CYBERSECURITY IMPERATIVES FOR SFM

Safeguarding Production Continuity, Intellectual Property
& Supply Chain Integrity in the Industry 4.0 Era

A Comprehensive Cybersecurity & Data Governance Framework

Threat Identification: External Threats

Attacks like ransomware campaigns are more prone to manufacturing because of its high downtime consequences, and attackers use IoT misconfigurations and remote access weaknesses to access the system [1].

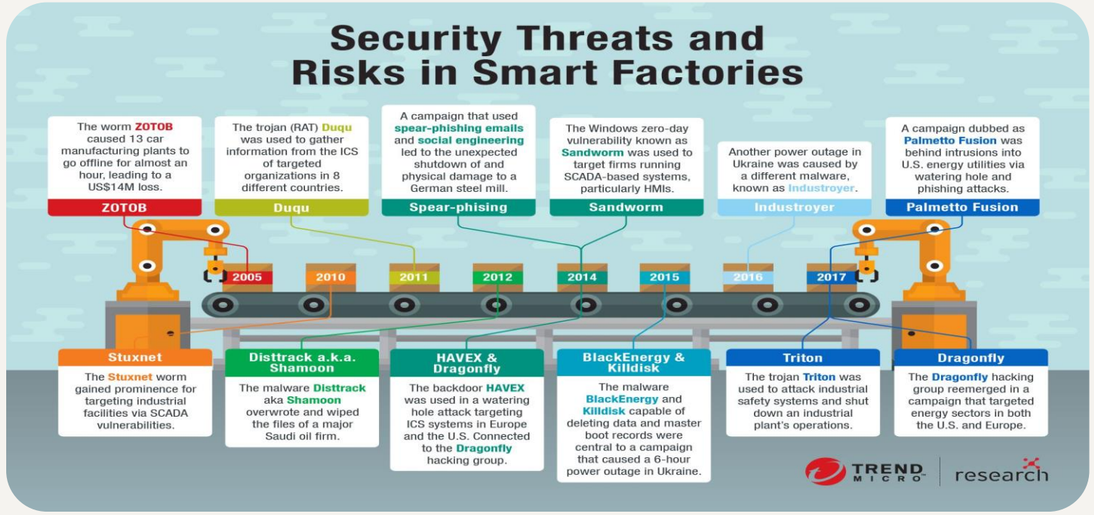
ICS threat modelling exposes poor segmentation and insecure protocols that foster horizontal movements across the OT networks [8].

Infiltration of the supply chain is a serious threat, with the third parties potentially having access to the production environment of SFM through breached systems [7].

The case of the JLR cyberattack illustrates the fast increase in external threats in the situation where governance gaps are present in the network of interconnected manufacturing systems [10].

Threat Type	Target Vector	Impact Level
Ransomware	IoT / Remote Access	HIGH
ICS Exploitation	OT Networks	HIGH
Supply Chain	Third-Party Systems	HIGH
Advanced Persistent Threats	Multi-Vector	CRITICAL

