharu untuk produktiviti dan kecekapan. Walau bagaimanapun, integrasi ini juga memberikan satu set cabaran keselamatan siber yang unik.

### 2.7.1 Kepentingan Keselamatan Siber dalam Integrasi OT-IT

Konvergensi rangkaian OT dan IT telah mewujudkan paradigma baharu dalam sektor Minyak dan Gas. Integrasi ini telah membawa banyak kelebihan, seperti kecekapan operasi yang lebih baik dan pembuatan keputusan berasaskan data. Walau bagaimanapun, ia juga telah memperkenalkan pelbagai risiko keselamatan siber. Keselamatan siber bukan lagi difikirkan semula atau kemewahan tetapi satu keperluan dalam persekitaran bersepadu ini. Potensi risiko dan akibat ancaman siber dalam sektor Minyak dan Gas adalah penting, daripada gangguan operasi kepada bahaya keselamatan. Oleh itu, pendekatan proaktif terhadap keselamatan siber adalah penting untuk melindungi infrastruktur kritikal sambil meraih faedah transformasi digital.

Dalam konteks ini, kepentingan keselamatan siber dalam integrasi OT-IT tidak boleh dilebih-lebihkan. Apabila garis antara OT dan IT kabur, keperluan untuk langkah keselamatan siber yang teguh menjadi semakin jelas. Sifat rangkaian yang saling berkait ini bermakna bahawa kelemahan dalam satu berpotensi boleh mendedahkan keseluruhan sistem kepada ancaman siber. Ini memerlukan pendekatan menyeluruh terhadap keselamatan siber yang menangani cabaran unik dan kerumitan integrasi OT-IT (G Lykou et al. 2018).

### 2.7.2 Landskap Ancaman Siber dalam Integrasi OT-IT

Landskap ancaman siber dalam konteks integrasi OT-IT adalah kompleks dan sentiasa berkembang. Apabila sektor Minyak dan Gas menjadi semakin digital, ia menjadi sasaran yang lebih menarik untuk penjenayah siber. Pelbagai jenis ancaman wujud, termasuk perisian hasad, perisian tebusan dan serangan yang disasarkan. Ancaman ini boleh memberi kesan yang besar terhadap operasi dan keselamatan sektor Minyak dan Gas. Sebagai contoh, serangan siber yang berjaya boleh mengganggu operasi, membawa kepada kerugian kewangan yang ketara dan potensi bahaya keselamatan.

Landskap ancaman siber dalam integrasi OT-IT dicirikan oleh pelbagai pelaku ancaman, daripada penggodam individu kepada kumpulan tajaan kerajaan. Pelakon ini semakin canggih dan berterusan, menggunakan pelbagai taktik, teknik dan prosedur untuk menjejaskan rangkaian OT dan IT. Tambahan pula, integrasi rangkaian OT dan

IT telah meluaskan permukaan serangan, menyediakan lebih banyak pintu masuk untuk penjenayah siber. Landskap ancaman yang berkembang ini menekankan keperluan untuk pemantauan berterusan dan pengemaskinian langkah keselamatan siber untuk melindungi daripada ancaman yang muncul (Progoulakis et al. 2021).

## 2.8 PEMATUHAN PIAWAIAN INDUSTRI DALAM INTEGRASI OT-IT

Dalam landskap integrasi Teknologi Operasi (OT) dan Teknologi Maklumat (IT) yang berkembang pesat, pematuhan terhadap piawaian industri telah muncul sebagai asas strategi keselamatan siber yang berkesan. Piawaian ini, yang dibangunkan oleh pakar industri dan badan kawal selia, menyediakan rangka kerja komprehensif untuk mendapatkan rangkaian bersepadu dan mengurangkan potensi ancaman siber.

### 2.8.1 Kepentingan Pematuhan Piawaian Industri

Kepentingan pematuhan dengan piawaian industri, seperti IEC62443, penting dalam konteks integrasi OT-IT. Piawaian ini menyediakan garis panduan terperinci untuk mendapatkan Sistem Automasi dan Kawalan Perindustrian (IACS), yang menggariskan keperluan untuk pembahagian rangkaian, pengerasan sistem, kawalan akses dan tindak balas insiden, antara lain. Pematuhan kepada piawaian ini memastikan penubuhan seni bina rangkaian OT-IT yang teguh dan selamat, yang penting untuk melindungi infrastruktur daripada potensi ancaman siber.

Selain itu, pematuhan terhadap piawaian industri selalunya merupakan keperluan kawal selia, menjadikannya kewajipan undang-undang untuk organisasi dalam sektor Minyak dan Gas. Ketidakpatuhan boleh membawa kepada hukuman yang berat, termasuk denda dan sekatan. Di luar implikasi undang-undang, pematuhan terhadap piawaian industri juga memberi isyarat kepada pihak berkepentingan, termasuk pelanggan, rakan kongsi dan pengawal selia, bahawa organisasi komited untuk mengekalkan tahap keselamatan siber yang tinggi, dengan itu meningkatkan reputasi dan kebolehpercayaannya.

### 2.8.2 Usaha dalam Pematuhan Piawaian Industri

Walaupun pematuhan amat penting, mencapai dan mengekalkan pematuhan piawaian industri adalah tugas yang kompleks dan intensif sumber. Ia memerlukan pemahaman yang mendalam tentang keperluan piawaian, penilaian risiko yang komprehensif untuk mengenal pasti potensi kelemahan, dan pelaksanaan tindakan balas yang diperlukan. Proses ini boleh menjadi sangat mencabar dalam konteks integrasi OT-IT, memandangkan kerumitan dan kelemahan unik yang dikaitkan dengan rangkaian ini.

Tambahan pula, pematuhan bukanlah usaha sekali sahaja tetapi proses berterusan yang memerlukan pemantauan berterusan dan pengemaskinian langkah keselamatan siber. Sifat pematuhan yang berterusan ini boleh menimbulkan cabaran yang ketara, terutamanya bagi organisasi yang mempunyai sumber terhad. Selain itu, landskap ancaman siber yang berkembang pesat bermakna keperluan pematuhan sentiasa berubah, memerlukan organisasi untuk mengikuti perkembangan terkini dan menyesuaikan strategi pematuhan mereka dengan sewajarnya.

### 2.8.3 Pendekatan Untuk Memastikan Pematuhan Piawaian Industri

Memandangkan kepentingan dan cabaran pematuhan, adalah penting bagi organisasi untuk melaksanakan usaha yang berkesan untuk memastikan pematuhan piawaian industri. Satu pendekatan utama ialah menjalankan audit berkala untuk menilai tahap pematuhan. Pengauditan ini boleh mengenal pasti bidang ketidakpatuhan dan memberikan pandangan yang boleh diambil tindakan untuk meningkatkan pematuhan.

Satu lagi usaha penting ialah menyediakan latihan untuk pekerja untuk memastikan mereka memahami keperluan piawaian. Ini boleh membantu memupuk budaya pematuhan dalam organisasi, dengan pekerja di semua peringkat memahami peranan dan tanggungjawab mereka dalam mengekalkan pematuhan.

Tambahan pula, organisasi boleh melaksanakan rangka kerja keselamatan siber yang teguh yang selaras dengan piawaian. Rangka kerja ini boleh berfungsi sebagai peta jalan untuk pematuhan, menggariskan langkah dan langkah yang diperlukan untuk mencapai dan mengekalkan pematuhan. Penggunaan teknologi canggih, seperti

automasi dan kecerdasan buatan, juga boleh dimanfaatkan untuk mengautomasikan pemantauan dan pelaporan pematuhan, dengan itu mengurangkan kerumitan dan keperluan sumber yang berkaitan dengan pematuhan.

