American Journal of Data Science and Analytics

Volume: 7; **Issue:** 7
Pages: 67-98

Cybersecurity of Industrial Control Systems in Oil and Gas Infrastructure: Threat Landscape, Frameworks, Case Studies, and a Defense-in-Depth Architecture

Md Mashfiqur Rahman[1];

[1]. *IT Network Administrator, Classic Southeast Texas Automotive Inc;*
Master of Science in Management Information Systems, Lamar University, Texas; USA;
Email: riyad72@gmail.com

Doi: 10.63125/30fha898
Received: *12 April 2026;* ***Revised:*** *21 May 2026;* ***Accepted:*** *16 June 2026;* ***Published:*** *08 July 2026;*

Abstract

Industrial Control Systems (ICS) are critical to the safe and reliable operation of oil and gas infrastructure. This paper analyzes cybersecurity threats affecting programmable logic controllers, SCADA systems, distributed control system platforms, safety instrumented systems, and the wider operational technology environment of the sector, and evaluates the frameworks available to defend them. It reviews the architecture of oil and gas control systems and the Purdue reference model, characterises the contemporary threat landscape of ransomware, insider misuse, nation-state malware, supply-chain compromise, credential theft, insecure remote access, and industrial-protocol exploitation, and maps adversary behaviour to the MITRE ATT&CK for ICS knowledge base. A qualitative risk assessment using likelihood and impact scales derived from NIST SP 800-30 identifies ransomware entering through business networks, manipulation of controller and safety logic, and exploitation of insecure remote access as the highest-priority scenarios. Two case studies, the 2021 Colonial Pipeline ransomware incident and the 2017 Triton attack on a safety instrumented system, are analysed alongside Stuxnet and Industroyer to extract lessons on IT–OT dependency, remote-access governance, and the protection of safety functions. NIST SP 800-82 Revision 3, the NIST Cybersecurity Framework 2.0, and the ISA/IEC 62443 series are compared and mapped, and a seven-layer defense-in-depth architecture covering governance, physical security, segmentation, identity and endpoint protection, monitoring, response and recovery, and lifecycle security is proposed and aligned with Purdue levels, framework functions, and ATT&CK tactics. The paper concludes that industrial cybersecurity must be treated as a safety and business-continuity function, and identifies zero trust for operational technology, AI-assisted detection, digital twins, autonomous vulnerability management, quantum-resistant cryptography, and safety–security co-engineering as priorities for future research.

Keywords

Industrial Control Systems, Operational Technology, Oil and Gas, SCADA, IEC 62443, NIST SP 800-82, MITRE ATT&CK for ICS, Defense in Depth.

I. INTRODUCTION

The oil and gas sector relies on highly interconnected industrial automation systems. Exploration, production, gathering, processing, pipeline transport, refining, storage, and distribution are each governed by control systems that measure physical variables, execute control logic, present the process to operators, and record its history. As information technology (IT) and operational technology (OT) environments converge, cyber risk increases: the proprietary serial networks and isolated control rooms of the 1990s have given way to Ethernet, Windows-based servers, remote vendor access, and cloud analytics, so that the systems which keep hydrocarbons flowing safely are reachable, directly or indirectly, from networks that adversaries can reach (Galloway & Hancke, 2013; McLaughlin et al., 2016; Stouffer et al., 2023). Threat actors target critical infrastructure for financial gain, espionage, disruption, and sabotage, and the historical record of ICS incidents shows a progression from opportunistic infections to purpose-built malware and, most recently, to ransomware campaigns whose business impact extends into operations even when the control systems themselves are not touched (Hemsley & Fisher, 2018; Miller et al., 2021; Slowik, 2019).

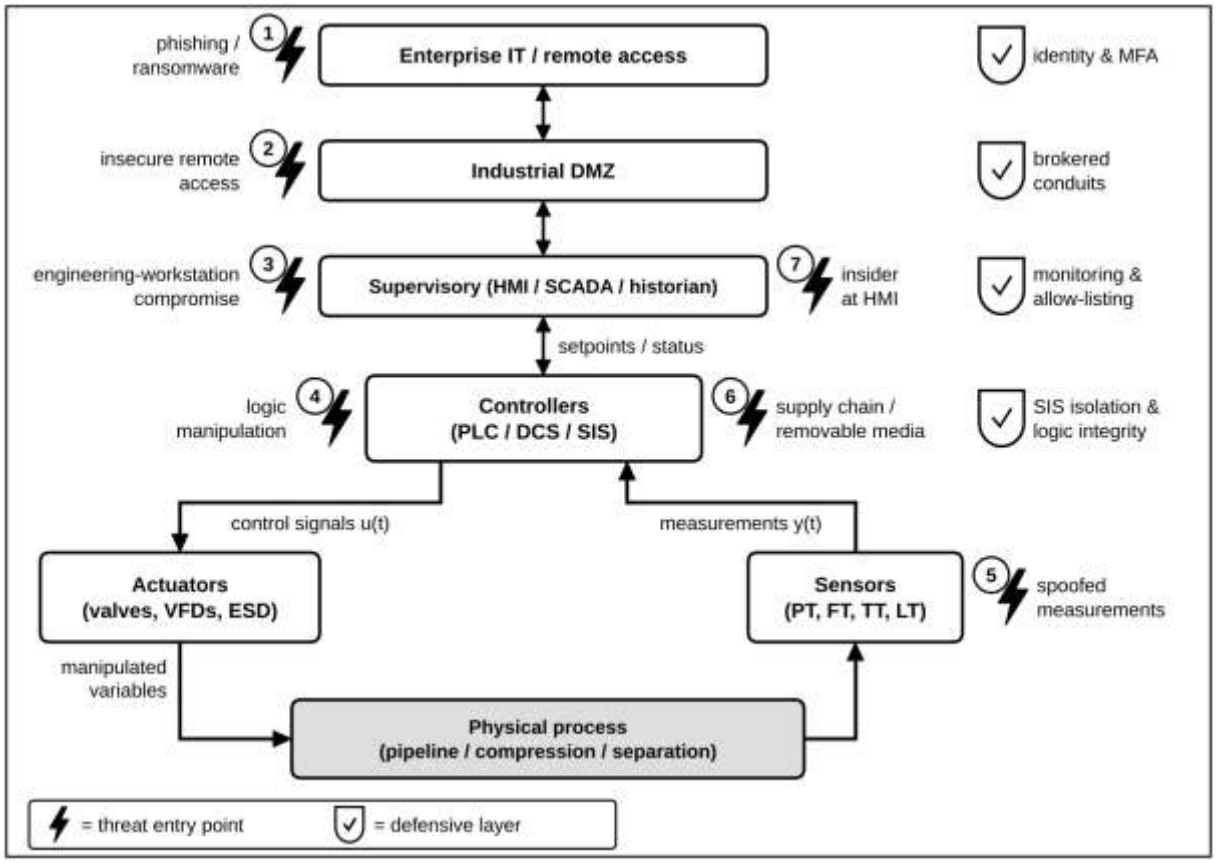
Three features distinguish ICS security from enterprise security and shape everything that follows. First, the priority ordering of security objectives is inverted: availability and the integrity of control actions come before confidentiality, because the consequence of a successful attack is physical, measured in loss of containment, equipment damage, environmental release, and injury, rather than in data loss alone (Stouffer et al., 2023; Cárdenas et al., 2011; Humayed et al., 2017). Second, the installed base is long-lived and heterogeneous; controllers and protocols designed decades ago without authentication remain in service, patch windows are constrained by production schedules, and conventional IT security tools can disrupt the deterministic communication that control loops require (Igure et al., 2006; Cheminod et al., 2013; Knowles et al., 2015). Third, safety and security are coupled: the safety instrumented systems that are the last line of defence against hazardous process conditions are themselves computers with network connections, and an attacker who can reach them can remove the protection on which process safety depends, as the Triton incident demonstrated (Johnson et al., 2017; Kriaa et al., 2015; Young & Leveson, 2014).

The regulatory and standards environment has responded to these realities. The National Institute of Standards and Technology (NIST) published the third revision of Special Publication 800-82 in 2023, broadening its scope from ICS to operational technology generally and aligning it with the Cybersecurity Framework, which in its 2.0 version added governance as a sixth function (Stouffer et al., 2023; National Institute of Standards and Technology, 2024a). The ISA/IEC 62443 series provides an international standard for industrial automation and control system security organised around zones, conduits, and security levels (International Society of Automation, 2024; International Electrotechnical Commission, 2023; Piggin, 2013). MITRE's ATT&CK for ICS, released in 2020, supplies a structured knowledge base of adversary tactics and techniques observed against control systems (Alexander et al., 2020; Strom et al., 2018). The Cybersecurity and Infrastructure Security Agency (CISA) issued cross-sector performance goals as a prioritised baseline, and, following the Colonial Pipeline incident, the Transportation Security Administration moved from voluntary pipeline guidelines to mandatory security directives, while the American Petroleum Institute issued the third edition of its pipeline control-system cybersecurity standard (Cybersecurity and Infrastructure Security Agency, 2023; U.S. Government Accountability Office, 2021; American Petroleum Institute, 2021). The electricity sector's NERC CIP standards provide a longer-running precedent for mandatory ICS security requirements (North American Electric Reliability Corporation, 2024; Leszczyna, 2018).

This paper has four objectives. The first is to describe the architecture of oil and gas control systems and the Purdue reference model in sufficient detail to reason about where threats enter and where controls belong. The second is to characterise the threat landscape and to map it onto ATT&CK for ICS, so that defensive investments can be tied to observed adversary behaviour. The third is to conduct a structured qualitative risk assessment and to test its conclusions against two case studies, Colonial Pipeline and Triton, which together span the two dominant risk types of the sector: business-driven ransomware and safety-targeted sabotage. The fourth is to evaluate NIST SP 800-82 and IEC 62443 and to propose a defense-in-depth architecture that operationalises both. Figure 1 frames the paper as a cyber-physical control loop, from the physical process through sensors, controllers, and actuators to

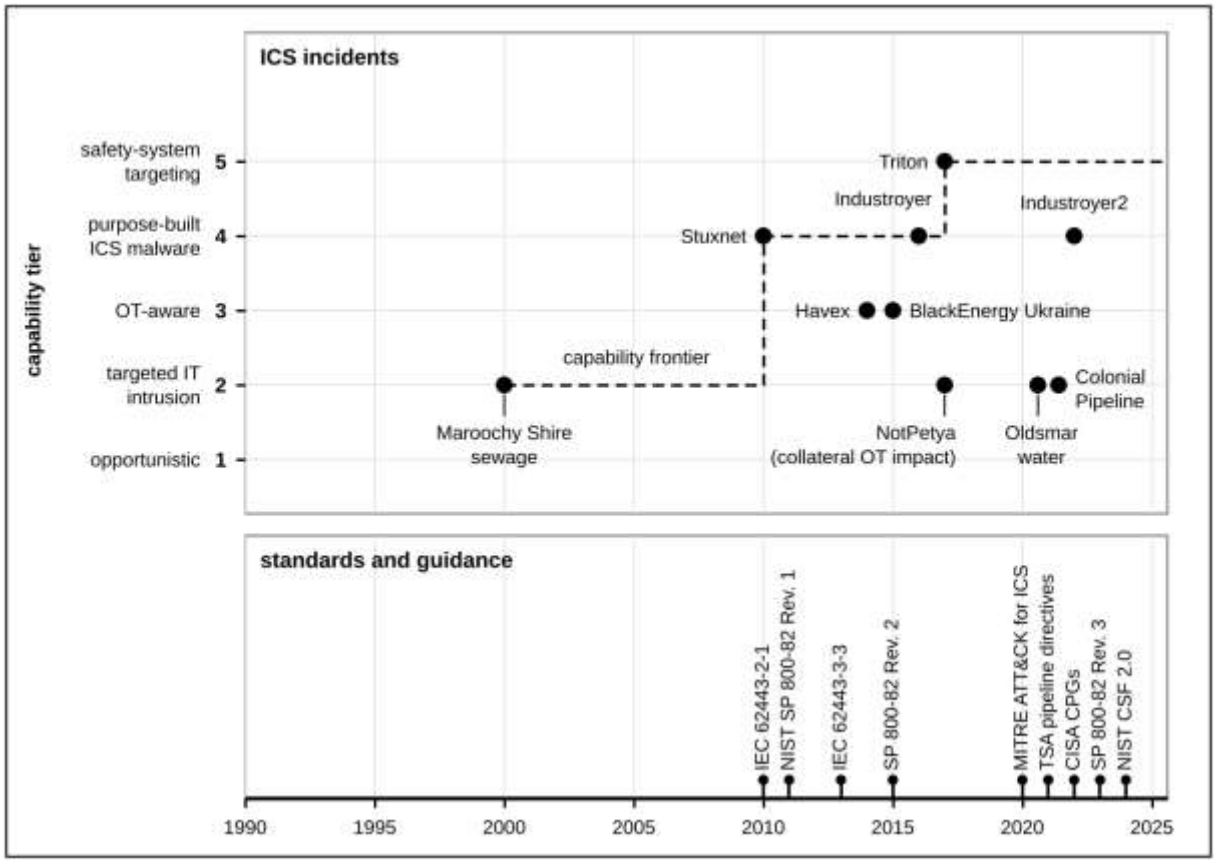
the supervisory, demilitarised, and enterprise layers above it, and marks the threat entry points and the defensive layers that the following sections analyse. Figure 2 places the landmark incidents of the past twenty-five years, graded by the capability tier they demonstrated, on a common timeline with the standards and guidance that responded to them (Hemsley & Fisher, 2018; Miller et al., 2021; Slowik, 2019).

Figure 1: Cyber-Physical Control Loop of an Oil and Gas Facility with Threat Entry Points and Defensive Layers



The remainder of the paper is organised as follows. Section II reviews the literature. Sections III and IV describe ICS architecture and the Purdue model. Section V characterises the threat landscape and Section VI analyses it through ATT&CK for ICS. Section VII presents the risk assessment. Sections VIII and IX present the Colonial Pipeline and Triton case studies. Section X compares NIST SP 800-82 and IEC 62443, Section XI proposes the defense-in-depth architecture, Section XII identifies future research, and Section XIII concludes.

Figure 2: Timeline of ICS Incidents by Capability Tier and of Standards and Guidance, 1990–2025



II. LITERATURE REVIEW

Academic and industry research consistently identifies OT environments as high-value targets. NIST, CISA, MITRE, ISA, and IEC have published guidance for securing industrial environments, and researchers emphasize availability and safety as primary security objectives. This section reviews that body of work in five strands: foundational surveys of ICS and SCADA security, the standards and guidance literature, the incident and threat-intelligence literature, the safety–security literature, and the emerging literature on detection, resilience, and artificial intelligence.

ICS and SCADA Security Research

The security of supervisory control and data acquisition networks was recognised as a distinct research problem in the mid-2000s, when early surveys catalogued the vulnerabilities created by connecting legacy control networks to corporate networks and the internet (Igure et al., 2006; Ralston et al., 2007). Subsequent work established the field's conceptual foundations: risk assessment, detection, and response for process control systems were framed in terms of the physical consequences of attacks rather than data breaches (Cárdenas et al., 2011), taxonomies of SCADA attacks were proposed (Zhu et al., 2011), and the deterministic, real-time character of industrial networks was shown to constrain the security mechanisms that could be deployed (Galloway & Hancke, 2013; Cheminod et al., 2013). Reviews of cyber security management in ICS and of risk assessment methods for SCADA systems documented the gap between the richness of proposed methods and their limited adoption in practice (Knowles et al., 2015; Cherdantseva et al., 2016). The cybersecurity landscape in ICS was surveyed from the perspective of hardware, firmware, and supply-chain trust (McLaughlin et al., 2016), and the broader cyber-physical systems security literature provided a unifying view across sectors (Humayed et al., 2017; Ashibani & Mahmoud, 2017; Lun et al., 2019). More recent surveys have updated the picture of attack trends and countermeasures, reviewed SCADA architecture and security, and examined the security of PLC networks specifically (Alladi et al., 2020; Bhamare et al., 2020; Yadav & Paul, 2021; Ghaleb et al., 2018). Sector-specific work has catalogued cyber-attacks on the oil and gas sector and the particular exposure of offshore assets (Stergiopoulos et al., 2020; Progoulakis et al., 2021), while the manufacturing, water, and electricity sectors have contributed parallel reviews whose lessons transfer

directly (Ani et al., 2017; Hassanzadeh et al., 2020; Sridhar et al., 2012; Mo et al., 2012; Wang & Lu, 2013). Research on attacks against controllers has shown that the integrity of control logic is a first-order concern. Specification-based payload generation demonstrated that an adversary with access to a PLC could synthesise logic that achieves a physical objective without prior knowledge of the plant (McLaughlin & McDaniel, 2012), and physics-aware rootkits showed that malicious code can conceal its effects by understanding the process it manipulates (Garcia et al., 2017). Stealthy deception attacks on water SCADA systems and work on data veracity in cyber-physical systems established that attacks which respect the physics of the process are difficult to detect with conventional tools (Amin et al., 2013; Krotofil et al., 2015), motivating the physics-based detection literature reviewed below. Attack and defence modelling for critical infrastructures provided the formal basis for reasoning about adversary pathways through control networks (Ten et al., 2010).

