Proceedings of the International Conference on Industrial Engineering and Operations Management

Publisher: IEOM Society International, USA DOI: 10.46254/BA08.20250190
Published: December 20, 2025

Modeling the Impact of APTs on Smart Factory Performance: An Operations Management Perspective

Md Anisuzzaman, Ovejite Saha and Musfique-Us-Salehin Arnob
Master of Science in Cyber Security
World University of Bangladesh
Dhaka, Bangladesh
26250446@student.wub.edu.bd, 26250445@student.wub.edu.bd,
26240340@student.wub.edu.bd, anisuzzaman@live.com, musfique-us-salehin@cse.wub.edu.bd

Abstract

The move toward Industry 4.0 means that smart factories are merging their Information Technology (IT) and Operational Technology (OT). This integration, while efficient, creates significant new risks, particularly from Advanced Persistent Threats (APTs). This paper's core idea is that an APT isn't just a data breach; it's a direct attack on production—an act of industrial sabotage. This makes it a central problem for Operations Management (OM), not just for the IT department. We look at famous attacks like Stuxnet and TRITON not as cybersecurity events, but as attacks on core manufacturing metrics. The main contribution of this work is a new framework that connects specific APT attack methods to the real-world operational damage they cause, measured by Overall Equipment Effectiveness (OEE) and its parts: Availability, Performance, and Quality. We then suggest using standard Industrial Engineering tools, like C-FMEA, and established OM simulation methods (DES, ABM, SD) to measure this impact. We conclude that this operations-first viewpoint requires a strategic change from just trying to prevent attacks to building true operational resilience, making cyber-risk a part of production philosophies like TPM 4.0.

Keywords

Advanced Persistent Threat (APT), Operations Management, Smart Factory, Industry 4.0, Overall Equipment Effectiveness (OEE)

1. Introduction

Over the last decade, the Fourth Industrial Revolution (Industry 4.0) has become the main driver for transforming manufacturing (Kagermann 2022). This new model is best seen in the 'smart factory,' which works by merging the real world of machines with the virtual world of data into what are called cyber-physical production systems (Kagermann et al. 2011). The ultimate goal is to change old, rigid value chains into flexible and highly adaptive value networks (Kagermann 2016).

The smart factory's heart is the tight, real-time link between physical production machines and their digital control systems. This is made possible by technologies like Cyber-Physical Systems (CPS), which create a "digital twin" of physical processes, and the Industrial Internet of Things (IIoT), which uses sensors to collect live data for better, often autonomous, decision-making (Sinha and Roy 2020; Tao and Zhang 2017).

However, this deep connection of Information Technology (IT) and Operational Technology (OT) also creates a massive new operational risk. For the first time, cyber attackers can directly control and damage physical machinery. The very network connection that optimizes a production line also exposes its core industrial controls—like Programmable Logic Controllers (PLCs) and SCADA systems—to internet-based threats they were never built to

handle. These systems, which were once isolated, are now vulnerable to the same threats as any IT network (NSTAC 2020).

This problem isn't just technical; it's organizational. Traditionally, a factory's IT and OT teams have worked in separate siloes, often with conflicting goals. The OT team's top priority is keeping the line running safely and reliably. The IT team, on the other hand, focuses on network security and data. This gap between departments is exactly what attackers exploit. The real challenge isn't just connecting IT and OT systems, but getting the management to unite these teams under a single strategy for handling cyber-physical risk (ResearchGate 2023).

The most dangerous of these new threats is the Advanced Persistent Threat (APT). An APT isn't a random virus. It is a "prolonged and targeted cyberattack" where a "qualified and skilled adversary" gets into a network and stays hidden for a long time (Journal of Management... 2022; MDPI 2023). These are strategic, well-funded campaigns, often backed by states, designed to achieve a specific goal—be it spying, crime, or, for a factory, physical destruction (Taleb et al. 2024). These attacks are a direct threat to the confidentiality, integrity, and, most importantly, the availability of a company's systems (Cybersecurity 2024).

This paper argues that we must fundamentally change how we think about APTs in a factory. This is not just an IT problem about data; it is a core Operations Management (OM) problem about keeping production running, maintaining performance, and ensuring quality. The OM field, which has a long history of studying and managing disruptions, is perfectly suited to treat cybersecurity as a new and critical source of operational risk (Ivanov 2017; Sodhi et al. 2012). This paper answers that call by creating a shared language between security and operations, linking APT tactics directly to the most important manufacturing metric: Overall Equipment Effectiveness (OEE).

