Journal of Applied Technology and Innovation
Vol. 10, Issue 2, 2026, pp. 74-90
e-ISSN:2600-7304-ISSN
doi: https://doi.org/10.65136/jati.v10i2.353

A Conceptual Framework for OT/ICS Cybersecurity Governance in Malaysian Manufacturing Environments Under Industry 4.0

Navenesh Kumar[1*]

[1]Asia Pacific University of Technology and Innovation, Kuala Lumpur, Malaysia
*Corresponding author: navenesh5903@gmail.com

Received: 2026-05-21; Accepted: 2026-08-21; Published: 2026-08-28

Abstract

The convergence of Information Technology (IT) and Operational Technology (OT) in Malaysian manufacturing environments has created a cybersecurity governance problem that existing frameworks were not designed to solve. Malaysia's manufacturing sector contributes 24.5% of national GDP (EPU, 2022) and is overwhelmingly made up of small and medium-sized enterprises (SMEs) that typically have no dedicated security function at all, let alone one capable of addressing OT/ICS-specific threats. The situation has become more urgent following the enactment of the Cyber Security Act 2024, which places binding legal obligations on critical infrastructure entities but provides no OT/ICS-specific operational guidance for manufacturers. This paper proposes the Malaysian Industrial Cybersecurity Governance Framework (MICGF), a five-pillar governance model developed through Design Science Research (DSR) methodology. The framework draws on IEC 62443, NIST SP 800-82 Revision 3, and NIST CSF 2.0, and contextualises these international standards within Malaysia's regulatory and industrial environment, including the National Cybersecurity Policy 2020, the Industry 4WRD Policy, the MyDIGITAL blueprint, and the Cyber Security Act 2024. The MICGF makes three contributions that no existing international standard provides: it aligns OT/ICS governance requirements with the full Malaysian regulatory stack; it introduces a three-tier SME implementation model providing resource-proportionate entry points for manufacturers with no dedicated security function; and it elevates workforce capability development to a co-equal governance pillar. The five pillars are: Asset Visibility and Classification, Network Architecture and Segmentation, Threat Detection and Incident Response, Governance Integration and Policy Alignment, and Workforce Capability Development. Each pillar operates across three capability tiers to accommodate the wide range of resource levels among Malaysian manufacturers. The framework was evaluated through a multi-layer non-contact validation approach comprising standards traceability mapping, comparative benchmark analysis, and scenario-based threat modelling across three documented OT/ICS attack patterns.

Keywords: *OT/ICS Cybersecurity; IT/OT Convergence; Industrial Control Systems; Cybersecurity Governance; Malaysian Manufacturing; SDG 9.*

1. Introduction

Industry 4.0 has fundamentally changed what a Malaysian factory looks like. Where production machinery was once isolated from external networks, it is now connected to enterprise systems, cloud platforms,

vendor maintenance portals, and management dashboards. This is precisely what the Industry 4WRD Policy and MyDIGITAL blueprint encourage (MITI, 2018; MDEC, 2021). The productivity benefits are real. However, OT systems, the PLCs, SCADA systems, and industrial controllers that keep production lines running, were designed with reliability as the only priority. Security was never part of their original design (Byres and Lowe, 2004; Knapp and Langill, 2014). Connecting them to IT networks does not make them secure. It makes them reachable by attackers in ways that were previously impossible (Stouffer et al., 2023).

Malaysia's manufacturing sector is too important to leave in this exposed position. The sector contributed 24.5% of national GDP in 2022 (EPU, 2022), and SMEs made up 98.5% of all business establishments in the country as of the Economic Census 2016 (SME Corp Malaysia, 2017). The majority of these SMEs have no IT security team, let alone an OT/ICS security function. The government is simultaneously funding their digitalisation and, since the Cyber Security Act 2024 came into force, placing legal compliance obligations on critical infrastructure entities that include industrial operators. Manufacturing was the single most targeted sector for cyberattacks in Malaysia in 2023, accounting for 20% of all organisational incidents (Ensign InfoSecurity, 2024). The gap between policy intent and security reality is wide, and it is growing.

Three problems drive this gap. First, no OT/ICS cybersecurity governance framework specifically built for Malaysian manufacturers exists. International standards such as IEC 62443 and NIST SP 800-82 were designed for large industrial operators with dedicated security teams, predominantly in North American and European contexts. They do not map to Malaysian regulations and they do not address the SME resource reality. Second, within most Malaysian manufacturers, IT security and OT engineering operate as completely separate functions with no shared governance, no shared risk register, and no shared accountability for the network boundary that sits between them, which is precisely where most attacks succeed. Third, Malaysia's cybersecurity talent pipeline produces IT security professionals, not OT/ICS security professionals (CyberSecurity Malaysia, 2022). The skills needed to govern converged environments do not yet exist at scale in the country.

This paper addresses these three problems by proposing the Malaysian Industrial Cybersecurity Governance Framework (MICGF). The framework makes four contributions: a structured analysis of OT/ICS cybersecurity governance gaps in Malaysian manufacturing; an original five-pillar governance framework grounded in IEC 62443, NIST SP 800-82 Rev.3, and NIST CSF 2.0 and contextualised for Malaysian regulatory and industrial conditions; a multi-layer non-contact validation comprising standards traceability mapping, comparative benchmark analysis, and three-scenario threat modelling; and a comparative analysis against existing international frameworks. The paper proceeds as follows. Section 2 reviews the relevant literature. Section 3 describes the research methodology. Section 4 presents the MICGF. Section 5 presents the validation. Section 6 discusses the findings. Section 7 concludes.

2. Literature Review

2.1. The IT/OT Convergence Security Problem

IT and OT systems do not share the same security logic, and this has real consequences for how governance frameworks must be designed. In an IT environment, patching and restarting a server is a routine and acceptable action. In an OT environment, restarting a PLC that is managing a live chemical process or a running assembly line can cause physical damage, safety incidents, or production loss. OT security is therefore built around a different priority ordering than IT security. Where IT follows the CIA triad of Confidentiality, Integrity, and Availability, OT inverts this to AIC: Availability comes first, Integrity second, and Confidentiality last (Knapp and Langill, 2014). Most IT security tools, IT security governance models, and IT-trained security professionals are not designed with this inversion in mind. Applying IT security approaches directly to OT/ICS environments without adaptation is not just ineffective; it is actively dangerous (Byres and Lowe, 2004).