Standards, Guidance, and Regulation

The standards literature is dominated by NIST SP 800-82 and the ISA/IEC 62443 series. The second revision of SP 800-82 established the structure that practitioners still use, with an overview of ICS, a risk-management framework, recommended architectures, and a tailored overlay of the SP 800-53 control catalogue (Stouffer et al., 2015; Joint Task Force, 2020); the third revision broadened the scope to OT and incorporated lessons from a decade of incidents (Stouffer et al., 2023). Companion NIST publications address risk assessment, incident handling, event recovery, supply-chain risk management, zero trust architecture, and a practice guide for protecting information and system integrity in ICS environments (Joint Task Force Transformation Initiative, 2012; Cichonski et al., 2012; Bartock et al., 2016; Boyens et al., 2022; Rose et al., 2020; Powell et al., 2022). The development of IEC 62443 from the ISA99 committee's work has been described from a standards-development perspective, and its concepts of zones, conduits, and security levels have become the lingua franca of ICS security engineering (Piggin, 2013; International Society of Automation, 2024; International Electrotechnical Commission, 2023). Reviews of standards with cybersecurity requirements for the smart grid illustrate how sectoral regulation layers on top of these generic standards (Leszczyna, 2018; North American Electric Reliability Corporation, 2024). In the United States, Executive Order 14028 and the TSA security directives that followed Colonial Pipeline marked a shift toward mandatory requirements for critical infrastructure, and GAO's reviews of TSA's pipeline security program document both the weaknesses that preceded the shift and the steps taken since (Executive Office of the President, 2021; U.S. Government Accountability Office, 2018; U.S. Government Accountability Office, 2021; American Petroleum Institute, 2021). Risk assessment methodology for cyber-physical systems has been integrated with these frameworks (Kure et al., 2018), and the generic risk management standards ISO 31000 and ISO/IEC 27005 supply the vocabulary of likelihood, consequence, and treatment used in Section VII (International Organization for Standardization, 2018; International Organization for Standardization, 2022).

Incidents and Threat Intelligence

The incident literature begins with Stuxnet. Technical dissections of the malware established that it was engineered to modify the logic of specific Siemens controllers while concealing its effects from operators, and that it propagated through removable media and supplier networks to reach an isolated facility (Falliere et al., 2011; Langner, 2011; T. M. Chen & Abu-Nimeh, 2011; Karnouskos, 2011). Analyses from the perspectives of strategy and systems theory examined its implications for cyber warfare and for the design of safer systems (Farwell & Rohozinski, 2011; Lindsay, 2013; Nourian & Madnick, 2018; Kushner, 2013; Zetter, 2014). The Ukrainian grid attacks of 2015 and 2016 were analysed in defence use cases and protective-relay literature, which documented the BlackEnergy intrusion and the Industroyer malware's modules for industrial protocols, and drew practical mitigation lessons (Lee et al., 2016; Cherepanov, 2017; Dragos, 2017b; Whitehead et al., 2017; Sullivan & Kamensky, 2017; Liang et al., 2017). The Triton attack on a safety instrumented system was reported by the incident responders and analysed by ICS security firms and government advisories (Johnson et al., 2017; Dragos, 2017a; Cybersecurity and Infrastructure Security Agency, 2022). The ransomware era is represented by Colonial Pipeline, analysed in a government advisory, a Congressional Research Service brief, and a peer-reviewed review (Cybersecurity and Infrastructure Security Agency, 2021a; Parfomak & Jaikaran, 2021; Beerman et al., 2023), and by the Oldsmar water-treatment intrusion, which illustrated the risk of

remote-access tools on OT hosts (Cybersecurity and Infrastructure Security Agency, 2021c). Threat-intelligence practice has been surveyed, and the intrusion kill chain and its ICS-specific extension provide the analytical structure used in Section VI (Tounsi & Rais, 2018; Hutchins et al., 2011; Assante & Lee, 2015). Insider threat has its own literature, including the CERT case base and taxonomies of insider behaviour and countermeasures (Cappelli et al., 2012; Homoliak et al., 2019; Greitzer et al., 2012), and supply-chain cyber risk has been reviewed from both security and supply chain management perspectives (Ghadge et al., 2020; Boyes, 2015; Cybersecurity and Infrastructure Security Agency, 2021b). Ransomware has been surveyed comprehensively (Oz et al., 2022).

Safety and Security

The literature on combining safety and security in ICS is directly relevant to oil and gas, where process safety management is mature and regulated. Surveys have catalogued approaches that integrate hazard analysis with threat analysis (Kriaa et al., 2015), and systems-theoretic approaches have argued that safety and security are both control problems amenable to the same analytical framework (Young & Leveson, 2014; Leveson, 2012). The functional-safety standard for the process sector, IEC 61511, governs the design of safety instrumented systems and now requires security risk assessment of those systems (International Electrotechnical Commission, 2016). Resilience, as distinct from protection, has been formalised with metrics for cyber systems and discussed as a design objective (Linkov et al., 2013; Ganin et al., 2016; Kott et al., 2021), and the interdependencies among critical infrastructures explain why an incident in one sector propagates to others (Rinaldi et al., 2001; Ouyang, 2014; Alcaraz & Zeadally, 2015).

Detection, Testbeds, and Artificial Intelligence

Detection research has moved from signature-based intrusion detection toward process-aware and physics-based approaches. State-based intrusion detection for Modbus and DNP3 was among the earliest proposals (Fovino et al., 2010); semantic monitoring through the PLC's own variables was demonstrated on real plants (Hadžiosmanović et al., 2014); and physics-based detection, which compares observed process behaviour with a model of what the process should do, was surveyed and its limits under stealthy attacks quantified (Giraldo et al., 2018; Urbina et al., 2016; Ahmed et al., 2018). Testbeds and datasets such as the water-treatment testbed have made reproducible research possible (Mathur & Tippenhauer, 2016; Conti et al., 2021; Hahn et al., 2013), and machine-learning methods, including recurrent and convolutional neural networks and unsupervised learning, have been applied to them (Goh et al., 2017; Kravchik & Shabtai, 2018; Inoue et al., 2017). Broader surveys of machine learning and deep learning for intrusion detection, and of artificial intelligence for cybersecurity, situate these ICS-specific results (Buczak & Guven, 2016; Ferrag et al., 2020; Sarker et al., 2021; Kaur et al., 2023). Digital twins have been proposed as security-aware virtual environments for evaluating attacks and defences without touching production systems (Eckhart & Ekelhart, 2018; Eckhart & Ekelhart, 2019; Bitton et al., 2018; Dietz & Pernul, 2020), zero trust has been reviewed as an architectural principle and codified by NIST (Buck et al., 2021; Rose et al., 2020), and post-quantum cryptography has moved from research to standardisation (Bernstein & Lange, 2017; L. Chen et al., 2016; National Institute of Standards and Technology, 2024b). The industrial Internet of Things extends the attack surface and the standards landscape further (Sadeghi et al., 2015; Dhirani et al., 2021; Lezzi et al., 2018).

Research Gaps

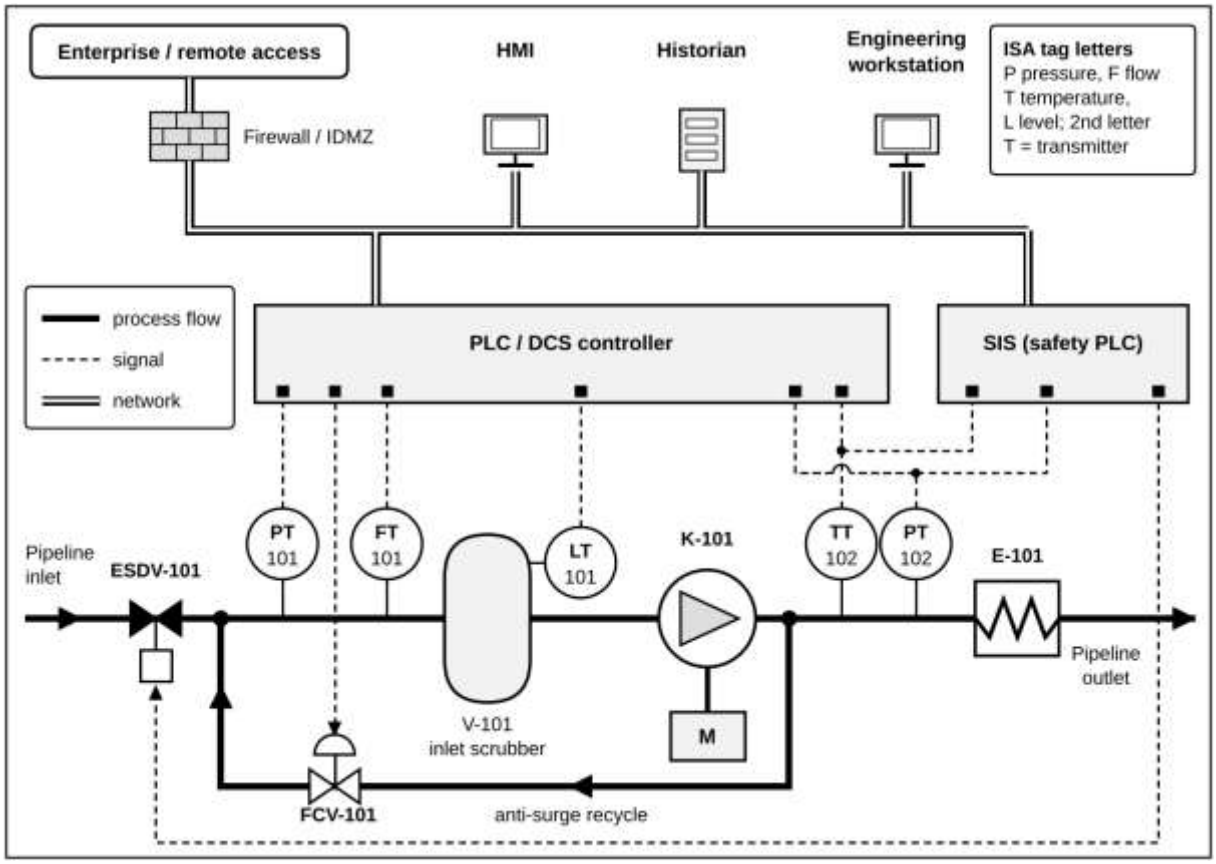
Several gaps motivate the present paper. Much of the literature treats ICS security generically, whereas the oil and gas sector combines pipeline SCADA, process DCS, and safety systems in ways that create sector-specific risk patterns (Stergiopoulos et al., 2020; Progoulakis et al., 2021). Risk assessment methods are plentiful but seldom connected to adversary-behaviour knowledge bases such as ATT&CK for ICS or to the lessons of specific incidents (Cherdantseva et al., 2016; Alexander et al., 2020). The frameworks are usually described separately rather than mapped to one another and to concrete architectural layers. Finally, the lessons of the ransomware era, in which the control systems may be untouched yet operations still stop, are not yet integrated with the older sabotage-oriented literature. The following sections address these gaps in turn.

III. ICS ARCHITECTURE

ICS architecture includes field devices, PLCs, RTUs, HMIs, historians, SCADA servers, engineering workstations, and enterprise systems. Network segmentation and visibility are fundamental security

requirements. Figure 3 presents a simplified process and control diagram of a gas compressor station, with its instrumentation, control and safety controllers, supervisory hosts, and network connections drawn in the conventions of a piping and instrumentation diagram, and Table 1 summarises the components, their functions, typical technologies, and primary security concerns.

Figure 3: Simplified Process and Control Diagram of a Gas Compressor Station



At the base of the architecture is the physical process: pumps, compressors, valves, actuators, and the sensors that measure pressure, flow, level, and temperature. These devices communicate with controllers through analogue signals, digital fieldbuses, and increasingly through wireless instrumentation, almost always without authentication, so that their security depends on physical access control and on the integrity of the controllers that read them (Galloway & Hancke, 2013; Stouffer et al., 2023). The control and safety band comprises PLCs and RTUs, which execute control logic in real time; DCS controllers, which handle continuous process control in refineries and gas plants; and the safety instrumented system, which is engineered to bring the process to a safe state when hazardous conditions are detected and is designed and maintained under IEC 61511 (International Electrotechnical Commission, 2016; Kriaa et al., 2015). In the compressor station of Figure 3, the PLC or DCS controller reads the inlet and discharge pressure, flow, temperature, and scrubber level transmitters and manipulates the anti-surge recycle valve, while the safety PLC reads the discharge pressure and temperature independently and drives the emergency shutdown valve; the two controllers share nothing but the process they protect, which is the separation that Section IX shows to be essential. Controllers communicate over industrial protocols such as Modbus/TCP, EtherNet/IP, PROFINET, DNP3, and IEC 60870-5-104, most of which lack authentication and integrity protection in their common deployments; the consequence is that any device with network reachability can issue commands, which is the structural weakness exploited by Industroyer and by PLC-targeting research (Cherepanov, 2017; Ghaleb et al., 2018; McLaughlin & McDaniel, 2012).

The supervision band contains SCADA servers and HMI operator stations, through which operators see the process and change setpoints; the historian, which stores time-series data for engineering and business use; and engineering workstations, which hold the software and project files needed to

configure and program controllers. The engineering workstation is the highest-privilege asset in the architecture, because it has the credentials and tools to change controller logic, and it was the pivot point in both Stuxnet and Triton (Falliere et al., 2011; Johnson et al., 2017). Loss of view, in which operators can no longer see the true state of the process, and loss of control, in which they can no longer act on it, are the two canonical failure modes of this band, and both appeared in the Ukrainian grid attacks (Lee et al., 2016; Whitehead et al., 2017).

The industrial demilitarised zone (IDMZ) mediates between operations and the enterprise. It hosts jump hosts for remote access, patch and antivirus relays, a replicated historian that serves business users without exposing the production historian, and, where unidirectional flows suffice, data diodes. Its purpose is to ensure that no session originates in the enterprise network and terminates in the control network, or vice versa, without being brokered (Stouffer et al., 2023; International Society of Automation, 2024). The enterprise band contains the business systems, corporate e-mail and internet access, cloud analytics, and vendor connections that are the usual point of initial access for adversaries. The Colonial Pipeline incident is the clearest demonstration that an attack confined to this band can halt operations, because business systems such as billing and scheduling have become operational dependencies (Cybersecurity and Infrastructure Security Agency, 2021a; Parfomak & Jaikaran, 2021; Beerman et al., 2023).

Table 1: ICS Components, Functions, Technologies, and Primary Security Concerns

ICS Component	Function	Typical Technology	Primary Security Concern
Field devices (sensors, actuators, drives)	Measure and manipulate the physical process	4–20 mA, HART, fieldbus, wireless instrumentation	Physical access; spoofed measurements; no authentication
Programmable logic controllers (PLCs)	Execute control logic in real time	IEC 61131-3 logic; Modbus/TCP, EtherNet/IP, PROFINET	Unauthenticated logic download; firmware integrity; protocol abuse
Remote terminal units (RTUs)	Remote monitoring and control of distributed assets	DNP3, IEC 60870-5-104, cellular or radio links	Insecure wide-area links; weak device credentials
Distributed control system (DCS)	Continuous process control and operator interface	Vendor controllers, redundant networks, operator consoles	Vendor remote access; flat control networks
Safety instrumented system (SIS)	Bring the process to a safe state on hazardous conditions	Safety controllers (SIL-rated), IEC 61511 design	Logic manipulation; engineering-workstation compromise
SCADA servers and HMI	Supervisory visualisation, alarms, setpoints	Windows servers, HMI software, alarm managers	Loss of view; unpatched software; credential theft
Historian	Store time-series process data	SQL-based historian, replicated to the DMZ	Data integrity; conduit into the control zone
Engineering workstation	Configure and program controllers	Vendor engineering software, project files	Highest-privilege asset; malware delivery path
Enterprise and remote-access systems	Business functions, vendor and remote support	ERP, e-mail, VPN, jump hosts	Initial access; IT-to-OT pivot; ransomware

Oil and gas introduces variations on this reference architecture that matter for security. Upstream and midstream operations are dominated by SCADA in the strict sense: a central control room supervises geographically dispersed wellheads, compressor stations, block valves, and metering stations through RTUs connected over leased lines, radio, satellite, or cellular networks, so that Level 1 and Level 2 are separated by wide-area conduits that may traverse third-party or public infrastructure (Yadav & Paul, 2021; American Petroleum Institute, 2021; Stergiopoulos et al., 2020). Downstream refining and gas processing are dominated by DCS, in which controllers, networks, and operator consoles are supplied as an integrated vendor system with its own remote-support arrangements, and in which the safety instrumented system is typically a separate vendor product with its own engineering tools (Stouffer et al., 2023; Kriaa et al., 2015). Offshore platforms combine both patterns under constraints of limited bandwidth, limited staffing, and vendor dependence that make remote access both indispensable and hazardous (Progoulakis et al., 2021). The practical consequence is that the conduit inventory of an oil

