# **Cybersecurity Threat Model Report: Exxon Mobil Process Control Terminal Server**

## **1. Executive Summary**

### **1.1. Purpose of the Report**

This report presents a comprehensive cybersecurity threat model for Exxon Mobil's Process Control Terminal Server (PCTS), a critical component enabling access to process control networks (PCN) and systems within processing facilities. Given the increasing sophistication and frequency of cyber threats targeting industrial control systems (ICS), particularly within the energy sector, a proactive and structured approach to understanding and mitigating these risks is paramount.1 This threat model aims to provide Exxon Mobil with a detailed assessment of the PCTS's cybersecurity posture, potential vulnerabilities, and likely threat actors.

### **1.2. Scope of the Assessment**

The scope of this assessment encompasses the Exxon Mobil PCTS, assumed to be deployed at various processing facilities. It includes the server's hardware, software (including operating systems and applications), network interfaces connecting to both corporate and process control networks, and any embedded components within the server itself. The analysis leverages the MITRE ATT&CK® framework for ICS 3, the EMB3D™ Threat Model for embedded systems 5, and findings from Open Source Intelligence (OSINT) gathering.7 Methodologies are further detailed in Section 3.

### **1.3. Key Findings**

The assessment identifies significant cybersecurity risks associated with the PCTS, stemming from its critical role as a gateway to sensitive process control environments. Key findings include:

* **High Target Value:** The PCTS represents a high-value target for adversaries (including nation-state actors, cybercriminals, and hacktivists) seeking to disrupt operations, steal sensitive process information, or cause physical damage.1
* **Multiple Attack Vectors:** Potential attack vectors include exploitation of public-facing interfaces (if present), compromised remote access credentials, phishing attacks targeting personnel with PCTS access, and vulnerabilities within the server's software or embedded components.3
* **ICS-Specific Threats:** The PCTS is susceptible to ICS-specific attack techniques aimed at inhibiting response functions, impairing process control, or causing denial of service, potentially leading to operational shutdowns or unsafe conditions.4
* **Embedded System Vulnerabilities:** Embedded components within the PCTS (e.g., network interface cards, management controllers) may possess unique vulnerabilities related to firmware, hardware interfaces, or insecure configurations, requiring specific analysis using models like EMB3D.5
* **Impact of IT/OT Convergence:** The connection of the PCTS between IT and OT networks creates a critical boundary that, if breached, could allow threats to propagate from the less-secure IT environment into the highly sensitive OT environment.11

Detailed threat analysis can be found in Sections 5, 6, and 7.

### **1.4. Recommendations**

Based on the identified threats and vulnerabilities, this report recommends a multi-layered, defense-in-depth security strategy aligned with industry best practices and standards such as IEC 62443.16 Key recommendations include:

* **Secure Network Architecture:** Implement robust network segmentation between IT and OT environments, utilizing firewalls and demilitarized zones (DMZs) to strictly control traffic to and from the PCTS.3
* **Access Control:** Enforce strong authentication (multi-factor authentication where possible) and the principle of least privilege for all access to the PCTS.18
* **Vulnerability Management:** Establish a rigorous patch management program for the PCTS operating system, applications, and firmware. Conduct regular vulnerability scanning and penetration testing.1
* **Monitoring and Detection:** Deploy security monitoring tools (e.g., SIEM, EDR, Network Detection and Response) capable of detecting anomalous behavior and known ICS attack techniques within the PCTS environment and its network connections.18
* **Secure Configuration:** Harden the PCTS configuration by disabling unnecessary services and ports, implementing secure protocols, and adhering to secure development practices if custom software is involved.16
* **Incident Response:** Develop and regularly test an incident response plan specifically addressing potential compromises of the PCTS and the PCN.18
* **Supply Chain Security:** Integrate IEC 62443 supplier requirements into procurement processes for PCTS hardware and software.17

Detailed recommendations are presented in Section 8. Implementing these measures will significantly enhance the cybersecurity resilience of Exxon Mobil's PCTS and the critical process control networks they protect.

## **2. Introduction**

### **2.1. Background on Exxon Mobil's Process Control Terminal Server (PCTS)**

Exxon Mobil operates complex processing facilities globally, relying heavily on Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems to manage and monitor critical operations safely and efficiently. The Process Control Terminal Server (PCTS) functions as a crucial gateway or access point, typically situated at each facility, mediating connections between the corporate Information Technology (IT) network and the isolated Process Control Network (PCN) or Operational Technology (OT) environment. Its primary role involves authenticating users and facilitating secure remote access for authorized personnel (e.g., engineers, maintenance staff) to monitor, manage, and maintain the control systems governing physical processes. This controlled access is vital for operational efficiency but also positions the PCTS as a critical security boundary.

### **2.2. Importance of Cybersecurity**

The cybersecurity of ICS, particularly within the oil and gas sector, is of paramount importance due to the potential for catastrophic consequences resulting from a compromise. Attacks targeting these systems can lead to operational disruptions, production losses, environmental damage, theft of proprietary process information, and, most critically, risks to human safety.1 The increasing connectivity of ICS environments, driven by IT/OT convergence for enhanced data analysis and remote operations, expands the attack surface and exposes previously isolated systems to a wider range of cyber threats.14 Protecting critical infrastructure components like the PCTS is therefore not merely an IT issue but a fundamental aspect of operational risk management and regulatory compliance. Failure to adequately secure these systems can result in significant financial penalties, reputational damage, and legal liabilities.

### **2.3. Report Objectives**

The primary objective of this report is to provide Exxon Mobil with a comprehensive cybersecurity threat model specifically focused on the PCTS. This involves:

1. **Identifying Potential Threats:** Analyzing the threat landscape relevant to ICS in the oil and gas sector, including known threat actors and their Tactics, Techniques, and Procedures (TTPs).1
2. **Analyzing Vulnerabilities:** Assessing potential weaknesses in the PCTS architecture, software, hardware, configuration, and embedded components.
3. **Mapping Threats to Frameworks:** Applying the MITRE ATT&CK® framework for ICS 3 and the EMB3D™ Threat Model 6 to systematically categorize potential adversary actions and device-specific vulnerabilities relevant to the PCTS.
4. **Utilizing OSINT:** Incorporating findings from Open Source Intelligence (OSINT) regarding real-world incidents, attack trends, and vulnerabilities affecting similar systems or industries.26
5. **Developing Actionable Recommendations:** Proposing specific, prioritized mitigation strategies and security controls, aligned with industry standards like IEC 62443 22, to enhance the security posture of the PCTS.

This report aims to be accurate, detailed, and actionable, equipping Exxon Mobil's security and operational teams with the insights needed to make informed decisions regarding risk mitigation for this critical asset.

## **3. Methodology**

### **3.1. MITRE ATT&CK® Framework for ICS**

The MITRE ATT&CK® (Adversarial Tactics, Techniques, and Common Knowledge) framework provides a globally recognized knowledge base of adversary tactics and techniques based on real-world observations.21 The specialized ATT&CK framework for Industrial Control Systems (ICS) focuses specifically on the actions adversaries may take while operating within an ICS or OT network, with the goal of disrupting industrial processes.3 It organizes adversary behavior into tactics (the adversary's technical goals, e.g., Initial Access, Execution, Impair Process Control) and techniques (how those goals are achieved, e.g., Exploit Public-Facing Application, Modify Control Logic).21 This framework was utilized to systematically map potential adversary TTPs against the PCTS across the entire attack lifecycle, from initial reconnaissance and access attempts to final impact on the process control environment.3 This structured approach helps anticipate attacker maneuvers and identify relevant defensive measures.21 The ICS matrix differs from the Enterprise matrix by including tactics specific to industrial environments, such as "Inhibit Response Function" and "Impair Process Control".4

### **3.2. EMB3D™ Threat Model**

Recognizing that the PCTS likely contains embedded system components (e.g., network interface controllers, baseboard management controllers, specialized hardware modules), the MITRE EMB3D™ Threat Model was employed.5 EMB3D is specifically designed for identifying threats against embedded devices found in critical infrastructure, IoT, automotive, and other sectors.25 It provides a curated knowledge base linking known cyber threats to specific device features/properties (hardware, firmware, software, networking protocols) and proposes corresponding mitigations.5 The methodology involves:

1. **Device Properties Enumeration:** Identifying key hardware and software characteristics of the PCTS's potential embedded components that could expose vulnerabilities.6
2. **Threat Mapping:** Linking identified device properties to specific threats cataloged within the EMB3D knowledge base.5
3. **Vulnerability Enumeration & Mitigation:** Identifying potential threat exposures based on device features and leveraging EMB3D's proposed mitigation strategies, categorized by implementation difficulty (Foundational, Intermediate, Leading), to inform security recommendations.6 This approach complements the ATT&CK framework by providing a deeper focus on the unique security challenges of embedded hardware and firmware within the PCTS.34

### **3.3. OSINT Gathering**

Open Source Intelligence (OSINT) techniques were used to gather publicly available information on cyber threats, vulnerabilities, threat actors, and incidents relevant to ICS, SCADA systems, terminal servers, and the oil and gas industry. Sources included:

* Government cybersecurity agencies (e.g., CISA ICS Advisories, alerts).7
* Security vendor reports and threat intelligence blogs.1
* Academic research papers and security conference proceedings.38
* News articles and incident databases detailing attacks on critical infrastructure.23
* Standards bodies and industry consortiums (e.g., ISA, NERC).8 This information provided context on the current threat landscape, common TTPs used in real-world attacks against similar targets, prevalent vulnerabilities, and the motivations and capabilities of relevant threat actors (nation-states, cybercriminals, hacktivists).1

### **3.4. Threat Modeling Process**

The threat modeling process involved the following steps:

1. **System Decomposition:** Defining the PCTS, its components, interfaces, and operational context based on the user query and general knowledge of such systems.
2. **Threat Identification:** Using OSINT findings and the ATT&CK for ICS framework to identify relevant threat actors and potential TTPs applicable to the PCTS. Applying EMB3D to identify threats specific to embedded components.
3. **Vulnerability Analysis:** Analyzing the PCTS architecture and assumed components for potential weaknesses that could be exploited by the identified threats.
4. **Attack Path Mapping:** Mapping potential sequences of TTPs (attack paths) using the ATT&CK for ICS framework, illustrating how an adversary might progress from initial access to impact.
5. **Risk Assessment (Qualitative):** Prioritizing threats based on estimated likelihood (considering actor capability/intent and vulnerability exploitability) and potential impact (considering operational disruption, safety, financial loss).
6. **Mitigation Identification:** Recommending security controls and countermeasures based on the ATT&CK mitigations, EMB3D mitigations, IEC 62443 requirements, and general cybersecurity best practices.