1.1 Objectives

The main goal of this research is to build a new, operations-focused way to analyze how APTs affect smart factories. To do this, we have four specific objectives:

1. To re-define APTs as acts of industrial sabotage, shifting the problem from the cybersecurity field to the Operations Management (OM) field.
2. To create a new conceptual framework that acts as a lingua franca for security and operations teams, showing how APT tactics directly cause OEE to decline.
3. To look back at major industrial attacks (Stuxnet, TRITON) using OM metrics to show their quantifiable impact on OEE.
4. To review standard simulation methods (DES, ABM, SD) and Industrial Engineering (IE) tools (C-FMEA, QFD) as a clear path forward for measuring and managing this new kind of cyber-physical risk.

2. Literature Review

This analysis brings together three separate fields of study: the engineering and computer science work that defines the smart factory (Industry 4.0); the cybersecurity research that defines the APT; and the business and industrial engineering field of Operations Management (OM).

The smart factory, also called Industry 4.0 or a Cyber-Physical Production System (CPPS), is a manufacturing environment defined by its blend of digital technology and physical machinery (Chen 2017). The foundation is the Cyber-Physical System (CPS), which allows machines, robots, and digital models to communicate in real-time, working together to optimize the production line (Sinha and Roy 2020). A key part of this is the 'digital twin,' which has evolved from a simple simulation to a live, virtual copy of a physical asset. This virtual model is "enabled through data and simulators for real-time prediction, optimization, monitoring, controlling, and improved decision making" (Tao and Zhang 2017). This is a critical point: the digital twin isn't just a passive dashboard; it's an active controller. An attack on the digital twin is therefore a direct attack on the physical machine it controls. The "glue" for all this is the convergence of IT and OT (NSTAC 2020). This is also the system's greatest weakness. As government reports note, OT systems like PLCs and SCADA controllers were designed for safety and reliability, not security, and were historically kept "air-gapped" or offline. Connecting them to IT networks for data analysis exposes these critical systems to a world of cyber threats they are not prepared for (NSTAC 2020).

An Advanced Persistent Threat (APT) is far more dangerous than common malware. The academic literature defines it by its three parts (Journal of Management... 2022). It is Advanced, using custom tools and zero-day exploits. It is Persistent, meaning attackers work for months or even years to stay inside a network, a period known as "dwell-time" (ResearchGate 2025). And it is a Threat, driven by "strategically-motivated," skilled, and well-funded groups, often state-sponsored (Taleb et al. 2024; MDPI 2023). The APT lifecycle is a multi-stage process (ResearchGate 2025). When targeting industrial systems, these attacks are now so common they have their own framework, the MITRE ATT&CK for ICS. This framework is widely used in academic research for "cyber threat modeling" (Amro and Gkioulos 2023a; Xiong et al. 2022) and "attack simulation" (Analyzing New... 2025). Our work builds on this by linking the tactics in that framework to the metrics used by operations managers.

The Operations Management (OM) perspective is a business discipline focused on how to design, run, and improve the processes that make products (Kazancoglu and Ozkan-Ozen 2018). It is obsessed with operational excellence, which it measures with metrics for productivity, efficiency, and quality. A large part of OM research is dedicated to disruptions and supply chain risk management (SCRM) (Chopra and Sodhi 2004; Ivanov 2017). This research analyzes how events like natural disasters or supplier failures ripple through a network and cause losses (Sodhi et al. 2012). Recently, leading OM scholars have called for the field to address cybersecurity as a new, critical, and under-studied source of operational disruption (Frank et al. 2019). This paper is a direct response to that call.

3. Methods

This paper uses a conceptual research approach, completed in three phases. This method is designed to connect the technical world of industrial cybersecurity with the managerial world of operations.

The first step, **Phase 1: Canonical Case Study Re-evaluation,** is a qualitative review of the two most famous industrial APT attacks: Stuxnet and TRITON. We use peer-reviewed forensic reports as our "data" to identify what the attackers were operationally trying to achieve, going beyond a simple IT analysis. The goal is to prove from the evidence that these attacks were intended to destroy physical operations, not just steal data.

The second step, **Phase 2: Conceptual Framework Development,** builds on the findings from Phase 1. We use a conceptual-modeling method to synthesize the case study evidence and the literature. This builds a formal, causal bridge between APT tactics (from the security world) and performance metrics (from the OM world). This framework, shown in Table 1, is meant to be a lingua franca that unifies the perspectives of security, engineering, and operations teams.