Table 1: External Threat Landscape for SFM



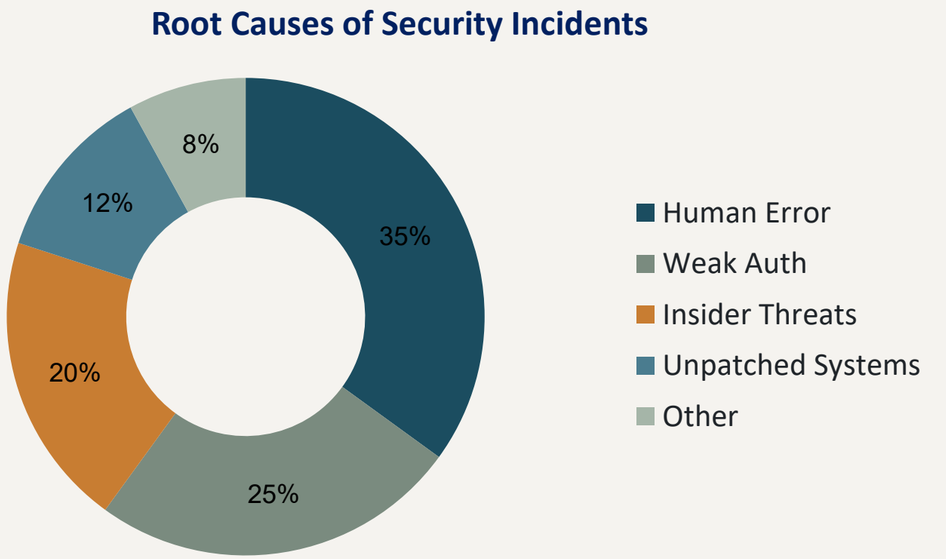
Threat Identification: Internal Threats

The most common weakness is human error, and engineers have an opportunity to go around security measures and engineers are prone to social engineering [3].

Poor authentication and workarounds lead to the existence of attack vectors that are not seen in ICS and IoT systems.

Lack of behavioural monitoring and inadequate access control increase the threat of insider attacks, both intentional and not.

Internal vulnerabilities tend to be catalysts that increase the effect of outside attacks, particularly in hybrid IT-OT setups.



Security Policies: International Framework Alignment

Figure 1: NIST Cybersecurity Framework Lifecycle

Dimension	ISO 27001	NIST CSF	CIA Triad
Focus Area 1	Access Control & Cryptography	Identify & Protect	Confidentiality
Focus Area 2	Incident Management	Detect & Respond	Integrity
Focus Area 3	Asset Protection	Recover	Availability
SFM Application	Policy backbone for governance	Continuous risk assessment cycle	Safety-critical ICS decisions

Table 2: Comparison of International Security Frameworks

- The ISO 27001 offers a well-organized governance over the access controls, cryptography, incident management and asset protection, which is the basis of the policy architecture of SFM.
- The CIA Triad concepts make sure that confidentiality, integrity and availability are taken into consideration in all policy decisions, especially, safety critical ICS systems.
- The policies should be tailored to the hybrid environment of SFM, where the IT and OT systems need controls that are differentiated and integrated, at the same time.

Security Policies: Supply Chain & Data Governance

To reduce the risks of third-party infiltration, it is important to strengthen the supplier agreements with compulsory cybersecurity terms [7].

The assessment of the vendor risk and continuous monitoring of compliance also make sure that the security standards of SFM are maintained by the external partners.

Fine-grained access control, encryption and audit trails should be included in data governance to safeguard sensitive production data [11].

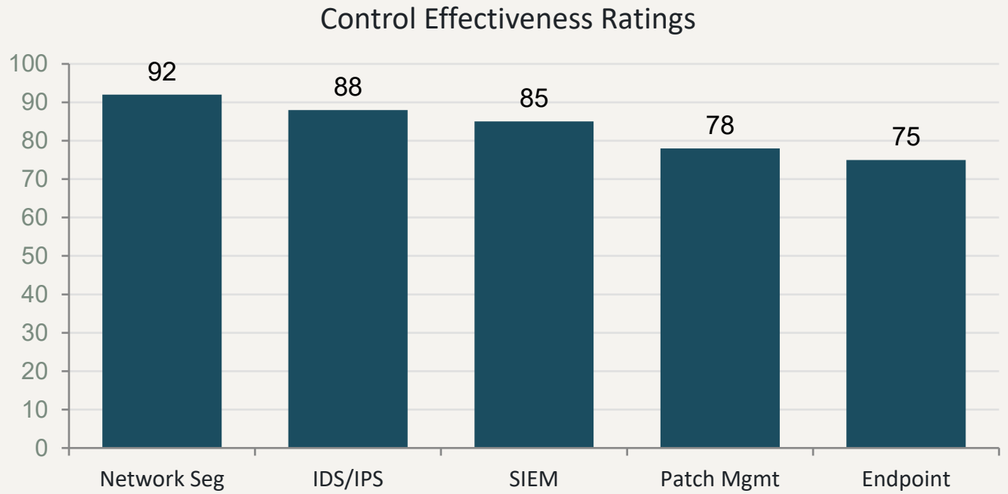
Manufacturing systems using clouds need stringent policies on the use of data to avoid unauthorised access and leakage of data.