### **3.5. Assumptions and Limitations**

This assessment is based on the following assumptions and limitations:

* **Limited Specific Data:** Detailed architectural diagrams, specific hardware/software bills of materials, network configurations, and existing security controls for Exxon Mobil's PCTS were not provided. The analysis relies on generalized models of typical terminal servers used in process control environments.
* **OSINT Reliance:** The threat landscape analysis is based on publicly available information, which may not capture all relevant threats or actor capabilities, particularly highly classified or covert activities.24
* **Dynamic Threat Landscape:** Cybersecurity threats and vulnerabilities evolve rapidly. This report represents a snapshot in time based on information available up to the date of publication. Continuous monitoring and reassessment are necessary.
* **Focus:** The primary focus is on cyber threats; physical security threats are considered only as potential vectors for cyber attacks (e.g., physical access enabling malware insertion).
* **Framework Scope:** While comprehensive, ATT&CK for ICS and EMB3D may not encompass every conceivable threat or vulnerability, particularly novel or zero-day exploits.10

## **4. Exxon Mobil Process Control Terminal Server (PCTS) System Overview**

*(Note: Due to the lack of specific information on Exxon Mobil's PCTS, this section describes a typical architecture and operational context for such a system within a processing facility, based on general ICS principles and the provided snippets. Assumptions made here should be validated against Exxon Mobil's actual implementation.)*

### **4.1. System Architecture**

A Process Control Terminal Server (PCTS) typically acts as a secure gateway or jump host, managing access between the enterprise IT network and the critical OT/PCN environment within a processing facility. Its architecture is designed to enforce security policies and isolate the sensitive control network.

* **4.1.1. Operations Control Center (OCC) / Enterprise Network Interface:** The PCTS connects to the broader corporate IT network, potentially accessible from an Operations Control Center (OCC) or other centralized management locations.41 This interface handles user authentication, often integrating with corporate directory services (e.g., Active Directory). Communication on this side typically uses standard IT protocols (e.g., RDP, SSH, HTTPS) over Ethernet. Software functions within the OCC might include monitoring, data acquisition (SCADA), and Human-Machine Interfaces (HMI) for visualizing processes.43
* **4.1.2. Process Control Network (PCN) Interface:** The PCTS possesses a separate, strictly controlled interface to the PCN/OT network. This network hosts critical control system components like PLCs, RTUs, DCS controllers, HMIs, and engineering workstations.1 Traffic passing through this interface is usually heavily restricted by firewall rules, allowing only specific protocols and connections necessary for authorized control system access and monitoring.
* **4.1.3. PCTS Server Components:** The server itself likely runs a hardened operating system (e.g., Windows Server, Linux) and hosts specific applications for managing remote sessions, enforcing access policies, and potentially logging user activity. It contains standard server hardware (CPU, RAM, storage) and potentially embedded components like Baseboard Management Controllers (BMCs) or specialized network interface cards that could be subject to EMB3D analysis.6 It may host or interact with SCADA/HMI software elements.43
* **4.1.4. Communication Networks:** The PCTS bridges two distinct network environments:
  + **IT Network:** Standard corporate Ethernet, TCP/IP based.
  + **OT/PCN Network:** Often utilizes Ethernet but may employ specific industrial protocols (e.g., Modbus/TCP, DNP3, PROFINET, EtherNet/IP) alongside TCP/IP. Strict segmentation, often via firewalls and potentially a DMZ, is crucial between these networks.10 Wireless communication might be used in parts of the broader facility but access via the PCTS to the core PCN is typically wired.

### **4.2. Operational Roles and Access Levels**

Access to and through the PCTS is typically restricted based on operational roles and responsibilities, adhering to the principle of least privilege.

* **4.2.1. Control System Engineers/Administrators:** Require privileged access through the PCTS to configure, program, troubleshoot, and maintain PLCs, DCS, SCADA/HMI systems, and other PCN components. They often have the highest level of access within the OT environment facilitated by the PCTS.
* **4.2.2. Maintenance Technicians:** May require access for diagnostics, calibration, and maintenance tasks on specific equipment connected to the PCN. Their access might be more restricted than engineers, limited to specific devices or functions.
* **4.2.3. Operators (OCC/Local):** Primarily interact with HMI/SCADA systems, often through dedicated operator consoles rather than directly via the PCTS. However, some supervisory or specialized operator roles might require limited PCTS access for specific tasks or monitoring functions.41
* **4.2.4. IT Administrators:** Responsible for managing the PCTS server itself (OS patching, user accounts linked to corporate directories, backups, network configuration on the IT side). Their access should ideally be limited to the server administration and not extend into the PCN unless explicitly required and authorized.
* **4.2.5. Third-Party Vendors/Contractors:** May require temporary, strictly controlled remote access via the PCTS for specialized support or maintenance of specific systems. This access poses a significant risk if not managed securely.11
* **4.2.6. External Stakeholders (Limited):** Depending on the facility and data sharing policies, certain external stakeholders (e.g., regulatory bodies, specific partners) might have highly restricted, view-only access to specific data aggregated from the PCN, potentially accessed via systems connected through, but segregated from, the PCTS pathway.45 Direct access to the PCN via the PCTS for external stakeholders is generally prohibited.

### **4.3. Potential Operational Disruptions (Cybersecurity Context)**

A compromise of the PCTS can lead to severe operational disruptions by enabling unauthorized access to the PCN.

* **4.3.1. Unauthorized Access and Control:** Attackers gaining access through the PCTS could potentially manipulate control logic, alter setpoints, issue unauthorized commands, or shut down processes, leading to production loss, equipment damage, or unsafe conditions.10
* **4.3.2. Malware Propagation:** The PCTS could serve as an entry point for malware (including ransomware) to spread from the IT network into the OT network, potentially crippling control systems and demanding ransom for recovery.10
* **4.3.3. Denial of Service (DoS):** An attack targeting the PCTS itself could render it unavailable, preventing authorized personnel from accessing the PCN for legitimate monitoring, control, or emergency response actions.11 Attacks could also target PCN components *through* the PCTS.
* **4.3.4. Data Theft/Espionage:** Adversaries could use access gained via the PCTS to steal sensitive process information, operational data, intellectual property, or network configurations for reconnaissance supporting future attacks.9
* **4.3.5. Loss of View/Control:** Manipulation of data flowing through the PCTS or compromise of HMI/SCADA systems accessed via it could blind operators or provide false information, leading to incorrect operational decisions.12

## **5. Threat Landscape Analysis**

### **5.1. Overview of Oil & Gas / ICS Threats**

The Industrial Control Systems (ICS) within the oil and gas sector, including components like the PCTS, face a diverse and escalating range of cyber threats. These systems are attractive targets due to their criticality and the potential for significant disruption or damage.1 Common threats include:

* **5.1.1. Ransomware Attacks:** Ransomware targeting OT environments is a growing concern. Attacks can encrypt critical systems like HMIs, engineering workstations, or even controllers accessed via the PCTS, disrupting operations and demanding payment.9 Some groups also exfiltrate data for double extortion.40
* **5.1.2. Data Breaches:** Theft of sensitive operational data, process formulas, intellectual property, or network configurations via compromised systems like the PCTS is a significant risk, often perpetrated by nation-state actors for espionage or cybercriminals for competitive advantage.10
* **5.1.3. Denial of Service (DoS/DDoS) Attacks:** Attacks aimed at overwhelming the PCTS, connected control systems, or communication networks can prevent legitimate access and disrupt operations.11 This can be achieved through network flooding or by exploiting vulnerabilities to crash devices.11
* **5.1.4. Supply Chain Attacks:** Compromising software or hardware components of the PCTS or related systems during manufacturing or distribution, or attacking third-party vendors with remote access, provides a stealthy way for attackers to gain initial access.1
* **5.1.5. Insider Threats:** Malicious or unintentional actions by employees or contractors with legitimate access to or through the PCTS can lead to sabotage, data theft, or the introduction of malware.10
* **5.1.6. Malware (Wipers, Trojans):** Custom or commodity malware designed to specifically target ICS protocols and devices (like Stuxnet, Industroyer, TRITON, PIPEDREAM/INCONTROLLER) can be introduced via the PCTS to manipulate or destroy control system functionality.1

### **5.2. Emerging Threat Actors**

Several types of threat actors actively target ICS environments, including those in the oil and gas sector:

* **5.2.1. Nation-State Actors:** Often sponsored by governments, these advanced persistent threat (APT) groups possess significant resources and expertise. Their motivations include espionage, sabotage, and positioning for future disruptive attacks on critical infrastructure. Groups like VOLTZITE (linked to Volt Typhoon/PRC), KAMACITE (Russia-linked), ELECTRUM (Russia-linked), XENOTIME (linked to TRITON/Russia), Dragonfly/Allanite (Russia-linked), and Earth Estries (China-linked) have demonstrated capabilities and intent to target energy and other critical sectors.1 They often use custom malware and focus on long-term persistence.9
* **5.2.2. Cybercriminals:** Primarily motivated by financial gain, these groups increasingly target ICS/OT environments with ransomware, seeing critical operations as high-pressure targets likely to pay ransoms.2 They often exploit known vulnerabilities, weak remote access, and phishing.9
* **5.2.3. Hacktivists:** Motivated by political or social agendas, hacktivist groups may target oil and gas companies for disruptive attacks (e.g., DoS, website defacement) to make a statement. While often less sophisticated than nation-states, some groups have shown increasing capability to impact OT systems, sometimes blurring the lines with state-sponsored operations.2

### **5.3. OSINT Analysis**

OSINT reveals numerous incidents and trends relevant to securing the PCTS:

* **5.3.1. Case Studies:**
  + **TRITON/TRISIS (2017):** Targeted Schneider Electric Triconex safety systems (SIS) in a Saudi petrochemical facility, aiming to disable safety functions. While accidentally triggering a shutdown, it demonstrated the potential for attacks causing physical consequences.1 This highlights the risk of attacks moving *through* access points like a PCTS to critical safety controllers.
  + **Industroyer (2016):** Used ICS-specific protocols (IEC-104) to cause a power outage in Ukraine, demonstrating tailored OT malware capabilities.2
  + **Colonial Pipeline (2021):** While primarily impacting IT systems, this ransomware attack forced the shutdown of major fuel pipelines due to concerns about the potential impact on OT billing and operational systems, showcasing the interdependence and risk introduced by IT/OT connections often mediated by servers like the PCTS.
  + **Attacks on Water Utilities (2023-2024):** Hacktivist groups and potentially state-linked actors (e.g., Cyber Av3ngers linked to Iran IRGC) targeted water facilities in the US, exploiting default passwords and vulnerabilities in HMIs and PLCs, demonstrating the risk of targeting basic security hygiene failures in critical infrastructure.9
  + **Transportation Sector Incidents:** Attacks on Network Rail (UK, 2024 - Wi-Fi compromise), Transport for London (2024 - data breach, service disruption), Port of Seattle (2024 - ransomware impacting airport/seaport), and various freight/logistics companies highlight the vulnerability of interconnected transportation and logistics infrastructure, often involving similar IT/OT integration points as a PCTS.23
* **5.3.2. Common TTPs:** OSINT confirms attackers frequently use:
  + Exploitation of known vulnerabilities in internet-facing systems or VPNs.19
  + Spear phishing to gain initial access credentials.3
  + Use of legitimate credentials (default or stolen) for access and lateral movement.12
  + Leveraging Living-off-the-Land Binaries (LOLBins) like WMIC, PowerShell, PsExec to blend in.37
  + Deployment of web shells for persistence on compromised servers.49
  + Network scanning and reconnaissance within the OT network.12
  + Use of open-source or commercially available tools (Metasploit, Mimikatz) alongside custom malware.1
* **5.3.3. Vulnerability Trends:** A significant number of vulnerabilities continue to be discovered in ICS products, with many allowing remote code execution or denial of service.1 Patching remains a major challenge in OT environments due to uptime requirements.1 Vulnerabilities in remote access solutions, web interfaces, and underlying operating systems are common exploitation points.10 CISA regularly publishes advisories on specific ICS vulnerabilities.7

## **6. MITRE ATT&CK® Mapping for Exxon Mobil PCTS**

This section maps potential adversary Tactics, Techniques, and Procedures (TTPs) from the MITRE ATT&CK for ICS framework to the Exxon Mobil PCTS, illustrating potential attack paths.