The final step, **Phase 3: Risk Methodology Adaptation,** proposes how to adapt established Industrial Engineering (IE) tools for this new problem. We specifically look at how Failure Modes and Effects Analysis (FMEA) and Quality Function Deployment (QFD) can be used to operationalize the conceptual framework. This gives managers a structured, familiar, and quantitative way to assess and manage these new cyber-physical threats.

4. Data Collection

The "data" for this conceptual work was gathered from a deep review of authoritative, peer-reviewed technical and forensic reports on the Stuxnet and TRITON attacks. We chose these two cases because they are the most significant, well-documented, and operationally-focused APT attacks against industrial control systems to date.

Data Set 1: Stuxnet (An Attack on Performance and Quality)

Stuxnet, found in 2010, is globally recognized as the first true cyber-physical weapon. Our data from forensic reports confirms it targeted a specific industrial setup: the Siemens S7-300 and S7-400 PLCs that controlled the gas centrifuge cascades at the Natanz uranium enrichment plant (Falco 2012).

The attack was a brilliant piece of operational sabotage. Stuxnet didn't just shut the plant down. It subtly changed the PLC logic that controlled the speed of the centrifuge motors (Langner 2011). Forensic data shows the attack code made the centrifuges' rotational speed swing wildly. First, it sped them up from their normal speed of 1,064 Hz to a dangerous 1,410 Hz. Then, it slowed them to a near-halt at 2 Hz, before returning to normal (MDPI 2021). The 1,410

Hz frequency was pure malice; it is a speed "very close to the maximum speed the spinning aluminum IR-1 rotor can withstand mechanically," all but guaranteeing the centrifuge would tear itself apart (Albright et al. 2010).

Crucially, Stuxnet also created an "OM Blind Spot." To hide what it was doing, the malware faked the data going to the operators' control screens (the Human-Machine Interface, or HMI). Scholarly analysis confirms that while the attack was running, "operators at Natanz were presented with outdated centrifuge sensor data from recordings... This meant that the operators observed centrifuge settings that were seemingly normal" (Langner 2011). The operators saw a healthy process on their screens, while on the factory floor, their equipment was being systematically destroyed.

Data Set 2: TRITON (An Attack on Safety and Availability)

The TRITON (or TRISIS) malware, found in 2017, shows a terrifying evolution in this attack philosophy. This incident is now thoroughly documented in technical literature (Developing Resilient... 2023). Our collected data confirms TRITON was built to attack one very specific piece of hardware: the Schneider Electric Triconex Safety Instrumented System (SIS).

An SIS is the last line of defense in a facility like the Middle Eastern petrochemical plant that was targeted. It's a separate, independent system that monitors for dangerous conditions (like extreme pressure or temperature) and automatically triggers a safe shutdown to prevent a catastrophe (Developing Resilient... 2023).

The TRITON malware was a Remote Access Trojan (RAT) that let attackers change the firmware on the SIS controllers. Technical reports are clear on the attackers' goal: to take control of the safety system itself (Cybersecurity 2020). This would let them first launch another attack to create a dangerous situation (like over-pressurizing a vessel) and then use TRITON to prevent the safety system from working, leading to a physical explosion and potential loss of life (Jeffries et al. 2022). By sheer luck, a flaw in the malware's code accidentally triggered a safe shutdown, which led to the investigation that uncovered the plot (Jeffries et al. 2022). From an OM view, TRITON is the ultimate attack on operational availability.

5. Results and Discussion

Analyzing the data from Section 4 gives us clear, measurable results when we use an Operations Management perspective. This section presents those results, develops them into a general framework, and proposes improvements based on the findings.

5.1 Numerical Results

The case study analysis provides quantifiable, numerical impacts that map directly to core OM performance metrics.
Stuxnet Numerical Impact: The attack's "result" was a direct hit on two OEE metrics:

1. **Attack on Performance:** Manipulating centrifuge speeds—from a normal 1,064 Hz to a damaging 1,410 Hz (a +32.5% deviation) and a near-stall 2 Hz—is a classic "Reduced Speed" loss. This is a direct, numerical attack on the Performance component of OEE.
2. **Attack on Quality:** The physical stress from these speed changes caused centrifuges to fail. The destruction of an estimated "over a thousand centrifuges" (Albright et al. 2010) is a catastrophic "Process Defect" and "Scrap" loss, directly attacking the Quality component of OEE.

