



The Guard Playbook

The compliance map for industrial AI in Malaysia.

Everything that applies to your plant on one page. The roadmap to compliance on the next. Read in 8 minutes.

INSIDE

One regulation summary table covering all Malaysian and international rules that apply. A 5-step roadmap to a compliance file. Three real failure cases. Where TGE fits and where it doesn't.

Dean Lai

Founder · TGE Corporation

01 Generic AI is not Industrial AI — the architecture is different

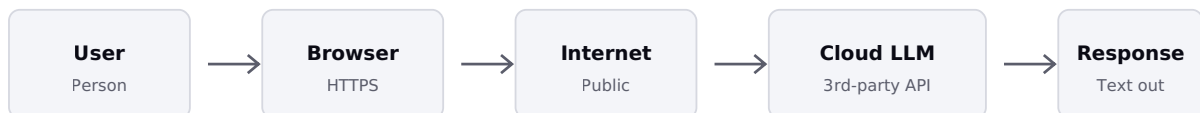
I keep having the same conversation with manufacturers in Malaysia. Someone shows me a generic AI tool — ChatGPT writing emails, a free chatbot answering FAQs — and asks “Can we use this in the plant?”

Generic AI and industrial AI are not the same animal. Generic AI lives on the internet. Mistake = bad day. Industrial AI lives on the plant floor. Mistake = line down, operator hurt, regulator visit, insurer call.

The technology may be the same underneath. The architecture is different. The compliance bar is completely different. Here is what that means for your plant.

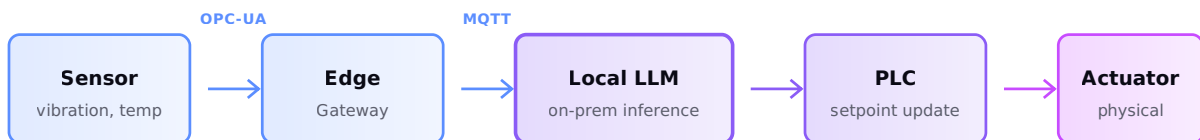
— Dean

GENERIC AI · CLOUD-HOSTED · STATELESS



Mistake = someone has a bad day. Data sent off-site. Stateless. No safety duty.

INDUSTRIAL AI · ON-PREM · CLOSED LOOP



CLOSED-LOOP FEEDBACK · data and decisions stay inside the plant

Mistake = line down. Operator hurt. Regulator visit. Insurer call.

Same technology underneath. Completely different architecture. Completely different compliance bar.

QUICK TAKE

If your AI touches a sensor, a PLC, an operator, or production data on the floor — the compliance bar of the rest of this guide applies to you. If it only touches emails and marketing copy — most of it doesn't.

02 The Malaysian regulation map

Four layers of Malaysian law apply to industrial AI deployment. None of them mention “AI” by name. All four reach into your plant.

REGULATION	ISSUED BY	STATUS	KEY REQUIREMENT	APPLIES IF YOU...
Occupational Safety & Health Act 1994 + Amendment Act 2022	DOSH dosh.gov.my	IN FORCE Since 1 June 2024	Coverage extended to all workplaces. Max fine raised to RM500,000 . OSH Coordinator role required.	Operate any workplace in Malaysia.
Personal Data Protection Act 2010 + Imminent ADM Guidelines	PDPD pdp.gov.my	IN FORCE Guidelines 2026	DPIA required for any automated decision-making or profiling — no volume exemption.	Handle personal data of employees, customers, or operators.
Malaysia AI Governance Bill + AI Action Plan 2026–2030	NAIO · MOSTI naio.gov.my	DRAFTING Cabinet mid-2026	Risk-based AI obligations across the AI lifecycle. Manufacturing flagged as a priority sector.	Deploy any AI in any sector (not yet enforceable).
Sector-specific Acts Petroleum, Electricity, Environment, CMA	Various sector regulators	IN FORCE	Sector-specific safety, environmental, and communications obligations on top of general law.	Operate in oil & gas, electricity, environmental, or telecoms.

QUICK TAKE

OSHA + PDPA already apply to your plant today. The Malaysia AI Bill is coming in 2026–2027. Direction of travel is from voluntary to enforceable, with manufacturing flagged a priority sector. Use the next 12 months as planning window, not panic window.

03 The international standards your customers will ask about

Even without a Malaysian AI Bill in force, customers, insurers, and ASEAN trading partners are starting to ask about international standards. Four matter most. They stack: ISO 27001 underpins everything, ISO/IEC 42001 sits on top.