### **6.1. Specialized Applications and Protocols**

The PCTS environment involves standard IT protocols (HTTPS, RDP, SSH) on the corporate side and potentially specialized ICS protocols (Modbus/TCP, DNP3, OPC UA, vendor-specific protocols) on the PCN side. Adversaries may target vulnerabilities in the implementations of these protocols on the PCTS or use them for command and control or data exfiltration once access is gained.19 The applications hosted on the PCTS for session management, authentication, and potentially HMI/SCADA access also present specific attack surfaces.

### **6.2. Mapping TTPs to PCTS (Illustrative Examples)**

*(Note: This is not exhaustive but provides examples across the attack lifecycle)*

* **6.2.1. Initial Access (TA0102):** Gaining entry to the PCTS or the network segment it resides on.
  + **T0849 Exploit Public-Facing Application:** If any PCTS management interface or related service is exposed externally, exploiting vulnerabilities.12
  + **T0856 External Remote Services:** Compromising legitimate VPN or remote desktop accounts used to access the PCTS from the IT network.3
  + **T0858 Spearphishing Attachment/Link:** Targeting personnel (IT admins, engineers) with access to the PCTS to install malware or steal credentials.3
  + **T0861 Drive-by Compromise:** Compromising a website frequently visited by personnel who access the PCTS.
* **6.2.2. Execution (TA0103):** Running malicious code on the PCTS.
  + **T0860 Command-Line Interface:** Using shell access gained via initial access to run commands, scripts, or malware.12
  + **T0867 Native API:** Using operating system APIs on the PCTS for malicious purposes.12
  + **T0869 Service Execution:** Running malware as a service on the PCTS server.
* **6.2.3. Persistence (TA0104):** Maintaining access to the PCTS.
  + **T0872 Modify Program:** Altering legitimate software on the PCTS (e.g., remote access tools) to include backdoors.12
  + **T0876 Valid Accounts:** Using stolen legitimate credentials (local or domain) to maintain access.1
  + **T0874 Create Account:** Creating new local or domain accounts for persistent access.
  + **T0873 Module Firmware:** (Advanced) Modifying firmware of embedded components (e.g., BMC, NIC) on the PCTS.12
* **6.2.4. Privilege Escalation (TA0105):** Gaining higher privileges on the PCTS.
  + **T0877 Exploitation for Privilege Escalation:** Exploiting OS or application vulnerabilities on the PCTS to gain administrator/root access.12
  + **T0878 Hooking:** Intercepting function calls of privileged processes.12
* **6.2.5. Evasion (TA0106):** Avoiding detection.
  + **T0879 Indicator Removal on Host:** Clearing logs, deleting malware files from the PCTS.12
  + **T0881 Masquerading:** Naming malicious processes or files similarly to legitimate ones on the PCTS.
  + **T0862 Change Operating Mode:** (If applicable to PCTS functions) Placing the server or its services in a diagnostic or less monitored state.12
* **6.2.6. Discovery (TA0107):** Learning about the PCTS and connected networks.
  + **T0884 Network Connection Enumeration:** Identifying active connections to/from the PCTS, especially into the PCN.12
  + **T0886 Remote System Discovery:** Scanning the IT and PCN networks reachable from the PCTS.12
  + **T0887 Network Service Scanning:** Identifying open ports and services on the PCTS and reachable PCN devices.
  + **T0885 Network Sniffing:** Capturing traffic passing through the PCTS to analyze protocols or steal credentials.12
* **6.2.7. Lateral Movement (TA0108):** Moving from the PCTS into the PCN.
  + **T0889 Default Credentials:** Using default passwords for ICS devices discovered on the PCN.12
  + **T0851 Exploitation of Remote Services:** Exploiting vulnerabilities on engineering workstations or HMIs within the PCN reachable from the PCTS.12
  + **T0854 Remote Services:** Using legitimate protocols like RDP or vendor-specific tools, authenticated via the PCTS, to access PCN systems.12
  + **T0890 Program Upload:** Uploading malicious logic or configuration to PLCs/controllers via engineering software accessed through the PCTS.
* **6.2.8. Collection (TA0109):** Gathering data from the PCTS or PCN.
  + **T0892 Adversary-in-the-Middle:** Intercepting communications passing through the PCTS between IT and OT.12
  + **T0897 I/O Image:** Collecting process state data from controllers accessed via the PCTS.12
  + **T0901 Screen Capture:** Capturing screens of operator sessions running through the PCTS.12
  + **T0898 Data from Information Repositories:** Accessing logs, configuration files, or operational databases stored on or accessible from the PCTS.
* **6.2.9. Command and Control (TA0110):** Communicating with compromised systems.
  + **T0902 Commonly Used Port:** Using standard ports (e.g., 80, 443) for C2 traffic from the PCTS to evade simple firewall rules.12
  + **T0904 Standard Application Layer Protocol:** Tunneling C2 traffic over legitimate protocols allowed through the PCTS (e.g., HTTPS, RDP channels).12
  + **T0903 Connection Proxy:** Using the compromised PCTS to relay C2 traffic to/from systems within the PCN.12
* **6.2.10. Inhibit Response Function (TA0111):** Preventing safety or operational responses. (Actions executed *through* the PCTS against PCN devices)
  + **T0906 Alarm Suppression:** Modifying HMI/SCADA configurations via the PCTS to hide critical alarms from operators.12
  + **T0907 Block Command Message:** Preventing legitimate operator commands initiated through the PCTS from reaching controllers.12
  + **T0911 Data Destruction:** Deleting logs or configurations on PCN devices needed for diagnostics or recovery, accessed via the PCTS.12
* **6.2.11. Impair Process Control (TA0112):** Manipulating the industrial process. (Actions executed *through* the PCTS against PCN devices)
  + **T0918 Modify Parameter:** Changing critical setpoints or operational parameters in controllers accessed via the PCTS.12
  + **T0919 Unauthorized Command Message:** Sending malicious commands (e.g., stop process, open valve) to controllers via the PCTS.12
  + **T0915 Modify Control Logic:** Altering PLC or DCS logic via engineering software accessed through the PCTS.
* **6.2.12. Impact (TA0113):** The ultimate goal of the attack.
  + **T0921 Denial of Control:** Preventing operators from controlling the process via systems accessed through the PCTS.12
  + **T0922 Denial of View:** Manipulating HMI displays accessed via the PCTS to show false information.
  + **T0929 Manipulation of Control:** Causing undesired physical actions or process states by manipulating controllers through the PCTS.12
  + **T0927 Loss of Safety:** Compromising safety instrumented systems (if accessible via PCTS pathways) or manipulating controls into unsafe states.12

### **6.3. Prioritized Threats**

Based on likelihood and potential impact, the following threat scenarios involving the PCTS are prioritized:

1. **Ransomware Propagation (High Likelihood, High Impact):** Exploiting vulnerabilities or using stolen credentials to gain access to the PCTS, then using it as a pivot point to deploy ransomware onto critical PCN assets like HMIs and engineering workstations. This is driven by the increasing prevalence of ransomware targeting OT 9 and the potential for significant operational disruption.
2. **Unauthorized Remote Access & Manipulation (Medium Likelihood, Critical Impact):** Nation-state or sophisticated criminal actors compromising PCTS access (via phishing, vulnerability exploitation, or vendor compromise) to gain persistent access to the PCN for espionage or to directly manipulate control parameters, potentially causing process disruption or unsafe conditions.1
3. **Denial of Service against PCTS/PCN (Medium Likelihood, High Impact):** Hacktivists or criminals launching DoS attacks against the PCTS itself or critical PCN components accessible through it, preventing legitimate access and potentially halting operations.11
4. **Insider Threat (Medium Likelihood, High Impact):** A disgruntled employee or compromised contractor using legitimate PCTS access to intentionally disrupt operations, steal data, or introduce malware.10

## **7. EMB3D™ Threat Model Application**

Applying the EMB3D™ framework provides a focused analysis of potential vulnerabilities within the embedded components likely present in the PCTS hardware.

### **7.1. Embedded System Vulnerabilities**

While the exact hardware is unknown, a typical server acting as a PCTS might contain embedded systems such as:

* **7.1.1. Baseboard Management Controller (BMC):** Provides out-of-band management capabilities (remote power cycling, hardware monitoring, console access). BMCs often run their own firmware and have network interfaces, presenting a distinct attack surface vulnerable to firmware manipulation, default credentials, or network protocol exploits.
* **7.1.2. Network Interface Controllers (NICs):** Modern NICs can have complex firmware and processing capabilities (e.g., TCP offload). Vulnerabilities in NIC firmware or drivers could potentially be exploited for persistence, evasion, or direct memory access attacks.
* **7.1.3. Trusted Platform Module (TPM):** While a security feature, vulnerabilities in TPM implementation or firmware could undermine secure boot or key storage functions.16
* **7.1.4. Specialized Hardware/Cards:** Depending on the PCTS role, it might include specialized communication cards for industrial protocols or security functions, each with its own embedded software/firmware.