For most of OT's history, the answer to this security problem was simple: keep OT systems physically disconnected from everything else. The air gap provided strong protection because an attacker could not reach a PLC through the internet if the PLC had no internet connection. Industry 4.0 has systematically dismantled this protection. ERP systems now connect to manufacturing execution systems. IIoT sensors stream data continuously through IP networks. Vendors access production equipment remotely for maintenance. The IT/OT boundary, which once existed as a physical wall, now exists as a network boundary that can be crossed by an attacker who has gained access to one side of it (Dragos, 2023). In 2017, the TRITON/TRISIS attack targeted safety instrumented systems in a petrochemical facility with malware specifically designed to cause physical harm (Dragos, 2018). In 2022, INDUSTROYER2 attacked Ukrainian power infrastructure (Slowik, 2022). More recently, ransomware groups have made IT/OT pivot attacks a standard tactic, with manufacturing the most targeted global sector in both 2023 and 2024 (Dragos, 2023; NTT Data, 2024).

2.2. International OT/ICS Cybersecurity Governance Frameworks

Three international frameworks provide the technical foundation for OT/ICS security governance globally. IEC 62443 is the most comprehensive, defining security levels, a zone-and-conduit network architecture, and personnel, process, and technology requirements across the full industrial automation and control systems lifecycle (IEC, 2018). NIST SP 800-82 Rev. 3 is more practically oriented and addresses IT/OT convergence scenarios the older Purdue Model was not designed to handle (Stouffer et al., 2023). NIST CSF 2.0 adds a Govern function, extending accountability and risk management across converged environments (NIST, 2024).

None of the three was built with Malaysian SMEs in mind. IEC 62443 in full form assumes an established security team and dedicated ICS expertise, and does not tell a small factory with one IT manager what to do first. NIST frameworks target US federal environments and reference none of the Computer Crimes Act 1997, the Personal Data Protection Act 2010, or the Cyber Security Act 2024. None offers a tiered entry point for organisations without dedicated security functions. No published framework bridges this technical rigour with the Malaysian regulatory context and SME resource constraints, which is the gap the MICGF addresses.

2.3. Malaysian Industrial Cybersecurity Context

Malaysia has built a national cybersecurity policy architecture in recent years. The National Cybersecurity Policy 2020 sets out six strategic thrusts covering governance, legislation, capacity building, infrastructure resilience, and international cooperation (CyberSecurity Malaysia, 2020). The Cyber Security Act 2024 (Act 854), in force since 26 August 2024, creates binding legal obligations rather than policy guidance: NCII entities across 11 sectors must conduct annual risk assessments, undergo biennial audits, follow sector-specific codes of practice, and report incidents within six hours, with non-compliance carrying penalties of up to RM500,000 or ten years' imprisonment (NACSA, 2024). Both instruments remain predominantly IT-centric, however, and no NCII sector lead has published a code of practice for OT/ICS security in manufacturing.

This gap is concerning given the scale of the threat. Manufacturing was the most targeted sector for cyberattacks in Malaysia in 2023, accounting for 20% of all organisational incidents, ahead of government at 18.2% (Ensign InfoSecurity, 2024), and MyCERT quarterly reports document consistent ransomware and malicious-code incidents affecting Malaysian organisations (MyCERT, 2024). The Industry 4WRD Policy continues to fund IT/OT integration without requiring security assessment (MITI, 2018), and while Singapore addressed this with an updated OT Cybersecurity Masterplan in August 2024 (CSA Singapore, 2024), Malaysia has no equivalent. SMEs made up 98.5% of Malaysian business establishments (SME Corp Malaysia, 2017), and most have no dedicated IT security person, let alone OT/ICS knowledge. Malaysian cybersecurity research has focused on IT security, data privacy, and cloud computing, leaving OT/ICS security in manufacturing underrepresented in the literature.

2.4. Research Gap Identification

Three gaps emerge from this review. First, while regional efforts exist, notably Singapore's OT Cybersecurity Masterplan and related Southeast Asian work, no published framework integrates OT/ICS governance requirements with the full Malaysian regulatory landscape, including the Cyber Security Act 2024; the MICGF is positioned within this specific gap rather than claiming nothing has been attempted more broadly. Second, no existing framework integrates IEC 62443, NIST SP 800-82, and Malaysian regulatory instruments into a single model. Third, workforce development, consistently identified as the binding constraint on OT/ICS programme effectiveness (ISC2, 2024; Dragos, 2023), is rarely treated as a co-equal governance pillar. The MICGF addresses all three.

3. Research Methodology

This paper uses Design Science Research (DSR) methodology, as established by Hevner et al. (2004). DSR is appropriate here because the objective is to produce a useful artefact, in this case a governance framework, rather than to test a hypothesis through empirical measurement. The methodology involves two phases: building the framework through integrative literature review, and evaluating it through a structured multi-layer validation approach that does not require field access.

3.1. Phase 1: Framework Development

The integrative literature review approach, as described by Torraco (2005), synthesises existing knowledge across diverse source types to produce new theoretical contributions rather than answering a specific empirical question (Snyder, 2019). A structured search was run across IEEE Xplore, Scopus, Web of Science, and Google Scholar using three concept clusters: domain terms (OT security, ICS cybersecurity, SCADA security, industrial cybersecurity); governance terms (governance, framework, policy, standards, guidelines); and contextual terms (Malaysia, Southeast Asia, developing economies, SME, manufacturing). Boolean AND operators linked the clusters and date filters restricted results to January 2015 through December 2024. Starting from 412 records, 68 sources met all inclusion criteria after deduplication and full-text review. Consistent with integrative review practice, as described by Torraco (2005) and Snyder (2019), the 68 sources collectively informed the framework synthesis, gap analysis, and conceptual argumentation across the paper. The reference list contains those sources directly cited in the text; the broader corpus of 68 sources shaped the analytical judgements, comparative positioning, and contextual framing without each source requiring individual citation. Framework synthesis extracted requirements from IEC 62443, NIST SP 800-82 Rev.3, and NIST CSF 2.0, mapped them against Malaysian contextual constraints, and synthesised them into the five-pillar MICGF structure.

