D7077E IoT/OT Security
LTU

Individual assignment 2

Title/assignment,
Conceptualization of a secure OT environment architecture for a car parts manufacturing industry

Stefanos Ntentopoulos, stente-5@student.ltu.se / s.ntentopoulos@gmail.com, +306946573480

Date, 2025-Dec-16
Resubmission Date, 2026-Jan-10

Introduction

The automotive manufacturing sector, like other sectors, is facing many cybersecurity challenges as global supply chains become digitized. The car parts manufacturers depend on operational technology (OT) systems for production management, traceability and just-in-time logistics operations. So, while OT systems require high availability to support 24/7 production cycles, they simultaneously face evolving cyber threats that can disrupt manufacturing processes, compromise product integrity, and threaten supply chain continuity. Understanding how to architect secure OT environments that fulfill both the operational and the security requirements is a serious challenge for both the manufacturing organizations and the IT personnel.

One of the challenges is the convergence of Information Technology (IT) and Operational Technology (OT) within modern manufacturing environments. In the past, OT systems were operating in isolated, air-gapped networks with minimal external connectivity [1]. This isolation provided security through obscurity, but the emergence of Industry 4.0, of IoT devices, and the demand for production visibility, predictive maintenance, and integrated supply chain management have lifted these systems from obscurity and created a need for new security approaches.

Contemporary OT security research emphasizes defense-in-depth using the Purdue Enterprise Reference Architecture (PERA) with layered network segmentation [1]. Emerging zero-trust principles mandate continuous authentication and microsegmentation [5], [6], while IEC 62443 standards provide compliance frameworks [7]. These approaches must balance security with operational constraints, encryption cannot compromise real-time control loops, and redundancy must enable continuous manufacturing [4], [8].

OT security is very different from IT security. Rather than implementing the CIA (Confidentiality-Integrity-Availability) triad, the OT environment requires an AIC (Availability-Integrity-Confidentiality) prioritization since manufacturing process interruption causes immediate losses, data tampering and corruption threatens product safety, while information disclosure can create competitive damage [1], [4]. These facts drive the architectural decisions: physical security controls like guarded entrances and surveillance systems [1], [3] to prevent unauthorized equipment access, SIEM systems and IDS/IPS technologies enabling real-time threat detection [1], [4], [6], [7], backup and restore mechanisms and VPN remote access controls for data protection and recovery [1], [3], [5], [6], data exchange gateways to enforce control between OT and external networks [1], [6], availability measures to ensure at least partial operation during failures [1], [2], [4] and formal Incident Response Plans (IRP) and Disaster Recovery Plans (DRP) establish resilience procedures [1], [2], [3], [4], [7].

This assignment conceptualizes a secure OT environment architecture for a car parts manufacturer which is designed to have three independent production lines. Traceability of manufactured parts must be preserved throughout product lifecycles. The current physical security infrastructure forces us to build our digital security upon it. Moreover, the operational demands of the company make it operate 24/7, leaving only a 00-06 maintenance window provides the only scheduled period for system updates and security patches every night, and not allowing any extended downtime. With these constraints in mind, we must design an OT architecture that will protect manufacturing processes against cyber threats, while maintaining operational responsiveness to just-in-time supply chain demands.

Conceptualization of a secure OT environment architecture for a car parts manufacturing industry

These constraints force us to reconsider and deviate from traditional information technology security priorities. Rather than implementing the CIA (Confidentiality-Integrity-Availability) model. The Availability requirement represents the primary security concern since manufacturing interruption causes immediate operational losses. The second priority should be the Integrity requirement, since data loss or corruption threatens product safety and regulatory compliance. Finally, the Confidentiality requirement has the lowest priority. Although we should protect information like proprietary manufacturing parameters which if exposed to competitors, could undermine the competitive advantage, which will create just secondary damage. [1],[4].

The above-mentioned security architecture and security goals could be achieved with the following:

Layered Network Segmentation: According to the Purdue Enterprise Reference Architecture (PERA) model, which divides the OT environment into layers with restricted data flows between them [1]. As a result the breach of one layer does not automatically compromise others, reducing lateral movement risk.

Zero-Trust Principles: By following the zero-trust security framework we continuously authenticate and verify every access point [5], [6]. Microsegmentation restricts access to only necessary resources, minimizing the blast radius of compromised credentials.

Physical Security Controls: Guarded entrances (RFID gates, CCTV, security personnel) & personnel verification prevent unauthorized access to equipment [1], [3]. Physical access control is important since attackers can bypass digital security through direct equipment manipulation.

SIEM and Real-Time Monitoring: Security Information and Event Management systems aggregate and analyze logs from all sources, enabling detection of anomalous patterns [1], [4], [6], [7]. Real-time detection because rapid response can prevent an attack from spreading.