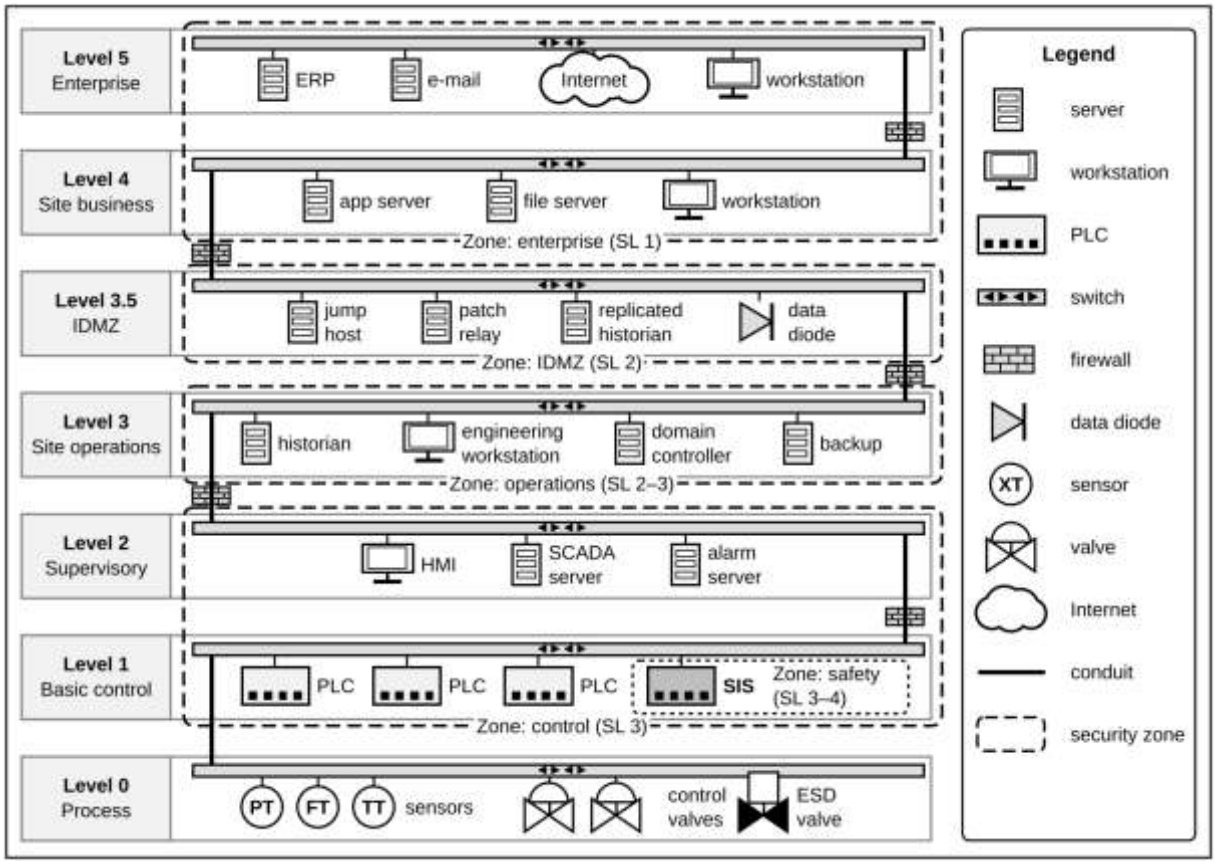
and gas operator is larger and more heterogeneous than that of a single plant, and that the security of wide-area links, vendor connections, and remote sites deserves the same engineering attention as the IDMZ.

Two cross-cutting requirements follow from this architecture. Segmentation, discussed in the next section, limits the pathways by which an adversary who has gained a foothold can reach the control and safety band. Visibility, the ability to inventory assets and observe traffic in each band, is the precondition for every other control, and its absence is the most commonly reported deficiency in OT security assessments (Knowles et al., 2015; Cybersecurity and Infrastructure Security Agency, 2023; Powell et al., 2022). Remote access deserves separate mention: vendors, integrators, and the operator's own engineers require remote connectivity for support and maintenance, and insecure implementations, from exposed remote-desktop services to shared VPN accounts without multi-factor authentication, have been the initial-access vector in a disproportionate share of recent incidents (Cybersecurity and Infrastructure Security Agency & National Security Agency, 2020; Cybersecurity and Infrastructure Security Agency, 2021c; Cybersecurity and Infrastructure Security Agency, 2021a).

IV. PURDUE MODEL

The Purdue Enterprise Reference Architecture divides industrial environments into levels ranging from physical processes to enterprise systems. Proper segmentation reduces lateral movement opportunities. Originally developed as a model of manufacturing enterprise integration (Williams, 1994), the Purdue model was adopted by ISA-95 and then by ISA-99/IEC 62443 and NIST SP 800-82 as the organising structure for network segmentation, and it remains the reference against which oil and gas control networks are designed and assessed (Stouffer et al., 2023; International Society of Automation, 2024). Figure 4 draws the model as a network topology, with the devices of each level, the firewalls on each conduit, and the zones with their target security levels, and Table 2 lists representative assets, the security emphasis of each level, and the guidance that applies.

Figure 4: Purdue Model as a Network Topology with Zones, Conduits, and Security Levels



Level 0 is the physical process and its instrumentation; Level 1 comprises the controllers, including the safety instrumented system; Level 2 is supervisory control, the HMI and SCADA servers; Level 3 is site

operations, including historians, engineering workstations, domain services, and backups; Level 3.5 is the industrial DMZ; Level 4 is site business planning; and Level 5 is the enterprise network. The model's security value lies not in the levels themselves but in the zones and conduits defined around them. In IEC 62443 terms, a zone is a grouping of assets with common security requirements, a conduit is a logical or physical communication path between zones, and each zone is assigned a target security level from SL 0 to SL 4 that reflects the capability of the adversary it must resist, from casual misuse to a well-resourced, motivated attacker using ICS-specific skills (International Society of Automation, 2024; International Electrotechnical Commission, 2023; Piggin, 2013). Conduits are where controls are concentrated: firewalls, data diodes, protocol-aware inspection, and brokered access through the IDMZ.

Table 2: Purdue Levels, Zones, Representative Assets, and Security Emphasis

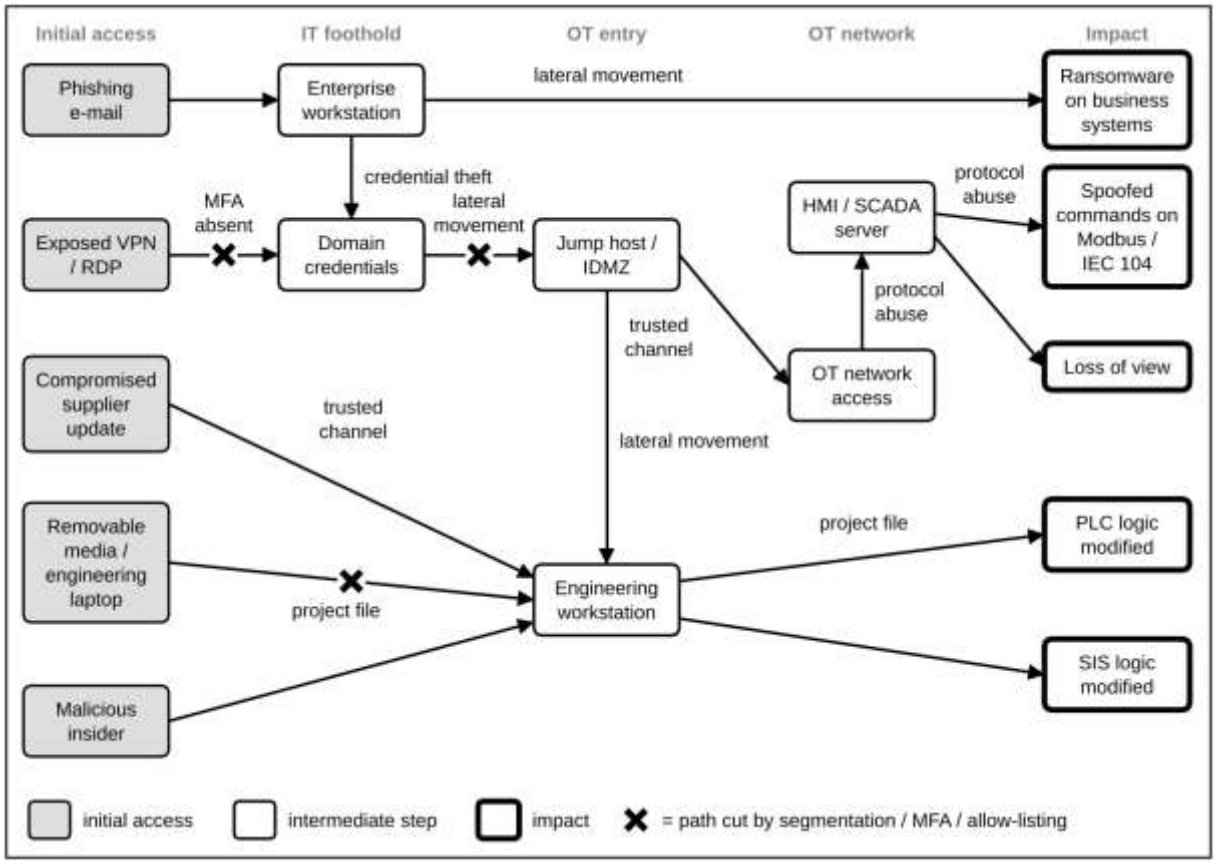
Purdue Level	Zone	Representative Assets	Security Emphasis	Relevant Guidance
Level 5	Enterprise network	ERP, e-mail, internet gateways, cloud services	Identity, perimeter, phishing defence	NIST SP 800-53; CSF 2.0
Level 4	Site business planning and logistics	Site IT, scheduling, reporting	Segmentation from OT, monitoring	NIST SP 800-82 Rev. 3 §5
Level 3.5	Industrial DMZ	Jump hosts, patch and antivirus relays, replicated historian, data diodes	Brokered conduits; no direct Level 4 to Level 3 traffic	IEC 62443-3-2 zones and conduits
Level 3	Site operations and control	Historians, engineering workstations, domain services, backups	Hardening, change control, privileged access	IEC 62443-3-3; CISA CPG
Level 2	Supervisory control	HMI, SCADA servers, alarm servers	Application allow-listing, protocol monitoring	NIST SP 800-82 Rev. 3 §6
Level 1	Basic control	PLCs, RTUs, DCS controllers, SIS	Logic integrity, physical access, SIS isolation	IEC 62443-4-2; IEC 61511
Level 0	Physical process	Sensors, actuators, drives, valves	Physical security, safety interlocks	IEC 61511; API 1164

Three design rules follow from the model and recur in every framework reviewed here. First, no direct traffic between Level 4 and Level 3: every flow crosses the IDMZ through a brokered service, so that compromise of the enterprise network does not yield a route into operations (Stouffer et al., 2023; Cybersecurity and Infrastructure Security Agency, 2023). Second, the safety instrumented system is placed in its own zone with the most restrictive conduits, ideally with no routable connection to the basic control network except through engineered interfaces, because an attacker who reaches the SIS can disable the last layer of protection (International Electrotechnical Commission, 2016; Johnson et al., 2017; Dragos, 2017a). Third, engineering workstations and remote-access paths are treated as high-value conduits in their own right, with multi-factor authentication, privileged access management, and session monitoring, since they carry the credentials and tools that change controller behaviour (Cybersecurity and Infrastructure Security Agency & National Security Agency, 2020; Rose et al., 2020). The model has limits that practitioners should recognise. It was conceived before cloud services, industrial Internet of Things devices, and vendor-managed equipment, each of which creates flows that cut across levels; modern interpretations treat the levels as a logical rather than a strictly physical hierarchy and use zero trust principles, identity-centric access control with continuous verification, to govern flows that the hierarchy cannot (Rose et al., 2020; Buck et al., 2021; Dhirani et al., 2021). In oil and gas, the geographic dispersion of pipeline RTUs and wellhead controllers over wide-area and cellular links means that Levels 1 and 2 are often separated by public or third-party networks, and the conduits across those networks require the same scrutiny as the IDMZ (Stergiopoulos et al., 2020; American Petroleum Institute, 2021). Nonetheless, the Purdue structure remains the most effective single mechanism for reducing lateral movement, and every case study in this paper involved a failure or absence of the segmentation it prescribes.

V. THREAT LANDSCAPE

Major threats include ransomware, insider threats, nation-state actors, supply-chain compromise, credential theft, insecure remote access, and exploitation of industrial protocols. Figure 5 presents the landscape as an attack graph, in which initial-access vectors lead through enterprise and OT footholds to the impacts an adversary can achieve, and marks the edges that the controls proposed in Section XI are designed to cut; Table 3 summarises each threat category with its typical vector, representative evidence, and primary OT impact.

Figure 5: Attack Graph of ICS Intrusion Paths and Control Cut-Points



Ransomware is the most frequent cause of operational disruption in the sector today. Criminal groups operating ransomware-as-a-service target enterprise networks through phishing, exposed remote services, and purchased credentials, encrypt business systems, and exfiltrate data for extortion; the control systems are usually not touched, but operations stop because business systems have become operational dependencies or because operators cannot be sure the intrusion has not spread (Oz et al., 2022; Cybersecurity and Infrastructure Security Agency, 2021a; Beerman et al., 2023). Colonial Pipeline is the canonical case, analysed in Section VIII. The structural lesson is that the boundary between IT and OT, if it is not engineered and monitored, is a boundary in name only.

Nation-state actors are responsible for every known instance of malware purpose-built to manipulate control systems. Stuxnet modified controller logic to damage centrifuges while feeding operators false readings (Falliere et al., 2011; Langner, 2011); Industroyer contained modules speaking the IEC 60870-5-104, IEC 61850, and OPC DA protocols used in electricity substations and was used to cause an outage in Kyiv in December 2016 (Cherepanov, 2017; Dragos, 2017b); and Triton targeted the Triconex safety controllers at a petrochemical facility (Johnson et al., 2017; Dragos, 2017a; Cybersecurity and Infrastructure Security Agency, 2022). These campaigns required long-term access, reconnaissance of the target process, and ICS-specific engineering, which is why their frequency is low and their potential consequence severe; the evolution of ICS attacks toward more capable and more disruptive tooling has been documented in threat-intelligence retrospectives (Slowik, 2019; Hemsley & Fisher, 2018).

Insider threats arise from employees, contractors, and vendors with legitimate access who misuse it,

whether maliciously or negligently. The CERT case base and subsequent taxonomies describe sabotage, fraud, and theft by insiders, and show that technical indicators are often preceded by behavioural precursors that organisations fail to act upon (Cappelli et al., 2012; Homoliak et al., 2019; Greitzer et al., 2012). In ICS, the insider risk is amplified by the concentration of privilege in engineering roles and by shared accounts on controllers and HMIs, which make attribution difficult and revocation slow (Stouffer et al., 2023; Knowles et al., 2015).

Supply-chain compromise reaches the control network through trusted channels. The SolarWinds intrusion of 2020 demonstrated that a trojanised software update can deliver a persistent foothold to thousands of organisations simultaneously, including critical infrastructure operators (Cybersecurity and Infrastructure Security Agency, 2021b); in ICS, the equivalent channels are vendor remote-support connections, integrator laptops, firmware updates, and engineering project files, the last of which was Stuxnet's propagation path into the target (Falliere et al., 2011; Boyens et al., 2022). Supply chain cyber risk has been reviewed as a management problem whose mitigation depends on contractual, procedural, and technical controls together (Ghadge et al., 2020; Boyes, 2015).

Credential theft and insecure remote access are the vectors through which most of the above threats operate. Reused passwords, the absence of multi-factor authentication on VPN and remote-desktop services, and remote-access tools installed on OT hosts have featured in Colonial Pipeline, in the Oldsmar water-treatment intrusion, where an attacker used a remote-access tool to raise the sodium hydroxide setpoint before an operator intervened, and in the joint CISA and NSA warning on exposure of OT assets to the internet (Cybersecurity and Infrastructure Security Agency, 2021a; Cybersecurity and Infrastructure Security Agency, 2021c; Cybersecurity and Infrastructure Security Agency & National Security Agency, 2020). Exploitation of industrial protocols is the final category: because Modbus, DNP3, IEC 104, and OPC commonly lack authentication, an adversary who reaches the control network can issue commands, spoof measurements, or deny service without exploiting any software vulnerability, as Industroyer did and as the PLC-security research literature has repeatedly shown (Cherepanov, 2017; Ghaleb et al., 2018; Fovino et al., 2010; Garcia et al., 2017).