These components are vulnerable due to factors like infrequent firmware updates, potential use of default credentials, lack of secure coding practices in firmware development, and physical access possibilities if server security is breached.5

### **7.2. Mapping EMB3D to PCTS (Illustrative Examples)**

Using the EMB3D structure 6:

* **7.2.1. Device Properties:**
  + **Hardware -> Management Controller (BMC):** Property: Network-accessible management interface. Property: Dedicated firmware.
  + **Hardware -> Network Interface Card:** Property: Firmware execution capability. Property: Direct Memory Access (DMA).
  + **Networking -> Network Protocols:** Property: Implementation of specific protocols (e.g., IPMI for BMC, TCP/IP for NICs).
  + **System Software -> Firmware:** Property: Update mechanism (or lack thereof). Property: Secure Boot capability.
* **7.2.2. Vulnerability Enumeration (Mapping Properties to Threats):**
  + *(BMC)* Network-accessible interface + Default Credentials -> **TID-401: Unauthorized Access to Networked Components**.6 Allows attacker remote control over server hardware functions.
  + *(BMC/NIC)* Firmware + Lack of Secure Update -> **TID-301: Injection of Malicious Code** 6 / **TID-302: Firmware Modification**. Enables persistent rootkit-like malware below the main OS. Threat Maturity: Often requires physical access or prior OS compromise, but exploits exist.25
  + *(Hardware)* Physical Access Ports (e.g., JTAG, UART on motherboard if accessible) -> **TID-105: Physical Tampering**.6 Allows direct firmware extraction/modification or hardware manipulation if physical security fails.
  + *(System Software)* Lack of Secure Boot Implementation -> **TID-301: Injection of Malicious Code**.6 Allows booting a compromised OS or pre-boot malware.
* **7.2.3. Mitigation Strategies (Based on EMB3D Mitigations** 6**):**
  + **MID-001: Secure Boot:** Ensure Secure Boot is enabled and properly configured for the PCTS OS and potentially firmware components (Foundational).6
  + **MID-016: Strong Authentication and Authorization:** Change default BMC passwords, use strong unique passwords, restrict network access to BMC interfaces (Foundational).6
  + **MID-034: Software Updates and Patch Management:** Regularly update server firmware (BIOS/UEFI, BMC, NICs) from trusted vendor sources (Foundational).6 This is often overlooked but critical for embedded components.
  + **MID-010: Network Segmentation:** Isolate BMC management networks from production IT and OT networks (Foundational).6
  + **MID-069: Physically Protect Circuit Board Traces and Chip Pins:** Ensure adequate physical security for the PCTS server hardware to prevent tampering (Foundational).33
  + **MID-040: Intrusion Detection and Prevention Systems (IDPS):** Monitor network traffic to/from management interfaces (e.g., BMC) for anomalous activity (Intermediate).6

Applying EMB3D highlights the need to consider the security of the underlying hardware and firmware of the PCTS, not just the operating system and applications. These embedded components can offer stealthy persistence mechanisms for advanced attackers.25

## **8. Security Recommendations for Exxon Mobil PCTS**

Based on the threat analysis using MITRE ATT&CK for ICS, EMB3D, OSINT, and considering the principles of IEC 62443, the following security recommendations are provided to enhance the cybersecurity posture of Exxon Mobil's Process Control Terminal Servers.

### **8.1. Design-Phase Security (for new deployments or upgrades)**

* **8.1.1. Secure Development Practices (IEC 62443-4-1):** If any custom software is developed for or deployed on the PCTS, adhere to secure software development lifecycle practices. For procured components, require suppliers to demonstrate conformance with IEC 62443-4-1.17 This includes threat modeling during design, secure coding practices, vulnerability testing, and secure update mechanisms.
* **8.1.2. Threat Modeling Integration:** Integrate threat modeling (using frameworks like ATT&CK for ICS and EMB3D) early in the design and procurement process for PCTS solutions to proactively identify and mitigate potential risks.5
* **8.1.3. Secure Configuration Baselines (IEC 62443-3-3 SR 3.1):** Develop hardened configuration baselines for the PCTS operating system, applications, and firmware. This includes disabling unnecessary services/ports, enforcing strong passwords, configuring audit logs, and implementing security features like Secure Boot.16 Ensure suppliers provide components capable of meeting these baseline requirements (IEC 62443-4-2).29

### **8.2. Operational Security (Continuous Measures)**

* **8.2.1. Access Controls (IEC 62443-3-3 FR 1, FR 2):**
  + Implement Role-Based Access Control (RBAC) based on the principle of least privilege for all users accessing the PCTS.16
  + Enforce strong, unique passwords for all accounts (local, domain, service).18
  + Mandate Multi-Factor Authentication (MFA) for all remote access to the PCTS from the IT network.
  + Implement strict controls and monitoring for third-party vendor access.11
  + Regularly review and audit access privileges.
* **8.2.2. Network Segmentation (IEC 62443-3-3 FR 5):**
  + Maintain strict network segmentation between the IT network, a DMZ (if applicable), the PCTS, and the PCN using firewalls.10
  + Configure firewall rules to deny all traffic by default and explicitly allow only necessary protocols, ports, and sources/destinations for PCTS communication.18
  + Isolate management interfaces (e.g., BMC) onto separate, secured networks.13
* **8.2.3. Intrusion Detection and Prevention (IEC 62443-3-3 FR 6):**
  + Deploy Network Intrusion Detection/Prevention Systems (NIDS/NIPS) capable of understanding ICS protocols on network segments connected to the PCTS.
  + Utilize Endpoint Detection and Response (EDR) or similar host-based monitoring on the PCTS server itself.21
  + Aggregate and analyze logs from the PCTS, firewalls, and relevant PCN systems in a Security Information and Event Management (SIEM) system, correlating events with ATT&CK for ICS TTPs.18
  + Monitor for anomalous behavior and known indicators of compromise (IoCs).3
* **8.2.4. Data Protection (IEC 62443-3-3 FR 4):**
  + Encrypt sensitive data at rest (e.g., configuration backups) and in transit (e.g., using TLS/SSH for remote sessions) where feasible and supported.
  + Implement measures to prevent unauthorized data exfiltration from the PCTS.
* **8.2.5. Incident Response (IEC 62443-3-3 FR 6):**
  + Develop, maintain, and regularly test an Incident Response (IR) plan specifically addressing scenarios involving PCTS compromise and potential impact on the PCN.18
  + Ensure capabilities for forensic analysis and system recovery are in place.
* **8.2.6. Supply Chain Security (IEC 62443-2-4):**
  + Establish and enforce cybersecurity requirements for suppliers of PCTS hardware, software, and support services, referencing IEC 62443-2-4 and 4-1.17
  + Validate the integrity of software and firmware updates before deployment.
* **8.2.7. Secure Remote Access:**
  + Utilize secure, encrypted protocols (e.g., SSH, HTTPS-based portals, properly configured RDP gateways) for all remote access.
  + Implement jump hosts within a DMZ; avoid direct remote access from IT to the PCTS if possible.
  + Strictly control and monitor all remote access sessions.10
* **8.2.8. Vulnerability and Patch Management (IEC 62443-2-3):**
  + Establish a timely process for identifying, assessing, and mitigating vulnerabilities affecting the PCTS OS, applications, and firmware, considering operational constraints.1
  + Test patches in a non-production environment before deploying to operational PCTS units.

### **8.3. Specific Mitigation Strategies**

* **8.3.1. Addressing Ransomware:** Implement robust endpoint protection (EDR, application allow-listing) on the PCTS, maintain offline backups, ensure strict network segmentation to limit lateral movement from IT, and disable unnecessary file sharing protocols.10
* **8.3.2. Protecting Data:** Enforce strict access controls, encrypt sensitive data stores, monitor for unusual data access or transfer patterns, and implement Data Loss Prevention (DLP) controls where applicable.18
* **8.3.3. Mitigating DDoS Attacks:** Implement rate limiting and traffic filtering on network ingress points, work with upstream network providers for DDoS mitigation services, and ensure PCTS resources are adequately provisioned.23
* **8.3.4. Securing Wireless Communications:** If any wireless is used for management or connectivity related to the PCTS (e.g., BMC access, though generally discouraged), ensure strong encryption (WPA2/WPA3 Enterprise), robust authentication, and network isolation.

Implementing these recommendations provides practical benefits by reducing the attack surface, increasing the difficulty for adversaries to compromise the PCTS, enhancing detection capabilities, and limiting the potential impact of a successful attack, thereby safeguarding Exxon Mobil's critical process control operations.

## **9. Conclusion**

### **9.1. Summary of Key Findings**

This threat model assessment concludes that the Exxon Mobil Process Control Terminal Server (PCTS) is a critical infrastructure component facing significant and evolving cybersecurity risks. Its position as a gateway between IT and OT networks makes it a prime target for diverse threat actors, including nation-states and cybercriminals, seeking to disrupt operations, steal data, or cause physical impact.1 Key vulnerabilities stem from potential weaknesses in software, firmware, configuration, network architecture, and the inherent risks associated with remote access and IT/OT convergence.10 The application of MITRE ATT&CK for ICS and EMB3D frameworks revealed numerous potential attack paths, from initial access via phishing or exploited vulnerabilities to lateral movement into the PCN and subsequent manipulation or disruption of control processes.6

### **9.2. Importance of Proactive Security**

The findings underscore the critical importance of adopting a proactive, defense-in-depth security posture for the PCTS and the broader ICS environment. Relying solely on reactive measures is insufficient given the potential speed and impact of modern cyber attacks, particularly those targeting critical infrastructure.2 Continuous monitoring, regular vulnerability management, robust access controls, and adherence to secure design principles are essential to maintaining operational resilience and safety.10 Integrating security considerations throughout the lifecycle of the PCTS, from procurement and design to operation and maintenance, is crucial.17

### **9.3. Call to Action**

Exxon Mobil is strongly encouraged to review the findings and recommendations presented in this report and take decisive action to implement the proposed mitigation strategies. Prioritizing measures such as strengthening network segmentation, enforcing multi-factor authentication, implementing robust monitoring and detection capabilities aligned with ATT&CK for ICS, managing vulnerabilities proactively, and adhering to the principles outlined in the IEC 62443 standard series will significantly enhance the security of the PCTS.10 Continuous investment in cybersecurity capabilities, regular training for personnel, and fostering a strong security culture are vital to staying ahead of the evolving threat landscape and ensuring the continued safe and reliable operation of Exxon Mobil's processing facilities.

## **10. Appendix**

### **10.1. Glossary of Terms**

* **APT (Advanced Persistent Threat):** A sophisticated, often state-sponsored, threat actor that gains unauthorized access to a network and remains undetected for an extended period.9
* **ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge):** A MITRE-developed knowledge base and framework for describing adversary actions and behaviors.21
* **BMC (Baseboard Management Controller):** An embedded microcontroller in servers used for remote monitoring and management, independent of the main CPU and OS.
* **CISA (Cybersecurity and Infrastructure Security Agency):** A U.S. federal agency responsible for cybersecurity and infrastructure protection.7
* **DCS (Distributed Control System):** A control system for a process or plant, wherein control elements are distributed throughout the system.20
* **DMZ (Demilitarized Zone):** A perimeter network segment separating an organization's internal network (e.g., IT or OT) from an external network (e.g., the internet or another corporate zone).
* **DoS (Denial of Service):** An attack intended to shut down a machine or network, making it inaccessible to its intended users.10
* **EDR (Endpoint Detection and Response):** Security solutions that continuously monitor end-user devices to detect and respond to cyber threats.21
* **EMB3D:** A MITRE threat model specifically for embedded devices.5
* **HMI (Human-Machine Interface):** A user interface or dashboard that connects a person to a machine, system, or device.43
* **IACS (Industrial Automation and Control System):** General term encompassing ICS, SCADA, DCS, etc., used in standards like IEC 62443.17
* **ICS (Industrial Control System):** General term covering various control systems and associated instrumentation used for industrial process control.10
* **IEC 62443:** An international series of standards for the security of industrial automation and control systems (IACS).16
* **IoC (Indicator of Compromise):** Forensic data identifying potentially malicious activity on a system or network.30
* **IT (Information Technology):** The use of computers, storage, networking, and other physical devices, infrastructure, and processes to create, process, store, secure, and exchange electronic data.
* **NIC (Network Interface Controller):** Hardware component connecting a computer to a computer network.
* **OSINT (Open Source Intelligence):** Intelligence collected from publicly available sources.
* **OT (Operational Technology):** Hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes, and events in the enterprise.15
* **PCN (Process Control Network):** The network segment dedicated to controlling the industrial process, part of the OT environment.
* **PCTS (Process Control Terminal Server):** The subject of this report; a server managing access to the PCN.
* **PLC (Programmable Logic Controller):** An industrial computer adapted for the control of manufacturing processes or robotic devices.20
* **RCE (Remote Code Execution):** A vulnerability allowing an attacker to execute arbitrary commands or code on a target machine remotely.1
* **RTU (Remote Terminal Unit):** A microprocessor-controlled electronic device that interfaces objects in the physical world to a distributed control system or SCADA system.44
* **SCADA (Supervisory Control and Data Acquisition):** A system for remote monitoring and control operating with coded signals over communication channels.20
* **SIEM (Security Information and Event Management):** Software solutions that aggregate and analyze activity from many different resources across an entire IT infrastructure.21
* **SL (Security Level):** In IEC 62443, a measure of the required or achieved security robustness of a zone, conduit, system, or component.16
* **TTP (Tactics, Techniques, and Procedures):** The patterns of activities and methods associated with specific threat actors or groups.30
* **TPM (Trusted Platform Module):** A specialized chip on an endpoint device that stores RSA encryption keys specific to the host system for hardware authentication.
* **VPN (Virtual Private Network):** Creates a secure connection over a public network.
* **Zone/Conduit:** Concepts in IEC 62443 for segmenting an IACS based on common security requirements (zones) and the communication paths between them (conduits).16