TRITON Numerical Impact: The attack's intended "result" was the ultimate OEE attack:

1. Attack on Availability: The TRITON malware was designed to enable a complete, catastrophic failure of the entire plant. This represents the most extreme "Equipment Failure" loss, resulting in a permanent Availability loss of 0%.

These numerical results ground our general framework in real-world data.

5.2 Graphical Results

The "results" of a conceptual study are the frameworks and models developed from the analysis. To model a disruption, we first need a baseline. In manufacturing, the gold standard for measuring performance is Overall Equipment Effectiveness (OEE). OEE was introduced by Nakajima (1988) to measure the success of Total Productive

Maintenance (TPM) programs (Garza-Reyes et al. 2010). It is a single key performance indicator (KPI) that measures productivity by quantifying the "six big losses" of production (Wudhikarn 2019). The formula is (Figure 1):

$$OEE = \text{Availability} \times \text{Performance} \times \text{Quality}$$

Figure 1. Formula Of OEE

- Availability measures "Stop Time Loss" (e.g., breakdowns).
- Performance measures "Speed Loss" (e.g., running slower than designed).
- Quality measures "Quality Loss" (e.g., scrap and defects).

The main contribution of this paper is explicitly linking cyber-attack tactics to these OEE components. An APT-caused disruption isn't just "downtime"; it's often a stealthy, specific attack on one of OEE's three pillars. Table 1 presents this mapping. It translates common cyber-attack tactics, drawn from frameworks like MITRE ATT&CK for ICS (Amro and Gkioulos 2023a), into their direct, measurable impact on production KPIs. This table helps IT, OT, and Management teams speak the same language.

Table 1. Conceptual Model for Mapping APT Attack Vectors to OEE Degradation

Tactic (from MITRE ATT&CK for ICS)	**Attack Example (Observed or Theoretical)**	**Primary OEE Component Affected**	**Specific Operational Impact (OM Metric)**
Impair Process Control	Ransomware on HMI/SCADA.	Availability	"Unplanned Stop." Operator cannot control or monitor the process, forcing a shutdown. Direct loss of Run Time.
Modify Control Logic	Stuxnet-like manipulation of PLC code.	Performance	"Slow Cycles" / "Reduced Speed." Process runs, but at a non-optimal (and perhaps damaging) speed.
Data Manipulation (of sensor/QC data)	Altering sensor readings for quality control; Stuxnet's HMI spoof.	Quality	"Process Defects." Bad parts are accepted. Leads to scrap, rework, and yield loss.
Network Disruption (e.g., Denial of Service, Latency)	"Death by a thousand cuts" - network jitter, latency, packet loss in real-time control loops.	Performance	"Minor Stops" / "Idling." Real-time control loops are delayed, causing micro-stoppages that degrade performance.

Inhibit Response Function	TRITON attack on Safety Instrumented System (SIS).	Availability (Catastrophic)	"Equipment Failure." A process-control attack is combined with disabling the safety system, causing a cascading physical failure.
Data Destruction	Targeting Manufacturing Operations Management (MOM) / MES systems.	Availability	"Planned Stop" (Forced). Loss of production schedules, recipes, or batch records. Production is halted until data is restored.

Now that we know what to measure (Table 1), we need to decide how to model the dynamic impact. The OM and IE fields offer many simulation tools (Ivanov 2020), but no single tool is perfect. The attack is a stealthy, smart "agent," which is behaviorally complex. The factory is a process-driven system full of randomness and bottlenecks. This "modeling mismatch" means we need to compare different methods, which we do in Table 2.

Table 2. Comparison of Modeling Methodologies for APT-OM Impact Analysis

Methodology	**Level of Abstraction**	**Primary Focus**	**Key Question Answered**
Discrete-Event Simulation (DES)	Micro (Shop-floor, Process)	Stochastic process flow; resource contention; queuing.	"If APT-event X (e.g., 30-min PLC outage) occurs, what is the precise, quantified impact on OEE, throughput, and cycle time?"
Agent-Based Modeling (ABM)	Meso (System, Network)	Emergent behavior from autonomous agent interactions.	"How will a stealthy APT (an 'agent') propagate through my network of IIoT 'agents' and which assets will be compromised first?"
System Dynamics (SD)	Macro (Business, Supply Chain)	High-level feedback loops; stocks and flows; long-term policy.	"How will a sustained 5% drop in Quality (from the APT) create a 'ripple effect' that damages customer trust and supply chain stability over 18 months?"