3.2. Phase 2: Multi-Layer Non-Contact Validation

Because the MICGF has not yet been deployed in real Malaysian factories, which is characteristic of a first-stage conceptual framework contribution, the validation approach used here does not rely on field data. Three structured non-contact validation methods are applied, consistent with DSR evaluation practice (Hevner et al., 2004). The first is standards traceability mapping, which checks whether each pillar is grounded in a specific provision of an internationally recognised standard. The second is comparative benchmark analysis, which positions the MICGF against the three primary existing frameworks across dimensions relevant to Malaysian manufacturing adoption. The third is scenario-based threat modelling, which traces three realistic and documented OT/ICS attack scenarios to evaluate whether the MICGF's controls would logically interrupt or contain each attack. Together, these three methods evaluate the framework against criteria of construct validity, comparative positioning, and practical utility (Snyder, 2019).

4. The Malaysian Industrial Cybersecurity Governance Framework (MICGF)

The MICGF makes three specific contributions that are absent, whether individually or in combination, from IEC 62443, NIST SP 800-82 Rev.3, and NIST CSF 2.0. First, it aligns the governance requirements derived from these international standards with the full Malaysian regulatory stack, including the Cyber

Security Act 2024, NCSP 2020, PDPA 2010, CCA 1997, MITI 4WRD, and MyDIGITAL. None of the three international standards references any Malaysian regulatory instrument. Second, it provides a three-tier SME implementation model that gives resource-proportionate entry points for manufacturers without dedicated security functions. IEC 62443 in full form assumes an organisation with an established ICS security team; the MICGF's Tier 1 foundational actions require no specialist budget and no external consultants. Third, it elevates workforce capability development to a co-equal governance pillar with four structured dimensions. IEC 62443-2-1 addresses personnel competency but does not treat it as a structural governance requirement equal in standing to asset management or network segmentation. NIST CSF 2.0 does not include a workforce pillar at all. The MICGF treats workforce capability as foundational because all other pillars ultimately depend on people who have been trained to implement and maintain them.

The framework organises OT/ICS cybersecurity governance around five pillars. Each pillar addresses a different but interconnected dimension of the problem. They are parallel requirements rather than a sequence, because each creates enabling conditions for the others. Asset visibility (P1) is the prerequisite: you cannot segment what you have not mapped, detect what you have not baselined, or govern what you have not identified. Segmentation (P2) creates the boundary that detection (P3) monitors and that governance (P4) must own across both IT and OT domains. Workforce capability (P5) makes all of the above function in practice. The framework structures implementation across three tiers: Tier 1, Foundational, for SMEs with no existing security function; Tier 2, Developing, for organisations with some IT security capability; and Tier 3, Advanced, for large manufacturers with dedicated OT/ICS security resources. Table 1 presents the full framework and Table 2 the detailed pillar mapping.

Table 1. The Malaysian Industrial Cybersecurity Governance Framework (MICGF)

Malaysian Industrial Cybersecurity Governance Framework (MICGF)					
P1 Asset Visibility and Classification	P2 Network Architecture and Segmentation	P3 Threat Detection and Incident Response	P4 Governance Integration and Policy Alignment	P5 Workforce Capability Development	Implementation Tiers
Objective: Complete OT asset inventory with criticality classification	Objective: Zone-and-conduit model; default-deny IT/OT boundary enforced	Objective: Passive OT monitoring deployed; ICS-specific IR plan maintained	Objective: Unified IT/OT governance aligned to enterprise risk management	Objective: OT security competency built across all organisational levels	Tier 3: Advanced Tier 2: Developing Tier 1: Foundational
Indicators: OT asset register; Tier A/B/C classification applied; passive discovery deployed	Indicators: IT/OT DMZ operational; conduit policies documented; boundary traffic logged	Indicators: Passive monitoring active; ICS IR plan tested annually; CERT Malaysia reporting active	Indicators: Unified IT/OT security policy; OT risk register maintained; board-level visibility established	Indicators: Training programme operational; GICSP and IEC 62443 certifications targeted;	

				blended teams formed	
Standard: IEC 62443-2-1 Sec. 4.3.3; NIST SP 800-82 Sec. 4.2	Standard: IEC 62443-3-3 SR 5.1; NIST SP 800-82 Sec. 5.5	Standard: IEC 62443-2-1 Sec. 4.3.6; NIST CSF 2.0 DE and RS	Standard: IEC 62443-2-1 Sec. 4.2; NIST CSF 2.0 GV function	Standard: IEC 62443-2-1 Sec. 4.3.2; NIST NICE Framework	
Policy: NCSP 2020 Thrust 5; MITI 4WRD Sec. 3.2	Policy: NCSP 2020 Thrust 3; CSM ICS Security Guidelines	Policy: NCSP 2020 Thrust 1; CERT Malaysia ICS Reporting Framework	Policy: NCSP 2020 Thrusts 1 and 2; CSA 2024 (Act 854); PDPA 2010; CCA 1997	Policy: MyDIGITAL Human Capital; HRD Corp; NICF Malaysia	
Policy Alignment: IEC 62443 | NIST SP 800-82 Rev.3 | NIST CSF 2.0 | NCSP 2020 | Cyber Security Act 2024 | MITI 4WRD | MyDIGITAL | PDPA 2010					

Source: Author's own construct (2025). CSM = CyberSecurity Malaysia; CSA = Cyber Security Act 2024; PDPA = Personal Data Protection Act 2010.

Table 2. MICGF Pillars: Core Objectives, Indicators, and Policy Alignment

Pillar	Core Objective	Key Implementation Indicators	International Standard	Malaysian Policy Alignment
P1: Asset Visibility and Classification	Complete inventory of all IT and OT assets with criticality classification	OT asset register maintained; Tier A/B/C classification applied; passive discovery tool deployed	IEC 62443-2-1 Sec. 4.3.3; NIST SP 800-82 Sec. 4.2	NCSP 2020 Thrust 5; MITI 4WRD Sec. 3.2
P2: Network Architecture and Segmentation	Zone-and-conduit network model with default-deny IT/OT boundary policy enforced	IT/OT DMZ operational; conduit policies documented and enforced; boundary traffic logged	IEC 62443-3-3 SR 5.1; NIST SP 800-82 Sec. 5.5	NCSP 2020 Thrust 3; CSM ICS Security Guidelines
P3: Threat Detection	Passive OT-native monitoring deployed; ICS-	Passive monitoring active; ICS IR plan tested annually;	IEC 62443-2-1 Sec. 4.3.6; NIST CSF 2.0 DE and RS functions	NCSP 2020 Thrust 1; CERT Malaysia ICS Reporting Framework