## 2.9 TREND MASA DEPAN DALAM INTEGRASI OT-IT

Ketika kita mengharungi era transformasi digital, integrasi Teknologi Operasi (OT) dan Teknologi Maklumat (IT) terus berkembang, dipacu oleh teknologi baru muncul dan keperluan perniagaan yang berubah. Bab ini meneroka arah aliran masa depan dalam integrasi OT-IT, memfokuskan pada kesan teknologi baru muncul, pengaruh transformasi digital dan potensi cabaran dan peluang yang menanti.

### 2.9.1 Teknologi Terbaharu dalam Integrasi OT-IT

Teknologi baru muncul memainkan peranan penting dalam membentuk masa depan integrasi OT-IT. Teknologi seperti Internet Perkara (IoT), Kepintaran Buatan (AI) dan Pembelajaran Mesin (ML) merevolusikan cara rangkaian OT dan IT berinteraksi, memacu kecekapan dan membuka kemungkinan baharu untuk inovasi.

IoT, sebagai contoh, membolehkan tahap ketersambungan yang lebih tinggi antara sistem OT dan IT, membolehkan pertukaran data masa nyata dan keterlihatan operasi yang dipertingkatkan. Peningkatan ketersambungan ini memudahkan membuat keputusan yang lebih termaklum, kawalan proses yang lebih baik dan kecekapan operasi yang lebih baik.

Begitu juga, AI dan ML sedang dimanfaatkan untuk menganalisis sejumlah besar data yang dijana oleh rangkaian OT-IT bersepadu, memberikan cerapan berharga untuk penyelenggaraan ramalan, pengesanan anomali dan pengoptimuman proses. Teknologi ini bukan sahaja meningkatkan prestasi rangkaian OT-IT tetapi juga membuka jalan untuk aplikasi yang lebih maju, seperti operasi autonomi dan pembuatan pintar.

### 2.9.2 Kesan Transformasi Digital Terhadap Integrasi OT-IT

Transformasi digital ialah satu lagi pemacu utama arah aliran masa depan dalam integrasi OT-IT. Memandangkan organisasi di seluruh sektor Minyak dan Gas menerima transformasi digital, integrasi rangkaian OT dan IT menjadi komponen penting dalam strategi digital mereka.

Transformasi digital mendorong organisasi untuk memikirkan semula pendekatan integrasi OT-IT mereka, beralih daripada rangkaian tradisional yang terbungkam ke arah sistem yang lebih bersepadu dan boleh dikendalikan. Anjakan ini membolehkan organisasi memanfaatkan potensi penuh data mereka, memacu kecekapan operasi dan memupuk inovasi.

Selain itu, transformasi digital mendorong organisasi untuk menggunakan pendekatan yang lebih proaktif terhadap keselamatan siber. Memandangkan rangkaian OT dan IT menjadi semakin saling berkaitan, keperluan untuk langkah keselamatan siber yang teguh menjadi lebih kritikal. Ini memacu penggunaan penyelesaian keselamatan siber termaju, seperti pengesanan ancaman berasaskan AI dan tindak balas insiden automatik, seterusnya membentuk masa depan integrasi OT-IT.



### 2.9.3 Cabaran dan Peluang Masa Depan dalam Integrasi OT-IT

Memandang ke hadapan, integrasi rangkaian OT dan IT membentangkan kedua-dua cabaran dan peluang. Di satu pihak, kerumitan rangkaian bersepadu yang semakin meningkat, ditambah pula dengan landskap ancaman siber yang semakin berkembang, menimbulkan cabaran besar bagi organisasi. Memastikan keselamatan dan kebolehpercayaan rangkaian bersepadu, di samping memanfaatkan potensi penuh mereka, akan memerlukan usaha dan pelaburan yang berterusan.

Sebaliknya, integrasi rangkaian OT dan IT membuka banyak peluang untuk organisasi. Rangkaian bersepadu boleh memacu kecekapan operasi, membolehkan model perniagaan baharu dan memupuk inovasi. Selain itu, apabila teknologi baru muncul terus berkembang, mereka berkemungkinan menawarkan lebih banyak kemungkinan untuk mempertingkatkan integrasi OT-IT.

## 2.10 KESIMPULAN

Kajian kesusasteraan ini telah mendedahkan beberapa cabaran utama dalam integrasi Teknologi Operasi (OT) dan rangkaian Teknologi Maklumat (IT) dengan mematuhi piawaian IEC62443. Cabaran ini termasuk kerumitan teknikal, isu keserasian, kekangan sumber dan perbezaan dalam pengetahuan, keutamaan dan amalan antara kakitangan OT dan IT. Kajian juga telah menekankan kepentingan pematuhan piawaian industri dan peranan teknologi baru muncul dalam membentuk masa depan integrasi OT-IT.

Penemuan kajian ini mempunyai implikasi kepada pihak berkepentingan industri. Bagi pembuat keputusan dan profesional yang terlibat dalam integrasi OT-IT, cabaran yang dikenal pasti memberikan pemahaman menyeluruh tentang kerumitan yang terlibat dalam proses migrasi kepada seni bina yang mematuhi IEC62443. Pemahaman ini boleh memaklumkan pembangunan strategi dan pendekatan yang berkesan untuk mengatasi cabaran ini, dengan itu meningkatkan keselamatan dan kebolehpercayaan rangkaian OT-IT dalam tetapan infrastruktur kritikal.

Bagi badan kawal selia dan organisasi penetapan piawai, penemuan menggariskan kepentingan garis panduan yang jelas dan praktikal untuk integrasi OT-IT. Cabaran yang dikenal pasti menyerlahkan keperluan untuk piawaian yang menangani kerumitan unik dan kelemahan rangkaian bersepadu, dengan itu membantu organisasi dalam mencapai pematuhan dan meningkatkan keselamatan siber.

Bagi penyelidik dan ahli akademik, penemuan ini menyumbang kepada badan pengetahuan mengenai integrasi OT-IT, menyediakan asas untuk kajian masa depan dalam bidang ini.

# BAB III

# KAEDAH KAJIAN

## 3.1 PENGENALAN

Projek kajian tidak hanya melibatkan menghimpun maklumat tetapi juga melibatkan mencari jawapan kepada soalan-soalan yang masih belum terjawab dan menjana atau mencipta pengetahuan baru. Kaedah kajian juga melibatkan penggunaan beberapa kaedah atau syarat yang digunakan dalam kajian serta menggunakan "prinsip, teori, dan nilai-nilai" yang dapat menyokong pendekatan kajian yang dilakukan. Dengan kata lain, kaedah kajian untuk projek kajian harus menjelaskan bagaimana mengumpul atau menjana data dan kemudian menunjukkan cara anda menganalisanya.

## 3.2 REKA BENTUK KAJIAN

Dalam projek ini, kajian dimulakan dengan melaksanakan kajian kesusasteraan untuk mengenal pasti dan merumuskan penyataan masalah untuk merangka objektif kajian yang jelas. Setelah skop kajian telah ditentukan, kajian akan melalui proses seterusnya iaitu dengan melaksanakan implementasi sebenar untuk menganalisa penyataan masalah yang dibangkitkan. Setelah hasil implementasi dianalisis dan dapat dirumuskan, satu kesimpulan akan dibuat dan satu garis panduan akan direka untuk mengurangkan masalah pertanyaan tersebut. Maklumat lengkap reka bentuk akan dibincangkan pada kaedah seterusnya. Secara ringkasnya proses kaedah kajian adalah seperti di Jadual 3.1.