5.3 Proposed Improvements

Based on these results, we propose key improvements from Industrial Engineering and Operations Management to build resilience against APTs.

Improvement 1: Cyber-Failure Modes and Effects Analysis (C-FMEA)

Failure Modes and Effects Analysis (FMEA) is a standard IE tool for systematically finding potential failures in a process, assessing their impact, and prioritizing what to fix (IEC 60812:2018). We can adapt this into a Cyber-

FMEA (C-FMEA). In a C-FMEA, the "failure modes" are the APT tactics from Table 1 (e.g., "Modify Control Logic"). The FMEA process calculates a Risk Priority Number (RPN):

$$RPN = \text{Severity (S)} \times \text{Occurrence (O)} \times \text{Detection (D)}$$

Figure 2. Formula Of RPN

The key improvement is how we re-define these terms from an OM perspective:

- **Severity (S):** This is the most critical change. Severity is not an abstract "high/medium/low" IT rating. It is quantitatively tied to OEE impact. A "10" (most severe) is an attack like TRITON that causes total failure (Availability = 0). A "3" might be a stealthy attack like Stuxnet that causes a small, hard-to-find drop in Quality or Performance.
- **Occurrence (O):** The likelihood a specific cyber-vulnerability will be found and used.
- **Detection (D):** The likelihood the attack will be detected. A high score (e.g., "10" = undetectable) would go to an attack like Stuxnet that faked the HMI screen (Langner 2011).

Improvement 2: Quality Function Deployment (QFD) for Resilience

Quality Function Deployment (QFD), or the "House of Quality," is another classic IE tool. It's a matrix that translates customer requirements ("WHATs") into engineering specifications ("HOWs"). We can adapt this for designing resilient systems. Here, the "customer" is the Operations Manager.

- **"WHATs" (OM Requirements):** The operational goals. Examples: "Maintain >95% Availability," "Ensure 99.9% First Pass Yield (Quality)," "Guarantee safe-shutdown capability."
- **"HOWs" (Technical/Security Controls):** The specific controls to achieve those goals. Examples: "Network Segmentation," "PLC Access Control," "Continuous OT Network Monitoring," "SIS-independent physical backups."

The QFD matrix would then map these, providing a structured way to prove that security spending (the "HOWs") is directly supporting the business goals (the "WHATs").

Improvement 3: TPM 4.0: Building Cybersecurity into Maintenance

Total Productive Maintenance (TPM) is an OM philosophy focused on maximizing OEE by eliminating all losses (Nakajima 1988). Since APTs directly attack OEE, it is a managerial necessity to build cybersecurity into the TPM framework. We call this "TPM 4.0" (Zarreh et al. 2019). Under TPM 4.0, the OEE metric becomes a cybersecurity sensor. An unexplained drop in Performance or Quality can no longer be assumed to be a simple mechanical fault. As Stuxnet proved, this OEE drop might be the only real sign of an attack (Langner 2011). It must trigger a joint investigation by both maintenance engineers and the IT/OT security team.

Improvement 4: Resilient Cyber-Physical Production Systems (CPPS) Design

Finally, operations managers and engineers must be part of the design of new production systems, not just the people who use them. Operational resilience must be designed in from day one. This includes:

- **Modularity:** Designing the factory in independent blocks, so a compromise in one area can't spread to the entire plant.
- **Fail-Safe Modes:** Ensuring that if a digital signal is lost or compromised (like in the TRITON attack), the physical machine defaults to a safe, non-destructive state (Jeffries et al. 2022).
- **Redundancy:** Building smart redundancy not just for IT servers, but for critical OT sensors and controllers.

5.4 Validation

The framework in Table 1 and the improvements in Section 5.3 need to be validated. We propose using the OM simulation methodologies from Table 2 to do this.

Validation via Discrete-Event Simulation (DES)

DES is the standard OM tool for modeling a factory's production flow (Sakib et al. 2022). A DES model of a production line can act as a "digital twin" testbed. We can inject the APT impacts from Table 1 as new random events. For example, an "Impair Process Control" attack (affecting Availability) would be modeled as a new "Time to Failure" event. A "Modify Control Logic" attack (affecting Performance) would be modeled by changing a machine's "Cycle

Time" variable. We can then run the simulation to get a statistical, risk-free forecast of the attack's real impact on OEE, throughput, and cost.