and Incident Response	specific incident response plan maintained	CERT Malaysia reporting active		
P4: Governance Integration and Policy Alignment	Unified IT/OT security governance aligned to enterprise risk management	Unified IT/OT security policy; OT risk register maintained; board-level visibility established	IEC 62443-2-1 Sec. 4.2; NIST CSF 2.0 GV function	NCSP 2020 Thrusts 1 and 2; Cyber Security Act 2024 (Act 854); PDPA 2010; CCA 1997
P5: Workforce Capability Development	OT security competency built across all organisational levels and functions	Training programme operational; GICSP and IEC 62443 certifications targeted; blended teams formed	IEC 62443-2-1 Sec. 4.3.2; NIST NICE Framework	MyDIGITAL Human Capital; HRD Corp; NICF Malaysia

Note: CSM = CyberSecurity Malaysia; CCA = Computer Crimes Act 1997; PDPA = Personal Data Protection Act 2010; NICF = National ICT Competency Framework; HRD Corp = Human Resources Development Corporation Malaysia.

4.1. Pillar 1: Asset Visibility and Classification

The most common finding when a manufacturer first assesses its OT/ICS security posture is that it does not actually know what is on its network. PLCs, HMIs, RTUs, IIoT sensors, engineering workstations, and safety instrumented systems have been added, modified, and replaced over years of operation, and in most cases nobody has maintained a comprehensive record of what is connected to what. This is not a minor administrative gap; it is the foundational vulnerability that attackers exploit. You cannot protect assets you do not know exist, and you cannot monitor communications you have not mapped (Dragos, 2023; Nozomi Networks, 2023). Standard IT discovery tools make this problem worse: active scanning tools that work well on IT networks can send unexpected commands to OT devices and cause them to crash or behave unpredictably. In OT/ICS environments, the only safe discovery method is passive traffic analysis, which monitors existing network communications without generating any new traffic.

MICGF P1 requires manufacturers to maintain an OT asset register documenting each device identity, firmware version, communication protocols, network zone, and criticality. Criticality uses three tiers from IEC 62443-1-1: Tier A (Safety Critical), Tier B (Production Critical), and Tier C (Operational Support). Tier A assets receive the tightest controls and fastest incident response. For a Tier 1 SME, this starts as a manual walkthrough where an engineer lists every networked device on the factory floor. It costs nothing except time, takes a few days, and almost always reveals devices nobody knew were network-accessible. Tier 3 organisations use automated passive discovery platforms that maintain real-time inventories continuously.

4.2. Pillar 2: Network Architecture and Segmentation

If there is one control that Malaysian manufacturers should implement first, it is IT/OT network segmentation. Nothing else provides as immediate and measurable a reduction in OT/ICS attack risk. The most common OT/ICS attack pattern, the ransomware pivot, works by gaining access to the IT network first and then moving laterally into the OT domain (Dragos, 2023). If there is no open network connection between IT and OT, lateral movement of this kind is not possible. A firewall with default-

deny rules between the enterprise IT network and the manufacturing floor eliminates this entire attack path. MICGF P2 uses the IEC 62443 zone-and-conduit model as its architectural foundation (IEC, 2018). Assets are grouped into security zones based on common security requirements, and all traffic between zones must flow through explicitly defined and managed conduits, not through open network connections that happen to exist.

The implementation path under P2 scales with organisational capability. A Tier 1 manufacturer starts by deploying a dedicated IT/OT firewall with default-deny rules; no traffic from the enterprise network reaches the manufacturing floor unless explicitly permitted by IP address and port. This is achievable with standard commercial hardware and is arguably the single most impactful security action a Malaysian SME can take. Tier 2 organisations go further, implementing zone-and-conduit segmentation within the OT domain itself. Tier 3 organisations implement micro-segmentation down to individual high-criticality devices and deploy unidirectional security gateways where data needs to flow in one direction only.

4.3. Pillar 3: Threat Detection and Incident Response

Detecting attacks in OT/ICS environments requires different tools from those used in IT security operations. EDR agents, signature-based intrusion detection systems, and vulnerability scanners are the standard IT security toolkit, but most cannot be installed on OT devices, which commonly run end-of-life operating systems and custom firmware. More critically, these tools do not understand OT communication protocols such as Modbus, DNP3, EtherNet/IP, or PROFINET. An IT security tool looking at OT network traffic cannot distinguish between a PLC operating normally and one receiving anomalous commands from an attacker (Nozomi Networks, 2023). MICGF P3 mandates passive, OT-protocol-aware network monitoring that does not generate any traffic of its own. It listens to existing communications, learns what normal process behaviour looks like, and alerts when something deviates. This approach provides detection without creating the operational risk that active scanning tools pose in OT/ICS environments.

Incident response in OT/ICS environments requires a different approach, for a reason that goes back to the AIC priority ordering. The standard IT instinct to isolate the affected system immediately can make things worse in an OT environment. Isolating a PLC managing an active process may cause a dangerous operational state. MICGF P3 therefore requires a dedicated ICS incident response plan, separate from the IT plan and developed with engineering team input. It must define OT-safe containment procedures, escalation pathways to plant management, and reporting obligations to CERT Malaysia. For NCII entities under the Cyber Security Act 2024, this is not optional: the Act requires incident reporting to NACSA within six hours, which is only achievable if the procedure has been documented and practised in advance.

4.4. Pillar 4: Governance Integration and Policy Alignment

Technical controls are only as effective as the governance structure that owns them. In most Malaysian manufacturing organisations, the IT security function, if it exists at all, has no authority over OT systems. The engineering team that manages OT systems has no cybersecurity training and no security obligations. The IT/OT boundary, which is where the most dangerous vulnerabilities reside, belongs to neither team. This governance fragmentation is a consistently documented condition in industrial organisations globally (PwC, 2024), and it is particularly acute in the Malaysian SME manufacturing context where dedicated security resources are scarce and organisational structures tend to separate IT and engineering functions completely.