Intrusion Detection and Prevention (IDS/IPS): Network-based IDS/IPS systems can identify suspicious traffic and block malicious connections in real-time [1], [5], [6], [7]. These systems are essential since production systems cannot tolerate extended downtime to perform detailed incident investigation.

Backup and Disaster Recovery: Up to date and multiple backups maintain redundant copies of critical data, enabling system recovery following successful attacks or failures [1], [3], [4], [7]. They also support both Availability (enabling failover) and Integrity (preserving traceability data).

Secure Remote Access: Virtual Private Networks enable authorized access from external locations while enforcing encryption and access restrictions [1], [5], [6]. In this design, VPN access is restricted to the 00-06 maintenance window.

Data Exchange Gateways: Enable selective data sharing with supply chain partners while preventing unauthorized access to production systems.

Availability Measure: Equipment redundancy like independent production lines, network path redundancy, and failover mechanisms enable continued operation during component failures or security incidents [1], [2], [4]. In this design, the three independent production lines allow continuous but with reduced output operation if one line is compromised or offline.

Incident Response Planning (IRP) and Disaster Recovery Planning (DRP): Formal procedures for threat detection, containment, and remediation establish clear guidelines and communication protocols [1], [2], [3]. Incident response planning enables organizations to detect and respond to active attacks before they propagate. Recovery procedures, backup activation sequences, and business continuity objectives ensure rapid restoration of critical systems following catastrophic failures [1], [3], [4], [7]. DRP is essential in just-in-time manufacturing where extended downtime creates cascading impacts across supply chains.

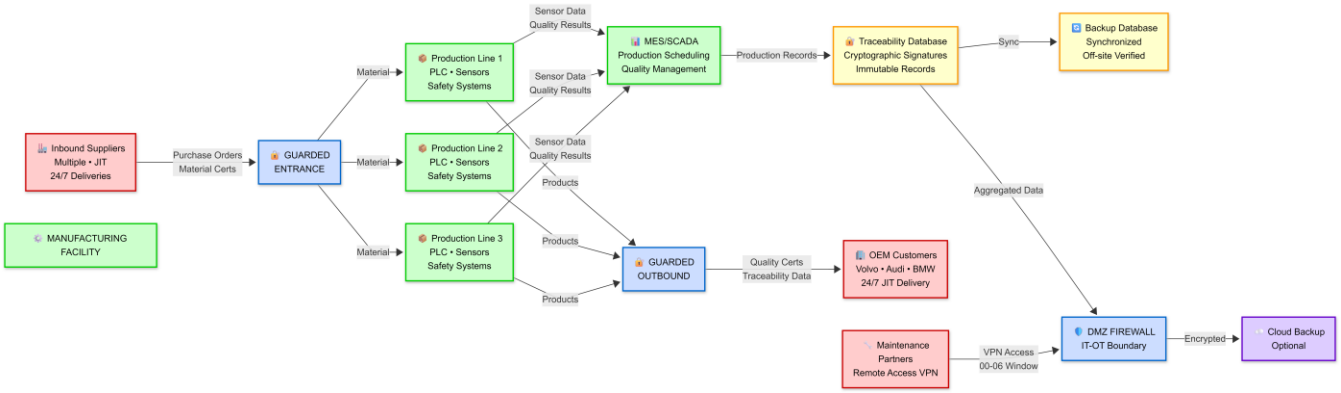

Figure 1 – Overview of value chain for car parts manufacturing

The above diagram illustrates the external ecosystem encompassing the car parts manufacturer. Inbound suppliers deliver components through 24/7 just-in-time logistics, passing through guarded entrances with physical security controls (RFID gates, CCTV, security personnel). The manufacturing facility as we mentioned contains three independent production lines,

each with programmable logic controllers (PLCs), sensors, and safety systems. Production data flows to the Manufacturing Execution System (MES), Supervisory Control and Data Acquisition (SCADA) systems and traceability database, where all manufacturing records are cryptographically signed and maintained immutably. A synchronized backup database provides redundancy for disaster recovery [1].

Manufactured components exit through guarded outbound entrances with quality certificates and traceability records, flowing to OEM customers (Volvo, Audi, BMW) operating 24/7 just-in-time delivery. The diagram shows data flows from production lines (sensor data, quality results) to MES/SCADA coordination systems, and from traceability databases to external partners. An IT-OT boundary (demilitarized zone) enforces firewall policies separating operational systems from business systems, with limited data export containing only aggregated, encrypted information [1], [6].

External connections include maintenance partners accessing the facility through VPN during the 00-06 maintenance window, and optional cloud backup services for traceability database copies. The value chain visualization emphasizes security at ecosystem boundaries, data sensitivity levels distinguish critical integrity-sensitive information (production parameters, traceability records) from confidential business information (delivery schedules, customer identity). This structure establishes the external security perimeter and identifies critical data flows that internal architecture must protect [1].