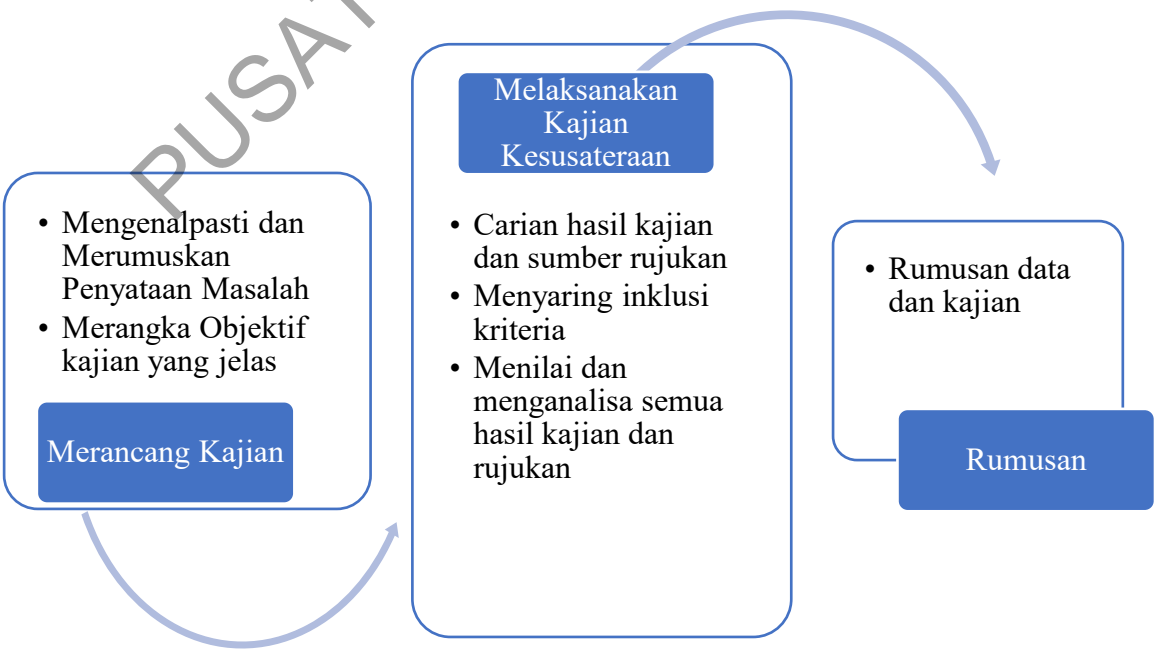
Jadual 3.1 Reka Bentuk Kajian Daripada Penyataan Masalah Sehinggalah Hasil Kajian

| Penyataan Masalah | Objektif Kajian | Skop Kajian | Hasil Kajian |
|---|---|---|---|
| 1. Keperluan transformasi digital memerlukan integrasi OT-IT yang mendedahkan persekitaran OT kepada ancaman siber.<br>2. Untuk mengurangkan risiko, seni bina mematuhi piawaian IEC62443.<br>3. Proses integrasi OT-IT dalam mematuhi piawaian IEC62443 mempunyai pelbagai cabaran. | 1. Mengenal pasti cabaran dalam proses migrasi ke seni bina OT-IT patuh piawaian EIC62443.<br>2. Mengenalpasti isu teknikal dan halangan lain yang menghalang kejayaan pelaksanaan seni bina patuh piawaian IEC62443 di sektor Minyak dan gas. | 1. Integrasi OT-IT dalam industri Minyak dan Gas berdasarkan model Purdue dan IEC62443.<br>2. Kajian secara praktikal<br>3. Fokus terhadap cabaran dihadapi semasa tahap penilaian, mereka bentuk, dan pelaksanaan proses migrasi | 1. Pelaksanaan proses migrasi<br>2. Perbincangan cabaran yang dihadapi<br>3. Perbincangan mengenai cabaran teknikal |



## 3.3 KAEDAH KAJIAN KESUSASTERAAN

Dalam projek ini, kaedah kajian kesusasteraan yang sistematik digunakan untuk mengumpul kesemua maklumat yang berkaitan tajuk ini untuk menjawab persoalan kajian secara spesifik. Ringkasan proses kajian kesusasteraan adalah seperti Rajah 3.1.




Rajah 3.1 Carta Alir Proses Kajian Kesusasteraan

### 3.3.1 Mengenalpasti Penyataan Masalah

Penyataan masalah akan disenaraikan secara luas pada permulaan kajian dan akan dikecilkan untuk menepati skop kajian serta tajuk kajian dan seterusnya dapat membuat pemilihan data yang jelas agar tidak terlalu banyak data yang diperlukan ketika membuat carian kajian kesusasteraan. Ini dapat meningkatkan kecekapan pengurusan ketika membuat kajian. Setelah kriteria pengecualian dapat dikenal pasti dan kriteria kajian dapat dirumuskan, langkah seterusnya dapat diteruskan

### 3.3.2 Carian Hasil Kajian dan Sumber Rujukan

Kajian kesusasteraan akan memfokuskan sumber-sumber rujukan yang berkaitan dengan skop kajian iaitu :

1) Pengenalan Teknologi Operasi dan Teknologi Maklumat
2) Piawaian IEC62443
3) Integrasi OT-IT dalam Sektor Minyak dan Gas
4) Keselamatan Siber dalam Integrasi OT-IT
5) Masa depan Integrasi OT-IT

Kajian akan dilakukan dengan membuat pembacaan, penilaian dan menyenaraikan rujukan yang penting yang boleh membantu untuk meneruskan kajian pada fasa pengujian. Analisis pada kajian-kajian yang lepas juga diambil agar dapat membantu untuk menganalisa hasil implementasi kajian di lapangan.



## 3.4 PELAKSANAAN KAJIAN SECARA PRAKTIKAL DI LAPANGAN

Dalam kajian ini, pendekatan praktikal diguna pakai, memanfaatkan pengalaman dan pemerhatian langsung penyelidik semasa proses migrasi daripada seni bina sistem kawalan sedia ada kepada seni bina yang mematuhi IEC62443 dalam lima unit Loji Gas dan Minyak Infrastruktur Kritikal Negara. Pendekatan ini amat sesuai untuk kajian ini kerana ia membolehkan penerokaan yang mendalam tentang cabaran dunia sebenar yang dihadapi semasa proses migrasi.

Penyelidik, yang terlibat secara langsung dalam projek migrasi, berfungsi sebagai sumber data utama. Penglibatan langsung ini memberikan perspektif yang unik, membolehkan penyelidik mendokumenkan dan menganalisis proses migrasi secara terperinci. Pemerhatian dan pandangan penyelidik membentuk sebahagian penting data, menyumbang kepada pemahaman menyeluruh tentang kerumitan yang terlibat dalam proses migrasi kepada seni bina yang mematuhi IEC62443.

Pendekatan praktikal yang diguna pakai dalam kajian ini selari dengan objektif kajian, iaitu mengenal pasti dan menganalisis cabaran yang dihadapi semasa proses migrasi. Dengan menggunakan pengalaman dan pemerhatian langsung penyelidik, pendekatan ini memastikan bahawa penemuan kajian berasaskan pengalaman dunia sebenar, meningkatkan kerelevanan dan kebolehgunaan keputusan.

### 3.4.1 Reka Bentuk Kajian Lapangan

Reka bentuk kajian bagi kajian ini adalah metodologi kajian kes. Pendekatan ini amat sesuai untuk kajian ini kerana tumpuannya pada penerokaan yang mendalam dan khusus konteks bagi satu kejadian atau fenomena. Metodologi kajian kes membolehkan pemahaman menyeluruh tentang kerumitan dan cabaran yang terlibat dalam proses migrasi kepada seni bina yang mematuhi IEC62443 dalam konteks dunia sebenar.

Dalam kajian ini, kes yang difokuskan ialah sektor Infrastruktur Kritikal Negara khusus dalam sektor Minyak dan Gas. Pilihan kes ini adalah strategik, kerana ia mewakili senario tipikal dalam industri di mana integrasi rangkaian Teknologi Operasi (OT) dan Teknologi Maklumat (IT) menjadi semakin diperlukan disebabkan oleh tuntutan transformasi digital.