### **10.2. MITRE ATT&CK Matrix for PCTS (High-Level Summary)**

*(A full, detailed matrix is extensive. This summarizes key applicable tactics and representative techniques discussed in Section 6.)*

| **Tactic (ICS)** | **Representative Techniques Targeting/Leveraging PCTS** |
| --- | --- |
| Initial Access (TA0102) | Exploit Public-Facing Application (T0849), External Remote Services (T0856), Spearphishing (T0858) |
| Execution (TA0103) | Command-Line Interface (T0860), Service Execution (T0869) |
| Persistence (TA0104) | Modify Program (T0872), Valid Accounts (T0876), Create Account (T0874) |
| Privilege Escalation (TA0105) | Exploitation for Privilege Escalation (T0877) |
| Evasion (TA0106) | Indicator Removal on Host (T0879), Masquerading (T0881) |
| Discovery (TA0107) | Network Connection Enumeration (T0884), Remote System Discovery (T0886), Network Sniffing (T0885) |
| Lateral Movement (TA0108) | Default Credentials (T0889), Exploitation of Remote Services (T0851), Remote Services (T0854), Program Upload (T0890) |
| Collection (TA0109) | Adversary-in-the-Middle (T0892), Screen Capture (T0901), Data from Information Repositories (T0898) |
| Command and Control (TA0110) | Commonly Used Port (T0902), Standard Application Layer Protocol (T0904), Connection Proxy (T0903) |
| Inhibit Response Function (TA0111) | (Via PCTS) Alarm Suppression (T0906), Block Command Message (T0907), Data Destruction (T0911) |
| Impair Process Control (TA0112) | (Via PCTS) Modify Parameter (T0918), Unauthorized Command Message (T0919), Modify Control Logic (T0915) |
| Impact (TA0113) | (Via PCTS) Denial of Control (T0921), Manipulation of Control (T0929), Loss of Safety (T0927) |

### **10.3. EMB3D Threat Model Details (Illustrative Examples for PCTS Embedded Components)**

*(Based on Section 7)*

| **Device Property (Example)** | **EMB3D Threat ID (Example)** | **Threat Description Summary** | **Mitigation ID (Example)** | **Mitigation Summary** | **Tier** |
| --- | --- | --- | --- | --- | --- |
| Hardware: Management Controller (BMC) | TID-401 | Unauthorized network access via management interface (e.g., using default credentials) | MID-016 | Strong Authentication and Authorization (change defaults, restrict access) | Foundational |
| System Software: Firmware (BMC/NIC) | TID-302 | Malicious modification of firmware for persistence or control | MID-001 | Secure Boot (verify firmware integrity) | Foundational |
| System Software: Firmware (BMC/NIC) | TID-302 | Malicious modification of firmware for persistence or control | MID-034 | Software Updates and Patch Management (apply vendor firmware updates) | Foundational |
| Hardware: Physical Access Ports | TID-105 | Physical tampering to extract data or modify hardware/firmware | MID-069 | Physically Protect Circuit Board Traces and Chip Pins (secure server chassis) | Foundational |
| Networking: Network Protocols (IPMI) | TID-401 | Exploiting vulnerabilities in management protocols | MID-010 | Network Segmentation (isolate management network) | Foundational |

### **10.4. OSINT Sources (General Categories)**

* CISA ICS Advisories & Alerts 7
* NIST Special Publications (SP 800 series) 8
* ICS-CERT / DHS Reports 8
* Security Vendor Threat Reports (e.g., Dragos, Claroty, Trend Micro, Mandiant, Forescout) 1
* Academic Cybersecurity Journals and Conference Proceedings (e.g., IEEE, ACM)
* Industry Standards Organizations (ISA, IEC, NERC) 8
* News Media Outlets covering Cybersecurity and Critical Infrastructure Incidents
* Public Vulnerability Databases (e.g., CVE, NVD)

## **Addendum A: References**

*(Note: This section would list full citations for all sources referenced by snippet IDs in a consistent format, e.g., APA, MLA, or IEEE. Due to the nature of the input, only snippet IDs are provided in the main text. A full reference list requires retrieving bibliographic details for each URL/source associated with the snippet IDs.)*

Example format (assuming APA style):

* 3 Exabeam. (n.d.). *MITRE ATT&CK for ICS: Tactics, Techniques, and Best Practices*. Retrieved from <https://www.exabeam.com/explainers/mitre-attck/mitre-attck-ics-tactics-techniques-and-best-practices/>
* 5 IriusRisk. (n.d.). *Elevating Embedded Device Security: The EMB3D™ Threat Modeling Framework*. Retrieved from <https://www.iriusrisk.com/resources-blog/elevating-embedded-device-security-mitre-emb3d>
* 16 Dell Technologies. (n.d.). *IEC 62443 Overview*. Dell Technologies Validated Design for Manufacturing Edge with Litmus Design Guide. Retrieved from <https://infohub.delltechnologies.com/it-it/l/dell-technologies-validated-design-for-manufacturing-edge-with-litmus-design-guide/iec-62443-overview-5/>
* 10 eSecurity Planet. (n.d.). *Industrial Control Systems (ICS) Cyber Security*. Retrieved from <https://www.esecurityplanet.com/cloud/industrial-control-systems-cyber-security/>
* ... (List all other snippet IDs with full citation details)...

## **Addendum B: Research Links**

*(This section organizes the URLs provided in the research snippets by category for easy reference.)*

**MITRE ATT&CK for ICS:**

* <https://www.exabeam.com/explainers/mitre-attck/mitre-attck-ics-tactics-techniques-and-best-practices/> 3
* <https://www.trellix.com/security-awareness/cybersecurity/what-is-mitre-attack-framework/> 21
* <https://industrialcyber.co/vulnerabilities/cisa-mitre-attck-for-ics-focuses-on-adversarial-tactics-techniques-disrupting-industrial-control-process/> 24
* <https://www.balbix.com/insights/what-is-the-mitre-attck-framework/> 31
* <https://www.picussecurity.com/mitre-attack-framework-beginners-guide> 30
* <https://www.nozominetworks.com/blog/your-guide-to-the-mitre-attack-framework-for-ics> 4
* <https://attack.mitre.org/matrices/ics/> 12

**EMB3D Threat Model:**

* <https://www.iriusrisk.com/resources-blog/elevating-embedded-device-security-mitre-emb3d> 5
* <https://industrialcyber.co/control-device-security/mitre-releases-enhanced-emb3d-threat-model-with-new-mitigations-isa-iec-62443-4-2-alignment/> 25
* <https://emb3d.mitre.org/> 6
* <https://asimily.com/blog/what-is-the-mitre-emb3d-framework/> 34
* <https://www.forescout.com/blog/securing-the-unseen-mitre-emb3d-framework-for-embedded-devices/> 13
* <https://emb3d.mitre.org/assets/EMB3D_Paper_09-23-24.pdf> 33
* <https://www.eenewseurope.com/en/cybersecurity-threat-model-for-embedded-devices/> 32

**IEC 62443 Standard:**

* <https://infohub.delltechnologies.com/it-it/l/dell-technologies-validated-design-for-manufacturing-edge-with-litmus-design-guide/iec-62443-overview-5/> 16
* <https://www.pilz.com/en-US/support/law-standards-norms/industrial-security-standards-iec-62443> 29
* <https://www.zscaler.com/zpedia/what-is-iec-62443> 51
* <https://www.upguard.com/blog/isa-62443-3-3-2013> 18
* <https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards> 17
* <https://gca.isa.org/blog/how-to-define-zones-and-conduits> 50
* <https://industrialcyber.co/features/the-essential-guide-to-the-iec-62443-industrial-cybersecurity-standards/> 22

**Automated Transit / General Transportation Systems (Contextual):**

* <https://www.vaia.com/en-us/explanations/architecture/urban-studies-in-architecture/automated-transport-systems/> 52
* <https://www.mhi.co.jp/technology/review/pdf/e572/e572030.pdf> 53
* <https://www.osti.gov/servlets/purl/1975541> 54
* <https://www.apta.com/wp-content/uploads/APTA-SS-CCS-WP-005-19.pdf> 55
* <https://highways.dot.gov/media/8556> 56
* <https://www.transit.dot.gov/sites/fta.dot.gov/files/docs/ftasesc.pdf> 57
* <http://dl1.wikitransport.ir/book/Automated_Transit_Planning_Operation_and_Applications_2017.pdf> 58
* <https://www.anritsu.com/en-us/test-measurement/solutions/automotive/v2x?tm_navigation=solution> 59
* <https://www.ettifos.com/post/dsrc-vs-cv2x> 60
* <https://www.keysight.com/blogs/en/inds/auto/2024/10/03/v2x-post> 61
* <https://www.iotforall.com/autonomous-vehicles-and-the-role-of-5g-cellular-technology> 62
* <https://www.repairerdrivennews.com/2024/12/11/fcc-adopts-final-rules-for-cellular-vehicle-to-everything-technology/> 63
* <https://resources.altium.com/p/designing-v2x-communication-wireless-protocols-and-standards> 64
* <https://www.continental-automotive.com/en/focus-topics/autonomous-mobility.html> 65
* <https://www.monolithicpower.com/en/learning/mpscholar/automotive-electronics/automotive-sensing-and-actuators/intro-to-automotive-sensors-actuators> 66
* <https://www.cambridgeconsultants.com/wp-content/uploads/2023/11/2022-AI-in-the-driving-seat-Whitepaper.pdf> 67
* <https://www.sintrones.com/application/understanding-vehicle-computer-system-key-components-and-how-it-works/> 68
* <https://www.transit.dot.gov/sites/fta.dot.gov/files/docs/research-innovation/118161/transit-bus-automation-project-transferability-automation-technologies-final-report-fta-report-no.pdf> 69
* <https://www.mdpi.com/2227-7080/11/5/117> 70
* <https://www.wsp.com/-/media/insights/us/bus-automation-whitepaper/bus-automation-whitepaper-wsp-2023.pdf> 71