Table 3: Threat Landscape Summary: Categories, Vectors, Evidence, and OT Impact

Threat Category	Typical Vector	Representative Incident or Evidence	Primary OT Impact
Ransomware and IT–OT spillover	Phishing, exposed remote services, credential reuse	Colonial Pipeline, 2021 (DarkSide)	Precautionary or forced shutdown; loss of business systems supporting operations
Nation-state ICS malware	Supplier laptops, removable media, long-term intrusion	Stuxnet, 2010; Industroyer, 2016; Triton, 2017	Equipment damage; loss of control; safety-system compromise
Insider threat	Legitimate credentials, physical access, engineering tools	Documented in CERT insider-threat case studies	Unauthorised logic or setpoint change; sabotage; data theft
Supply-chain compromise	Trojanised software updates, compromised integrators	SolarWinds, 2020 (CISA AA20-352A)	Trusted-channel access into OT; persistent foothold
Credential theft and reuse	Password reuse, absence of MFA, shared accounts	Colonial Pipeline VPN account; Oldsmar remote-access tool, 2021	Remote manipulation of process parameters
Insecure remote access	Vendor VPNs, remote-desktop tools, cellular modems	CISA/NSA Alert AA20-205A	Direct access to HMIs and controllers
Industrial-protocol exploitation	Unauthenticated Modbus, DNP3, IEC 104, OPC commands	Industroyer protocol modules; research on PLC payloads	Spoofed commands; loss of view; process manipulation

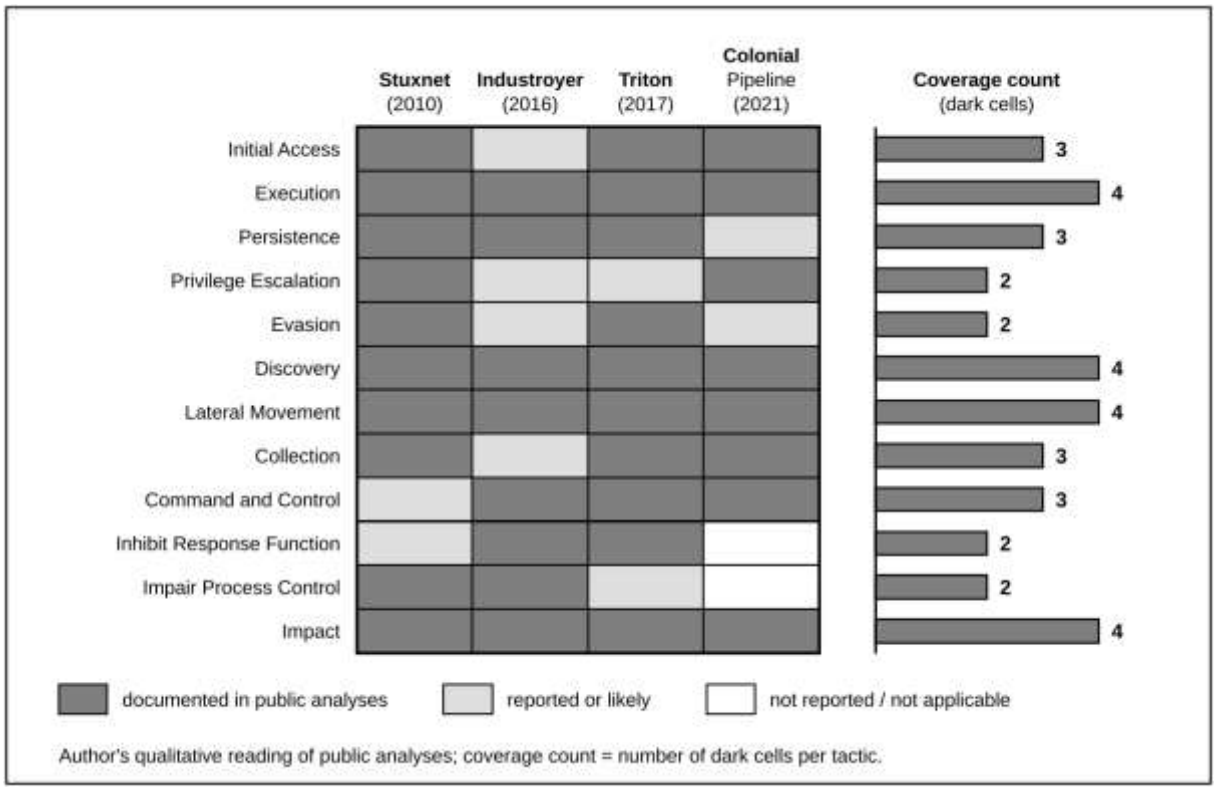
Two cross-cutting observations frame the risk assessment that follows. First, the consequence of an ICS attack is determined less by the sophistication of the intrusion than by what the adversary can reach: a ransomware operator who reaches an engineering workstation can do as much damage as a nation-state, which is why segmentation and privileged-access control dominate the recommended

architecture (McLaughlin et al., 2016; Stouffer et al., 2023). Second, the threats interact. Insider access, supply-chain channels, and stolen credentials are often the means by which an external actor obtains the foothold from which protocol exploitation or logic manipulation proceeds; the risk register therefore treats them as scenarios rather than as independent categories (Assante & Lee, 2015; Nicholson et al., 2012).

VI. MITRE ATT&CK FOR ICS ANALYSIS

The ATT&CK framework provides a structured view of adversary behavior including Initial Access, Execution, Persistence, Discovery, Lateral Movement, Collection, Command and Control, and Impact. The ICS matrix, released by MITRE in 2020, adapts the enterprise knowledge base to control systems by adding tactics that have no enterprise analogue, Inhibit Response Function and Impair Process Control, and by defining techniques in terms of the assets of the Purdue model, from engineering workstations and HMIs to controllers and safety systems (Alexander et al., 2020; Strom et al., 2018). Its purpose is to let defenders describe observed adversary behaviour in a common vocabulary, map detections and controls to that behaviour, and identify coverage gaps. Figure 6 maps four landmark incidents onto the twelve tactics as a coverage matrix, shaded by whether public analyses document each tactic, with a count of fully documented tactics per row; Table 4 lists each tactic's objective, representative techniques, and case mapping.

Figure 6: ATT&CK for ICS Tactic Coverage Across Four Landmark Incidents



The chain begins with Initial Access, whose ICS techniques include spearphishing attachments, exploitation of remote services, replication through removable media, supply-chain compromise, and the use of engineering workstations as an entry point; all of the cases studied here entered through one of these routes (Alexander et al., 2020; Falliere et al., 2011; Johnson et al., 2017). Execution and Persistence cover the running of adversary code and its survival across restarts, including the modification of controller programs and project files, which Stuxnet used to persist inside the engineering environment. Privilege Escalation and Evasion include exploitation for privilege and the rootkit and masquerading techniques by which Stuxnet concealed its presence from operators and engineers (Langner, 2011; T. M. Chen & Abu-Nimeh, 2011). Discovery, Lateral Movement, and Collection describe how adversaries learn the environment, move from IT into OT and between OT hosts, and gather the process and configuration information that a physical attack requires;

Industroyer's reconnaissance of substation networks and Triton's collection of safety-controller configuration are examples (Cherepanov, 2017; Dragos, 2017a). Command and Control covers communication with compromised systems, often over commonly used ports to blend with legitimate traffic.

The ICS-specific tactics are where the knowledge base is most valuable. Inhibit Response Function groups techniques that prevent safety and protection mechanisms from responding, including manipulation of safety logic, alarm suppression, and denial of service against controllers; Triton is its defining case, since the objective of modifying the safety controller's logic was to remove the plant's ability to shut down safely (Johnson et al., 2017; Alexander et al., 2020). Impair Process Control groups techniques that manipulate the process itself, including parameter modification, unauthorised command messages, and spoofed reporting messages; Stuxnet's manipulation of centrifuge speeds and Industroyer's breaker commands are the canonical examples (Langner, 2011; Dragos, 2017b). Impact describes the mission effect: loss of view, loss of control, damage to property, loss of safety, and loss of productivity and revenue, the last of which is the effect of ransomware even when no ICS technique is used (Cybersecurity and Infrastructure Security Agency, 2021a).

Table 4: MITRE ATT&CK for ICS Tactics, Representative Techniques, and Case Mapping

ATT&CK for ICS Tactic	Adversary Objective	Representative Techniques (examples)	Case Mapping
Initial Access	Gain a foothold in the ICS environment	Spearphishing attachment; exploitation of remote services; replication through removable media; supply-chain compromise	Stuxnet; Triton; Colonial Pipeline
Execution	Run adversary code or commands	Command-line interface; scripting; modify controller tasking	Triton; Industroyer
Persistence	Maintain access across restarts	Valid accounts; modify program; project file infection	Stuxnet; Triton
Privilege Escalation	Obtain higher-level permissions	Exploitation for privilege escalation	Stuxnet
Evasion	Avoid detection	Masquerading; rootkit; indicator removal	Stuxnet rootkit; Triton
Discovery	Learn the environment	Network sniffing; remote system discovery; I/O module discovery	Industroyer; Triton
Lateral Movement	Move between IT and OT hosts	Remote services; valid accounts; lateral tool transfer	All three malware cases
Collection	Gather process and configuration data	Screen capture; point and tag identification; program upload	Stuxnet; Triton
Command and Control	Communicate with compromised systems	Commonly used ports; connection proxy	Industroyer; Triton
Inhibit Response Function	Prevent safety and protection functions	Modify alarm settings; denial of service; manipulate safety logic	Triton
Impair Process Control	Manipulate the physical process	Modify parameter; unauthorized command message; spoof reporting message	Stuxnet; Industroyer
Impact	Achieve the mission effect	Loss of control; loss of view; damage to property; loss of safety	Stuxnet; Industroyer; Triton

Three analytical uses of the matrix follow. First, it links threat intelligence to defence: when a new campaign is reported, its techniques can be mapped and the organisation's detections and controls checked for coverage (Tounsi & Rais, 2018; Assante & Lee, 2015). Second, it structures detection engineering: OT network security monitoring, protocol-aware anomaly detection, and host monitoring on engineering workstations each cover particular tactics, and the matrix shows where coverage is thin, typically in Inhibit Response Function and Impair Process Control, which require process-aware detection rather than network signatures (Giraldo et al., 2018; Hadžiosmanović et al., 2014; Urbina et al., 2016). Third, it supports the risk assessment in Section VII by making explicit which tactics each risk scenario would involve, so that the controls proposed in Section XI can be mapped to the tactics they

mitigate. The coverage matrix in Figure 6 also reveals the common structure of ICS attacks that the ICS cyber kill chain formalised: a first stage of enterprise intrusion and reconnaissance, followed by a second stage of ICS-specific development, testing, and delivery, which is why defences that detect the first stage, such as monitoring of IT-to-OT conduits and of engineering workstations, offer the longest warning time (Assante & Lee, 2015; Hutchins et al., 2011).

VII. RISK ASSESSMENT

Risk assessment was conducted using qualitative likelihood and impact metrics. Ransomware, SIS compromise, and remote-access exploitation were identified as high-risk scenarios. This section describes the method, presents the scales and the resulting register, and discusses the limitations of the approach.

Method

The assessment follows the structure of NIST SP 800-30, in which risk is a function of the likelihood that a threat event occurs and the impact if it does, and of the IEC 62443-3-2 zone-and-conduit assessment, in which scenarios are defined against the architecture of Sections III and IV (Joint Task Force Transformation Initiative, 2012; International Society of Automation, 2024; Kure et al., 2018). Risk scenarios were derived from the threat landscape of Section V and expressed in ATT&CK for ICS terms, so that each scenario corresponds to a pathway through the tactic chain rather than to a threat category in the abstract (Alexander et al., 2020; Cherdantseva et al., 2016). Likelihood and impact were each rated on five-point ordinal scales, defined in Table 5, with likelihood anchored to a three-year horizon and to evidence of targeting in the sector, and impact anchored to operational, safety, and environmental consequence rather than to data loss, consistent with the inverted priority ordering of ICS security (Stouffer et al., 2023; Cárdenas et al., 2011). The risk score is the product of the two ratings, and priority bands were set at low (1–4), moderate (5–9), high (10–14), and critical (15–25). The ratings are expert judgements by the author, informed by the incident evidence cited for each scenario and by the sector surveys reviewed in Section II; they are not measurements, and their purpose is prioritisation rather than quantification (Stergiopoulos et al., 2020; Miller et al., 2021).

Table 5: Likelihood and Impact Rating Scales Used in the Risk Assessment

Score	Likelihood (within three years)	Impact on Operations, Safety and Environment
1	Rare: no credible pathway; strong compensating controls	Negligible: no process effect; contained within IT
2	Unlikely: pathway exists but requires multiple failures	Minor: brief loss of view; no production loss
3	Possible: pathway demonstrated in peer organisations or public incidents	Moderate: short production interruption; no safety consequence
4	Likely: active targeting of the sector; controls partially effective	Major: multi-day shutdown; regulatory reporting; financial loss
5	Almost certain: observed in the sector within the period; control gaps known	Severe: safety-system compromise, equipment damage, environmental release or loss of life

Risk Register and Prioritisation

Table 6 presents the register of eight scenarios, and Figure 8 plots them against likelihood and impact with iso-risk contours, the area of each marker proportional to its risk score. Three scenarios fall in the critical band. R1, ransomware entering through the enterprise network and forcing an OT shutdown, is rated almost certain and severe: it has been observed in the sector within the period, the control gaps that enable it are widely documented, and its consequence, demonstrated at Colonial Pipeline, is a multi-day interruption of supply with national effects (Cybersecurity and Infrastructure Security Agency, 2021a; Parfomak & Jaikaran, 2021; Oz et al., 2022). R2, manipulation of PLC or safety-controller logic, is rated possible and severe: the pathway has been demonstrated by Stuxnet and Triton and in the research literature, and its consequence is equipment damage, loss of safety, or environmental release (Langner, 2011; Johnson et al., 2017; McLaughlin & McDaniel, 2012). R3, exploitation of insecure remote access to HMIs or controllers, is rated likely and major: remote-access tools and VPN accounts without multi-factor authentication are common in the sector, the Oldsmar intrusion and the

CISA/NSA warning show active exploitation, and the consequence is direct manipulation of process parameters (Cybersecurity and Infrastructure Security Agency, 2021c; Cybersecurity and Infrastructure Security Agency & National Security Agency, 2020).

Table 6: Qualitative Risk Register for Oil and Gas ICS

Code	Risk Scenario	Likelihood	Impact	Risk Score	Priority	Principal Evidence
R1	Ransomware entering through IT and forcing OT shutdown	5	5	25	Critical	Colonial Pipeline, 2021; CISA AA21-131A
R2	Manipulation of PLC or safety-controller logic	3	5	15	Critical	Stuxnet; Triton; ATT&CK Impair Process Control
R3	Exploitation of insecure remote access to HMI or controllers	4	4	16	Critical	Oldsmar, 2021; CISA/NSA AA20-205A
R4	Supply-chain or integrator compromise	3	4	12	High	SolarWinds, 2020; NIST SP 800-161
R5	Insider misuse of engineering access	3	4	12	High	CERT insider-threat case base
R6	Credential theft and reuse without MFA	4	3	12	High	Colonial Pipeline VPN account
R7	Industrial-protocol exploitation on the control network	3	3	9	Moderate	Industroyer protocol modules; PLC security research
R8	Malware via removable media or engineering laptops	2	3	6	Moderate	Stuxnet propagation

Three scenarios fall in the high band. R4, supply-chain or integrator compromise, and R5, insider misuse of engineering access, are both rated possible and major, reflecting demonstrated pathways with consequences that depend on what the actor reaches (Cybersecurity and Infrastructure Security Agency, 2021b; Cappelli et al., 2012; Boyens et al., 2022). R6, credential theft and reuse without multi-factor authentication, is rated likely but moderate in direct impact, because its consequence is realised through the other scenarios it enables; it is nonetheless a priority because it is the most tractable to mitigate (Cybersecurity and Infrastructure Security Agency, 2021a; Cybersecurity and Infrastructure Security Agency, 2023). R7, industrial-protocol exploitation, and R8, malware via removable media or engineering laptops, fall in the moderate band: both are demonstrated, but the first requires prior access to the control network and the second has become less likely as port control and engineering-laptop hygiene have improved since Stuxnet (Cherepanov, 2017; Falliere et al., 2011).