MICGF P4 requires four governance actions: a unified IT/OT security policy naming who is responsible for what across both domains; an OT risk register integrated into enterprise risk management; a cross-functional IT/OT security committee with engineering, IT, and management representation and actual decision-making authority; and periodic OT security visibility at board or senior management level. These requirements are consistent with the NIST CSF 2.0 Govern function, IEC 62443-2-1, and Malaysia's

NCSP 2020 Thrust 1, and support compliance with annual risk assessment obligations under the Cyber Security Act 2024.

4.5. Pillar 5: Workforce Capability Development

All four of the other pillars ultimately depend on people. A complete asset register requires someone who knows what to look for and how to classify it. A properly configured IT/OT firewall requires someone who understands both OT network architecture and IT firewall management. Passive OT monitoring requires someone who can interpret the alerts it generates and distinguish a genuine anomaly from routine process variation. An ICS incident response plan requires people who have actually read it, understand their role in it, and have practised it. The OT/ICS cybersecurity workforce deficit is a recognised global challenge (ISC2, 2024; Dragos, 2023), and in Malaysia it is particularly acute because the cybersecurity talent pipeline has historically been entirely IT-focused (CyberSecurity Malaysia, 2022). There is essentially no formal pathway for producing OT/ICS security professionals through Malaysian universities.

MICGF P5 addresses this through four dimensions. The Awareness dimension covers all manufacturing staff through basic OT security training: what threats look like, what to report, and what not to connect to the network. The Practitioner dimension targets IT staff and OT engineers through cross-domain training covering OT/ICS security fundamentals, industrial protocols, and risk assessment methodology for physical process environments. The Specialist dimension targets dedicated security roles through the GICSP (Global Industrial Cyber Security Professional) and the IEC 62443 Cybersecurity Professional certifications. The Institutional dimension calls for OT/ICS security content to be integrated into Malaysian university cybersecurity programmes and polytechnic curricula aligned with the National ICT Competency Framework. The HRD Corp levy system provides a funding mechanism for the first three dimensions without additional budget.

5. Multi-Layer Non-Contact Validation

The MICGF is evaluated through three non-contact validation methods that together assess construct validity, comparative positioning, and practical effectiveness against documented attack patterns. This multi-layer approach is appropriate for a conceptual framework at the pre-empirical stage of its research programme, consistent with DSR evaluation practice (Hevner et al., 2004).

5.1. Standards Traceability Mapping

Standards traceability mapping checks whether the MICGF's requirements are grounded in specific provisions of internationally recognised standards. IEC 62443 and NIST SP 800-82 Rev.3 were developed through decades of expert review, international consensus, and refinement against real industrial security incidents. Requirements that are traceable to specific provisions of these standards inherit the credibility of the standards themselves. Table 3 presents this mapping for all five pillars.

Table 3. Standards Traceability Mapping for MICGF Pillars

MICGF Pillar	IEC 62443 Provision	NIST SP 800-82 Rev.3 Provision	Traceability Outcome
P1: Asset Visibility and Classification	IEC 62443-2-1 Section 4.3.3: Asset inventory and classification requirements for industrial automation and control systems	NIST SP 800-82 Section 4.2: OT asset management, identification of components and their security classifications	Fully traceable. Both standards mandate OT asset inventory and criticality classification as foundational controls.

P2: Network Architecture and Segmentation	IEC 62443-3-3 SR 5.1: Zone-and-conduit network architecture; security level requirements for network segmentation	NIST SP 800-82 Section 5.5: Network segmentation and boundary protection for OT environments	Fully traceable. Zone-and-conduit model and IT/OT DMZ requirement are directly grounded in both standards.
P3: Threat Detection and Incident Response	IEC 62443-2-1 Section 4.3.6: Monitoring, detection, and incident response requirements for IACS environments	NIST SP 800-82 Section 6.2: OT-specific monitoring; NIST CSF 2.0 Detect and Respond functions	Fully traceable. Passive monitoring mandate and ICS IR plan requirement are grounded in both standards.
P4: Governance Integration and Policy Alignment	IEC 62443-2-1 Section 4.2: Security management system requirements including policy, roles, and risk management	NIST CSF 2.0 Govern function: Organisational cybersecurity governance, risk management, and accountability	Fully traceable. Unified policy, OT risk register, and board visibility requirements are grounded in both standards.
P5: Workforce Capability Development	IEC 62443-2-1 Section 4.3.2: Personnel security competency and training requirements for IACS roles	NIST NICE Framework: Workforce development categories for cybersecurity roles across organisational levels	Fully traceable. Four workforce dimensions are grounded in both standards' personnel development requirements.

Note: IACS = Industrial Automation and Control Systems.

The mapping confirms that every MICGF pillar is fully traceable to specific provisions in both IEC 62443 and NIST SP 800-82 Rev.3. This establishes that the framework's technical requirements are not arbitrary recommendations but are directly derived from internationally validated sources. The traceability mapping also confirms that the MICGF is not a restatement of either standard. It extracts the most critical requirements from both, synthesises them into a coherent five-pillar structure, and adds the Malaysian policy alignment layer and the three-tier SME implementation model that neither standard provides.

5.2. Comparative Benchmark Analysis

Table 4 presents the comparative benchmark analysis across nine dimensions relevant to Malaysian manufacturing adoption.

Table 4. Comparative Benchmark Analysis: MICGF vs. Existing Frameworks

Dimension	IEC 62443	NIST SP 800-82 Rev.3	NIST CSF 2.0	MICGF (This Paper)
Malaysian policy alignment	None	None	None	**Explicit: NCSP 2020, 4WRD, MyDIGITAL, CSA 2024, PDPA 2010, CCA 1997**
SME-tiered implementation	No	No	Partial	**Yes; three explicit capability tiers**

OT/ICS workforce governance pillar	Partial	Partial	No	**Co-equal pillar with four development dimensions**
Technical OT/ICS controls depth	High	High	Medium	**Medium-High; synthesised from IEC 62443 and NIST SP 800-82**
Governance integration	Partial	Partial	High	**High; explicit cross-functional requirements**
Practical SME entry point	Low	Low	Medium	**High; Tier 1 requires no specialist budget**
Malaysian regulatory mapping	None	None	None	**Full: CSA 2024, NCSP 2020, PDPA 2010, CCA 1997**
Addresses all three literature gaps	No	No	No	**Yes; policy alignment, integrated standards, workforce pillar**
Standards traceability confirmed	Yes	Yes	Yes	**Yes; all five pillars fully traceable to IEC 62443 and NIST**

Note: Partial indicates the framework addresses the dimension but incompletely relative to the MICGF's Malaysian-contextualised treatment. This comparison is qualitative and based on published framework documentation.