**ICS/SCADA Cybersecurity Threats & Vulnerabilities:**

* <https://www.esecurityplanet.com/cloud/industrial-control-systems-cyber-security/> 10
* <https://www.balbix.com/insights/ots-and-ics-security-the-next-big-challenge/> 20
* <https://industrialcyber.co/expert/why-scada-and-dcs-face-different-cyber-threats/> 48
* <https://www.infosecinstitute.com/resources/scada-ics-security/ics-scada-threats-and-threat-actors/> 1
* <https://www.infosecinstitute.com/resources/scada-ics-security/biggest-threats-to-ics-scada-systems/> 11
* <https://claroty.com/blog/a-comprehensive-guide-to-scada-cybersecurity> 14
* <https://www.paloaltonetworks.com/cyberpedia/ot-vs-ics-vs-scada-security> 15

**OSINT Sources & Government Resources:**

* <https://www.cisa.gov/topics/industrial-control-systems> 7
* <https://www.cisa.gov/resources-tools/resources/free-cybersecurity-services-and-tools> 35
* <https://inl.gov/national-security/ics-cybersecurity-training/> 72
* <https://www.sans.org/blog/reflections-on-the-us-governments-oig-report-on-cisas-automated-indicator-sharing-program/> 73
* <https://icscsi.org/library/index.html> 8
* <https://www.cisa.gov/resources-tools/programs/ics-training-available-through-cisa> 36
* <https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-103a> 19

**OCC / SCADA HMI Functions:**

* <https://www.solutionspt.com/automation-and-control-scada-hmi> 43
* <https://www.tm-robot.com/en/scada-automation-systems/> 44
* <https://www.al-enterprise.com/en/blog/comms-heart-of-ops-control-ctr> 41
* <https://www.mta.info/document/161176> 74
* <https://www.systra.com/usa/project/scvta-scada-control-center-and-systems-replacement/> 75
* <https://www.isarsoft.com/knowledge-hub/occ> 42

**Cyber Attack Case Studies & Threat Actors:**

* <https://wisdiam.com/publications/recent-cyber-attacks-transport-logistics-sector/> 26
* <https://www.itarchiteks.com/8-recent-cyber-attacks-that-have-affected-the-transportation-industry> 39
* <https://ati.ua.edu/wp-content/uploads/2021/05/72.pdf> 27
* <https://dxc.com/us/en/insights/perspectives/paper/protecting-critical-rail-infrastructure-from-cyber-attacks> 23
* <https://darktrace.com/cyber-ai-glossary/cybersecurity-in-transportation> 40
* <https://www.researchgate.net/publication/344947562_Cyber-attacks_in_the_next-generation_cars_mitigation_techniques_anticipated_readiness_and_future_directions> 38
* <https://documents.trendmicro.com/assets/white_papers/wp-cyberattacks-against-intelligent-transportation-systems.pdf> 28
* <https://www.dragos.com/resources/press-release/dragos-reports-ot-ics-cyber-threats-escalate-amid-geopolitical-conflicts-and-increasing-ransomware-attacks/> 9
* <https://www.forescout.com/blog/since-stuxnet-a-brief-history-of-critical-infrastructure-attacks/> 2
* <https://industrialcyber.co/critical-infrastructure/uat-5918-apt-group-targets-taiwan-critical-infrastructure-possible-linkage-to-volt-typhoon/> 49
* <https://industrialcyber.co/ransomware/chinese-apt-group-earth-estries-targets-critical-infrastructure-sectors-with-advanced-cyber-attacks/> 37

**Operational Roles (Contextual):**

* <https://www.yardstick.team/job-description/public-transit-operations-manager> 45
* <https://careers.sf.gov/role/?id=3743990006670901> 76
* <https://www.nationalrtap.org/Toolkits/Transit-Managers-Toolkit/Operations-and-Planning/Planning-and-Evaluation> 46
* <https://ops.fhwa.dot.gov/tsmo/> 47
* <https://ftp.txdot.gov/pub/txdot-info/trf/tsmo/hou-tsmo-program-plan.pdf> 77
* <https://www.sanjoseca.gov/your-government/departments-offices/transportation/about/planning-and-project-delivery-job-duties> 78
* [https://www.riometro.org/DocumentCenter/View/244/American-Public-Transportation-Association-Transit-Board-Member-Handbook-PDF?bidId=](https://www.riometro.org/DocumentCenter/View/244/American-Public-Transportation-Association-Transit-Board-Member-Handbook-PDF?bidId) 79

## **Addendum C: Threat Analysis and Mitigation Strategies for Industrial Terminal Servers - A Case Study of the Exxon Mobil PCTS**

This addendum provides a focused analysis of cybersecurity threats and mitigation strategies specifically relevant to systems like the Exxon Mobil Process Control Terminal Server (PCTS), which act as critical gateways to Industrial Control System (ICS) environments. It integrates findings from the MITRE ATT&CK for ICS and EMB3D frameworks, emphasizing the unique challenges posed by specialized protocols and embedded components within such systems.

**Unique Challenges of PCTS Security:**

1. **Critical Chokepoint:** The PCTS inherently acts as a security chokepoint between the less trusted IT environment and the highly sensitive OT/PCN environment. Its compromise provides a direct pathway for attackers to reach critical control systems.11
2. **Protocol Bridging:** It must handle both standard IT protocols (RDP, SSH, HTTPS) and potentially specialized ICS protocols (OPC UA, Modbus, DNP3, etc.), increasing complexity and the potential attack surface related to protocol parsing and handling vulnerabilities.19
3. **IT/OT Convergence Risk:** The PCTS embodies the risks of IT/OT convergence. Vulnerabilities or compromises originating in the IT domain (e.g., phishing leading to credential theft, malware on IT workstations) can directly translate into threats against the OT domain via the PCTS.14
4. **Embedded Component Security:** Servers used as PCTS contain embedded components (BMCs, NICs, firmware) that have their own vulnerabilities and are often overlooked in standard IT patching cycles. These require specific attention using models like EMB3D.5
5. **Operational Constraints:** Like other OT assets, PCTS maintenance (patching, updates) may be constrained by operational requirements for high availability, making vulnerability management challenging.1

**Applying Frameworks for Deeper Analysis:**

* **MITRE ATT&CK for ICS:** Mapping TTPs (as detailed in Section 6) reveals likely attack paths:
  + *Initial Access:* Focus on compromising user credentials (phishing 3), exploiting remote access services 3, or vulnerabilities in any exposed PCTS interface.12
  + *Execution/Persistence:* Running malware/scripts on the PCTS OS, modifying configurations, or using valid accounts.12
  + *Discovery/Lateral Movement:* Using the PCTS to scan the PCN, identify targets (PLCs, HMIs), and move laterally using stolen credentials, default passwords, or exploiting vulnerabilities on PCN devices.12
  + *Impact:* Leveraging PCTS access to execute ICS-specific tactics like Modify Parameter (T0918), Unauthorized Command Message (T0919), or Alarm Suppression (T0906) against downstream control systems.12
* **EMB3D Threat Model:** Applying EMB3D to assumed PCTS embedded components (Section 7) highlights risks like:
  + Firmware manipulation (TID-302) for stealthy persistence.6
  + Unauthorized access via insecure management interfaces (TID-401) like BMCs.6
  + Exploitation of hardware-level vulnerabilities if physical access is gained (TID-105).6

**Multi-Layered Mitigation Strategy:**

A robust strategy requires layers of defense addressing people, processes, and technology, aligned with IEC 62443 principles:

1. **Network Architecture (IEC 62443 Zones & Conduits):**
   * Establish the PCTS within a well-defined DMZ between IT and OT zones.16
   * Utilize firewalls to strictly enforce communication conduit rules: Allow only necessary protocols (e.g., specific RDP/SSH ports from authorized IT subnets to PCTS, specific ICS protocols from PCTS to authorized PCN devices).18 Deny all else.
   * Isolate management networks (e.g., for BMCs) completely or via separate firewalls.
2. **Access Control (IEC 62443 FR 1 & 2):**
   * Enforce MFA for all IT-side access to the PCTS.18
   * Implement granular RBAC, ensuring users only have access to the specific PCN systems required for their role, facilitated *through* the PCTS.16
   * Use unique, strong passwords for all accounts, including service accounts and embedded component defaults (BMC).18
   * Implement session time-outs and monitoring.
3. **System Hardening (IEC 62443-3-3, 4-2):**
   * Apply hardened OS and application configuration baselines.16 Disable unused services/ports.
   * Enable and configure Secure Boot.6
   * Implement application allow-listing on the PCTS to prevent unauthorized software execution.
4. **Vulnerability Management (IEC 62443-2-3):**
   * Regularly patch the PCTS OS, applications, AND firmware (BIOS, BMC, NICs) based on risk assessment and vendor guidance.22
   * Conduct regular vulnerability scanning (authenticated scans preferred for the PCTS itself).
5. **Monitoring & Detection (IEC 62443 FR 6):**
   * Deploy EDR on the PCTS server.21
   * Monitor network traffic entering and leaving the PCTS (both IT and OT interfaces) using NIDS/NDR tools aware of ICS protocols.3
   * Centralize and analyze logs (OS, application, firewall, network) in a SIEM, correlating with ATT&CK for ICS TTPs.18 Monitor for anomalous login patterns, network connections, and process execution.
6. **Incident Response:**
   * Develop specific playbooks for PCTS compromise scenarios, including containment (network isolation), eradication, and recovery steps.18 Ensure backup and recovery procedures are regularly tested.
7. **Embedded Security (EMB3D Mitigations):**
   * Prioritize foundational EMB3D mitigations like Secure Boot (MID-001), Strong Authentication (MID-016), Patch Management (MID-034), Network Segmentation (MID-010), and Physical Protection (MID-069) for the server hardware itself.6

By implementing these practical, multi-layered steps tailored to the specific risks identified through ATT&CK for ICS and EMB3D, Exxon Mobil can significantly improve the security resilience of its PCTS infrastructure, reducing the likelihood and potential impact of cyber attacks targeting its critical process control environments.