Figure 7: ICS Risk Prioritization

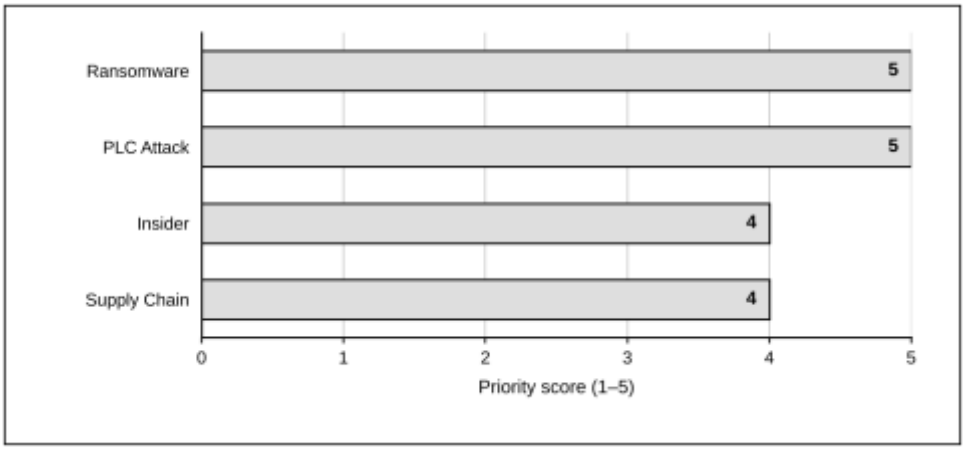
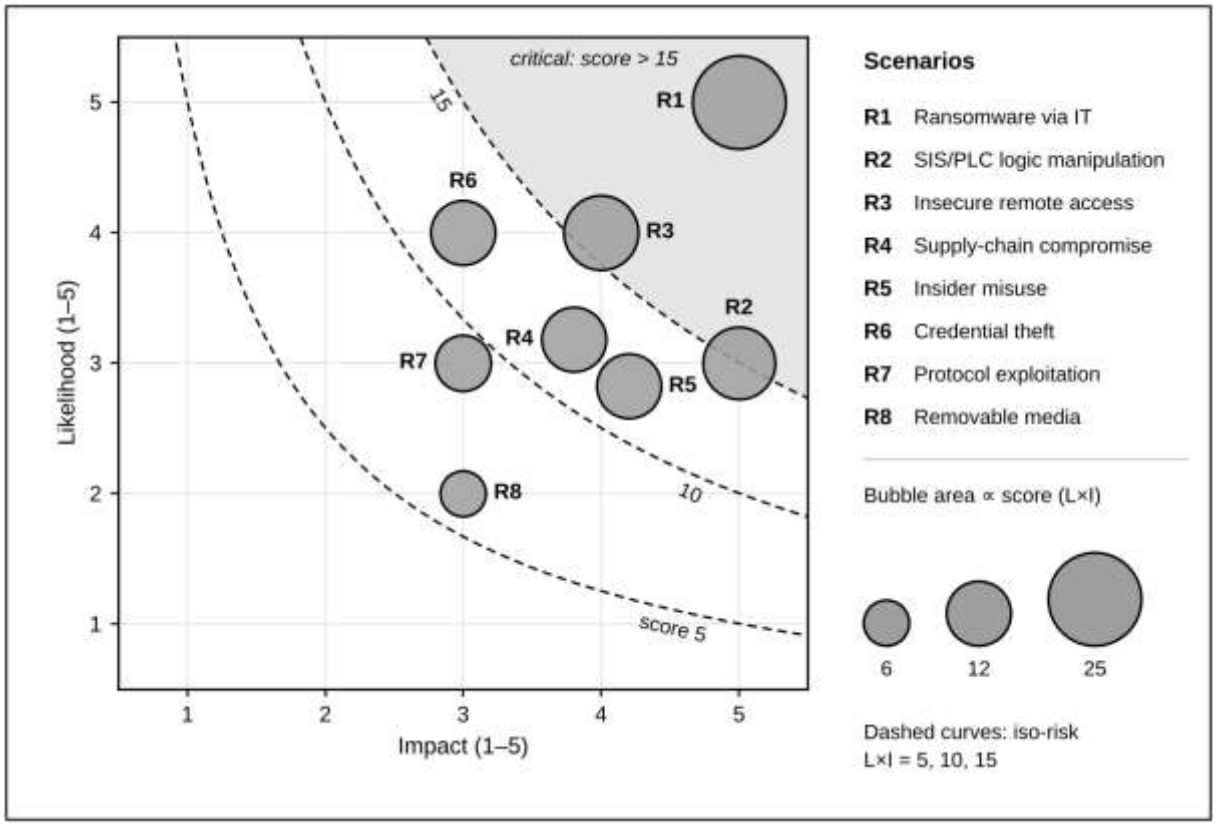


Figure 7 summarises the prioritisation at the level of the four threat families that the defense-in-depth architecture addresses most directly: ransomware and attacks on PLCs and safety controllers receive

the highest priority score of 5, and insider and supply-chain threats a score of 4. The ordering reflects the combination of likelihood and consequence in Table 6 rather than frequency alone; supply-chain and insider threats are less frequent than credential theft but reach deeper into the architecture when they occur.

Figure 8: Likelihood–Impact Bubble Chart of the Risk Scenarios with Iso-Risk Contours



Limitations of the Assessment

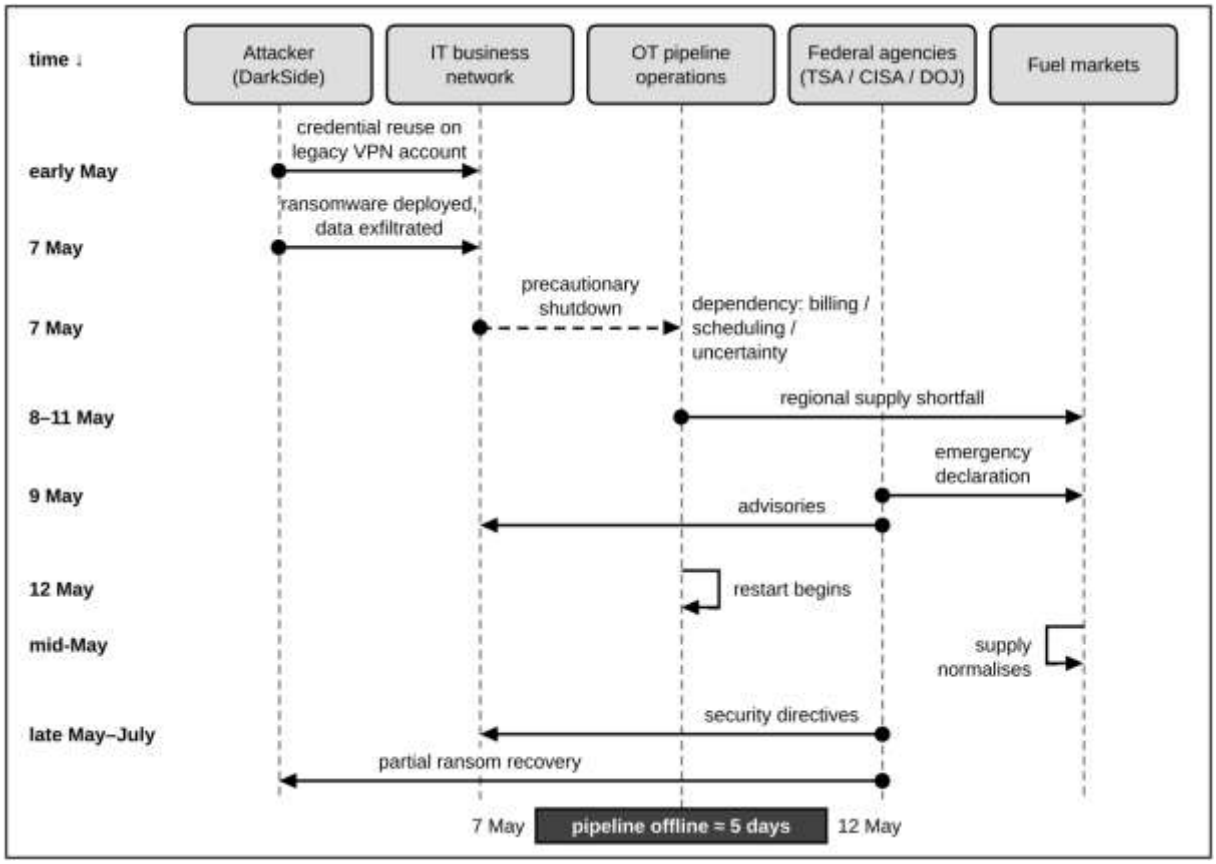
Qualitative risk matrices are widely used in industry and are required by several of the frameworks reviewed here, but their limitations are well known. Ordinal scales cannot be multiplied in any strict sense, the product score compresses distinct combinations of likelihood and impact into the same band, and matrices can rank risks inconsistently when the underlying quantities are uncertain (Cox, 2008; Hubbard & Seiersen, 2016). The classical definition of risk as a set of scenarios, likelihoods, and consequences, and its modern extensions that treat uncertainty and knowledge strength explicitly, point to the improvements that a more mature programme should pursue: scenario-based quantification with ranges, explicit statements of the evidence behind each rating, and periodic recalibration against incident data (Kaplan & Garrick, 1981; Aven, 2016; International Organization for Standardization, 2018). The register presented here should accordingly be read as a prioritisation for the architecture that follows, grounded in cited evidence, and as a template that an operator would populate with site-specific likelihoods, asset criticality, and safety consequence analysis under IEC 61511 and IEC 62443-3-2 (International Electrotechnical Commission, 2016; International Society of Automation, 2024; Kriaa et al., 2015).

VIII. COLONIAL PIPELINE CASE STUDY

The 2021 Colonial Pipeline incident demonstrated the operational impact of ransomware affecting business systems and highlighted dependencies between IT and OT environments. Colonial operates one of the largest refined-products pipeline systems in the United States, carrying gasoline, diesel, and jet fuel from Gulf Coast refineries to the East Coast; its shutdown produced fuel shortages and emergency federal measures within days (Parfomak & Jaikaran, 2021; Beerman et al., 2023). Figure 9 presents the incident as a sequence diagram across the attacker, the IT business network, OT pipeline operations, federal agencies, and fuel markets, with the five-day outage marked, and shows the IT–OT

dependency that turned an IT intrusion into an operational outage.

Figure 9: Colonial Pipeline 2021 Sequence Diagram: From IT Compromise to Operational Shutdown



According to the public record, the DarkSide ransomware group gained access to Colonial's IT network through a legacy virtual private network account that was no longer in active use and was not protected by multi-factor authentication, using a password that had apparently been exposed elsewhere; the ransomware was deployed on 7 May 2021, encrypting business systems and exfiltrating data, and the company shut down pipeline operations the same day as a precaution, restarting on 12 May after about five days (Parfomak & Jaikaran, 2021; Cybersecurity and Infrastructure Security Agency, 2021a; Beerman et al., 2023). The precise entry details come from company testimony and press reporting summarised in those sources, and the account given here is limited to what they state. The company reportedly paid a ransom, part of which was later recovered by the Department of Justice; the ransom amount and the recovery are reported in the Congressional Research Service brief and the review article and are not independently verified here (Parfomak & Jaikaran, 2021; Beerman et al., 2023).

Three features of the incident matter for this paper. First, the control systems were not reported to have been compromised; the pipeline stopped because the business systems on which operations depend, including billing and scheduling, were unavailable and because the operator could not immediately establish that the intrusion had not reached OT (Parfomak & Jaikaran, 2021; Beerman et al., 2023). This is the IT–OT dependency that the Purdue model and IEC 62443 zone design are meant to make explicit: if operations cannot continue without business systems, then those systems are operationally critical and must be protected and made recoverable accordingly, or operations must be designed to run without them for a defined period (Stouffer et al., 2023; Bartock et al., 2016). Second, the initial-access vector, a dormant account without multi-factor authentication, is the most common and most preventable weakness in the sector, and it maps directly to scenarios R3 and R6 of the register and to the first performance goals in CISA's cross-sector list (Cybersecurity and Infrastructure Security Agency, 2023; Cybersecurity and Infrastructure Security Agency & National Security Agency, 2020). Third, the incident changed the regulatory landscape. GAO had reported in 2018 on significant

weaknesses in TSA's pipeline security program management, and within weeks of the incident TSA issued its first mandatory security directives for pipeline owners and operators, requiring incident reporting, designation of a cybersecurity coordinator, and vulnerability assessment, followed by a second directive specifying mitigation measures; GAO's 2021 review documents these steps and the remaining gaps (U.S. Government Accountability Office, 2018; U.S. Government Accountability Office, 2021). The American Petroleum Institute published the third edition of Standard 1164 in August 2021, extending its scope from SCADA to all pipeline control systems and aligning it with IEC 62443 and the NIST Cybersecurity Framework (American Petroleum Institute, 2021).

The lessons map directly onto the architecture of Section XI. Segment IT from OT with an engineered IDMZ so that an IT compromise cannot reach controllers and so that the operator can establish that it has not. Enforce multi-factor authentication on every remote-access path and retire unused accounts. Design and rehearse the ability to operate the pipeline, at least in a degraded mode, independently of business systems, and maintain tested backups and recovery procedures for both environments (Cichonski et al., 2012; Bartock et al., 2016; Cybersecurity and Infrastructure Security Agency, 2021a). The incident also illustrates the interdependency literature's central claim: a disruption in one infrastructure propagates to others, in this case from a pipeline to fuel distribution, transport, and aviation, so that the consequence of an OT outage is a societal rather than a corporate matter (Rinaldi et al., 2001; Ouyang, 2014; Alcaraz & Zeadally, 2015).

IX. TRITON/TRISIS CASE STUDY

Triton targeted Safety Instrumented Systems. The malware attempted to manipulate safety controllers, representing one of the most significant threats to industrial safety. Discovered in 2017 at a petrochemical facility in the Middle East, Triton, also called Trisis, was a framework designed to interact with Schneider Electric Triconex safety controllers; it was deployed from an engineering workstation on the safety network after the attackers had gained access to the plant's IT network and moved into the OT environment (Johnson et al., 2017; Dragos, 2017a; Cybersecurity and Infrastructure Security Agency, 2022). Figure 10 presents the incident as a process-safety bow-tie diagram: the threats and attack path on the left, the compromise of the safety controller's logic as the top event, the consequences on the right, and the preventive and mitigative barriers between them, marking the barriers that failed and the one that held; Table 7 compares Triton with Stuxnet, Industroyer, and Colonial Pipeline.

A safety instrumented system is the engineered layer of protection that brings a process to a safe state when sensors detect a hazardous condition, such as high pressure or loss of flame; it is designed to a safety integrity level under IEC 61511 and sits above basic process control and operator response in the layers-of-protection model, with physical relief devices as the final layer (International Electrotechnical Commission, 2016; Leveson, 2012; Kriaa et al., 2015). Its controllers are computers, and their logic is programmed from engineering workstations. The Triton attackers deployed a tool that implemented the proprietary protocol used to communicate with the Triconex controllers and attempted to modify the controller's logic; according to the incident responders, the attempt caused the controllers to enter a failed-safe state, shutting down the process, which led to the investigation that discovered the malware (Johnson et al., 2017; Dragos, 2017a). The responders assessed that the attackers' objective was to develop the capability to cause physical damage, since a safety system that no longer trips removes the protection on which the plant's hazard analysis depends; the facility was fortunate that an error in the attack tool, rather than a successful modification, ended the campaign (Johnson et al., 2017; Cybersecurity and Infrastructure Security Agency, 2022).

Triton's significance is threefold. It was the first publicly known malware to target safety systems specifically, moving the threat from loss of production to loss of life (Dragos, 2017a; Slowik, 2019). It demonstrated that the safety network, which many operators had treated as isolated, was reachable from the IT network through the same lateral-movement techniques used in enterprise intrusions, and that the engineering workstation was the decisive pivot (Johnson et al., 2017; Alexander et al., 2020). And it exposed a gap between the safety and security disciplines: the safety analysis assumed that the SIS could fail only through random hardware faults or systematic design errors, not through deliberate logic modification, an assumption that IEC 61511 has since amended by requiring a security risk assessment of safety systems (International Electrotechnical Commission, 2016; Young & Leveson,

2014; Kriaa et al., 2015).