Penglibatan langsung penyelidik dalam projek migrasi di loji ini memberikan peluang unik untuk mendokumentasikan dan menganalisis proses serta cabarannya secara terperinci. Penglibatan ini membolehkan perspektif orang dalam tentang proses migrasi, membolehkan penyelidik menangkap nuansa dan selok-belok yang mungkin terlepas dalam pendekatan kajian yang lebih terpisah.

Penyelidik akan terlibat secara langsung pada tahap penilaian jurang, penilaian risiko, mereka bentuk dan melaksanakan migrasi Sistem Kawalan Komputer dan Integrasi OT-IT menurut piawaian IEC62443 berasaskan Model Purdue, dan berfungsi sebagai Ketua Jurutera Sistem Kawalan dan Instrumentasi bagi projek tersebut.

Metodologi kajian kes juga membolehkan pengumpulan data yang kaya dan terperinci, yang penting untuk mencapai objektif kajian. Melalui dokumentasi terperinci proses migrasi, penyelidik boleh mengenal pasti dan menganalisis cabaran khusus yang dihadapi, kerumitan teknikal, isu keserasian dan kekangan sumber yang dialami semasa setiap peringkat migrasi.

Secara umumnya, metodologi kajian kes menyediakan reka bentuk kajian yang mantap dan fleksibel untuk kajian ini. Ia membolehkan penerokaan mendalam tentang proses migrasi dalam konteks dunia sebenar, menyumbang kepada pemahaman menyeluruh tentang cabaran yang terlibat dalam proses migrasi kepada seni bina yang mematuhi IEC62443.



### 3.4.2 Kaedah Pengumpulan Data

Pengumpulan data adalah komponen penting dalam proses kajian, menyediakan bahan mentah yang menjadi asas untuk analisis dan tafsiran. Dalam kajian ini, kaedah pengumpulan data direka bentuk untuk menangkap maklumat terperinci secara langsung tentang proses migrasi daripada seni bina sistem kawalan sedia ada kepada seni bina yang mematuhi IEC62443 dalam sektor Infrastruktur Kritikal Negara.

Kaedah utama pengumpulan data dalam kajian ini ialah dokumentasi. Penyelidik, yang terlibat secara langsung dalam projek migrasi, akan mengekalkan rekod proses yang komprehensif, mendokumentasikan setiap peringkat secara terperinci. Dokumentasi ini akan merangkumi penerangan tentang tugas yang dilakukan, cabaran yang dihadapi, kerumitan teknikal yang dihadapi, isu keserasian yang timbul dan kekangan sumber yang dialami. Penyelidik juga akan merekodkan sebarang pemerhatian atau pandangan berkaitan yang timbul semasa proses migrasi.

Kaedah pengumpulan data ini amat sesuai untuk kajian ini kerana penglibatan penyelidik secara langsung dalam proses migrasi. Ia membolehkan pengumpulan data yang kaya dan terperinci, menangkap nuansa dan selok-belok proses migrasi yang mungkin terlepas dalam pendekatan kajian yang lebih terpisah.

Selain dokumentasi, penyelidik juga akan menggunakan refleksi sebagai kaedah pengumpulan data. Refleksi melibatkan penyelidik secara kritis memeriksa pengalaman, pemikiran dan perasaan mereka sendiri tentang proses migrasi. Kaedah ini membolehkan penyelidik menangkap elemen subjektif proses migrasi, seperti cabaran dan kesukaran yang dialami pada peringkat peribadi.

Penyelidik turut menjalankan soalan kaji selidik (rujuk Lampiran A) kepada jurutera yang terlibat di dalam kerja-kerja migrasi untuk mengetahui perspektif mereka tentang cabaran yang dihadapi ketika pelaksanaan projek. Soalan kaji selidik ini dijalankan bertujuan mengurangkan dan mengimbangi potensi bias atau berat sebelah penemuan kajian ini.

Secara ringkasnya, kaedah pengumpulan data untuk kajian ini melibatkan dokumentasi dan refleksi terperinci, memberikan gambaran menyeluruh tentang proses migrasi. Kaedah ini selaras dengan reka bentuk dan objektif kajian, memastikan data yang dikumpul adalah relevan dan berguna untuk mencapai matlamat kajian. Bahagian berikut akan memperincikan kaedah analisis data yang digunakan dalam kajian ini



### 3.4.3 Kaedah Analisis Data

Kaedah analisis data untuk kajian ini direka bentuk untuk memberikan pemahaman menyeluruh tentang cabaran yang terlibat dalam proses migrasi kepada seni bina yang mematuhi IEC62443 dalam sektor Infrastruktur Kritikal Negara. Data yang dikumpul, yang terdiri daripada dokumentasi terperinci dan refleksi daripada penyelidik, akan tertakluk kepada analisis menyeluruh menggunakan pendekatan kualitatif.

Langkah pertama dalam proses analisis data akan melibatkan penyusunan data yang dikumpul ke dalam format yang koheren dan boleh diurus. Ini akan melibatkan

pengkategorian data mengikut peringkat proses migrasi, jenis cabaran yang dihadapi dan aspek khusus proses migrasi yang berkaitan dengannya.

Setelah data disusun, penyelidik akan menyemak dan memeriksa dengan teliti cabaran yang didokumenkan untuk mengenal pasti tema, corak dan faktor berulang yang muncul semasa proses migrasi. Ini akan melibatkan proses pengekodan, di mana tema atau kategori tertentu dikenal pasti dan ditanda dalam data.

Penyelidik kemudiannya akan meneruskan analisa kualitatif menerusi proses analisis tematik, di mana data berkod diperiksa untuk mengenal pasti corak dan tema yang ketara. Proses ini memerlukan pemberian tag ringkas kepada segmen data tertentu yang merangkumi intipati terasnya. Selepas itu, "tema" melibatkan menganalisis kod ini untuk membezakan corak yang lebih luas, mengumpulkan kod berkaitan ke dalam kategori menyeluruh. Kategori atau "tema" ini mewakili konsep atau cerapan utama yang diperoleh daripada data. Perkembangan daripada pengekodan kepada penemaan ialah satu langkah daripada pemerhatian yang terperinci dan bernuansa kepada pemahaman tafsiran yang lebih umum tentang set data.

Walau bagaimanapun, adalah penting untuk ambil perhatian bahawa disebabkan sifat sensitif isu keselamatan siber dalam Infrastruktur Kritikal Negara, butiran terperinci penemuan kajian tidak dapat didedahkan sepenuhnya dalam kertas kajian. Oleh itu, hasil analisis kajian dibentangkan secara umum, memfokuskan pada tema dan corak yang lebih luas yang muncul semasa proses migrasi, dan bukannya butiran teknikal tertentu atau kelemahan keselamatan.

Analisis akan memberikan pemahaman yang komprehensif tentang cabaran yang terlibat dalam proses migrasi kepada seni bina yang mematuhi IEC62443 dalam sektor Infrastruktur Kritikal Negara. Ia akan mengenal pasti kerumitan teknikal tertentu, isu keserasian, kekangan sumber dan halangan lain yang menghalang kejayaan pelaksanaan seni bina yang mematuhi IEC62443.

Penggunaan kaedah kaji selidik dalam metodologi keseluruhan berfungsi sebagai alat pengesahan penting untuk penemuan kajian. Tiga rakan sekerja yang

berpengalaman dalam projek integrasi OT-IT diminta berkongsi cabaran yang mereka hadapi semasa projek migrasi. Maklum balas mereka kemudiannya dikod dan dikategorikan, dan dianalisa sama ada boleh diselaraskan dengan empat tema utama yang dikenal pasti sebelum ini dalam kajian. Pendekatan ini bukan sahaja menyokong penemuan awal tetapi juga menawarkan potensi untuk mendedahkan cabaran tambahan. Kaji selidik itu memperkayakan kajian dengan menyediakan perspektif praktikal, mengurangkan bias, dan meningkatkan kredibiliti penyelidikan.