Several things stand out from this comparison. IEC 62443 is technically the strongest framework available, but it scores low on SME feasibility and has no Malaysian policy alignment. NIST CSF 2.0 has the strongest governance integration through its Govern function, but does not go deep enough on OT/ICS-specific technical controls. The MICGF occupies a distinct position: it is the only framework that provides Malaysian policy alignment, explicit SME tiering, a workforce governance pillar, and a Tier 1 entry point requiring no specialist budget. Its technical depth is Medium-High rather than High; it does not replicate the full comprehensiveness of IEC 62443, and it should not, because that is not what Malaysian SMEs need. What they need is a starting point grounded in real standards, aligned with real Malaysian law, and actionable without a team of ICS security specialists.

5.3. Scenario-Based Threat Modelling

Three scenarios are evaluated, representing the three most prevalent OT/ICS attack vectors documented in industrial cybersecurity literature: the IT/OT ransomware pivot attack, the supply chain compromise via vendor remote access, and the insider threat via engineering workstation misuse (Williams, 1994; Dragos, 2023). The selection of these three specific attack patterns was deliberate and grounded in the realities of the Malaysian manufacturing environment. The ransomware pivot is the single most documented OT/ICS incident vector globally, and manufacturing has been consistently ranked as the most targeted sector in both 2023 and 2024 (Dragos, 2023; NTT Data, 2024), making it essential for any framework claiming practical utility for Malaysian manufacturers to address. The vendor remote access scenario reflects the growing reliance of Malaysian SMEs on third-party OT maintenance arrangements, a pattern that is directly enabled by Industry 4WRD digitalisation funding where remote vendor connectivity is encouraged but security governance for that access is not required. The insider threat via engineering workstation was selected because it addresses a governance failure mode, specifically the absence of OT/ICS change management procedures, that is distinct from the two external attack vectors and is consistently documented in industrial incident investigations (PwC, 2024). Together, the three scenarios span the external attacker, trusted third party, and internal actor threat categories, providing coverage of the principal threat agent types applicable to the Malaysian manufacturing context. For each scenario, the analysis traces what happens without MICGF controls and what happens with them in place.

5.3.1. Scenario A: Ransomware Pivot Attack

A Malaysian SME manufacturer has connected its production floor to its enterprise IT network to enable real-time production reporting, a common outcome of Industry 4WRD-funded digitalisation. No OT/ICS-specific security controls exist. A phishing email successfully compromises an IT staff member's credentials and the attacker establishes a foothold on the enterprise network.

Without MICGF controls, there is no unified IT/OT security policy and no awareness training, so the initial compromise goes unreported. The attacker scans the network and finds direct, unsegmented access to the manufacturing floor. There is no OT asset register, so the attacker discovers OT devices that the manufacturer itself did not know were reachable. Ransomware is deployed across both IT and OT systems simultaneously. There is no passive OT monitoring to detect the anomalous command traffic, and there is no ICS incident response plan to coordinate a response. Production halts. Recovery is slow because there is no documented asset inventory and no rollback procedure.

With MICGF controls, the situation is different at every stage. P5 workforce awareness training means the compromised staff member or a colleague is more likely to recognise and report the suspicious activity early. P4 governance controls mean escalation pathways are defined and the cross-functional committee is activated promptly. When the attacker attempts lateral movement from IT to OT, P2 segmentation blocks the attempt at the IT/OT DMZ; the default-deny firewall prevents any unauthorised traffic from reaching the manufacturing floor. P1 asset visibility means defenders know exactly what OT devices exist and what their normal communications look like. P3 passive monitoring detects the anomalous scanning activity at the boundary and generates an alert. The ICS incident response plan activates and the incident is contained within the IT domain. Production continues.

5.3.2. Scenario B: Supply Chain Compromise via Vendor Remote Access

A Malaysian automotive parts manufacturer relies on a third-party OT vendor for remote maintenance of its PLC systems. The vendor has been granted persistent remote access credentials that connect directly into the OT network, a common arrangement when in-house OT expertise is limited. The vendor's own systems are compromised by a threat actor, who uses the legitimate vendor credentials to gain access to the manufacturer's OT environment.

Without MICGF controls, the vendor's remote connection goes directly into the OT network with no logging and no boundary monitoring. There is no OT asset register documenting which devices the vendor is authorised to access. The threat actor starts issuing subtle modifications to PLC production parameters. No OT monitoring is in place to detect the behavioural deviation. The modifications cause quality defects that accumulate over several weeks before being identified through production quality control failures. By the time the incident is identified, significant production damage has occurred.

With MICGF controls, P1 documents all OT assets and their authorised communication relationships, including what the vendor is and is not permitted to access. P2 implements a zone-and-conduit architecture that constrains vendor remote access to a defined conduit with logged traffic. P3 passive monitoring has established normal process behaviour baselines for the PLCs, so the anomalous parameter changes are detected as deviations from those baselines within hours rather than weeks. P4 governance controls include a third-party access management policy. P5 training ensures engineering staff can respond appropriately. The vendor access is suspended through the conduit policy and production impact is minimised.

5.3.3. Scenario C: Insider Threat via Engineering Workstation

A Malaysian food processing manufacturer's OT engineer wants to test a process modification on the production line. There is no formal change management procedure for OT configuration changes. The engineer accesses the SCADA engineering workstation and modifies the PLC parameters directly without review or approval. The modification contains an error that destabilises a critical process.

Without MICGF controls, the error propagates across the production line before it is manually identified. There is no automated monitoring to detect the anomalous PLC command pattern. Recovery requires the OT vendor to be called in, and production is halted for an extended period.

With MICGF controls, P4 governance requires a unified IT/OT security policy that includes a change management procedure for OT configuration changes: any modification to PLC parameters must be reviewed and approved before being applied to a production system. P3 passive monitoring detects the anomalous PLC command pattern immediately as it deviates from the established process behaviour baseline, generating an alert before the error propagates further. The ICS incident response plan includes a configuration rollback procedure. P5 workforce training ensures the OT engineers understand and follow the change management procedure. The incident is detected within minutes and resolved through the documented rollback procedure without extended production outage.