Figure 10: Bow-Tie Analysis of the Triton Attack on a Safety Instrumented System

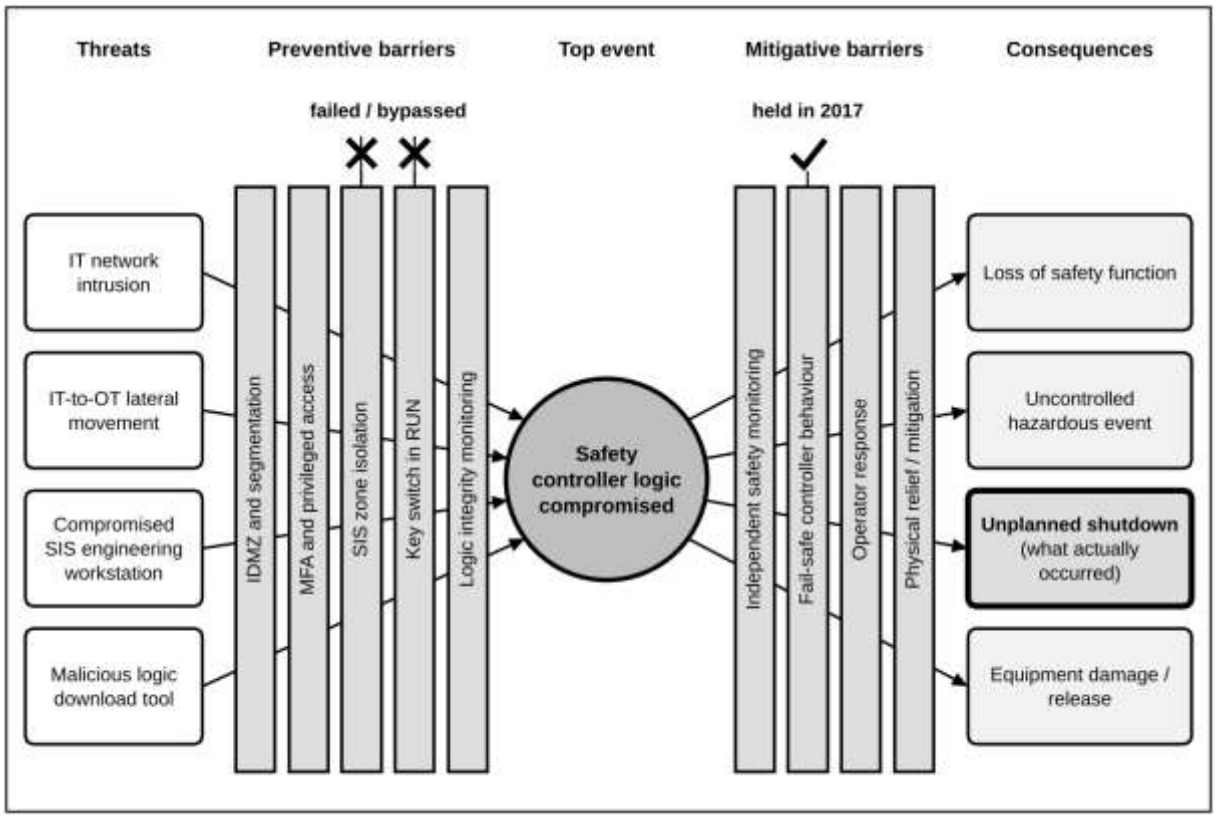


Table 7: Comparison of Four Landmark ICS Incidents

Attribute	Stuxnet (2010)	Industroyer (2016)	Triton/Trisis (2017)	Colonial Pipeline (2021)
Target	Siemens PLCs controlling centrifuges	Electricity substation control (Ukraine)	Triconex safety controllers at a petrochemical plant	IT systems of a U.S. fuel pipeline operator
Actor type (as reported)	Nation-state	Nation-state	Nation-state	Criminal ransomware group (DarkSide)
Initial access	Removable media; supplier laptops	IT network compromise	IT-to-OT pivot; engineering workstation	Legacy VPN account without MFA
ICS-specific capability	PLC logic modification with rootkit	Modules for IEC 104, IEC 61850, OPC DA	Safety-controller protocol implementation	None (IT ransomware)
Physical or operational effect	Centrifuge damage	Approximately one-hour outage in Kyiv region	Controllers failed safe; plant shutdown	Precautionary pipeline shutdown of about five days
Detection	Months after deployment, by security researchers	Post-outage forensic analysis	SIS fault investigation	Operator discovery of ransomware
Principal lesson	Air gaps are porous; logic integrity matters	Protocol abuse needs monitoring	SIS must be isolated and monitored	IT–OT dependency and MFA on all remote access

The lessons are specific. The SIS must be placed in its own zone with no routable path from the basic control network except through engineered, monitored interfaces, and the physical key switch that controls whether the controller accepts program changes must be left in the run position except during authorised maintenance, with the change logged (International Society of Automation, 2024; Cybersecurity and Infrastructure Security Agency, 2022; Stouffer et al., 2023). The SIS engineering workstation must be hardened, dedicated, and monitored, with privileged access management and application allow-listing, because it is the only host from which logic can be changed (Powell et al., 2022; Cybersecurity and Infrastructure Security Agency, 2023). Monitoring of the safety network should be independent of the control network's monitoring, so that an adversary who has

compromised the control network cannot blind the safety network's defenders (Hadžiosmanović et al., 2014; Giraldo et al., 2018). Finally, safety and security assessments should be conducted jointly: a hazard analysis that identifies the scenarios the SIS protects against is also a list of the outcomes an attacker would seek, and the layers-of-protection analysis should treat deliberate attack as an initiating event (Young & Leveson, 2014; Leveson, 2012; Kriaa et al., 2015).

Table 7 places Triton among the other landmark incidents. Stuxnet and Triton share the pattern of ICS-specific engineering delivered through engineering workstations; Industroyer shares with Triton the implementation of industrial protocols as attack modules; and Colonial Pipeline differs in kind, involving no ICS technique at all, yet produced the largest operational effect of the four. The comparison supports the central argument of the risk assessment: the architecture must defend against both the rare, engineered attack on safety and control and the frequent, opportunistic attack on the business systems that operations depend upon (Miller et al., 2021; Hemsley & Fisher, 2018; Ding et al., 2018).

X. NIST SP 800-82 AND IEC 62443

Both frameworks advocate defense-in-depth, asset management, access control, monitoring, incident response, and lifecycle security management. They differ in origin, structure, and the way they are used, and an operator in the oil and gas sector will typically use both: NIST SP 800-82 and the Cybersecurity Framework as the programme-level structure that regulators and auditors recognise, and IEC 62443 as the engineering standard for designing zones, specifying requirements to suppliers, and certifying products (Stouffer et al., 2023; International Society of Automation, 2024; American Petroleum Institute, 2021). Table 8 presents the author's mapping of the Cybersecurity Framework functions to IEC 62443 counterparts, extended with the Govern function introduced in CSF 2.0 and with the IEC 62443 parts and foundational requirements that implement each function; Table 9 compares the two frameworks along nine dimensions.

Table 8: NIST Cybersecurity Framework to IEC 62443 Mapping

NIST CSF Function	IEC 62443 Counterpart (Author's Mapping)	Representative IEC 62443 Parts and Requirements
Govern (CSF 2.0)	Security program and policies	62443-2-1 security program requirements; roles and risk governance
Identify	Asset Inventory & Zones	62443-3-2 zone and conduit definition; asset inventory and initial risk assessment
Protect	Access Control	62443-3-3 system requirements (FR 1 identification and authentication, FR 2 use control, FR 5 restricted data flow)
Detect	Monitoring	62443-3-3 FR 6 timely response to events; audit logs and continuous monitoring
Respond	Incident Response	62443-2-1 incident handling; 62443-3-3 FR 6 response capability
Recover	Business Continuity	62443-2-1 continuity planning; 62443-3-3 FR 7 resource availability and backup

NIST SP 800-82 Revision 3 is a guidance document rather than a standard. It describes OT and its differences from IT, sets out a risk-management approach built on SP 800-30 and the Cybersecurity Framework, recommends architectures based on segmentation and the Purdue model, describes the elements of an OT security programme, and provides an overlay that tailors the SP 800-53 Revision 5 control catalogue to OT, indicating which controls apply and how they should be adapted where conventional implementations would interfere with availability or safety (Stouffer et al., 2023; Joint Task Force, 2020; Joint Task Force Transformation Initiative, 2012). Its third revision broadened the scope from ICS to OT generally, encompassing building automation, physical access control, and industrial Internet of Things devices, and incorporated lessons from the incidents of the preceding decade, including guidance on remote access, on safety systems, and on recovery (Stouffer et al., 2023; Bartock et al., 2016). The Cybersecurity Framework 2.0 provides the six-function structure, Govern, Identify, Protect, Detect, Respond, and Recover, that organisations use to describe their programme's

maturity and to communicate with executives and regulators, and its addition of Govern reflects the recognition that cybersecurity risk is an enterprise risk requiring board-level oversight (National Institute of Standards and Technology, 2024a). CISA's cross-sector performance goals distil both documents into a prioritised list of practices, with an emphasis on the controls most often missing in incidents, including multi-factor authentication, asset inventory, segmentation, logging, and incident-response planning (Cybersecurity and Infrastructure Security Agency, 2023).

The ISA/IEC 62443 series is an international consensus standard organised in four groups of parts: general concepts and terminology; policies and procedures for asset owners, including the requirements for a security programme in 62443-2-1; system-level requirements, including the zone-and-conduit risk assessment in 62443-3-2 and the system security requirements and security levels in 62443-3-3; and component-level requirements, including the secure product development lifecycle in 62443-4-1 and technical requirements for components in 62443-4-2 (International Society of Automation, 2024; International Electrotechnical Commission, 2023; Piggin, 2013). Its distinctive contributions are the formalisation of zones and conduits, the definition of security levels from SL 0 to SL 4 that specify the adversary capability a zone must resist, and seven foundational requirements, identification and authentication control, use control, system integrity, data confidentiality, restricted data flow, timely response to events, and resource availability, each with four levels of rigour. Because it addresses asset owners, integrators, and product suppliers separately, it supports procurement: an operator can specify a target security level for a zone and require suppliers to provide components certified to 62443-4-2 and developed under 62443-4-1 (International Society of Automation, 2024; Boyens et al., 2022). Reviews of standards in adjacent sectors show how national regulations reference these parts, and API Standard 1164 aligns pipeline requirements with both IEC 62443 and the NIST framework (Leszczyna, 2018; American Petroleum Institute, 2021).

Table 9: Comparison of NIST SP 800-82 Revision 3 and the ISA/IEC 62443 Series

Dimension	NIST SP 800-82 Rev. 3 (with CSF 2.0)	ISA/IEC 62443 Series
Nature	Guidance document (non-binding), U.S. federal origin	International consensus standard series (ISA/IEC)
Scope	Operational technology broadly: ICS, building automation, physical access control, IIoT	Industrial automation and control systems across asset owners, integrators and product suppliers
Structure	OT overview, risk management, architecture, security program, control baseline overlay on SP 800-53	Parts on general concepts, policies and procedures (2-x), system (3-x) and component (4-x) requirements
Risk approach	SP 800-30 style risk assessment integrated with CSF functions	62443-3-2 zone and conduit risk assessment with target security levels
Segmentation	Recommends defense-in-depth and network segmentation aligned with Purdue levels	Formal zones, conduits and security levels SL 0–4
Requirements	Tailored SP 800-53 Rev. 5 control overlay for OT	Seven foundational requirements with four levels of rigour
Lifecycle	Security program lifecycle; incident response and recovery guidance	Secure development lifecycle (4-1); component requirements (4-2); maintenance and decommissioning
Certification	No certification scheme	Product and process certification schemes available
Regulatory linkage	Referenced by TSA directives, CISA CPGs, API 1164	Referenced by API 1164, many national regulations

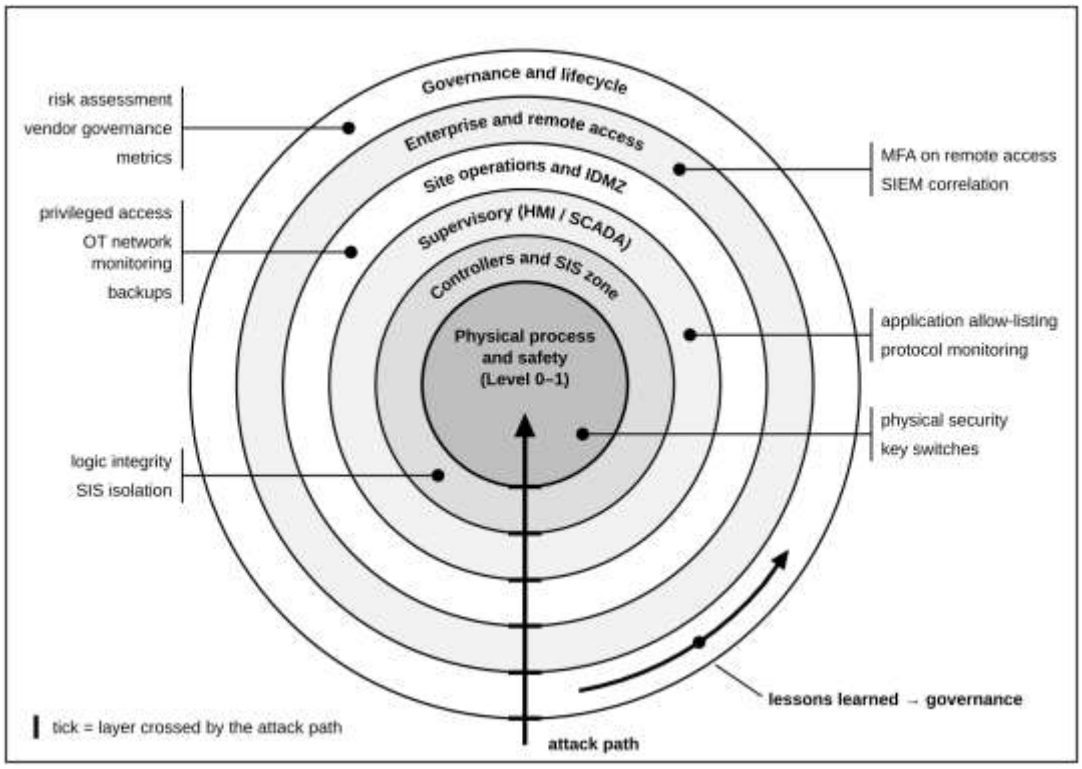
The two frameworks are complementary rather than competing. SP 800-82 and the Cybersecurity Framework describe what a programme should do and how to communicate about it; IEC 62443 describes how to engineer and certify systems that do it. Both place segmentation, access control, and monitoring at the centre, both treat the safety system as requiring special protection, and both require lifecycle management from procurement to decommissioning (Stouffer et al., 2023; International Society of Automation, 2024; International Electrotechnical Commission, 2016). The gaps lie in

operational detail: neither prescribes how to monitor industrial protocols, how to detect process-aware attacks, or how to integrate safety and security assessments, which is where the research reviewed in Section II and the architecture proposed in Section XI add value (Giraldo et al., 2018; Kriaa et al., 2015; Maglaras et al., 2018). A further gap is sectoral: the frameworks are generic, and oil and gas operators must map them to pipeline SCADA with its wide-area conduits, to process DCS with its vendor-managed systems, and to safety systems under IEC 61511, a mapping that API 1164 begins and that the architecture below continues (American Petroleum Institute, 2021; Stergiopoulos et al., 2020).

XI. PROPOSED DEFENSE-IN-DEPTH ARCHITECTURE

Recommended controls include physical security, segmentation, MFA, PAM, SIEM, OT monitoring, threat intelligence, incident response, backup strategies, and vendor governance. Figure 11 presents the defense-in-depth architecture as concentric layers around the physical process, from the controller and safety zone outward to governance and lifecycle, with the seven control families distributed across the rings and an attack path that must cross every one of them; Table 10 maps each layer's controls to Purdue levels, Cybersecurity Framework functions, IEC 62443 linkages, and the ATT&CK for ICS tactics they mitigate. The architecture is derived from the risk register of Section VII and the case-study lessons of Sections VIII and IX: each critical and high scenario is addressed by at least two layers, so that the failure of any single control does not expose the process.

Figure 11: Proposed Defense-in-Depth Architecture as Concentric Layers Around the Physical Process



The governance and risk layer is the foundation. It comprises an asset inventory covering every device in Levels 0 to 5, a risk assessment conducted by zone and conduit and revisited on a defined cycle, policies that assign ownership of OT security, vendor governance that specifies security requirements in contracts and controls vendor access, and awareness training that addresses the phishing and credential hygiene through which most intrusions begin (National Institute of Standards and Technology, 2024a; Boyens et al., 2022; Ghadge et al., 2020; Cybersecurity and Infrastructure Security Agency, 2023). Without an inventory, nothing else can be verified; without governance, segmentation decays as projects add connections. The physical security layer protects the assets that have no logical protection: control rooms, controller cabinets, and field enclosures are access-controlled, USB and console ports on controllers and workstations are blocked or monitored, and the key switches on safety

and basic controllers are kept in run mode with changes logged, a control that would have constrained both Stuxnet and Triton (Stouffer et al., 2023; Cybersecurity and Infrastructure Security Agency, 2022; Falliere et al., 2011).

The network segmentation layer implements the Purdue zones and conduits of Section IV: an IDMZ brokers every flow between enterprise and operations, firewalls and, where flows are unidirectional, data diodes enforce conduit policy, the safety instrumented system is placed in its own zone with engineered interfaces only, and pipeline wide-area conduits to RTUs are encrypted and authenticated (International Society of Automation, 2024; Stouffer et al., 2023; American Petroleum Institute, 2021). This layer directly mitigates lateral movement and command-and-control, the tactics that converted IT intrusions into OT effects in every case study. The identity and endpoint layer addresses the vectors of the critical scenarios R1, R3, and R6: multi-factor authentication on every remote-access path, with no exceptions for vendors; privileged access management that vaults, rotates, and records the use of engineering and administrative credentials; application allow-listing on HMIs, servers, and engineering workstations, which are rarely changed and therefore well suited to it; and hardened, dedicated engineering workstations for both control and safety systems (Cybersecurity and Infrastructure Security Agency & National Security Agency, 2020; Powell et al., 2022; Rose et al., 2020; Cybersecurity and Infrastructure Security Agency, 2021a).

The monitoring and detection layer provides the visibility that the frameworks require and that the case studies lacked. OT network security monitoring, deployed passively on span ports in Levels 1 to 3, builds the asset inventory, baselines normal communication, and detects new devices, new conduits, and anomalous protocol use; protocol-aware anomaly detection extends this to the content of industrial protocol messages, detecting unauthorised commands and parameter changes; integration with the enterprise SIEM correlates OT events with the IT intrusions that precede them; and threat intelligence, mapped through ATT&CK for ICS, keeps detections aligned with observed adversary behaviour (Hadžiosmanović et al., 2014; Fovino et al., 2010; Giraldo et al., 2018; Tounsi & Rais, 2018; Alexander et al., 2020). Physics-based detection, which compares the process's observed behaviour with its expected behaviour, is the research frontier for the tactics that network monitoring covers least well, Inhibit Response Function and Impair Process Control (Urbina et al., 2016; Ahmed et al., 2018; Goh et al., 2017).