Validation via Agent-Based Modeling (ABM)
ABM is a "bottom-up" method that models a system as a group of autonomous "agents" (Sodhi et al. 2012). ABM is the perfect tool to model the attacker (an agent) moving through the factory's assets (also agents, like PLCs, HMIs, and firewalls). The ABM's output—the probability of an asset being compromised—can then be used to set the "Occurrence" variable in the C-FMEA and provide more realistic event data for the DES model.

Validation via System Dynamics (SD)
System Dynamics (SD), which started as "Industrial Dynamics" (Forrester 1961), is a tool for modeling high-level, long-term behavior. SD can validate the strategic "ripple effects" of an attack (Dolgui et al. 2020). The output from the DES model (e.g., "a 5% drop in OEE") becomes an input for the SD model. The SD model would then show the long-term impact on inventory, order fulfillment, and, ultimately, customer trust.

6. Conclusion

This paper has made the case for a fundamental shift in how we view Advanced Persistent Threats in smart manufacturing. We must move this problem from the technical domain of cybersecurity to the practical, quantitative field of Operations Management.

This research has met its objectives. We re-defined APTs as industrial sabotage by re-evaluating Stuxnet and TRITON through an operational lens. We then proposed a new conceptual framework (Table 1) to act as a lingua franca, connecting specific cyber-attack tactics to their quantifiable impact on Overall Equipment Effectiveness (OEE). We also proposed adapting standard Industrial Engineering tools like C-FMEA and QFD to create a structured process for managing these new cyber-physical risks. Finally, we reviewed the primary OM simulation tools (DES, ABM, and SD) as a clear path for validating this framework and concluded that this new understanding requires a strategic shift from simple prevention to a focus on operational resilience, powered by concepts like TPM 4.0.
This conceptual paper opens several important paths for future research. The most urgent need is to build hybrid simulation models that combine ABM (to model the attacker) with DES (to model the factory floor) in a single environment. This framework must also be validated with empirical data from real-world incident reports to build statistical models of attack frequency and duration. Future work should also extend the model to explicitly link OEE degradation to financial metrics like Cost Per Unit and Return on Assets. Finally, this research should be expanded to model the supply chain consequences of an APT, analyzing how the compromise of one smart supplier can ripple through an entire industrial ecosystem.

References

Albright, D., Brannan, P. and Walrond, C., Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?, Institute for Science and International Security (ISIS) Report, Washington, DC, 2010.
Amro, A. and Gkioulos, V., Integrating MITRE ATT&CK for ICS in Risk Assessment Methodologies, arXiv, 2502.10825v1, 2023a.
Analyzing New and Emerging Cyber Threats in Industrial Control Systems and Their Impact on Critical Infrastructure, DiVA portal, 2025.
Chen, Y., Integrated and intelligent manufacturing: Perspectives and enablers, Engineering, vol. 3, no. 5, pp. 588-595, 2017.
Chopra, S. and Sodhi, M.S., Managing Risk to Avoid Supply-Chain Breakdown, MIT Sloan Management Review, vol. 46, no. 1, pp. 53–61, 2004.
Cybersecurity, Advanced persistent threats (APTs) pose significant challenges, Cybersecurity, vol. 10, no. 1, 2024.
Cybersecurity, TRITON Malware and its impact on industrial control systems, Cybersecurity, vol. 6, no. 1, 2020.
Developing Resilient Cyber-Physical Systems: A Review of State-of-the-Art Malware Detection Approaches, Gaps, and Future Directions, MDPI, 2023.
Dolgui, A., Ivanov, D. and Rozhkov, M., Does the ripple effect influence the bullwhip effect? An integrated analysis of structural and operational dynamics in the supply chain, International Journal of Production Research, vol. 58, no. 5, pp. 1285–1301, 2020.
Falco, G., Stuxnet: A real-world cyber-physical attack, NATO CCDCOE, Tallinn, 2012.
Forrester, J.W., Industrial Dynamics, MIT Press, Cambridge, MA, 1961.

Frank, A.G., Dalenogare, L.S. and Ayala, N.F., Industry 4.0 technologies: implementation, adoption and management, International Journal of Production Economics, vol. 208, pp. 165-181, 2019.

Garza-Reyes, J. A., et al., From measuring overall equipment effectiveness (OEE) to overall resource effectiveness (ORE), Journal of Quality in Maintenance Engineering, vol. 16, no. 1, pp. 88-103, 2010.