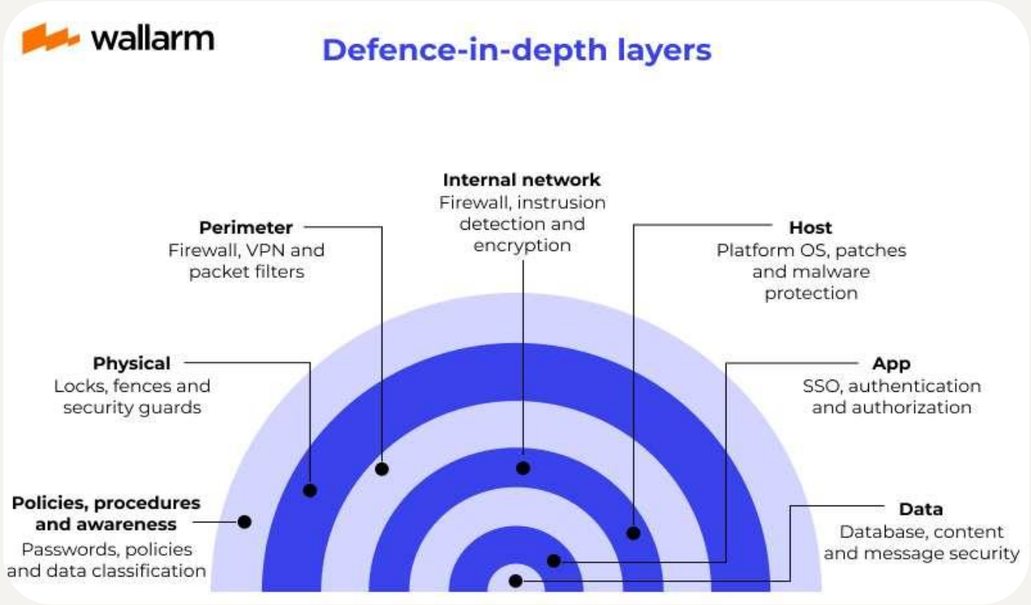
Governance Area	Key Control Measure
Supplier Contracts	Mandatory cybersecurity clauses
Vendor Assessment	Continuous compliance monitoring
Data Protection	Encryption & audit trails
Cloud Security	Strict data usage policies

Table 3: Supply Chain & Data Governance Controls

Mitigation Measures: Technical Controls

- Defence-in-depth architecture of network, application, endpoint and data layers minimizes exploitability and minimizes attacks.
- IDS/IPS and SIEM systems offer real-time threat detection and analytics, which is needed to detect anomalies in ICS and IoT environments.
- Vulnerabilities added in the process of IIoT retrofitting are mitigated with the help of secure configuration baselines, patch management, and firmware updates [6].
- The isolation of IT and OT networks is very essential in averting cross-domain compromise in the face of cyberattacks.





Mitigation Measures: Human-Centred Controls

Multi-factor authentication and role-based access control help to minimize the misuse of privileges and compromise of [3].

User activity can be tracked to identify abnormal behaviour in users and identify insider threats or compromised accounts early.

Periodic phishing exercises, and training based on scenarios enhance employee awareness and decrease exposure to social engineering.

Human-centred controls are used to supplement technical measures to form an effective and robust security posture.

Dimension	Technical	Human-Centred
Focus	Systems & Networks	People & Processes
Key Tools	SIEM, IDS, Firewalls	RBAC, MFA, Training
Response	Automated	Behavioural
Strength	Real-time detection	Cultural change
Weakness	Zero-day gaps	Human variability

Table 4: Technical vs. Human-Centred Controls

Key Insight

A balanced approach combining both technical and human-centred controls delivers the most resilient security posture.

Monitoring & Incident Response

- SIEM systems are used to bring together log gathering and threat analytics to ensure that there is continuous monitoring in IT and OT settings.
- Digital twins are used to model the behaviour of cyber-physical systems, which is then used to make proactive decisions about anomalies and predictive response to an incident [15].
- The detection, containment, eradication, and recovery will be the main components of a structured incident response cycle that will guarantee quick and coordinated response when breaches occur [14].
- The forensic analysis and post-incident reviews enhance organisational learning and policy improvements.