Table 10: Defense-in-Depth Controls Mapped to Purdue Levels, Framework Functions, and ATT&CK for ICS Tactics

Defense Layer	Key Controls	Purdue Levels	CSF 2.0 Function	IEC 62443 Linkage	ATT&CK for ICS Tactics Mitigated
Governance and risk	Asset inventory; risk assessment; policies; vendor governance; awareness training	All	Govern, Identify	2-1; 3-2	Initial Access (supply chain, phishing)
Physical security	Control-room and cabinet access control; USB port blocking; key-switch controllers	0–2	Protect	3-3 FR 2	Initial Access (removable media); Impair Process Control
Network segmentation	Zones and conduits; IDMZ; firewalls and data diodes; SIS isolation	1–3.5	Protect	3-2; 3-3 FR 5	Lateral Movement; Command and Control
Identity and endpoint	MFA on all remote access; privileged access management; application allow-listing; hardened workstations	2–5	Protect	3-3 FR 1, FR 2, FR 3	Initial Access; Persistence; Execution
Monitoring and detection	OT network security monitoring; SIEM; protocol-aware anomaly detection; threat intelligence	1–4	Detect	3-3 FR 6	Discovery; Collection; Impair Process Control
Response and recovery	OT incident-response playbooks; tested backups of logic and configurations; manual-operation procedures	All	Respond, Recover	2-1; 3-3 FR 7	Inhibit Response Function; Impact
Lifecycle security	Secure procurement; patch and vulnerability management; change control; decommissioning	All	Govern, Protect	4-1; 4-2	Initial Access (exploitation); Persistence

The response and recovery layer turns detection into action and limits consequence. OT-specific incident-response playbooks define who may isolate a conduit or shut down a process and how safety

is maintained while they do so; tested backups of controller logic, HMI configurations, and historian data, stored offline, allow recovery after ransomware or logic manipulation; and manual-operation procedures, exercised periodically, allow the plant or pipeline to run in a degraded mode independent of business systems, the capability whose absence prolonged the Colonial Pipeline outage (Cichonski et al., 2012; Bartock et al., 2016; Parfomak & Jaikaran, 2021; Beerman et al., 2023). Resilience metrics, which measure the ability to absorb and recover from disruption rather than only to prevent it, provide the yardstick for this layer (Linkov et al., 2013; Ganin et al., 2016; Kott et al., 2021). The lifecycle security layer, finally, ensures that the other layers persist: secure procurement specifies IEC 62443-4-1 and 4-2 requirements to suppliers; patch and vulnerability management prioritises by exposure and exploitability within the constraints of production schedules, with compensating controls where patching is infeasible; change control governs every modification to logic, configuration, and network; and decommissioning removes accounts, connections, and devices that would otherwise become the dormant VPN account of the next incident (International Society of Automation, 2024; Boyens et al., 2022; Cybersecurity and Infrastructure Security Agency, 2021a; Knowles et al., 2015).

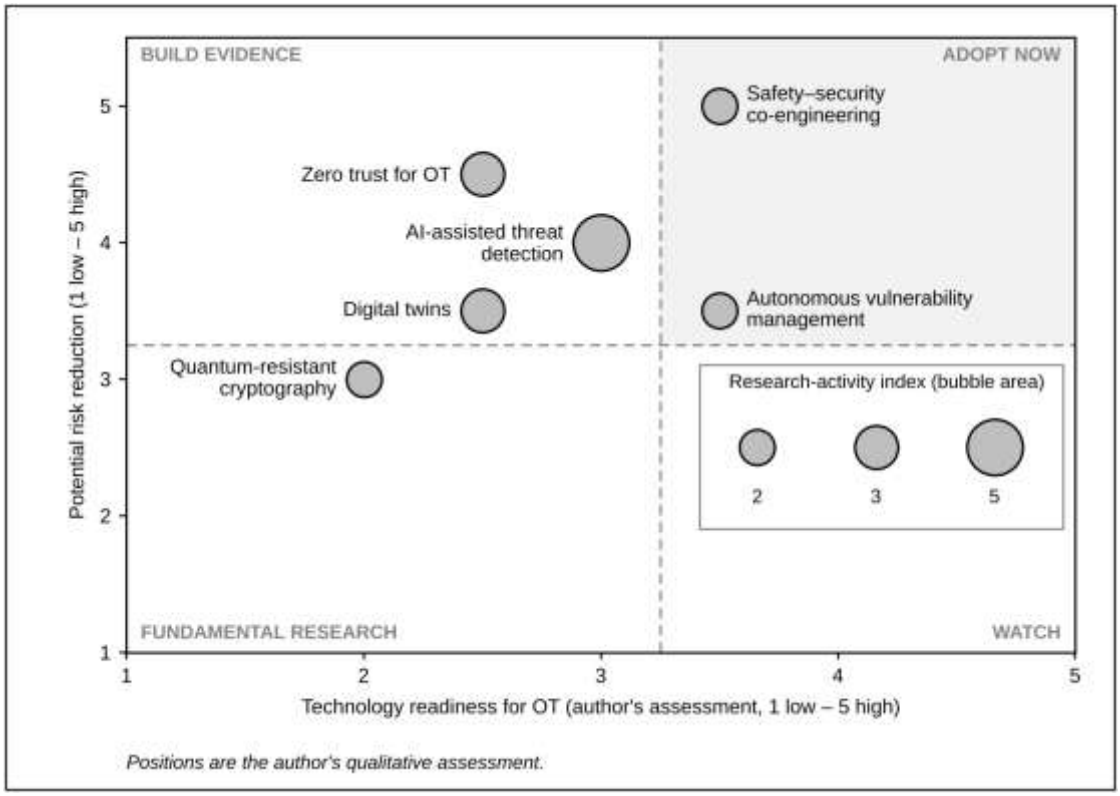
Implementation should be measured. The Cybersecurity Framework's tiers and profiles, IEC 62443-2-1's maturity levels, and CISA's performance goals each provide a basis for assessing where a programme stands and for setting targets; the metrics that matter most for the architecture proposed here are the completeness of the asset inventory, the share of remote-access paths protected by multi-factor authentication, the number of unbrokered conduits between enterprise and operations, the coverage of OT network monitoring by zone, the age of the most recent tested recovery of controller logic, and the time taken to detect and contain exercised incidents (National Institute of Standards and Technology, 2024a; Cybersecurity and Infrastructure Security Agency, 2023; Linkov et al., 2013). Metrics of this kind convert the architecture from a design into a managed programme, and they are the evidence that regulators under the TSA directives and auditors against API 1164 will ask for (U.S. Government Accountability Office, 2021; American Petroleum Institute, 2021). They also expose the trade-offs that OT security always involves: a monitoring sensor on a fragile network segment, a patch to a controller that cannot be taken offline, or an authentication requirement on a safety-critical remote link each carries an availability risk that must be weighed against the security benefit, and the weighing should be explicit and recorded (Knowles et al., 2015; Stouffer et al., 2023).

Several properties of the architecture deserve emphasis. It is layered in the sense that each critical scenario is mitigated at more than one layer: ransomware (R1) is addressed by governance, identity, segmentation, monitoring, and recovery; logic manipulation (R2) by physical security, segmentation of the SIS, hardened engineering workstations, process-aware monitoring, and backups of logic; remote-access exploitation (R3) by identity, segmentation, and monitoring. It is framework-aligned, as Table 10 shows, so that an operator can demonstrate coverage of Cybersecurity Framework functions and IEC 62443 requirements and can map the controls to the TSA directives and API 1164 (National Institute of Standards and Technology, 2024a; International Society of Automation, 2024; U.S. Government Accountability Office, 2021; American Petroleum Institute, 2021). It is incremental: the governance, identity, and segmentation layers correspond to CISA's highest-priority performance goals and can be implemented first, with monitoring and process-aware detection following as visibility matures (Cybersecurity and Infrastructure Security Agency, 2023). And it treats safety and security as one function: the SIS zone, the SIS engineering workstation, independent safety-network monitoring, and joint hazard and threat analysis run through every layer (International Electrotechnical Commission, 2016; Young & Leveson, 2014; Kriaa et al., 2015). The feedback arc in Figure 11, from the outer ring back to governance, carries lessons learned, metrics, and audit findings into the next planning cycle, which is what distinguishes a programme from a project (National Institute of Standards and Technology, 2024a; Stouffer et al., 2023).

XII. FUTURE RESEARCH

Future work should examine Zero Trust for OT, AI-assisted threat detection, digital twins, autonomous vulnerability management, and quantum-resistant cryptography. Figure 12 positions these directions, together with safety–security co-engineering, by their technology readiness for OT and their potential risk reduction, in the author's qualitative assessment, and this section outlines the research questions in each.

Figure 12: Future Research Map: Technology Readiness Versus Potential Risk Reduction



Zero trust for OT is the architectural question of the decade. NIST's zero trust architecture replaces network location with identity and continuous verification as the basis for access decisions, and a multivocal literature review has catalogued both its promise and the gaps in its evidence base (Rose et al., 2020; Buck et al., 2021). In OT, the obstacles are concrete: controllers and field devices cannot run agents or authenticate strongly, protocols lack identity, and continuous verification must not introduce latency into control loops. Research is needed on identity-centric conduits that wrap legacy devices, on policy enforcement points that understand industrial protocols, and on how zero trust principles coexist with the Purdue zoning that current standards require (Stouffer et al., 2023; International Society of Automation, 2024; Dhirani et al., 2021).

AI-assisted threat detection has produced promising results on testbeds, with recurrent, convolutional, and unsupervised models detecting attacks on water-treatment and power systems (Goh et al., 2017; Kravchik & Shabtai, 2018; Inoue et al., 2017; Mathur & Tippenhauer, 2016). The open problems are generalisation from testbeds to heterogeneous plants, explainability for operators who must act on alerts, robustness to adversaries who understand the process and the detector, and integration of physics-based and learned models (Giraldo et al., 2018; Urbina et al., 2016; Kaur et al., 2023; Sarker et al., 2021). Evaluation on shared datasets and testbeds, and reporting standards for detection research, would allow results to be compared (Conti et al., 2021; Ferrag et al., 2020).

Digital twins, virtual replicas of plants and control systems, offer a way to evaluate attacks and defences, to train responders, and to test patches without touching production (Eckhart & Ekelhart, 2018; Eckhart & Ekelhart, 2019; Bitton et al., 2018; Dietz & Pernul, 2020). Research questions include the fidelity required for security evaluation, the cost of constructing and maintaining twins of legacy systems, and the security of the twin itself, which holds a complete model of the plant. Autonomous vulnerability management addresses the scale problem: oil and gas operators manage thousands of devices across dispersed sites, vulnerability disclosures for industrial products are frequent, and patch windows are rare. Research is needed on automated asset discovery that is safe for fragile devices, on risk-based prioritisation that accounts for exposure and consequence rather than severity scores alone, and on the automated selection and verification of compensating controls (Knowles et al., 2015;

Cybersecurity and Infrastructure Security Agency, 2023; Stouffer et al., 2023).

Quantum-resistant cryptography is a longer-horizon but unavoidable transition. NIST's post-quantum standards are now published, and the cryptographic protections being added to industrial protocols and remote-access conduits must be designed for crypto-agility so that algorithms can be replaced on devices with twenty-year lifetimes (National Institute of Standards and Technology, 2024b; L. Chen et al., 2016; Bernstein & Lange, 2017). Research on lightweight post-quantum implementations for constrained controllers and on migration strategies for brownfield plants is needed. Finally, safety–security co-engineering remains the sector's most consequential gap. Systems-theoretic methods that treat safety and security as control problems, the integration of threat analysis into layers-of-protection analysis, and independent monitoring of safety systems are each supported by the literature, but their adoption in oil and gas engineering practice is limited, and Triton shows the cost of that gap (Young & Leveson, 2014; Leveson, 2012; Kriaa et al., 2015; International Electrotechnical Commission, 2016). Cross-cutting both the roadmap and the architecture are standards harmonisation, so that operators are not asked to satisfy overlapping requirements with different vocabularies, and workforce development, since the architecture proposed here cannot be operated without engineers who understand both the process and its security (Leszczyna, 2018; U.S. Government Accountability Office, 2021; Kim et al., 2020).

XIII. CONCLUSION

Industrial cybersecurity must be treated as a safety and business continuity function. Organizations should align programs with NIST and IEC guidance while continuously improving resilience. This paper has argued that case from four directions. The architecture of oil and gas control systems, read through the Purdue model, locates the assets that matter, the controllers and safety systems, and the conduits through which they are reached, the engineering workstations, remote-access paths, and the IT–OT boundary. The threat landscape, mapped through ATT&CK for ICS, shows that the consequence of an intrusion depends on what the adversary can reach rather than on how the adversary entered, and that the rare, engineered attack on safety and control and the frequent, opportunistic attack on business systems must both be defended against. The qualitative risk assessment, grounded in incident evidence, prioritises ransomware entering through the enterprise network, manipulation of controller and safety logic, and exploitation of insecure remote access, and the Colonial Pipeline and Triton case studies confirm that prioritisation from opposite ends of the threat spectrum: one incident touched no control system yet stopped a national fuel artery, the other touched only the safety system yet threatened lives. NIST SP 800-82 Revision 3, the Cybersecurity Framework 2.0, and IEC 62443 provide complementary structures, programme-level and engineering-level, for responding, and the seven-layer defense-in-depth architecture proposed here operationalises both, mitigating each priority scenario at more than one layer and treating safety and security as a single function. The sector's regulatory direction, from voluntary guidelines to mandatory directives and an updated API standard, confirms that the question is no longer whether to invest in OT security but how to do so in a way that is architecturally sound, measurable, and resilient. The research roadmap, from zero trust and AI-assisted detection to digital twins, autonomous vulnerability management, quantum-resistant cryptography, and safety–security co-engineering, indicates where the next decade's gains will come from; the lessons of the last decade indicate that the fundamentals, inventory, segmentation, identity, monitoring, and rehearsed recovery, remain the first priority.

REFERENCES

[1]. Ahmed, C. M., Zhou, J., & Mathur, A. P. (2018). Noise matters: Using sensor and process noise fingerprint to detect stealthy cyber attacks and authenticate sensors in CPS. *Proceedings of the 34th Annual Computer Security Applications Conference*, 566–581. https://doi.org/10.1145/3274694.3274748

[2]. Alcaraz, C., & Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection*, *8*, 53–66. https://doi.org/10.1016/j.ijcip.2014.12.002

[3]. Alexander, O., Belisle, M., & Steele, J. (2020). *MITRE ATT&CK for industrial control systems: Design and philosophy*. The MITRE Corporation. https://attack.mitre.org/docs/ATTACK_for_ICS_Philosophy_March_2020.pdf

[4]. Alladi, T., Chamola, V., & Zeadally, S. (2020). Industrial control systems: Cyberattack trends and countermeasures. *Computer Communications*, *155*, 1–8. https://doi.org/10.1016/j.comcom.2020.03.007

[5]. American Petroleum Institute. (2021). *New edition of cybersecurity standard for pipelines provides comprehensive approach to cyber defense for critical infrastructure [Press release announcing API Standard 1164, 3rd ed.]*. American Petroleum Institute. https://www.api.org/news-policy-and-issues/news/2021/08/18/third-edition-of-api-standard-1164

[6]. Amin, S., Litrico, X., Sastry, S., & Bayen, A. M. (2013). Cyber security of water SCADA systems—Part I: Analysis and experimentation of stealthy deception attacks. *IEEE Transactions on Control Systems Technology*, *21*(5), 1963–1970. https://doi.org/10.1109/TCST.2012.2211873

[7]. Ani, U. P. D., He, H., & Tiwari, A. (2017). Review of cybersecurity issues in industrial critical infrastructure: Manufacturing in perspective. *Journal of Cyber Security Technology*, *1*(1), 32–74. https://doi.org/10.1080/23742917.2016.1252211

[8]. Ashibani, Y., & Mahmoud, Q. H. (2017). Cyber physical systems security: Analysis, challenges and solutions. *Computers & Security*, *68*, 81–97. https://doi.org/10.1016/j.cose.2017.04.005

[9]. Assante, M. J., & Lee, R. M. (2015). *The industrial control system cyber kill chain*. SANS Institute. https://www.sans.org/white-papers/36297/

[10]. Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research*, *253*(1), 1–13. https://doi.org/10.1016/j.ejor.2015.12.023

[11]. Bartock, M., Cichonski, J., Souppaya, M., Smith, M., Witte, G., & Scarfone, K. (2016). *Guide for cybersecurity event recovery* (NIST Special Publication 800-184). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-184

[12]. Beerman, J., Berent, D., Falter, Z., & Bhunia, S. (2023). A review of Colonial Pipeline ransomware attack. *2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW)*, 8–15. https://doi.org/10.1109/CCGridW59191.2023.00017

[13]. Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. *Nature*, *549*(7671), 188–194. https://doi.org/10.1038/nature23461

[14]. Bhamare, D., Zolanvari, M., Erbad, A., Jain, R., Khan, K., & Meskin, N. (2020). Cybersecurity for industrial control systems: A survey. *Computers & Security*, *89*, 101677. https://doi.org/10.1016/j.cose.2019.101677

[15]. Bitton, R., Gluck, T., Stan, O., Inokuchi, M., Ohta, Y., Yamada, Y., Yagyu, T., Elovici, Y., & Shabtai, A. (2018). Deriving a cost-effective digital twin of an ICS to facilitate security evaluation. *Computer Security – ESORICS 2018, Lecture Notes in Computer Science*, *11098*, 533–554. https://doi.org/10.1007/978-3-319-99073-6_26

[16]. Boyens, J., Smith, A., Bartol, N., Winkler, K., Holbrook, A., & Fallon, M. (2022). *Cybersecurity supply chain risk management practices for systems and organizations* (NIST Special Publication 800-161 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-161r1

[17]. Boyes, H. (2015). Cybersecurity and cyber-resilient supply chains. *Technology Innovation Management Review*, *5*(4), 28–34. https://doi.org/10.22215/timreview/888

[18]. Buck, C., Olenberger, C., Schweizer, A., Völter, F., & Eymann, T. (2021). Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust. *Computers & Security*, *110*, 102436. https://doi.org/10.1016/j.cose.2021.102436

[19]. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials*, *18*(2), 1153–1176. https://doi.org/10.1109/COMST.2015.2494502

[20]. Cappelli, D. M., Moore, A. P., & Trzeciak, R. F. (2012). *The CERT guide to insider threats: How to prevent, detect, and respond to information technology crimes (theft, sabotage, fraud)*. Addison-Wesley.