Hermann, M., Pentek, T. and Otto, B., Design principles for Industrie 4.0 scenarios, Proceedings of the 49th Hawaii International Conference on System Sciences (HICSS), pp. 3928–3937, 2016.

Huang, Y. et al., Assessing the Physical Impact of Cyber-Attacks on Industrial Cyber-Physical Systems, Proceedings of the 2018 IEEE Industrial Cyber-Physical Systems (ICPS), 2018.

IEC 60812:2018, Failure modes and effects analysis (FMEA and FMECA), International Electrotechnical Commission, Geneva, 2018.

Ivanov, D., Operations and Supply Chain Management: A Review of Disruptions, Risk and Resilience, International Journal of Production Research, vol. 55, no. 1, 2017.

Ivanov, D., Predicting the impacts of epidemic outbreaks on global supply chains: A simulation-based analysis on the coronavirus (COVID-19) pandemic, Transportation Research Part E: Logistics and Transportation Review, vol. 136, 101922, 2020.

Jeffries, B., Saravia, S., Carter, C., and Ankuda, Z., Cyber Risk to Mission Case Study: Triton, Technical Paper, PRS-22-3170, The MITRE Corporation, 2022.

Johnson, B., Caban, D., Krotofil, M., et al., Attackers Deploy New ICS Attack Framework TRITON and Cause Operational Disruption to Critical Infrastructure, FireEye Blog, 2017.

Journal of Management Information and Decision Sciences, Advanced persistent threats (apt): an awareness review, Journal of Management Information and Decision Sciences, vol. 21, no. 6, 2022.

Kagermann, H., Industrie 4.0: A global perspective, acatech—National Academy of Science and Engineering, 2016.

Kagermann, H., Lukas, W.D. and Wahlster, W., Industrie 4.0: Mit dem Internet der Dinge auf dem Weg zur 4. industriellen Revolution, VDI Nachrichten, 2011.

Kagermann, H., Ten Years of Industrie 4.0, Sci, vol. 4, no. 3, p. 26, 2022.

Kazancoglu, Y. and Ozkan-Ozen, Y.D., Analyzing workforce 4.0 in the fourth industrial revolution and proposing a road map from operations management perspective with fuzzy DEMATEL, Journal of Enterprise Information Management, vol. 31, no. 6, pp. 891–907, 2018.

Langner, R., Stuxnet: Dissecting a cyberwarfare weapon, IEEE Security & Privacy, vol. 9, no. 3, pp. 49-51, 2011.

MDPI, Advanced persistent threats (APTs): A systematic review of literature, MDPI, 2023.
MDPI, Stuxnet and centrifuge speeds, MDPI, 2021.
Nakajima, S., Introduction to TPM: Total Productive Maintenance, Productivity Press, 1988.
Norrman, A. and Jansson, U., Ericsson's proactive supply chain risk management approach after a serious sub-supplier accident, International Journal of Physical Distribution & Logistics Management, vol. 34, no. 5, pp. 434–456, 2004.
NSTAC, NSTAC Report on IT/OT Convergence, Cybersecurity and Infrastructure Security Agency (CISA), 2020.
ResearchGate, A Comprehensive Survey on Advanced Persistent Threat (APT) Detection Techniques, ResearchGate, 2025.
ResearchGate, A threat model method for ICS malware: the TRISIS case, ResearchGate, 2020.
ResearchGate, The Impact of IT/OT Convergence on Digital Transformation in Manufacturing, ResearchGate, 2023.
Sakib, M.S., et al., Development of Low-cost Automated Guided Vehicle (AGV) to Step towards Industry 4.0, Proceedings of the 5th International Conference on Industrial & Mechanical Engineering and Operations Management, Dhaka, Bangladesh, 2022.
Sinha, A. and Roy, B., Reviewing Cyber-Physical System as a Part of Smart Factory in Industry 4.0, Proceedings of the 2020 IEEE International Conference for Convergence in Engineering (ICCE), 2020.
Sodhi, M.S., Son, B.G. and Koc, C.P., Researchers' Perspectives on Supply Chain Risk Management, Production and Operations Management, vol. 21, no. 1, pp. 1-13, 2012.
Taleb, H., et al., Strategically-Motivated Advanced Persistent Threat: Definition, Process, Tactics, and a Disinformation Model of Counterattack, ResearchGate, 2024.
Tao, F. and Zhang, M., Digital Twin Shop-Floor: A New Framework for Smart Manufacturing, IEEE Access, vol. 5, pp. 20419-20428, 2017.
The Economist, A worm in the centrifuge, The Economist, 2010.
Tuptuk, N. and Hailes, S., Security of Smart Manufacturing Systems, Journal of Manufacturing Systems, vol. 47, pp. 93-106, 2018.
Wan, J., et al., Cyber-Physical Systems and IoT as Key Enabling Technologies for Industry 4.0, IEEE Transactions on Industrial Informatics, vol. 15, no. 2, pp. 913-920, 2019.
Wudhikarn, R., Overall equipment effectiveness (OEE): a review and development of an integrated improvement framework, International Journal of Productivity and Quality Management, vol. 27, no. 3, pp. 308-333, 2019.
Xiong, W., et al., Threat modeling language for enterprise IT integrating MITRE ATT&CK, arXiv, 2502.10825v1, 2022.
Zarreh, A., Wan, H., Lee, Y., Al Janahi, R. and Saygin, C., Cybersecurity Concerns for Total Productive Maintenance in Smart