Secara ringkasnya, kaedah analisis data untuk kajian ini melibatkan pendekatan kualitatif, menggunakan pengekodan dan analisis tematik untuk mengenal pasti dan mentafsir cabaran yang dihadapi semasa proses migrasi. Kaedah ini selaras dengan reka bentuk dan objektif kajian, memastikan bahawa analisis memberikan pandangan yang bermakna dan relevan tentang masalah kajian, sambil menghormati keperluan untuk kerahsiaan dan keselamatan dalam konteks Infrastruktur Kritikal Negara. Bahagian berikut akan membincangkan batasan metodologi kajian.



## 3.5 KESIMPULAN

Kajian ini menggunakan pendekatan praktikal, memanfaatkan pengalaman dan pemerhatian langsung penyelidik semasa proses migrasi di sektor Infrastruktur Kritikal Negara. Reka bentuk kajian menggabungkan metodologi kajian kes, memfokuskan pada loji tertentu dalam sektor Minyak dan Gas.

Pengumpulan data melibatkan dokumentasi terperinci proses migrasi, termasuk cabaran yang dihadapi, kerumitan teknikal, isu keserasian dan kekangan sumber. Data ini kemudiannya tertakluk kepada analisis kualitatif yang menyeluruh untuk mengenal pasti tema, corak dan faktor berulang yang muncul semasa proses migrasi.

Walau bagaimanapun, metodologi kajian juga mempunyai batasannya. Penemuan mungkin tidak boleh digeneralisasikan kepada konteks atau sektor lain, dan potensi bias wujud disebabkan oleh pergantungan pada pengalaman dan pemerhatian penyelidik sendiri. Kajian memfokuskan kepada cabaran yang dihadapi semasa proses migrasi, tetapi tidak meneroka secara meluas penyelesaian atau strategi untuk

mengatasi cabaran ini. Sifat kualitatif kaedah analisis data juga memperkenalkan tahap subjektiviti.

Walaupun berhadapan dengan batasan tersebut, kaedah kajian direka bentuk untuk memberikan pandangan berharga tentang cabaran yang terlibat dalam proses migrasi kepada seni bina yang mematuhi IEC62443 dalam sektor Infrastruktur Kritikal Negara. Penemuan ini akan menyumbang kepada pemahaman tentang cabaran ini dan menyediakan asas untuk kajian masa depan dalam bidang ini.

# BAB IV

# HASIL KAJIAN

## 4.1 PENGENALAN

Integrasi rangkaian Teknologi Operasi (OT) dan Teknologi Maklumat (IT) adalah proses yang kompleks, terutamanya apabila proses migrasi ke seni bina yang mematuhi IEC62443. Bab ini membentangkan dapatan kajian yang dijalankan semasa pelaksanaan praktikal migrasi ini di lima loji Minyak dan Gas. Penyelidikan bertujuan untuk mengenal pasti cabaran utama dan kesukaran teknikal yang dihadapi semasa proses, memberikan pemahaman yang menyeluruh tentang selok-belok yang terlibat dalam integrasi OT-IT.

Proses migrasi melibatkan beberapa langkah utama, termasuk pengenalan Zon Demiliterisasi (DMZ), pengasingan rangkaian OT melalui pengezonan, penerapan strategi pertahanan mendalam dengan pengurusan antivirus dan tampalan melalui pelayan IT yang diuruskan secara berpusat, dan pemantauan rangkaian OT. Setiap langkah ini membentangkan cabaran dan kesukaran teknikal yang unik, yang diterokai secara terperinci dalam bab ini.

Proses migrasi telah dijalankan dalam dua peringkat utama: Penilaian dan Reka Bentuk & Pelaksanaan. Peringkat Penilaian melibatkan penilaian menyeluruh rangkaian OT sedia ada, mengenal pasti jurang dan kawasan untuk penambahbaikan. Peringkat Reka Bentuk & Pelaksanaan, sebaliknya, memfokuskan pada pembangunan seni bina rangkaian yang teguh dan selamat yang mematuhi piawaian IEC62443. Kedua-dua peringkat adalah penting dalam membentuk strategi migrasi dan menangani cabaran yang dihadapi.

Penemuan yang dibentangkan dalam bab ini adalah berdasarkan pengalaman dan pemerhatian secara langsung, memberikan perspektif praktikal tentang cabaran integrasi OT-IT. Cerapan yang diperoleh daripada penyelidikan ini menyumbang kepada pemahaman tentang kerumitan yang terlibat dalam proses migrasi kepada seni bina yang mematuhi IEC62443, menawarkan panduan berharga untuk projek integrasi masa hadapan dalam sektor Minyak dan Gas serta industri lain dengan infrastruktur kritikal.

Bahagian seterusnya dalam bab ini menyelidiki keutamaan berbeza OT dan IT, jurang kemahiran antara kakitangan OT dan IT, cabaran yang berkaitan dengan legasi OT dan sistem proprietari, dan kesukaran teknikal dalam melaksanakan keperluan tertentu. Setiap bahagian membentangkan gambaran keseluruhan isu, kesannya terhadap proses integrasi dan contoh kes khusus yang menggambarkan cabaran yang dihadapi. Bab ini diakhiri dengan ringkasan penemuan utama dan implikasinya terhadap objektif kajian.

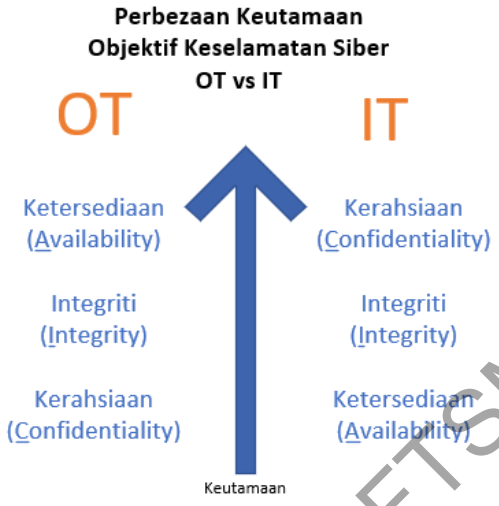


## 4.2 KEUTAMAAN BERBEZA OT DAN IT

Konvergensi rangkaian Teknologi Operasi (OT) dan Teknologi Maklumat (IT) dalam sektor Minyak dan Gas merupakan proses yang kompleks yang memerlukan pemahaman yang jelas tentang keutamaan yang berbeza bagi kedua-dua domain. OT dan IT secara tradisinya beroperasi dalam silo yang berasingan, masing-masing dengan set keutamaan dan objektifnya sendiri. Walau bagaimanapun, integrasi rangkaian ini memerlukan anjakan dalam pemikiran ini, memerlukan kedua-dua OT dan IT untuk menyelaraskan keutamaan mereka ke arah matlamat bersama untuk operasi yang selamat dan cekap.

Dalam konteks keselamatan siber, OT dan IT mempunyai keutamaan yang berbeza. OT mengutamakan Ketersediaan, Integriti dan Kerahsiaan (AIC), dalam susunan tersebut, manakala IT mengutamakan Kerahsiaan, Integriti dan Ketersediaan (CIA). Perbezaan keutamaan ini boleh menyebabkan konflik semasa proses integrasi. Sebagai contoh, kakitangan IT mungkin mengutamakan keselamatan data dan sistem, yang berpotensi menjejaskan ketersediaan sistem OT, yang boleh mempunyai implikasi

operasi yang ketara dalam loji Minyak dan Gas. Ilustrasi perbezaan tersebut seperti Rajah 4.1 di bawah.