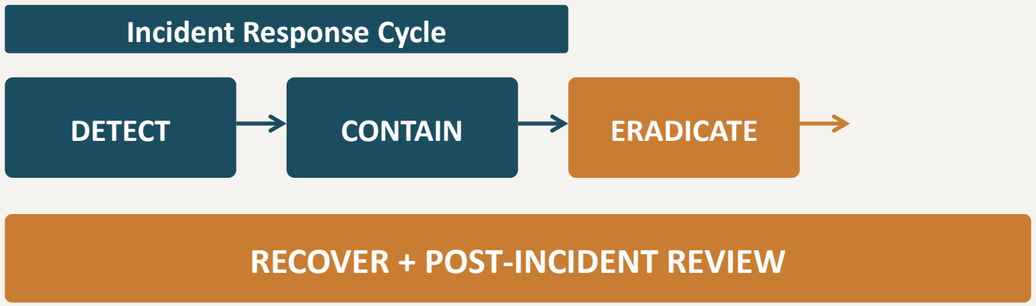


Figure 2: Structured Incident Response Cycle

Training & Awareness

- Role training makes sure that engineers, procurement employees and managers acquire competencies that are related to their risk exposure [5].
- Cyber4Me framework enhances individualised awareness pathways, which enhance engagement and change of behaviour [12].
- Ongoing awareness campaigns of phishing exercises, newsletters, visual icons and reminders incorporate cybersecurity in the organisational culture [13].
- Secure behaviours should be normalised and accountability reinforced with the involvement of leadership.

Initiative	Target Audience	Expected Outcome
Role-Specific Training	Engineers, Managers	Competency building
Cyber4Me Framework	All Staff	Personalised pathways
Phishing Simulations	All Staff	Vigilance improvement
Newsletters	All Staff	Awareness embedding
Leadership Engagement	Senior Management	Cultural normalisation

Table 5: Training & Awareness Program Components

Conclusion & Strategic Recommendations

01 SFM needs to implement a multi-layered approach to cybersecurity that combines both technical and human-centred interventions and governance frameworks.

02 **Policy development and continuous improvement should be based on ISO 27001 and NIST CSF.**

03 Resilience-specific digital twins and ICS-specific measures of resilience will greatly improve detection and response in case of emergency investment in SIEM.

04 Cybersecurity embedded in organisational culture through training, creation of awareness and involvement of leaders is a long-term resiliency and competitive advantage.

Cybersecurity is not a destination — it is a continuous journey of vigilance and adaptation.

References

[1] Adel Alqudhaibi et al., “Proactive cybersecurity in industry 4.0: A survey of cybersecurity threat prediction approaches in manufacturing systems,” International Journal of Information Security, vol. 25, no. 1, Dec. 2025, doi: 10.1007/s10207-025-01188-9 https://link.springer.com/article/10.1007/s10207-025-01188-9

[2] A. Alqudhaibi, M. Albarrak, S. Jagtap, N. Williams, and K. Salonitis, “Securing Industry 4.0: Assessing Cybersecurity Challenges and Proposing Strategies for Manufacturing Management,” Cyber Security and Applications, vol. 3, pp. 100067–100067, Dec. 2025, doi: 10.1016/j.csa.2024.100067 https://www.sciencedirect.com/science/article/pii/S277291842400033X

[3] U. D. Ani, J. Watson, H. He, Petar Radanliev, and G. Epiphaniou, “Minimising cybersecurity risk exposures in industrial control system environments: A techno-human vulnerability analysis approach,” Journal of Cyber Security Technology, pp. 1–40, Nov. 2024, doi:10.1080/23742917.2024.2421589 https://www.tandfonline.com/doi/abs/10.1080/23742917.2024.2421589