## **Addendum D: Overview of the IEC 62443 Framework for Industrial Automation and Control Systems (IACS)**

Introduction:

The ISA/IEC 62443 series of standards provides a comprehensive framework for securing Industrial Automation and Control Systems (IACS), also commonly referred to as Operational Technology (OT) or Industrial Control Systems (ICS).17 Developed through international consensus, it addresses cybersecurity throughout the entire lifecycle, from component design to system integration, operation, and maintenance.17 Its holistic approach aims to bridge the gap between IT and OT security practices and considers the unique requirements of industrial environments, including safety, reliability, and availability.16 These standards are applicable across various sectors using IACS, including oil and gas, manufacturing, power generation, transportation, and building automation.17

**Key Concepts:**

1. **Foundational Requirements (FRs):** The framework is built upon seven Foundational Requirements (FRs) that define the essential security objectives for an IACS 18:
   * **FR 1: Identification and Authentication Control (AC):** Ensuring only authorized entities (humans, software, devices) can access the system.
   * **FR 2: Use Control (UC):** Enforcing privileges assigned to authenticated entities.
   * **FR 3: System Integrity (SI):** Ensuring the integrity of the IACS assets (hardware, software, firmware, information).
   * **FR 4: Data Confidentiality (DC):** Protecting sensitive information from unauthorized disclosure.
   * **FR 5: Restricted Data Flow (RDF):** Controlling the flow of data between different security zones.
   * **FR 6: Timely Response to Events (TRE):** Responding to security violations in a timely manner.
   * **FR 7: Resource Availability (RA):** Ensuring the IACS is resilient against events that could impact availability. *18*
2. **Zones and Conduits:** A core principle for architecting secure IACS environments.
   * **Zone:** A grouping of logical or physical assets that share common security requirements.16 Assets within a zone should have similar criticality and exposure. Examples include the Process Control Network (PCN), a Safety Instrumented System (SIS) zone, or a DMZ.
   * **Conduit:** A logical grouping of communication channels connecting two or more zones, sharing common security requirements.16 Conduits define the pathways where security controls (like firewalls) are applied to enforce the Restricted Data Flow (FR 5) between zones.
   * *Application to PCTS:* The PCTS would typically reside in a specific zone (e.g., a DMZ or a dedicated terminal server zone) and utilize conduits to connect to the IT zone and the OT/PCN zone. Security requirements for these conduits would be strictly defined and enforced by firewalls.
3. **Security Levels (SLs):** IEC 62443 defines four Security Levels (SLs) to specify the required security robustness of a zone, conduit, system, or component, based on the anticipated threat actor capabilities.16
   * **SL 1:** Protection against casual or coincidental violation. (Threat Actor: Accidental, simple means, low resources/motivation).16
   * **SL 2:** Protection against intentional violation using simple means. (Threat Actor: Hacker, low skills/resources, low motivation).16
   * **SL 3:** Protection against intentional violation using sophisticated means. (Threat Actor: Terrorist/Hacktivist, moderate skills/resources, moderate motivation).16
   * **SL 4:** Protection against intentional violation using sophisticated means with extended resources. (Threat Actor: Nation-state, high skills/resources, high motivation).16
   * *Application:* A risk assessment (defined in IEC 62443-3-2) determines the target Security Level (SL-T) for each zone and conduit.22 The PCTS zone and its connecting conduits would likely require a high SL-T (e.g., SL 3 or SL 4) given its criticality and exposure to threats from both IT and potentially OT networks. System requirements (SRs) defined in IEC 62443-3-3 are mapped to these SLs, meaning a higher SL requires more stringent security controls.18 Components must meet specific capability requirements (SL-C) defined in IEC 62443-4-2 to support the overall system SL.18

**Roadmap for Integrating IEC 62443 for the PCTS:**

1. **Risk Assessment (IEC 62443-3-2):** Conduct a formal risk assessment focused on the PCTS and its role within the IACS architecture. Identify threats, vulnerabilities, and potential consequences.22
2. **Zoning and Conduits:** Define the security zones relevant to the PCTS (e.g., IT Zone, DMZ/PCTS Zone, PCN Zone) and the conduits connecting them.50
3. **Determine Target Security Levels (SL-T):** Based on the risk assessment, assign appropriate SL-Ts to the PCTS zone and its conduits.22 This will likely be SL 3 or 4.
4. **Define System Requirements (IEC 62443-3-3):** Identify the specific System Requirements (SRs) from IEC 62443-3-3 necessary to achieve the target SLs for the PCTS zone and conduits. This covers areas like access control, integrity, confidentiality, data flow restriction, event response, and availability.18
5. **Component Selection/Design (IEC 62443-4-1, 4-2):** Select PCTS hardware and software components that meet the required capability Security Levels (SL-C) defined in IEC 62443-4-2.18 Ensure suppliers follow secure development lifecycle practices as defined in IEC 62443-4-1.18
6. **Implementation:** Implement the required technical controls (firewalls, authentication, monitoring, hardening) and procedural controls (patch management, incident response, access reviews) based on the defined SRs.
7. **Operational Procedures (IEC 62443-2-1, 2-3, 2-4):** Establish and maintain secure operating procedures, including patch management, incident response, backup/recovery, and management of service providers (vendors) involved with the PCTS.22
8. **Continuous Monitoring and Improvement:** Regularly assess the achieved Security Level (SL-A) through audits and testing, and continuously improve the security posture based on monitoring results and evolving threats.51

**Establishing Supplier Standards (IEC 62443-2-4, 4-1, 4-2):**

IEC 62443 provides specific guidance for establishing requirements for suppliers (product vendors and service providers):

* **IEC 62443-4-1 (Secure Product Development Lifecycle):** Require suppliers of PCTS hardware and software to demonstrate adherence to secure development practices. This can be verified through certifications like ISASecure SDLA (Security Development Lifecycle Assurance).17 Key practices include security requirements definition, secure design, secure implementation (coding), verification and validation testing, defect management, patch management, and security documentation.
* **IEC 62443-4-2 (Technical Security Requirements for IACS Components):** Specify the required capability Security Level (SL-C) for PCTS components based on the system's SL-T. Suppliers should provide components certified to meet these requirements (e.g., ISASecure CSA - Component Security Assurance).17 This standard defines detailed technical requirements for components related to the seven FRs.
* **IEC 62443-2-4 (Security Program Requirements for IACS Service Providers):** Define security requirements for third-party vendors providing installation, integration, maintenance, or remote support services for the PCTS.22 This includes requirements for personnel security, remote access procedures, incident handling, and information protection.

By incorporating these IEC 62443 requirements into procurement specifications and contracts, Exxon Mobil can ensure that suppliers contribute positively to the overall security posture of the PCTS and the IACS environment it protects, fostering a shared responsibility model for cybersecurity.17