Rajah 4.1 Perbezaan Keutamaan Objektif Keselamatan Siber OT dan IT

Semasa proses migrasi di lima loji Minyak dan Gas, perbezaan keutamaan ini terbukti. Kakitangan IT, menumpukan pada keselamatan rangkaian, selalunya akan melaksanakan langkah-langkah yang berpotensi mengganggu operasi OT. Sebagai contoh, kakitangan IT akan menjadualkan kemas kini sistem atau dimulakan semula tanpa mempertimbangkan sepenuhnya kesan ke atas operasi OT. Kekurangan pemahaman dan pertimbangan keutamaan OT oleh kakitangan IT ini menimbulkan cabaran besar semasa proses migrasi.

Untuk menangani cabaran ini, adalah penting untuk memupuk budaya kerjasama dan persefahaman antara kakitangan OT dan IT. Pertemuan dan sesi latihan tetap diadakan untuk mendidik kedua-dua pihak tentang keutamaan dan keperluan pihak yang lain. Ini membantu merapatkan jurang antara OT dan IT, memudahkan integrasi yang lebih lancar dan mengurangkan konflik.

### 4.2.1 Gambaran Keseluruhan Keutamaan OT dan IT

Teknologi Operasi (OT) dan Teknologi Maklumat (IT) mempunyai keutamaan tersendiri yang mencerminkan peranan dan tanggungjawab unik mereka dalam sesebuah organisasi. Memahami keutamaan ini adalah penting untuk integrasi OT-IT

yang berjaya, terutamanya dalam konteks sektor Minyak dan Gas di mana integrasi rangkaian ini menjadi semakin diperlukan.

OT memberi fokus utama berkenaan dengan kawalan langsung dan pemantauan proses perindustrian. Keutamaan utamanya ialah memastikan ketersediaan proses ini, kerana sebarang gangguan boleh mempunyai implikasi operasi dan keselamatan yang ketara. Melalui ketersediaan, OT mengutamakan integriti sistem dan datanya untuk memastikan proses industri beroperasi dengan betul dan boleh dipercayai. Kerahsiaan, walaupun masih penting, selalunya menjadi kebimbangan kedua dalam OT, kerana data yang terlibat biasanya berkaitan proses dan tidak bersifat sensitif.

Sebaliknya, fokus IT terutamanya berkaitan dengan pemprosesan, penyimpanan dan penghantaran data. Keutamaan utamanya ialah kerahsiaan data ini, terutamanya dalam era digital hari ini di mana pelanggaran data boleh membawa akibat kewangan dan reputasi yang teruk. Mengikuti kerahsiaan, IT mengutamakan integriti sistem dan datanya untuk memastikan maklumat itu tepat dan boleh dipercayai. Ketersediaan, walaupun masih penting, sering menjadi kebimbangan kedua dalam IT, kerana gangguan sementara kepada perkhidmatan IT adalah kurang kritikal berbanding gangguan kepada proses OT.

Semasa proses migrasi di lima loji Minyak dan Gas, diperhatikan bahawa keutamaan yang berbeza ini boleh membawa kepada konflik dan salah faham. Sebagai contoh, kakitangan IT, dalam usaha mereka untuk menjamin rangkaian, melaksanakan langkah-langkah yang berpotensi mengganggu operasi OT, tidak menghargai sepenuhnya kritikal ketersediaan dalam persekitaran OT. Sebaliknya, kakitangan OT menentang langkah keselamatan IT yang mereka anggap mengancam ketersediaan atau integriti sistem mereka.

### 4.2.2 Perbezaan Keutamaan dan Kesannya Terhadap Proses Integrasi

Keutamaan yang berbeza antara OT dan IT bukan sahaja membentuk pendekatan masing-masing terhadap kerja mereka tetapi juga memberi kesan ketara kepada proses integrasi. Pengalaman praktikal proses migrasi ke seni bina yang mematuhi IEC62443

dalam lima loji Minyak dan Gas mendedahkan beberapa keadaan di mana perbezaan ini menimbulkan cabaran kepada proses integrasi.

Salah satu cabaran utama ialah pandangan yang berbeza tentang kemas kini dan penyelenggaraan sistem. Kakitangan IT, mengutamakan kerahsiaan dan integriti data, sering menyokong kemas kini sistem yang kerap untuk menambal kelemahan keselamatan. Walau bagaimanapun, kemas kini ini berpotensi mengganggu operasi OT, bercanggah dengan keutamaan OT untuk mengekalkan ketersediaan sistem. Perbezaan dalam pendekatan ini sering menyebabkan konflik semasa proses integrasi, dengan kakitangan IT mendesak kemas kini dan kakitangan OT menentang mereka kerana kebimbangan tentang kemungkinan gangguan kepada operasi.

Cabaran lain ialah perspektif yang berbeza tentang masa henti sistem. Dalam alam IT, beberapa tahap masa henti boleh diterima, dijadualkan, dan juga dijangka semasa penyelenggaraan atau peningkatan sistem. Walau bagaimanapun, dalam persekitaran OT, terutamanya dalam infrastruktur kritikal seperti loji Minyak dan Gas, sebarang masa henti boleh mempunyai implikasi operasi dan keselamatan yang ketara. Perbezaan dalam toleransi untuk masa henti ini sering menyebabkan salah faham dan perselisihan faham semasa proses integrasi.

Tambahan pula, proses integrasi juga dipengaruhi oleh tahap pemahaman dan pengetahuan yang berbeza antara kakitangan OT dan IT. Kakitangan IT sering tidak mempunyai pemahaman yang mendalam tentang proses operasi dan kritikal sistem, yang membawa kepada keputusan yang berpotensi memberi kesan kepada operasi. Sebaliknya, kakitangan OT sering tidak mempunyai pemahaman yang komprehensif tentang risiko keselamatan siber dan keperluan untuk langkah keselamatan IT tertentu.

Perbezaan keutamaan antara OT dan IT memberi kesan ketara kepada proses integrasi. Menyedari dan menangani perbezaan ini adalah penting untuk integrasi yang berjaya. Ia memerlukan pemupukan budaya kerjasama dan persefahaman bersama, di mana kedua-dua kakitangan OT dan IT menghargai keutamaan masing-masing dan bekerjasama untuk mencapai integrasi OT-IT yang selamat dan cekap.

### 4.2.3 Kajian Kes yang Menggambarkan Keutamaan Berbeza OT dan IT

Untuk menggambarkan lagi perbezaan keutamaan antara OT dan IT, tiga contoh kes daripada proses migrasi dalam loji Minyak dan Gas dianalisa.

**a. Contoh Kes 1: Segmentasi Rangkaian**

Pembahagian rangkaian ialah aspek kritikal seni bina yang mematuhi IEC62443. Ia melibatkan pembahagian rangkaian kepada zon berasingan untuk mengehadkan penyebaran potensi ancaman siber. Amalan ini ialah komponen piawaian langkah keselamatan siber IT, direka untuk mengasingkan sistem dan melindunginya daripada potensi ancaman yang berpunca daripada bahagian lain rangkaian.

Walau bagaimanapun, dalam konteks OT, pembahagian rangkaian memberikan cabaran yang unik. Persekitaran OT dalam loji Minyak dan Gas dicirikan oleh interaksi kompleks sistem dan peranti yang perlu berkomunikasi antara satu sama lain dalam masa nyata untuk memastikan operasi lancar. Sebarang gangguan dalam komunikasi ini, seperti yang mungkin disebabkan oleh pembahagian rangkaian, boleh mempunyai implikasi yang ketara untuk kecekapan operasi.