STANDARD	ISSUED BY	STATUS	KEY REQUIREMENT	APPLIES IF YOU...
ISO/IEC 27001 Information Security Management	ISO · IEC iso.org/standard/27001	VOLUNTARY Certifiable	Risk-based information security management. Foundation every other standard sits on top of.	Handle customer production data in B2B Malaysian manufacturing.
IEC 62443 Industrial Cybersecurity (OT)	IEC · ISA isa.org/iec-62443	VOLUNTARY Procurement baseline	Zones + conduits architecture. Security Levels SL-1 to SL-4 (SL-2 typical baseline).	Run any OT — PLCs, SCADA, sensors, or AI layer on top.
IEC 61508 / 61511 Functional Safety	IEC iec.ch	VOLUNTARY Sector-mandatory	Safety Integrity Levels (SIL 1–4) for systems where failure can cause harm.	AI influences pressure, temperature, restart, or other safety-critical setpoints.
ISO/IEC 42001:2023 AI Management Systems	ISO · IEC iso.org/standard/42001	VOLUNTARY Certifiable	Plan-Do-Check-Act methodology applied to the full AI lifecycle. The world's first AI management standard.	Deploy any AI system — rapidly becoming a customer-audit baseline.

QUICK TAKE

Pick one standard to build toward first. For most Malaysian manufacturers, **IEC 62443 at SL-2** is the right starting point. Add ISO/IEC 42001 once your AI deployments are running and at least one customer asks for it. Customer demand drives the order, not internal preference.

04 Five steps to an audit-ready compliance file

Most plants get stuck at Step 1. The ones who finish stay ahead of the regulator. Realistic timeline: 6 to 12 months for the first cycle, then continuous.



QUICK TAKE

Assign **one person** as the compliance file owner. Not a committee. Accountable and empowered to call the conversation across operations, IT, legal, and your insurer. Plants that move fastest assign the owner before they assign the technology.

05 Three failure patterns — what going wrong looks like

The fastest way to internalise the compliance bar is to look at what failure has cost others. One verified public case, two illustrative Malaysian scenarios.

VERIFIED

2019 • Norway / Global

Norsk Hydro ransomware

LockerGoga ransomware impacted around 22,000 computers across 170 sites in 40 countries. Aluminium production switched to manual operation across multiple plants. Public company estimate: NOK 800 million to 1 billion (USD 70–100M).

Lesson. Enterprise IT compromise cascades into OT shutdown. The DMZ between business IT and the plant floor exists precisely to contain this. ISO 27001 + IEC 62443 zone separation is the structural answer; incident response drills are what make it work in practice. *Source: Norsk Hydro public quarterly disclosures.*

ILLUSTRATIVE

Composite • Malaysia

The vibration model that never moved

A mid-size Malaysian palm oil mill deploys vendor predictive-maintenance AI. No DPIA, no cybersecurity baseline, no model governance records. Eighteen months later, the largest customer audits for ISO/IEC 42001 alignment. The mill cannot produce a file. Customer pauses the contract pending remediation.

Pattern. "Deploy first, document later" combined with treating AI compliance as a vendor problem. The compliance file is the deliverable that protects the contract. Build it alongside the deployment. *Composite pattern observed across Malaysian heavy industry and FMCG; not a specific incident.*