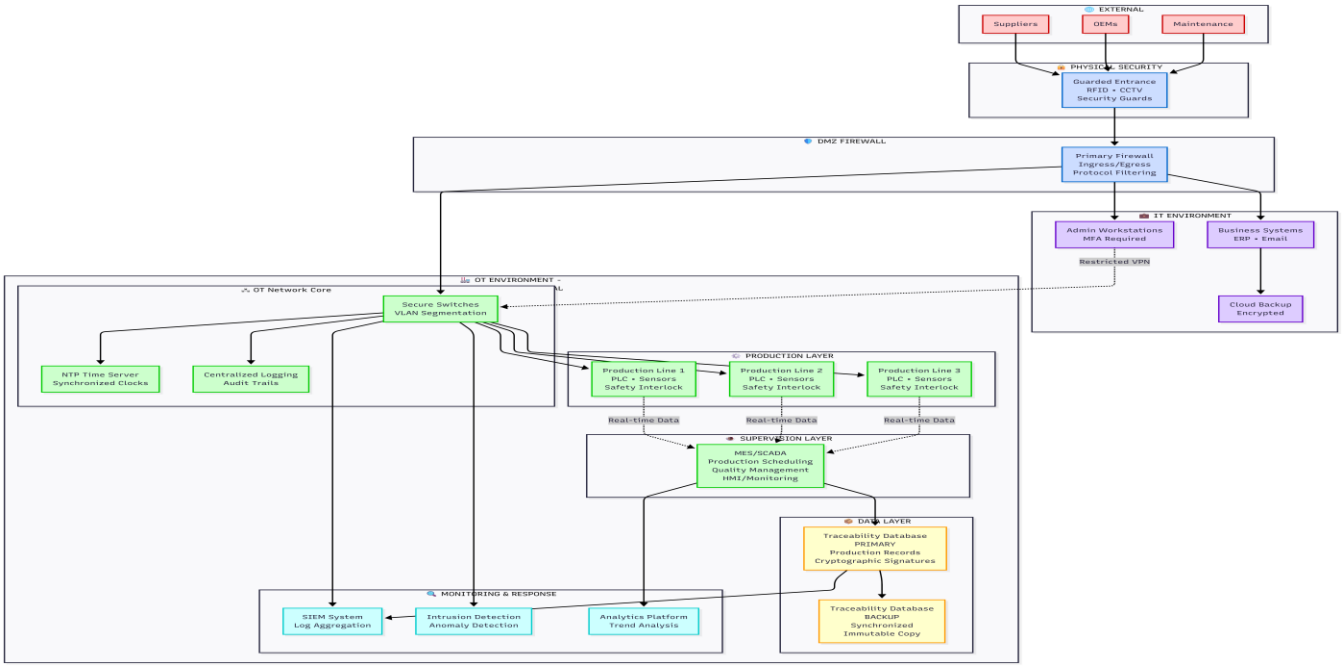

Figure 2 – Detailed secure OT environment architecture with IT environment for a car parts manufacturing company

The above diagram presents the OT environment architecture implementing the Purdue Enterprise Reference Architecture (PERA) model with four functional layers. Layer 1 (Production Layer) contains three independent production lines, each with PLC, sensors, actuators, and safety interlocks. Layer 2 (OT Network Core) manages network infrastructure, secure switches with VLAN segmentation, NTP time servers for synchronized clocks, and centralized logging for audit trails. Layer 3 (Supervision) integrates MES/SCADA systems for production scheduling, quality management, and real-time monitoring. Layer 4 (Data Layer) maintains primary traceability database with cryptographic signatures and a synchronized backup database for redundancy [1], [2].

The IT-OT boundary is enforced through a demilitarized zone (DMZ) firewall with strict ingress/egress rules, and protocol filtering. The IT environment contains business systems, administrative workstations, and cloud backup connectivity through

encrypted channels. Inbound connections from maintenance service partners (MSPs) route through VPN, restricted to the 00-06 maintenance window. One-way data flows from OT to IT carry only aggregated, non-sensitive information [1], [5], [6].

Monitoring and incident response infrastructure includes SIEM systems aggregating logs, intrusion detection identifying anomalies in real-time, and analytics platforms for trend analysis. This defense-in-depth approach combines network segmentation, access control, encryption, and monitoring to address AIC requirements, redundant databases support Availability through failover and degradation, cryptographic signatures and audit logging protect Integrity, network isolation and access control maintain Confidentiality without compromising real-time operations [1], [5], [6], [7].