Di salah satu loji Minyak dan Gas yang menjalani proses migrasi, pembahagian rangkaian yang dicadangkan telah dipenuhi dengan kebimbangan daripada kakitangan OT. Berdasarkan maklum balas ketika perbincangan analisa risiko, kakitangan OT menyuarakan kebimbangan bahawa mewujudkan zon rangkaian yang berasingan akan mengganggu aliran data masa nyata antara bahagian berlainan loji. Aliran data ini adalah penting untuk memantau dan mengawal proses operasi, dan sebarang gangguan boleh berpotensi memberi kesan kepada produktiviti dan keselamatan loji.

Perbezaan keutamaan ini membawa kepada beberapa perbincangan dan rundingan antara pasukan IT dan OT. Pasukan IT perlu menjelaskan kepentingan pembahagian rangkaian untuk keselamatan siber, manakala pasukan OT perlu menyerlahkan potensi implikasi operasi.

Akhirnya, kompromi dicapai apabila rangkaian dibahagikan dengan cara yang memenuhi keperluan keselamatan siber tanpa mengganggu proses operasi dengan ketara. Ini melibatkan perancangan dan reka bentuk yang teliti bagi zon rangkaian, memastikan sistem yang perlu berkomunikasi antara satu sama lain diletakkan di zon yang sama. Selain itu, saluran komunikasi selamat telah diwujudkan antara zon berbeza untuk membolehkan aliran data yang diperlukan.

Contoh kes ini menggariskan kerumitan yang terlibat dalam melaksanakan langkah keselamatan siber IT dalam persekitaran OT. Ia menyerlahkan keperluan untuk pemahaman yang mendalam tentang kedua-dua keperluan operasi OT dan prinsip keselamatan siber IT untuk berjaya mengintegrasikan kedua-duanya. Ia juga menekankan kepentingan komunikasi dan kerjasama yang berkesan antara pasukan IT dan OT untuk mengemudi kerumitan ini dan mencapai integrasi OT-IT yang berjaya.

**b. Contoh Kes 2: Kemas Kini Sistem**

Kemas kini sistem ialah amalan biasa dalam persekitaran IT untuk memastikan semua sistem menjalankan versi perisian terkini, yang selalunya termasuk tampung keselamatan yang penting. Walau bagaimanapun, dalam persekitaran OT, kemas kini sistem boleh menjadi proses yang rumit dan rumit.

Dalam persekitaran OT loji Minyak dan Gas, sistem selalunya direka untuk berjalan secara berterusan tanpa gangguan. Sistem ini mengawal proses kritikal dan sebarang masa henti boleh mempunyai implikasi yang ketara untuk operasi loji. Oleh itu, kemas kini sistem, yang selalunya memerlukan sistem untuk dibawa ke luar talian buat sementara waktu, boleh menjadi cabaran besar.

Semasa proses pemindahan di salah satu loji Minyak dan Gas, pasukan IT mencadangkan jadual untuk kemas kini sistem biasa sebagai sebahagian daripada seni bina mematuhi IEC62443 baharu. Cadangan ini telah mendapat tentangan daripada kakitangan OT, yang bimbang tentang kemungkinan gangguan operasi yang disebabkan oleh kemas kini.

Kakitangan OT menjelaskan bahawa sistem dalam loji itu tidak direka bentuk untuk dibawa ke luar talian dengan kerap. Sesetengah sistem ini dijalankan pada versi perisian lama yang serasi sepenuhnya dengan operasi loji, dan mengemas kininya berpotensi menyebabkan masalah keserasian. Selain itu, loji itu mempunyai jadual yang ketat untuk proses operasi, dan sebarang masa henti yang tidak dirancang boleh mengakibatkan kerugian pengeluaran yang ketara.

Perbezaan keutamaan ini membawa kepada satu siri perbincangan antara pasukan IT dan OT. Pasukan IT perlu memahami kekangan operasi dan bekerja di dalamnya untuk merancang kemas kini sistem. Mereka perlu menjadualkan kemas kini dengan teliti untuk meminimumkan gangguan operasi dan memastikan semua sandaran dan kontingensi yang diperlukan telah disediakan.

Sebaliknya, pasukan OT perlu memahami kepentingan kemas kini sistem untuk mengekalkan keselamatan siber. Mereka terpaksa bekerjasama dengan pasukan IT untuk mengenal pasti tingkap peluang untuk menjalankan kemas kini, seperti semasa tempoh penyelenggaraan yang dijadualkan.

Contoh kes ini menyerlahkan cabaran yang terlibat dalam melaksanakan amalan IT dalam persekitaran OT. Ia menekankan keperluan untuk pemahaman yang mendalam tentang kekangan operasi dalam persekitaran OT dan keupayaan untuk menyesuaikan amalan IT dengan sewajarnya. Ia juga menekankan kepentingan kerjasama dan komunikasi antara pasukan IT dan OT untuk berjaya mengharungi cabaran ini.



**c. Contoh Kes 3: Kemas Kini Pelayan dan Strategi Gulung Semula**

Dalam contoh lain semasa proses migrasi, pasukan IT mencadangkan strategi gulung semula sebagai langkah pengurangan risiko untuk kemas kini pelayan. Ideanya ialah jika kemas kini pelayan tidak berjalan seperti yang dirancang, sistem boleh digulung semula ke keadaan sebelumnya, dengan itu meminimumkan kesan ke atas operasi.

Cadangan ini adalah berdasarkan amalan IT piawaian di mana kemas kini sistem adalah kerap dan gulung semula adalah penyelesaian biasa untuk menangani sebarang

isu yang timbul daripada kemas kini ini. Walau bagaimanapun, cadangan ini telah mendapat tentangan ketara daripada kakitangan OT.

Pasukan OT menjelaskan bahawa walaupun strategi gulung semual mungkin berfungsi dengan baik dalam persekitaran IT, ia boleh menimbulkan risiko yang ketara dalam persekitaran OT. Dalam konteks OT loji Minyak dan Gas, sistem direka bentuk untuk operasi berterusan dan sebarang gangguan, termasuk pengembalian sistem, berpotensi mengganggu proses kritikal.

Selain itu, sistem OT sering dijalankan pada versi perisian proprietari yang lebih lama yang direka khusus untuk operasi loji. Pemulihan semula boleh berpotensi mengakibatkan masalah keserasian, menyebabkan gangguan selanjutnya pada operasi loji.

Selain itu, pasukan OT menunjukkan bahawa masa yang diperlukan untuk melakukan pemulangan semula boleh mengakibatkan masa operasi yang tidak berfungsi yang ketara. Dalam infrastruktur kritikal seperti loji Minyak dan Gas, walaupun tempoh masa henti yang singkat boleh mempunyai implikasi yang ketara, termasuk potensi risiko keselamatan dan kerugian kewangan yang besar.

Contoh kes ini menyerlahkan perbezaan ketara dalam amalan IT dan OT dan cabaran yang boleh timbul apabila cuba melaksanakan penyelesaian IT dalam persekitaran OT. Ia menekankan keperluan untuk kakitangan IT untuk mendapatkan pemahaman yang mendalam tentang persekitaran OT dan kekangan dan keperluan uniknya. Ia juga menekankan kepentingan kerjasama dan komunikasi terbuka antara pasukan IT dan OT untuk mencari penyelesaian yang memenuhi keperluan operasi dan keselamatan siber.