Table 5. Scenario-Based Validation Summary: Three Documented OT/ICS Attack Patterns

Attack Stage	Outcome Without MICGF	Outcome With MICGF	MICGF Pillar Providing Control
Scenario A: Initial Compromise	Compromise unreported; escalation undefined; attack proceeds	Awareness training accelerates reporting; escalation pathways activated	P4: unified policy and escalation; P5: workforce awareness
Scenario A: Lateral Movement	Flat network; unrestricted IT-to-OT access; unknown OT devices reached	IT/OT DMZ blocks movement; full OT asset inventory known to defenders	P1: OT asset register; P2: IT/OT DMZ default-deny
Scenario A: OT Compromise	No OT monitoring; no ICS IR plan; production halted	Anomaly detected; ICS IR plan activates; incident contained in IT domain	P3: passive OT monitoring and ICS IR plan; P4: response committee
Scenario B: Vendor Access Exploitation	Unmonitored access; no asset register; no conduit policy; undetected	Access constrained to conduit; relationships documented and logged	P1: asset register with communication mapping; P2: conduit policy
Scenario B: Anomalous PLC Commands	No OT/ICS baseline; alterations undetected for weeks	Passive monitoring detects deviation from process behaviour baseline	P3: passive OT monitoring with process baseline detection
Scenario C: Configuration Change	No change management; error propagates before	Change management policy requires approval; error prevented at source	P4: IT/OT policy including OT/ICS change management procedure

	detection; extended outage		
Scenario C: Error Detection	Identified manually after extended impact; no rollback procedure	Passive monitoring detects anomaly within minutes; rollback activated	P3: passive OT monitoring; ICS IR plan with configuration rollback
Overall Outcome	All three scenarios: OT systems compromised or disrupted; significant production impact	All three scenarios: incidents detected early; OT systems protected	All five pillars provide complementary, non-redundant controls

Note: This analysis is a theoretical assessment of control adequacy based on documented attack patterns and established security principles. It does not constitute empirical measurement of incident reduction in deployed environments.

6. Discussion

6.1 Framework Contributions

The MICGF contributes to the literature in four ways. First, it fills a documented gap: while partial and regional efforts exist, no published OT/ICS cybersecurity governance framework integrates international technical standards with the full Malaysian regulatory stack for manufacturing, despite the sector being the most attacked in Malaysia in 2023 (Ensign InfoSecurity, 2024). Second, it treats workforce development as a primary governance requirement, reflecting the consistent finding that human capital is the binding constraint on OT/ICS security programme effectiveness (ISC2, 2024; Dragos, 2023). Third, it provides a tiered implementation model that acknowledges most Malaysian manufacturers are SMEs with no dedicated security function. Fourth, the three-layer validation provides a stronger evidential base than a purely conceptual contribution, demonstrating standards grounding, comparative positioning, and logical effectiveness against three documented attack vectors.

6.2 MICGF and IEC 62443: Clarifying the Relationship and Novelty

The MICGF is not an alternative to IEC 62443 or a replacement for it. IEC 62443 remains the most technically comprehensive OT security standard available, and organisations with the resources to pursue full implementation should do so. The MICGF serves a different purpose and audience: making IEC 62443's principles accessible and actionable in the Malaysian SME manufacturing environment, where full implementation is not currently feasible for most operators.

Section 4 sets out the specific gaps the MICGF closes relative to IEC 62443. Building on that, the MICGF extracts the standard's most critical requirements, as documented in Table 3, and expresses them as tier-appropriate indicators a Malaysian factory engineer can act on without a security certification; Tier 1 foundational actions are consistent with the intent of IEC 62443-2-1 but expressed in operational language suited to the SME context. The MICGF thus bridges IEC 62443 and the practical reality of Malaysian manufacturing governance without replicating its full technical scope.

6.3 Practical Implications for Malaysian Manufacturers

For a typical Malaysian SME at Tier 1, four actions form the practical starting point. The first is to conduct a manual OT asset census, listing every networked device and classifying each as Tier A, B, or C. The second is to install a dedicated firewall between the enterprise IT network and the manufacturing floor with default-deny rules. The third is to write a one-page OT incident response contact list documenting who calls who, in what order, and when something looks wrong. The fourth is to assign one named OT security focal point from the engineering team. These four actions require no external consultants,

specialist tools, or significant budget. They address the exact conditions that Scenario A in Section 5.3 demonstrates are exploited in the most common OT/ICS attack pattern. For manufacturers designated as NCII entities under the Cyber Security Act 2024, documented risk assessment and incident response procedures are now a legal requirement.

6.4 Policy Implications

The MICGF has several implications for Malaysian government agencies. The NCSP 2020 would benefit from an OT/ICS-specific annex that establishes minimum security controls for manufacturing entities in NCII sectors; the current policy does not provide this level of operational specificity for OT environments. The Industry 4WRD programme should require OT security self-assessments as a condition for technology adoption grant disbursement, because at present the programme accelerates IT/OT integration without requiring manufacturers to assess the security implications. CyberSecurity Malaysia should consider developing a publicly available Malaysian OT Security Implementation Guide for manufacturers without specialist security teams. The Ministry of Higher Education should work with Malaysian universities and polytechnics to integrate OT/ICS security content into cybersecurity programmes aligned with NICF Malaysia. Singapore's experience with its OT Cybersecurity Masterplan 2024 (CSA Singapore, 2024) provides a useful reference for what this kind of national coordination effort can produce.

6.5 Limitations

Three limitations should be acknowledged. The multi-layer non-contact validation confirms standards grounding, comparative positioning, and logical effectiveness against three attack patterns, but does not constitute empirical measurement of incident reduction in deployed environments. Whether the Tier 1 actions are achievable within SME resource constraints, and whether adoption of the MICGF produces measurable OT/ICS security posture improvements, requires field studies, which is the next stage of this research programme. Second, the framework addresses manufacturing broadly; sub-sectors with distinctive OT profiles such as semiconductor fabrication, petrochemicals, and food processing may need pillar-level adaptation. Third, the scenario validation covers three attack vectors; additional scenarios including advanced persistent threats and availability-focused attacks would provide more complete coverage.