#### Works cited

1. ICS/SCADA Threats: Securing Infrastructure | Infosec, accessed April 9, 2025, <https://www.infosecinstitute.com/resources/scada-ics-security/ics-scada-threats-and-threat-actors/>
2. Since Stuxnet: A History of Critical Infrastructure Attacks - Forescout, accessed April 9, 2025, <https://www.forescout.com/blog/since-stuxnet-a-brief-history-of-critical-infrastructure-attacks/>
3. MITRE ATT&CK ICS: Tactics, Techniques, and Best Practices | Exabeam, accessed April 9, 2025, <https://www.exabeam.com/explainers/mitre-attck/mitre-attck-ics-tactics-techniques-and-best-practices/>
4. Your Guide to the MITRE ATT&CK Framework for ICS - Nozomi Networks, accessed April 9, 2025, <https://www.nozominetworks.com/blog/your-guide-to-the-mitre-attack-framework-for-ics>
5. Elevating Embedded Device Security: The EMB3D™ Threat Modeling Framework - IriusRisk, accessed April 9, 2025, <https://www.iriusrisk.com/resources-blog/elevating-embedded-device-security-mitre-emb3d>
6. MITRE EMB3D™, accessed April 9, 2025, <https://emb3d.mitre.org/>
7. Industrial Control Systems | Cybersecurity and Infrastructure Security Agency CISA, accessed April 9, 2025, <https://www.cisa.gov/topics/industrial-control-systems>
8. Library of Resources for Industrial Control System Cyber Security - ICSCSI, accessed April 9, 2025, <https://icscsi.org/library/index.html>
9. Dragos Reports OT/ICS Cyber Threats Escalate Amid Geopolitical Conflicts and Increasing Ransomware Attacks, accessed April 9, 2025, <https://www.dragos.com/resources/press-release/dragos-reports-ot-ics-cyber-threats-escalate-amid-geopolitical-conflicts-and-increasing-ransomware-attacks/>
10. What Is Industrial Control System (ICS) Cyber Security? - eSecurity Planet, accessed April 9, 2025, <https://www.esecurityplanet.com/cloud/industrial-control-systems-cyber-security/>
11. Biggest threats to ICS/SCADA systems - Infosec, accessed April 9, 2025, <https://www.infosecinstitute.com/resources/scada-ics-security/biggest-threats-to-ics-scada-systems/>
12. Matrix - ICS | MITRE ATT&CK®, accessed April 9, 2025, <https://attack.mitre.org/matrices/ics/>
13. Securing the unseen: MITRE's EMB3D framework for embedded devices - Forescout, accessed April 9, 2025, <https://www.forescout.com/blog/securing-the-unseen-mitre-emb3d-framework-for-embedded-devices/>
14. A Comprehensive Guide to SCADA Cybersecurity - Claroty, accessed April 9, 2025, <https://claroty.com/blog/a-comprehensive-guide-to-scada-cybersecurity>
15. What Are the Differences Between OT, ICS, & SCADA Security? - Palo Alto Networks, accessed April 9, 2025, <https://www.paloaltonetworks.com/cyberpedia/ot-vs-ics-vs-scada-security>
16. IEC 62443 Overview | Dell Technologies Validated Design for Manufacturing Edge with Litmus, accessed April 9, 2025, <https://infohub.delltechnologies.com/it-it/l/dell-technologies-validated-design-for-manufacturing-edge-with-litmus-design-guide/iec-62443-overview-5/>
17. ISA/IEC 62443 Series of Standards - ISA, accessed April 9, 2025, <https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards>
18. What is IEC/ISA 62443-3-3:2013? Cybersecurity & Compliance | UpGuard, accessed April 9, 2025, <https://www.upguard.com/blog/isa-62443-3-3-2013>
19. APT Cyber Tools Targeting ICS/SCADA Devices - CISA, accessed April 9, 2025, <https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-103a>
20. Key Differences of OT, ICS, and SCADA Security | Balbix, accessed April 9, 2025, <https://www.balbix.com/insights/ots-and-ics-security-the-next-big-challenge/>
21. What Is the MITRE ATT&CK Framework? | Get the 101 Guide - Trellix, accessed April 9, 2025, <https://www.trellix.com/security-awareness/cybersecurity/what-is-mitre-attack-framework/>
22. The Essential Guide to the IEC 62443 industrial cybersecurity standards, accessed April 9, 2025, <https://industrialcyber.co/features/the-essential-guide-to-the-iec-62443-industrial-cybersecurity-standards/>
23. Protecting critical rail infrastructure from cyber attacks | DXC Technology Insights, accessed April 9, 2025, <https://dxc.com/us/en/insights/perspectives/paper/protecting-critical-rail-infrastructure-from-cyber-attacks>
24. CISA MITRE ATT&CK for ICS focuses on adversarial tactics, techniques disrupting industrial control process, accessed April 9, 2025, <https://industrialcyber.co/vulnerabilities/cisa-mitre-attck-for-ics-focuses-on-adversarial-tactics-techniques-disrupting-industrial-control-process/>
25. MITRE releases enhanced EMB3D Threat Model with new mitigations, ISA/IEC 62443-4-2 alignment - Industrial Cyber, accessed April 9, 2025, <https://industrialcyber.co/control-device-security/mitre-releases-enhanced-emb3d-threat-model-with-new-mitigations-isa-iec-62443-4-2-alignment/>
26. 14 recent cyber attacks on the transport & logistics sector - Wisdiam, accessed April 9, 2025, <https://wisdiam.com/publications/recent-cyber-attacks-transport-logistics-sector/>
27. Transportation Cybersecurity Incidents - Alabama Transportation Institute, accessed April 9, 2025, <https://ati.ua.edu/wp-content/uploads/2021/05/72.pdf>
28. Cyberattacks Against Intelligent Transportation Systems: Assessing Future Threats to ITS - Trend Micro, accessed April 9, 2025, <https://documents.trendmicro.com/assets/white_papers/wp-cyberattacks-against-intelligent-transportation-systems.pdf>
29. IEC 62443 - Industrial Security standards and laws - Pilz US, accessed April 9, 2025, <https://www.pilz.com/en-US/support/law-standards-norms/industrial-security-standards-iec-62443>
30. MITRE ATT&CK Framework Guide for Beginners - Picus Security, accessed April 9, 2025, <https://www.picussecurity.com/mitre-attack-framework-beginners-guide>
31. Guide to the MITRE ATT&CK Framework - Balbix, accessed April 9, 2025, <https://www.balbix.com/insights/what-is-the-mitre-attck-framework/>
32. Cybersecurity threat model for embedded devices ... - eeNews Europe, accessed April 9, 2025, <https://www.eenewseurope.com/en/cybersecurity-threat-model-for-embedded-devices/>
33. The EMB3D™ Threat Model for Embedded Devices, accessed April 9, 2025, <https://emb3d.mitre.org/assets/EMB3D_Paper_09-23-24.pdf>
34. What is the MITRE EMB3D Framework and Why It Matters - Asimily, accessed April 9, 2025, <https://asimily.com/blog/what-is-the-mitre-emb3d-framework/>
35. Free Cybersecurity Services & Tools - CISA, accessed April 9, 2025, <https://www.cisa.gov/resources-tools/resources/free-cybersecurity-services-and-tools>
36. ICS Training Available Through CISA, accessed April 9, 2025, <https://www.cisa.gov/resources-tools/programs/ics-training-available-through-cisa>
37. Chinese APT Group Earth Estries targets critical infrastructure sectors with advanced cyber attacks, accessed April 9, 2025, <https://industrialcyber.co/ransomware/chinese-apt-group-earth-estries-targets-critical-infrastructure-sectors-with-advanced-cyber-attacks/>
38. (PDF) Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions - ResearchGate, accessed April 9, 2025, <https://www.researchgate.net/publication/344947562_Cyber-attacks_in_the_next-generation_cars_mitigation_techniques_anticipated_readiness_and_future_directions>
39. Cyber Attacks in Transportation - IT ArchiTeks, accessed April 9, 2025, <https://www.itarchiteks.com/8-recent-cyber-attacks-that-have-affected-the-transportation-industry>
40. Cybersecurity in Transportation | Risks and Challenges - Darktrace, accessed April 9, 2025, <https://darktrace.com/cyber-ai-glossary/cybersecurity-in-transportation>
41. Communications: The heart of an Operations Control Center - Alcatel-Lucent Enterprise, accessed April 9, 2025, <https://www.al-enterprise.com/en/blog/comms-heart-of-ops-control-ctr>
42. What is an Operation Control Center (OCC)? OCC Meaning | Isarsoft, accessed April 9, 2025, <https://www.isarsoft.com/knowledge-hub/occ>
43. Automation & Control | SCADA and HMI Solutions - SolutionsPT, accessed April 9, 2025, <https://www.solutionspt.com/automation-and-control-scada-hmi>
44. On SCADA Operating Systems and Automation - Techman Robot, accessed April 9, 2025, <https://www.tm-robot.com/en/scada-automation-systems/>
45. Example Job Description for Public Transit Operations Manager - Yardstick, accessed April 9, 2025, <https://www.yardstick.team/job-description/public-transit-operations-manager>
46. Planning and Evaluation - National Rural Transit Assistance Program, accessed April 9, 2025, <https://www.nationalrtap.org/Toolkits/Transit-Managers-Toolkit/Operations-and-Planning/Planning-and-Evaluation>
47. What is Transportation Systems Management and Operations (TSMO)?, accessed April 9, 2025, <https://ops.fhwa.dot.gov/tsmo/>
48. Why SCADA and DCS Face Different Cyber Threats, accessed April 9, 2025, <https://industrialcyber.co/expert/why-scada-and-dcs-face-different-cyber-threats/>
49. UAT-5918 APT group targets Taiwan critical infrastructure, possible linkage to Volt Typhoon, accessed April 9, 2025, <https://industrialcyber.co/critical-infrastructure/uat-5918-apt-group-targets-taiwan-critical-infrastructure-possible-linkage-to-volt-typhoon/>
50. How to Define Zones and Conduits - ISA Global Cybersecurity Alliance, accessed April 9, 2025, <https://gca.isa.org/blog/how-to-define-zones-and-conduits>
51. What Is IEC 62443? | Definition & Methodology - Zscaler, accessed April 9, 2025, <https://www.zscaler.com/zpedia/what-is-iec-62443>
52. Automated Transport Systems: Techniques & Architecture - Vaia, accessed April 9, 2025, <https://www.vaia.com/en-us/explanations/architecture/urban-studies-in-architecture/automated-transport-systems/>
53. Macau Light Rapid Transit (MLRT): Mainstay transport system for a world-leading tourist city, accessed April 9, 2025, <https://www.mhi.co.jp/technology/review/pdf/e572/e572030.pdf>
54. Safe Operations at Roadway Junctions - Design Principles from Automated Guideway Transit - OSTI.GOV, accessed April 9, 2025, <https://www.osti.gov/servlets/purl/1975541>
55. Securing Control and Communications Systems in Transit Bus Vehicles and Supporting Infrastructure - American Public Transportation Association, accessed April 9, 2025, <https://www.apta.com/wp-content/uploads/APTA-SS-CCS-WP-005-19.pdf>
56. Advanced Public Transportation Systems - Federal Highway Administration, accessed April 9, 2025, <https://highways.dot.gov/media/8556>
57. Transit Security Design Considerations Final Report November 2004, accessed April 9, 2025, <https://www.transit.dot.gov/sites/fta.dot.gov/files/docs/ftasesc.pdf>
58. AUTOMATED TRANSIT, accessed April 9, 2025, <http://dl1.wikitransport.ir/book/Automated_Transit_Planning_Operation_and_Applications_2017.pdf>
59. Cellular V2X & DSRC | Anritsu America, accessed April 9, 2025, <https://www.anritsu.com/en-us/test-measurement/solutions/automotive/v2x?tm_navigation=solution>
60. DSRC vs. C-V2X: Understanding the Two Technologies - Ettifos, accessed April 9, 2025, <https://www.ettifos.com/post/dsrc-vs-cv2x>
61. V2X Vehicle-to-Everything Communication – The Future of Autonomous Connectivity | Keysight Blogs, accessed April 9, 2025, <https://www.keysight.com/blogs/en/inds/auto/2024/10/03/v2x-post>
62. Autonomous Vehicles & the Role of C-V2X Cellular Technology | IoT For All, accessed April 9, 2025, <https://www.iotforall.com/autonomous-vehicles-and-the-role-of-5g-cellular-technology>
63. FCC adopts final rules for cellular-vehicle-to-everything technology | Repairer Driven News, accessed April 9, 2025, <https://www.repairerdrivennews.com/2024/12/11/fcc-adopts-final-rules-for-cellular-vehicle-to-everything-technology/>
64. Designing for V2X Communication: Wireless Protocols and Standards | Blogs | Altium, accessed April 9, 2025, <https://resources.altium.com/p/designing-v2x-communication-wireless-protocols-and-standards>
65. Focus Topics | Autonomous Mobility - Continental Automotive, accessed April 9, 2025, <https://www.continental-automotive.com/en/focus-topics/autonomous-mobility.html>
66. Introduction to Automotive Sensors and Actuators - Monolithic Power Systems, accessed April 9, 2025, <https://www.monolithicpower.com/en/learning/mpscholar/automotive-electronics/automotive-sensing-and-actuators/intro-to-automotive-sensors-actuators>
67. AI in the driving seat: - Cambridge Consultants, accessed April 9, 2025, <https://www.cambridgeconsultants.com/wp-content/uploads/2023/11/2022-AI-in-the-driving-seat-Whitepaper.pdf>
68. Understanding Vehicle Computer System: Key Components and How It Works - sintrones, accessed April 9, 2025, <https://www.sintrones.com/application/understanding-vehicle-computer-system-key-components-and-how-it-works/>
69. Transit Bus Automation Project: Transferability of Automation Technologies Final Report, accessed April 9, 2025, <https://www.transit.dot.gov/sites/fta.dot.gov/files/docs/research-innovation/118161/transit-bus-automation-project-transferability-automation-technologies-final-report-fta-report-no.pdf>
70. Connected and Automated Vehicles: Infrastructure, Applications, Security, Critical Challenges, and Future Aspects - MDPI, accessed April 9, 2025, <https://www.mdpi.com/2227-7080/11/5/117>
71. Bus Automation: - WSP, accessed April 9, 2025, <https://www.wsp.com/-/media/insights/us/bus-automation-whitepaper/bus-automation-whitepaper-wsp-2023.pdf>
72. ICS Cybersecurity Training - Idaho National Laboratory, accessed April 9, 2025, <https://inl.gov/national-security/ics-cybersecurity-training/>
73. Reflections on the US Government's OIG Report on CISA's Automated Indicator Sharing Program | SANS Institute, accessed April 9, 2025, <https://www.sans.org/blog/reflections-on-the-us-governments-oig-report-on-cisas-automated-indicator-sharing-program/>
74. Future Operational Control Center Development Unifying Centralized Operations Management System - MTA, accessed April 9, 2025, <https://www.mta.info/document/161176>
75. SCVTA SCADA Control Center and Systems Replacement - SYSTRA USA, accessed April 9, 2025, <https://www.systra.com/usa/project/scvta-scada-control-center-and-systems-replacement/>
76. Assistant Operations Manager II (9172) - Transit Division, SF Municipal Transportation Agency - (155016) | City and County of San Francisco - SF Careers, accessed April 9, 2025, <https://careers.sf.gov/role/?id=3743990006670901>
77. Houston District Transportation Systems Management and Operations (TSMO) Program, accessed April 9, 2025, <https://ftp.txdot.gov/pub/txdot-info/trf/tsmo/hou-tsmo-program-plan.pdf>
78. Planning and Project Delivery Job Duties | City of San José, accessed April 9, 2025, <https://www.sanjoseca.gov/your-government/departments-offices/transportation/about/planning-and-project-delivery-job-duties>
79. AMERICAN PUBLIC TRANSPORTATION ASSOCIATION - Transit Board Member Handbook, accessed April 9, 2025, [https://www.riometro.org/DocumentCenter/View/244/American-Public-Transportation-Association-Transit-Board-Member-Handbook-PDF?bidId=](https://www.riometro.org/DocumentCenter/View/244/American-Public-Transportation-Association-Transit-Board-Member-Handbook-PDF?bidId)