Analysis of strengths and weaknesses of the proposed conceptualization

The strength of the proposed security architecture are the following: We enable practical redundancy through the three independent production lines which enable 66% operation when one line is compromised, providing operational flexibility and redundancy. The PERA-based layered segmentation, monitoring infrastructure, DMZ boundary, and IEC 62443 alignment collectively achieve defense-in-depth protection while respecting manufacturing's 00-06 maintenance and other constraints. And the various compensating controls which are enabled allow the legacy equipment vulnerabilities to be addressed through network isolation rather than relying solely on patch management, acknowledging the legacy manufacturing equipment that possibly exist.

However, weaknesses exist. The operational complexity of the proposed security architecture introduces many specialization requirements like the need for cybersecurity - IT personnel that specializes in OT security and misconfiguration risks, which cannot be avoided if we want to achieve defense in depth. There is also some trade-offs due to the design, since the maintenance window limits the rapid incident response during production hours, the detailed and continuous monitoring can generate false-positive alerts causing fatigue to the personnel and the encryption adds latency to the real-time operations. Finally, in the case of network-wide compromises or against attacks from sophisticated nation-state actors exploiting zero-days, all three production lines may be affected, and as a result the just-in-time supply chains will create out of ordinary recovery time pressures.

Summary and conclusions

In the earlier sections we analyzed why the OT security requires AIC prioritization, instead of the traditional CIA model, driving availability-centric design. The conceptualization of the proposed architecture achieves a strong protection against realistic threats, while we acknowledge that there are trade-offs that cannot be eliminated, such as maintenance windows restrict incident response timing, segmentation introduces latency, monitoring generates alert fatigue and maybe more.

Moreover, through this assignment we understand that OT security architecture must be context-specific, since generic IT frameworks prove inadequate for operational requirements. Also, our approach is transferable to other OT sectors (power, oil/gas, pharma) while requiring sector-specific adaptations.

In conclusion, effective OT security is pragmatic and realistic security. It succeeds by aligning availability protection with business objectives, not by pursuing security ideals that conflict with them. Also, to implement effective OT security, we have to understand operational context deeply, identify realistic threat profiles, prioritize by business impact, and manage trade-offs transparently rather than denying they exist.

References

[1] Raich, R., Raich, A. and Kinhekar, N. (2025) Securing the Convergence of IT and OT Networks in Cyber Physical System: Policy, Architecture and Implementation Challenges. Proceedings of the International Conference on Cyber Security for Critical Infrastructures (KEIS), 2025.

[2] Oudina, Z., Derdour, M., Dib, A. and Aouidate, A. M. (2025) Model Based System Engineering for Trust SCADA and ICS Systems in Oil & Gas Industry. Proceedings of the IEEE Conference on Systems Engineering, 2025.

[3] Alladi, T., Chamola, V. and Zeadally, S. (2020) Industrial Control Systems Cyberattack Trends and Countermeasures. IEEE Access, Vol. 8, pp. 183897-183937.

[4] Mesbah, M., Elsayed, M. S., Jurcut, A. D. and Azer, M. (2023) Analysis of ICS and SCADA Systems Attacks Using Honeypots. Proceedings of the 23rd International Conference on Enterprise Information Systems (ICEIS), pp. 580-589.

[5] Bukhari, T. T., Oladimeji, O., Etim, E. D. and Ajayi, J. O. (2019) Toward Zero-Trust Networking: A Holistic Paradigm Shift for Enterprise Security in Digital Transformation Landscapes. IEEE Access, Vol. 7, pp. 186745-186765.

[6] Ravi, C. S., Shaik, M., Saini, V., Chitta, S. and Bonam, V. S. M. (2025) Beyond the Firewall: Implementing Zero Trust with Network Microsegmentation. IEEE Security & Privacy, Vol. 23, No. 2, pp. 45-54.

[7] Leander, B., Čaušević, A. and Hansson, H. (2019) Applicability of the IEC 62443 Standard in Industry 4.0/IIoT. Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES), Canterbury, United Kingdom, 26-29 August 2019, pp. 1-8.

[8] Maidl, M., Kröselberg, D., Christ, J. and Beckers, K. (2018) A Comprehensive Framework for Security in Engineering Projects - Based on IEC 62443. Proceedings of the IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW), Memphis, USA, October 2018, pp. 1-8.

[9] Bandur, V., Selim, G., Pantelic, V. and Lawford, M. (2021) Making the Case for Centralized Automotive EE Architectures. IEEE Transactions on Industrial Informatics, Vol. 17, No. 9, pp. 6234-6251.

[10] Ma, Y., Lu, C., Sinopoli, B. and Zeng, S. (2020) Exploring Edge Computing for Multitier Industrial Control. Proceedings of the IEEE/ACM Symposium on Edge Computing (SEC), San Jose, USA, November 2020, pp. 88-101.

[11] Labaran, M. J. and Masood, T. (2023) Industry 4.0 Driven Green Supply Chain Management in Renewable Energy Sector: A Critical Systematic Literature Review. Journal of Cleaner Production, Vol. 391, pp. 136148.