7. Conclusion

This paper has argued that Malaysia faces an OT/ICS cybersecurity governance problem in its manufacturing sector that is both urgent and structurally unaddressed. The urgency comes from three converging factors: manufacturing is the most targeted sector for cyberattacks in Malaysia, the Cyber Security Act 2024 has created binding legal obligations that manufacturers must meet, and the Industry 4WRD Policy continues to accelerate IT/OT integration without security governance requirements. The structural gap is the absence of a published OT/ICS governance framework that bridges international technical standards with Malaysian regulatory instruments and the practical constraints of an SME-dominated manufacturing sector. The MICGF addresses this gap.

The five-pillar framework, comprising Asset Visibility and Classification, Network Architecture and Segmentation, Threat Detection and Incident Response, Governance Integration and Policy Alignment, and Workforce Capability Development, addresses the full spectrum of governance requirements for securing converged IT/OT manufacturing environments. Standards traceability mapping confirms all five pillars are grounded in IEC 62443 and NIST SP 800-82 Rev.3. The comparative benchmark confirms the MICGF addresses dimensions no existing framework covers for Malaysia. Three-scenario validation confirms the framework logically addresses the most prevalent documented OT/ICS attack patterns. The three-tier implementation model ensures the framework is actionable across the full manufacturer capability spectrum.

Three directions should guide future research. Most immediately, empirical validation through implementation studies with Malaysian manufacturers is needed to test whether the framework's assumptions about SME capability tiers are accurate and whether MICGF adoption produces measurable OT/ICS security improvement. Second, a quantitative OT security maturity assessment instrument, specifically a scored questionnaire aligned with the five pillars and three tiers, would enable systematic baseline measurement across the sector and provide practitioners and policymakers with a practical tool for tracking security posture improvement over time. Third, policy development work is needed to translate the MICGF's recommendations into sector-specific OT security codes of practice under the Cyber Security Act 2024 framework, following the model Singapore has used in its OT Cybersecurity Masterplan.

Declarations

Funding
This research received no external funding.

Acknowledgements
The author gratefully acknowledges Asia Pacific University of Technology and Innovation (APU), Kuala Lumpur, for the academic environment and institutional support that made this research possible. The author also thanks the anonymous reviewers and the editorial team of the Journal of Applied Technology and Innovation for their careful evaluation and constructive comments, which substantially strengthened the clarity, rigour, and positioning of this manuscript. No individuals other than the author contributed to the conception, development, or validation of the MICGF framework presented in this paper.

Conflict of Interest
The author declares no conflict of interest.

Data Availability Statement
This is a conceptual framework paper. No primary datasets were generated or analysed during this study. All sources cited are publicly available and fully referenced below.

Ethical Approval
Not applicable. This paper does not involve human participants, animals, or personal data.

References

Byres, E., & Lowe, J. (2004). The myths and facts behind cyber security risks for industrial control systems. Proceedings of the VDE Congress, 213-218.

Cyber Security Agency of Singapore (CSA Singapore). (2024). OT cybersecurity masterplan 2024. Cyber Security Agency of Singapore. https://www.csa.gov.sg

CyberSecurity Malaysia. (2020). National cybersecurity policy 2020. Ministry of Communications and Multimedia Malaysia. https://www.cybersecurity.my

CyberSecurity Malaysia. (2022). Malaysia cybersecurity industry landscape report 2022. CyberSecurity Malaysia. https://www.cybersecurity.my

Dragos. (2018). TRISIS malware: Analysis of safety system targeted attack. Dragos. https://www.dragos.com

Dragos. (2023). OT cybersecurity year in review 2023. Dragos. https://www.dragos.com/year-in-review

Economic Planning Unit (EPU). (2022). Malaysia economic indicators and finance 2022. Prime Minister's Department, Malaysia. https://www.epu.gov.my

Ensign InfoSecurity. (2024). Cyber threat landscape report 2024. Ensign InfoSecurity. https://www.ensigninfosecurity.com

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. MIS Quarterly, 28(1), 75-105. https://doi.org/10.2307/25148625

IEC. (2018). IEC 62443 series: Industrial communication networks, IT security for networks and systems. International Electrotechnical Commission. https://www.iec.ch

ISC2. (2024). Cybersecurity workforce study 2024. ISC2. https://www.isc2.org/workforce-study

Knapp, E. D., & Langill, J. T. (2014). Industrial network security: Securing critical infrastructure networks for smart grid, SCADA, and other industrial control systems (2nd ed.). Syngress.

Malaysia Digital Economy Corporation (MDEC). (2021). MyDIGITAL: Malaysia digital economy blueprint 2021-2030. MDEC. https://www.mdec.my

Ministry of International Trade and Industry (MITI). (2018). Industry4WRD: National policy on industry 4.0. MITI Malaysia. https://www.miti.gov.my

MyCERT. (2024). Cyber incident quarterly summary report Q1 2024. CyberSecurity Malaysia. https://mycert.org.my

National Cyber Security Agency (NACSA). (2024). Cyber Security Act 2024 (Act 854). Attorney General's Chambers of Malaysia. https://www.nacsa.gov.my/act854.php

NIST. (2024). The NIST cybersecurity framework 2.0. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29

Nozomi Networks. (2023). OT/IoT security report: Trends and countermeasures for critical infrastructure. Nozomi Networks Labs. https://www.nozominetworks.com

NTT Data. (2024). 2024 global threat intelligence report. NTT Data Corporation. https://www.nttdata.com

PwC. (2024). Geopolitical shifts amplify OT security risks. PricewaterhouseCoopers. https://www.pwc.com

Slowik, J. (2022). INDUSTROYER2: Analyzing the threats to electric grid operations. Dragos Intelligence. https://www.dragos.com

SME Corp Malaysia. (2017). Economic census 2016: Profile of small and medium enterprises. Department of Statistics Malaysia. https://www.smecorp.gov.my

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. Journal of Business Research, 104, 333-339. https://doi.org/10.1016/j.jbusres.2019.07.039

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2023). Guide to operational technology (OT) security. NIST Special Publication 800-82 Revision 3. https://doi.org/10.6028/NIST.SP.800-82r3

Torraco, R. J. (2005). Writing integrative literature reviews: Guidelines and examples. Human Resource Development Review, 4(3), 356-367. https://doi.org/10.1177/1534484305278283

Williams, T. J. (1994). The Purdue enterprise reference architecture. Computers in Industry, 24(2-3), 141-158. https://doi.org/10.1016/0166-3615(94)90017-5