Biographies

Mr. Md Anisuzzaman is the Head of Cloud Operations at MeghnaCloud (BDCCL), bringing over 20 years of experience in IT project management and architecture. He specializes in leading complex cloud and infrastructure projects, and in his current role, he architects Opensource-based private cloud environments, drives cloud strategy, and leads cross-functional teams across Cloud, NOC, SOC, and DevOps. Prior to joining MeghnaCloud, he spent over 12 years at GETCO Telecommunications Limited, where he served as Head of IT & Billing, managing telecom BSS infrastructure and large-scale billing implementations. His earlier career included roles as an Application Development Manager for International Turnkey Systems (ITS) in Lagos, Nigeria. Mr. Anisuzzaman holds a BSc in Computer Science from East West University, is completing an MSc in Cyber Security from World University of Bangladesh, and holds professional certifications, including the Six Sigma (DMAIC) Black Belt, Red Hat Virtualization, OCA Cloud Infra, GCP Cloud Certification, and ITIL® Foundation.

Ovejite Saha is a Network Engineer specializing in network design, cybersecurity, and industrial network systems. He holds a Master's degree in Cyber Security from the World University of Bangladesh, a Bachelor of Science in Computer Science and Engineering from Sonargaon University, and a Diploma in Environmental Engineering from Sherpur Polytechnic Institute. He has extensive professional experience at Nextech Limited and the Public Works Department (PWD), MIS Division-2, where he designed and deployed scalable LAN/WAN infrastructures supporting over 800 endpoints. His work included configuring Cisco and Fortinet devices, implementing VPNs and network access controls, and monitoring network performance using tools such as SolarWinds, PRTG, and Wireshark. As a System Support Engineer at Nextech Limited, he optimized network performance, migrated legacy systems to modern infrastructure, and ensured high network availability. His research interests focus on networking and industrial

network systems, with expertise in routing protocols, VLANs, firewalls, VPNs, and security mechanisms. He holds certifications in IT Support, Mikrotik Networking, and Faronics Expertise. Driven by a commitment to secure and resilient network infrastructures, Mr. Saha aspires to advance as a Network and Security Administrator, contributing to reliable and high-performance industrial networks.

Mr. Musfique-us-Salehin Arnob is a Graduate Assistant in the Department of Computer Science and Engineering at the World University of Bangladesh. He specializes in the intersection of artificial intelligence, information systems, and cybersecurity with particular expertise in deep learning–based vulnerability detection and AI-driven security automation. In his current role, Mr. Arnob contributes to academic and research coordination, supervises undergraduate projects, assists in course accreditation processes, and mentors students in AI and cybersecurity research. He played an active role in guiding student research teams showcased at the BTRC Telecom & Digital Innovation Fair 2025 by supporting project development, documentation and technical presentations. Mr. Arnob completed his Bachelor of Science in Computer Science and Engineering at the World University of Bangladesh, where his undergraduate thesis, “Identifying and Detecting Backdoor Attack using Deep Neural Network,” achieved over 99% accuracy in detecting malicious URLs and backdoor vulnerabilities using NLP and LSTM models. His research interests include Natural Language Processing (NLP), Large Language Models (LLMs), Machine Learning, Program Analysis, and Secure Software Systems, with an academic vision to advance AI-enabled, autonomous, and privacy-preserving cybersecurity solutions.