[4] M. M. Babu, M. Rahman, A. Alam, and B. L. Dey, “Exploring big data-driven innovation in the manufacturing sector: Evidence from UK firms,” Annals of Operations Research, vol. 333, Apr. 2021, doi: 10.1007/s10479-021-04077-1
https://link.springer.com/article/10.1007/s10479-021-04077-1

[5] Charalambous, A., Piki, A. and Stavrou, E., “Redesigning cybersecurity awareness-raising and training programs: Insights from professionals on knowledge, skills and educational practices. Information & Computer Security, 34(2), pp.273-294.,” 2026.
https://www.emerald.com/ics/article/doi/10.1108/ICS-04-2025-0163/1275195

[6] M. Comert, A. Ahmed, and H. Ahmed, “Identifying security challenges in the transition from traditional to smart manufacturing through IIoT retrofitting - White Rose Research Online,” Whiterose.ac.uk, Mar. 31, 2025. https://eprints.whiterose.ac.uk/id/eprint/225576/

[7] B. Gokkaya, K. Spanaki, and E. Karafili, “Strengthening the UK regulatory framework: Enhancing cybersecurity in supply chains,” International Journal of Information Management Data Insights, vol. 5, no. 2, p. 100370, Sept. 2025, doi: 10.1016/j.jjimei.2025.100370
https://www.sciencedirect.com/science/article/pii/S2667096825000527

[8] Granata, D., Iannaccone, A., Nardone, R. and Romano, L., “From Systematic Threat Search to pentesting: Industrial Control Systems threat models. Computers & Security, 170, p.105000,” 2026.
https://www.sciencedirect.com/science/article/pii/S0167404826001768

[9] M. A. Jarwar, J. Watson, and S. Ali, “Modeling Industrial IoT Security Using Ontologies: A Systematic Review,” IEEE Open Journal of the Communications Society, vol. 6, pp. 2792–2821, 2025, doi: 10.1109/ojcoms.2025.3532224.
https://ieeexplore.ieee.org/abstract/document/10847994/

[10] T. C. McAuley, “JLR Cyberattack: Lessons from a Major Manufacturing Crisis,” The Security Brief, Sept. 28, 2025. https://the-security-brief.com/2025/09/28/jlr-cyberattack-lessons-from-a-major-manufacturing-crisis/

[11] Pfeiffer, J., Maisch, N., Friedl, S., Strljic, M.M., Lechler, A., Riedel, O. and Wortmann, A., “Eclarative Policy Control for Data Spaces: A DSL-Based Approach for Manufacturing-X. Procedia CIRP, 142, pp.1082-1087,” https://www.sciencedirect.com/science/article/pii/S2212827126009844, 2026

[12] Rahman, M.A., Ibrahim, M., Ahmed, B., Refat, N., Wei, T.S. and Pillai, P., “A Quantitative Evaluation of Cyber4Me: A Holistic Framework for Enhancing Individual Cybersecurity Awareness. Computers, 15(7), p.418.,” 2026.
https://www.mdpi.com/2073-431X/15/7/418

[13] R. Shillair, P. Esteve-González, W. H. Dutton, S. Creese, E. Nagyfejeo, and B. von Solms, “Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise,” Computers & Security, vol. 119, no. 0167–4048, p. 102756, Aug. 2022, doi: 10.1016/j.cose.2022.102756
https://www.sciencedirect.com/science/article/pii/S0167404822001511

[14] A. Staves, T. Anderson, H. Balderstone, B. Green, A. Gouglidis, and D. Hutchison, “A Cyber Incident Response and Recovery Framework to Support Operators of ICS and Critical National Infrastructure,” International Journal of Critical Infrastructure Protection, vol. 37, p. 100505, Jan. 2022, doi: 10.1016/j.ijcip.2021.100505
https://www.sciencedirect.com/science/article/pii/S187454822100086X

[15] S. Suhail, M. Iqbal, K. McLaughlin, B. Lee, and B. Imtiaz, “A framework for enhancing cyber incident response with Security-Enhancing Digital Twins in Cyber-Physical Systems,” Internet of Things, p. 101547, Feb. 2025, doi: 10.1016/j.iot.2025.101547.
https://www.sciencedirect.com/science/article/pii/S2542660525000605