ILLUSTRATIVE

Composite • Malaysia

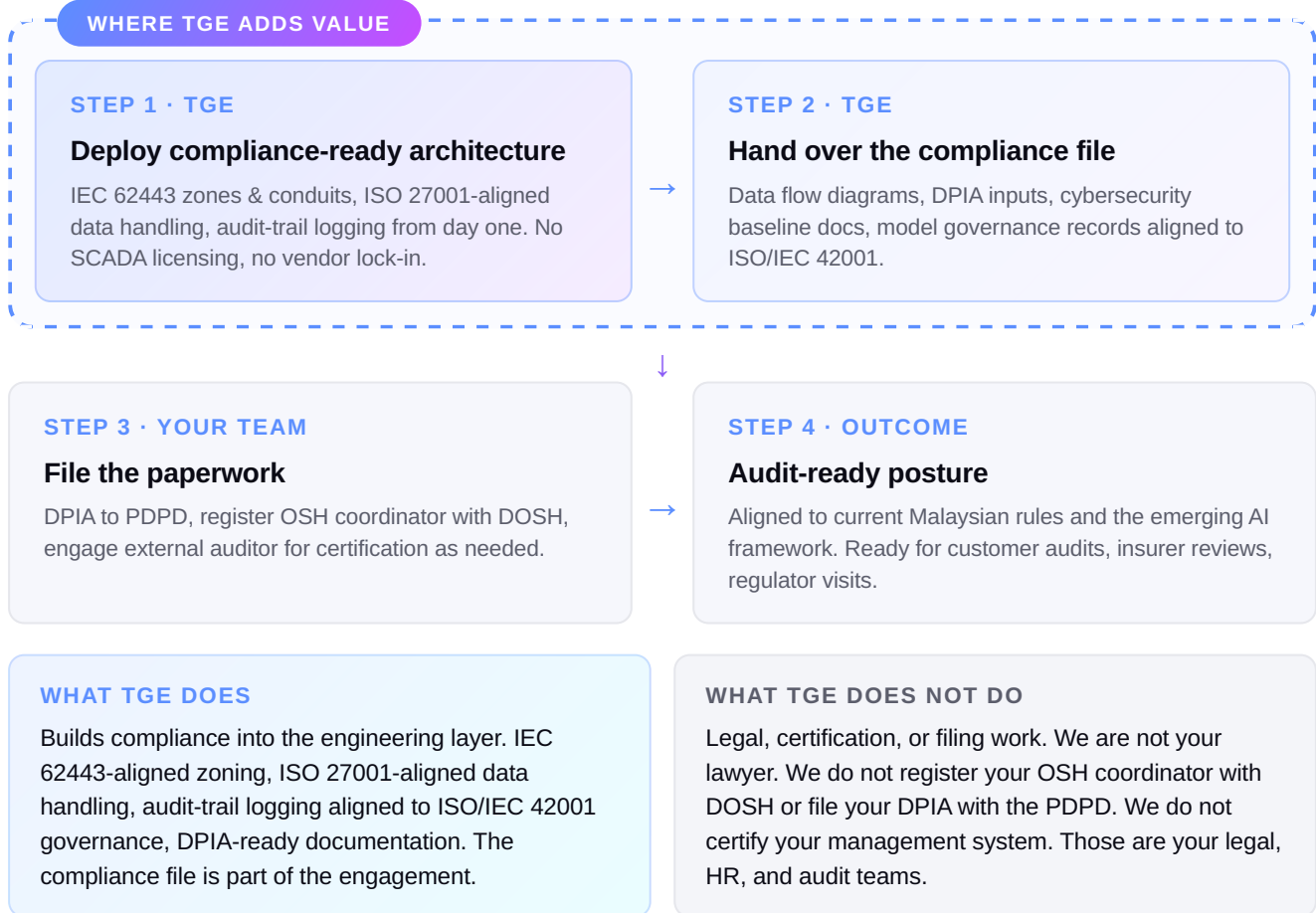
The QC system that learned the wrong thing

A semiconductor test facility deploys AI defect classification trained on six months of operational data that include a calibration drift. The model learns drifted readings as normal. Three months in production, a customer detects elevated defects across 12,000 wafers. A PDPA audit also reveals operator personal data was used in training without DPIA.

Pattern. Model governance and personal-data governance run by different teams — same conversation. The DPIA catches data-origin issues early. Model retraining records and validation runs catch calibration drift before it ships. *Composite pattern observed in semiconductor and QC AI deployments; not a specific incident.*

06 Where TGE fits in your compliance roadmap

TGE builds the industrial AI in compliance-ready form. Your team files the paperwork. We hand over the engineering artefacts that make their filing clean.



07 Your next three steps

1

Map your AI use cases against the regulation tables on pages 3 and 4

Identify every current and planned use case. The further into the high-stakes end of the tables it sits, the more stakeholders the conversation needs.

2

Pick one standard to build toward first

For most Malaysian manufacturers, **IEC 62443 at SL-2** is the right starting point. Add ISO/IEC 42001 once AI deployments mature and at least one customer asks for it.

3

Assign one accountable owner for the compliance file

One person. Accountable. Empowered to call the conversation across operations, IT, legal, and your insurer. Plants that move fastest assign the owner first.

About TGE Corporation

TGE builds AI-driven operational technology platforms for Malaysian manufacturers. Local LLM models trained on customer OT data, MQTT and OPC-UA ingestion, no SCADA licensing dependency, no vendor lock-in. Built to deploy fast across heavy industry, semiconductors, FMCG, process manufacturing, and palm oil. Every deployment comes with the engineering artefacts your compliance team needs.

- **Predictive maintenance** for rotating equipment — motors, pumps, compressors, fans.
- **Root cause analysis and quality control** for production-line defects.
- **Production optimisation** through real-time setpoint and recipe tuning.

DISCLAIMER

General information about Malaysian and international compliance frameworks for industrial AI. Not legal or compliance advice. Specific obligations vary by business size, sector, and use case. Confirm with a licensed Malaysian lawyer, your compliance officer, and the relevant regulators (DOSH, PDPD, MOSTI, NAIQ) before binding decisions. Regulatory references current to June 2026.



Ready to scope an audit-ready AI deployment?

DM me on Instagram with your industry and a one-line description of the production problem you're solving. The compliance file comes with the engagement.

INSTAGRAM

@dean.tge

WEB

deantge.com

TGE

tgecorporation.com

Version 1 · 2026. General information about Malaysian and international compliance frameworks for industrial AI — not legal advice. Verify specifics with official sources (DOSH, PDPD, MOSTI, NAIIO, ISO, IEC) and licensed advisors before binding decisions.

© 2026 TGE Corporation