Rumusan perbezaan keutamaan OT dan IT, kesan, dan contoh kes adalah seperti Rajah 4.2 di bawah.

| Keutamaan | OT | IT | Kesan terhadap Integrasi OT-IT | Pemerhatian semasa Migrasi | Contoh Kes |
|---|---|---|---|---|---|
| **Kerahsiaan** | Rendah | Tinggi | Langkah-langkah IT untuk melindungi data mungkin ditentang oleh kakitangan OT jika mereka menganggapnya sebagai ancaman kepada ketersediaan atau integriti sistem. | Tiada isu | Tiada |
| **Integriti** | Tinggi | Tinggi | Kakitangan IT mungkin melaksanakan langkah-langkah yang menyebabkan terputusnya hubungan antara dua sistem kawalan, lalu mengubah interpretasi data oleh sistem kawalan lain | Tiada isu | Tiada |
| **Ketersediaan** | Tinggi | Rendah | Kakitangan IT mungkin melaksanakan langkah-langkah yang boleh mengganggu operasi OT, tidak menghargai sepenuhnya kritikal ketersediaan dalam persekitaran OT. | KakitanganKakitangan IT melaksanakan langkah-langkah yang mengganggu operasi OT, menunjukkan kekurangan pemahaman tentang kritikal ketersediaan dalam persekitaran OT. | Contoh Kes 1: Segmentasi Rangkaian<br>Contoh Kes 2: Kemas Kini Sistem<br>Contoh Kes 3: Kemas Kini Pelayan dan Strategi Rollback |

Rajah 4.2 Perbezaan Keutamaan OT dan IT, Kesan, dan Contoh Kes

## 4.3 KEKURANGAN KOMPETENSI DAN SET KEMAHIRAN KOMPREHENSIF OLEH KAKITANGAN KESELAMATAN SIBER OT-IT

Penghijrahan kepada seni bina yang mematuhi IEC62443 dalam sektor Infrastruktur Kritikal Negara, khususnya dalam sektor Minyak dan Gas, merupakan proses kompleks yang memerlukan gabungan kemahiran yang unik. Salah satu penemuan penting penyelidikan ini ialah mengenal pasti jurang kemahiran yang besar dalam kakitangan keselamatan siber OT-IT. Jurang ini bukan sekadar kekurangan pemahaman antara mekanisme operasi sistem OT dan IT, tetapi juga kekurangan dalam pengetahuan komprehensif yang diperlukan untuk memastikan langkah keselamatan siber yang berkesan dalam rangkaian bersepadu.

Bab ini menyelidiki penemuan penyelidikan yang berkaitan dengan kekurangan set kemahiran komprehensif dalam kakitangan keselamatan siber OT-IT. Ia meneroka jurang kemahiran yang dikenal pasti antara kakitangan OT dan IT, cabaran yang timbul daripada pengkhususan dalam disiplin IT, dan kesan jurang kemahiran ini terhadap proses integrasi. Penyelidikan itu juga menyerlahkan kekurangan pengalaman kakitangan IT dalam aspek keselamatan siber industri Minyak dan Gas, sektor yang baru-baru ini mula menyedari kepentingan keselamatan siber.

Satu siri contoh kes akan menggambarkan implikasi praktikal daripada jurang kemahiran dan cabaran pengkhususan ini. Ini akan diakhiri dengan membincangkan strategi yang berpotensi untuk menangani kekurangan set kemahiran dalam kakitangan keselamatan siber OT-IT, menyumbang kepada kejayaan pelaksanaan seni bina yang

mematuhi IEC62443 dalam sektor Infrastruktur Kritikal Negara. Penemuan yang dibentangkan ini memberikan pandangan berharga tentang salah satu cabaran utama yang dihadapi semasa proses migrasi, menawarkan asas untuk strategi masa depan untuk menangani isu ini.

### 4.3.1 Jurang Kemahiran Antara OT dan Kakitangan IT: Pemerhatian dan Kesan

Jurang kemahiran antara kakitangan OT dan IT diperhatikan pada pelbagai peringkat proses integrasi, dan jurang ini mempunyai kesan yang ketara ke atas kecekapan dan keberkesanan pemindahan kepada seni bina yang mematuhi IEC62443.

Salah satu pemerhatian yang paling ketara ialah perbezaan pemahaman prinsip keselamatan siber antara kakitangan OT dan IT. Kakitangan OT, dengan tumpuan mereka untuk mengekalkan kesinambungan operasi, sering bergelut untuk memahami keperluan untuk langkah keselamatan siber tertentu yang dicadangkan oleh kakitangan IT. Sebagai contoh, konsep pembahagian rangkaian, amalan keselamatan IT biasa, sering mendapat tentangan daripada kakitangan OT yang bimbang tentang kemungkinan gangguan kepada proses operasi. Rintangan ini bukan disebabkan oleh mengabaikan keselamatan, sebaliknya kurangnya pemahaman tentang risiko keselamatan siber dan peranan pembahagian rangkaian dalam mengurangkan risiko ini.

Sebaliknya, kakitangan IT sering kurang memahami implikasi operasi cadangan keselamatan siber mereka. Sebagai contoh, kakitangan IT selalunya mencadangkan kemas kini atau tampalan sistem tanpa mempertimbangkan sepenuhnya potensi kesan ke atas proses operasi. Dalam dunia IT, kemas kini sistem adalah rutin dan perlu untuk mengekalkan keselamatan. Walau bagaimanapun, dalam dunia OT, kemas kini sistem boleh menyebabkan gangguan kepada proses operasi, yang boleh membawa kesan yang ketara.

Jurang kemahiran ini tidak terhad kepada pemahaman prinsip keselamatan siber. Terdapat juga jurang yang ketara dalam pemahaman operasi dan proses sistem. Kakitangan OT sering mempunyai pemahaman yang mendalam tentang proses operasi dan keperluan khusus sistem OT. Walau bagaimanapun, mereka sering kurang memahami sistem IT dan peranan sistem ini dalam menyokong proses operasi.

Sebaliknya, kakitangan IT, walaupun mahir dalam menguruskan sistem IT, sering tidak mempunyai pemahaman yang menyeluruh tentang proses operasi dan keperluan khusus sistem OT.

Kesan daripada jurang kemahiran ini adalah ketara. Salah faham dan salah komunikasi antara kakitangan OT dan IT sering menyebabkan kelewatan dan ketidakcekapan dalam proses integrasi. Dalam sesetengah kes, jurang kemahiran ini membawa kepada pelaksanaan penyelesaian yang kukuh dari segi teknikal tetapi tidak memenuhi sepenuhnya keperluan operasi sistem OT. Dalam kes lain, jurang kemahiran mengakibatkan terlepas peluang untuk meningkatkan keselamatan sistem OT.

### 4.3.2 Pengkhususan dalam Disiplin IT dan Cabarannya

Bidang IT adalah luas dan kompleks, dengan pelbagai disiplin dan pengkhususan. Setiap disiplin ini memerlukan satu set kemahiran dan pengetahuan yang unik. Sebagai contoh, jurutera rangkaian pakar dalam mereka bentuk dan mengurus infrastruktur rangkaian, pentadbir sistem memberi tumpuan kepada mengurus dan menyelenggara sistem IT, dan pakar keselamatan siber menumpukan pada melindungi sistem IT daripada ancaman. Pengkhususan dalam disiplin IT ini diperlukan kerana kerumitan dan keluasan bidang IT. Walau bagaimanapun, ia juga memberikan cabaran dalam konteks integrasi OT-IT.

Semasa proses migrasi, adalah diperhatikan bahawa kakitangan IT, walaupun pakar dalam disiplin masing-masing, sering tidak mempunyai pemahaman yang komprehensif tentang disiplin IT yang lain. Sebagai contoh, jurutera rangkaian mungkin tidak memahami sepenuhnya selok-belok pentadbiran sistem, dan pentadbir sistem mungkin tidak mahir sepenuhnya dalam spesifik reka bentuk rangkaian. Kekurangan pemahaman merentas disiplin dalam disiplin IT ini sering menyebabkan salah komunikasi dan salah faham, yang seterusnya mengakibatkan ketidakcekapan dan kelewatan dalam proses integrasi.

Selain itu, pengkhususan dalam disiplin IT juga bermakna kakitangan IT sering tidak mempunyai pemahaman yang menyeluruh tentang keseluruhan landskap IT. Mereka adalah pakar dalam bidang masing-masing, tetapi mereka tidak selalu