[21]. Cheminod, M., Durante, L., & Valenzano, A. (2013). Review of security issues in industrial networks. *IEEE Transactions on Industrial Informatics*, *9*(1), 277–293. https://doi.org/10.1109/TII.2012.2198666

[22]. Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). *Report on post-quantum cryptography* (NISTIR 8105). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8105

[23]. Chen, T. M., & Abu-Nimeh, S. (2011). Lessons from Stuxnet. *Computer*, *44*(4), 91–93. https://doi.org/10.1109/MC.2011.115

[24]. Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computers & Security*, *56*, 1–27. https://doi.org/10.1016/j.cose.2015.09.009

[25]. Cherepanov, A. (2017). *WIN32/INDUSTROYER: A new threat for industrial control systems*. ESET. https://web-assets.esetstatic.com/wls/2017/06/Win32_Industroyer.pdf

[26]. Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer security incident handling guide* (NIST Special Publication 800-61 Rev. 2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r2

[27]. Conti, M., Donadel, D., & Turrin, F. (2021). A survey on industrial control system testbeds and datasets for security research. *IEEE Communications Surveys & Tutorials*, *23*(4), 2248–2294. https://doi.org/10.1109/COMST.2021.3094360

[28]. Cox, L. A., Jr. (2008). What's wrong with risk matrices? *Risk Analysis*, *28*(2), 497–512. https://doi.org/10.1111/j.1539-6924.2008.01030.x

[29]. Cybersecurity and Infrastructure Security Agency, & National Security Agency. (2020). *NSA and CISA recommend immediate actions to reduce exposure across all operational technologies and control systems* (Alert AA20-205A). Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-205a

[30]. Cybersecurity and Infrastructure Security Agency. (2021a). *DarkSide ransomware: Best practices for preventing business disruption from ransomware attacks* (Alert AA21-131A). Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-131a

[31]. Cybersecurity and Infrastructure Security Agency. (2021b). *Advanced persistent threat compromise of government agencies, critical infrastructure, and private sector organizations* (Alert AA20-352A). Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-352a

[32]. Cybersecurity and Infrastructure Security Agency. (2021c). *Compromise of U.S. water treatment facility* (Alert AA21-042A). Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-042a

[33]. Cybersecurity and Infrastructure Security Agency. (2022). *HatMan – Safety system targeted malware (update B)* (ICS Advisory MAR-17-352-01). Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/news-events/ics-advisories/mar-17-352-01-hatman-safety-system-targeted-malware-update-b

[34]. Cybersecurity and Infrastructure Security Agency. (2023). *Cross-sector cybersecurity performance goals*. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/cross-sector-cybersecurity-performance-goals

[35]. Cárdenas, A. A., Amin, S., Lin, Z.-S., Huang, Y.-L., Huang, C.-Y., & Sastry, S. (2011). Attacks against process control systems: Risk assessment, detection, and response. In *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security* (pp. 355–366). ACM. https://doi.org/10.1145/1966913.1966959

[36]. Dhirani, L. L., Armstrong, E., & Newe, T. (2021). Industrial IoT, cyber threats, and standards landscape: Evaluation and roadmap. *Sensors*, *21*(11), 3901. https://doi.org/10.3390/s21113901

[37]. Dietz, M., & Pernul, G. (2020). Digital twin: Empowering enterprises towards a system-of-systems approach. *Business & Information Systems Engineering*, *62*(2), 179–184. https://doi.org/10.1007/s12599-019-00624-0

[38]. Ding, D., Han, Q.-L., Xiang, Y., Ge, X., & Zhang, X.-M. (2018). A survey on security control and attack detection for industrial cyber-physical systems. *Neurocomputing*, *275*, 1674–1683. https://doi.org/10.1016/j.neucom.2017.10.009

[39]. Dragos. (2017a). *TRISIS malware: Analysis of safety system targeted malware*. Dragos, Inc.. https://www.dragos.com/wp-content/uploads/TRISIS-01.pdf

[40]. Dragos. (2017b). *CRASHOVERRIDE: Analysis of the threat to electric grid operations*. Dragos, Inc.. https://www.dragos.com/wp-content/uploads/CrashOverride-01.pdf

[41]. Eckhart, M., & Ekelhart, A. (2018). Towards security-aware virtual environments for digital twins. In *Proceedings of the 4th ACM Workshop on Cyber-Physical System Security* (pp. 61–72). ACM. https://doi.org/10.1145/3198458.3198464

[42]. Eckhart, M., & Ekelhart, A. (2019). Digital twins for cyber-physical systems security: State of the art and outlook. *Security and Quality in Cyber-Physical Systems Engineering*, 383–412. https://doi.org/10.1007/978-3-030-25312-7_14

[43]. Executive Office of the President. (2021). *Improving the nation's cybersecurity (Executive Order 14028)*. Federal Register, 86 FR 26633. https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

[44]. Falliere, N., Murchu, L. O., & Chien, E. (2011). *W32.Stuxnet dossier (Version 1.4)*. Symantec Corporation. https://docs.broadcom.com/doc/security-response-w32-stuxnet-dossier-11-en

[45]. Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. *Survival*, *53*(1), 23–40. https://doi.org/10.1080/00396338.2011.555586

[46]. Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications*, *50*, 102419. https://doi.org/10.1016/j.jisa.2019.102419

[47]. Fovino, I. N., Carcano, A., Murel, T. D. L., Trombetta, A., & Masera, M. (2010). Modbus/DNP3 state-based intrusion detection system. *2010 24th IEEE International Conference on Advanced Information Networking and Applications*, 729–736. https://doi.org/10.1109/AINA.2010.86

[48]. Galloway, B., & Hancke, G. P. (2013). Introduction to industrial control networks. *IEEE Communications Surveys & Tutorials*, *15*(2), 860–880. https://doi.org/10.1109/SURV.2012.071812.00124

[49]. Ganin, A. A., Massaro, E., Gutfraind, A., Steen, N., Keisler, J. M., Kott, A., Mangoubi, R., & Linkov, I. (2016). Operational resilience: Concepts, design and analysis. *Scientific Reports*, *6*, 19540. https://doi.org/10.1038/srep19540

[50]. Garcia, L., Brasser, F., Cintuglu, M. H., Sadeghi, A.-R., Mohammed, O., & Zonouz, S. A. (2017). Hey, my malware knows physics! Attacking PLCs with physical model aware rootkit. In *Proceedings of the 2017 Network and Distributed System Security Symposium*. Internet Society. https://doi.org/10.14722/ndss.2017.23313

[51]. Ghadge, A., Weiß, M., Caldwell, N. D., & Wilding, R. (2020). Managing cyber risk in supply chains: A review and research agenda. *Supply Chain Management: An International Journal*, *25*(2), 223–240. https://doi.org/10.1108/SCM-10-2018-0357

[52]. Ghaleb, A., Zhioua, S., & Almulhem, A. (2018). On PLC network security. *International Journal of Critical Infrastructure Protection*, *22*, 62–69. https://doi.org/10.1016/j.ijcip.2018.05.004

[53]. Giraldo, J., Urbina, D., Cardenas, A., Valente, J., Faisal, M., Ruths, J., Tippenhauer, N. O., Sandberg, H., & Candell, R. (2018). A survey of physics-based attack detection in cyber-physical systems. *ACM Computing Surveys*, *51*(4), Article 76. https://doi.org/10.1145/3203245

[54]. Goh, J., Adepu, S., Tan, M., & Lee, Z. S. (2017). Anomaly detection in cyber physical systems using recurrent neural networks. In *2017 IEEE 18th International Symposium on High Assurance Systems Engineering (HASE)* (pp. 140–145). IEEE. https://doi.org/10.1109/HASE.2017.36

[55]. Greitzer, F. L., Kangas, L. J., Noonan, C. F., Dalton, A. C., & Hohimer, R. E. (2012). Identifying at-risk employees: Modeling psychosocial precursors of potential insider threats. *Proceedings of the 45th Hawaii International Conference on System Sciences*, 2392–2401. https://doi.org/10.1109/HICSS.2012.309

[56]. Hadžiosmanović, D., Sommer, R., Zambon, E., & Hartel, P. H. (2014). Through the eye of the PLC: Semantic security monitoring for industrial processes. In *Proceedings of the 30th Annual Computer Security Applications Conference* (pp. 126–135). ACM. https://doi.org/10.1145/2664243.2664277

[57]. Hahn, A., Ashok, A., Sridhar, S., & Govindarasu, M. (2013). Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid. *IEEE Transactions on Smart Grid*, *4*(2), 847–855. https://doi.org/10.1109/TSG.2012.2226919

[58]. Hassanzadeh, A., Rasekh, A., Galelli, S., Aghashahi, M., Taormina, R., Ostfeld, A., & Banks, M. K. (2020). A review of cybersecurity incidents in the water sector. *Journal of Environmental Engineering*, *146*(5), 03120003. https://doi.org/10.1061/(ASCE)EE.1943-7870.0001686

[59]. Hemsley, K. E., & Fisher, R. E. (2018). *History of industrial control system cyber incidents* (INL/CON-18-44411). Idaho National Laboratory. https://doi.org/10.2172/1505628

[60]. Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y., & Ochoa, M. (2019). Insight into insiders and IT: A survey of insider threat taxonomies, analysis, modeling, and countermeasures. *ACM Computing Surveys*, *52*(2), Article 30. https://doi.org/10.1145/3303771

[61]. Hubbard, D. W., & Seiersen, R. (2016). *How to measure anything in cybersecurity risk*. John Wiley & Sons. https://doi.org/10.1002/9781119162315

[62]. Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-physical systems security—A survey. *IEEE Internet of Things Journal*, *4*(6), 1802–1831. https://doi.org/10.1109/JIOT.2017.2703172

[63]. Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). *Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains*. Lockheed Martin Corporation. https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

[64]. Igure, V. M., Laughter, S. A., & Williams, R. D. (2006). Security issues in SCADA networks. *Computers & Security*, *25*(7), 498–506. https://doi.org/10.1016/j.cose.2006.03.001

[65]. Inoue, J., Yamagata, Y., Chen, Y., Poskitt, C. M., & Sun, J. (2017). Anomaly detection for a water treatment system using unsupervised machine learning. In *2017 IEEE International Conference on Data Mining Workshops (ICDMW)* (pp. 1058–1065). IEEE. https://doi.org/10.1109/ICDMW.2017.149

[66]. International Electrotechnical Commission. (2016). *Functional safety – Safety instrumented systems for the process industry sector (IEC 61511)*. International Electrotechnical Commission. https://webstore.iec.ch/en/publication/24241

[67]. International Electrotechnical Commission. (2023). *Understanding IEC 62443*. International Electrotechnical Commission. https://www.iec.ch/blog/understanding-iec-62443

[68]. International Organization for Standardization. (2018). *Risk management – Guidelines (ISO 31000:2018)*. International Organization for Standardization. https://www.iso.org/standard/65694.html

[69]. International Organization for Standardization. (2022). *Information security, cybersecurity and privacy protection – Guidance on managing information security risks (ISO/IEC 27005:2022)*. International Organization for Standardization. https://www.iso.org/standard/80585.html

[70]. International Society of Automation. (2024). *ISA/IEC 62443 series of standards*. International Society of Automation. https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

[71]. Johnson, B., Caban, D., Krotofil, M., Scali, D., Brubaker, N., & Glyer, C. (2017). *Attackers deploy new ICS attack framework "TRITON" and cause operational disruption to critical infrastructure*. Mandiant. https://cloud.google.com/blog/topics/threat-intelligence/attackers-deploy-new-ics-attack-framework-triton

[72]. Joint Task Force Transformation Initiative. (2012). *Guide for conducting risk assessments* (NIST Special Publication 800-30 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-30r1

[73]. Joint Task Force. (2020). *Security and privacy controls for information systems and organizations* (NIST Special Publication 800-53 Rev. 5). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5

[74]. Kaplan, S., & Garrick, B. J. (1981). On the quantitative definition of risk. *Risk Analysis*, *1*(1), 11–27. https://doi.org/10.1111/j.1539-6924.1981.tb01350.x

[75]. Karnouskos, S. (2011). Stuxnet worm impact on industrial cyber-physical system security. In *IECON 2011 – 37th Annual Conference of the IEEE Industrial Electronics Society* (pp. 4490–4494). IEEE. https://doi.org/10.1109/IECON.2011.6120048

[76]. Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, *97*, 101804. https://doi.org/10.1016/j.inffus.2023.101804

[77]. Kim, S., Heo, G., Zio, E., Shin, J., & Song, J. (2020). Cyber attack taxonomy for digital environment in nuclear power plants. *Nuclear Engineering and Technology*, *52*(5), 995–1001. https://doi.org/10.1016/j.net.2019.11.001

[78]. Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P., & Jones, K. (2015). A survey of cyber security management in industrial control systems. *International Journal of Critical Infrastructure Protection*, *9*, 52–80. https://doi.org/10.1016/j.ijcip.2015.02.002

[79]. Kott, A., Golan, M. S., Trump, B. D., & Linkov, I. (2021). Cyber resilience: By design or by intervention? *Computer*, *54*(8), 112–117. https://doi.org/10.1109/MC.2021.3082836

[80]. Kravchik, M., & Shabtai, A. (2018). Detecting cyber attacks in industrial control systems using convolutional neural networks. In *Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and PrivaCy* (pp. 72–83). ACM. https://doi.org/10.1145/3264888.3264896

[81]. Kriaa, S., Pietre-Cambacedes, L., Bouissou, M., & Halgand, Y. (2015). A survey of approaches combining safety and security for industrial control systems. *Reliability Engineering & System Safety*, *139*, 156–178. https://doi.org/10.1016/j.ress.2015.02.008

[82]. Krotofil, M., Larsen, J., & Gollmann, D. (2015). The process matters: Ensuring data veracity in cyber-physical systems. *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security*, 133–144. https://doi.org/10.1145/2714576.2714599

[83]. Kure, H. I., Islam, S., & Razzaque, M. A. (2018). An integrated cyber security risk management approach for a cyber-physical system. *Applied Sciences*, *8*(6), 898. https://doi.org/10.3390/app8060898

[84]. Kushner, D. (2013). The real story of Stuxnet. *IEEE Spectrum*, *50*(3), 48–53. https://doi.org/10.1109/MSPEC.2013.6471059

[85]. Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy*, *9*(3), 49–51. https://doi.org/10.1109/MSP.2011.67

[86]. Lee, R. M., Assante, M. J., & Conway, T. (2016). *Analysis of the cyber attack on the Ukrainian power grid: Defense use case*. SANS Institute and Electricity Information Sharing and Analysis Center. https://www.sans.org/white-papers/analysis-of-the-cyber-attack-on-the-ukrainian-power-grid/

[87]. Leszczyna, R. (2018). A review of standards with cybersecurity requirements for smart grid. *Computers & Security*, *77*, 262–276. https://doi.org/10.1016/j.cose.2018.03.011

[88]. Leveson, N. G. (2012). *Engineering a safer world: Systems thinking applied to safety*. MIT Press. https://doi.org/10.7551/mitpress/8179.001.0001

[89]. Lezzi, M., Lazoi, M., & Corallo, A. (2018). Cybersecurity for Industry 4.0 in the current literature: A reference framework. *Computers in Industry*, *103*, 97–110. https://doi.org/10.1016/j.compind.2018.09.004

[90]. Liang, G., Weller, S. R., Zhao, J., Luo, F., & Dong, Z. Y. (2017). The 2015 Ukraine blackout: Implications for false data injection attacks. *IEEE Transactions on Power Systems*, *32*(4), 3317–3318. https://doi.org/10.1109/TPWRS.2016.2631891

[91]. Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. *Security Studies*, *22*(3), 365–404. https://doi.org/10.1080/09636412.2013.816122

[92]. Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J., & Kott, A. (2013). Resilience metrics for cyber systems. *Environment Systems and Decisions*, *33*(4), 471–476. https://doi.org/10.1007/s10669-013-9485-y

[93]. Lun, Y. Z., D'Innocenzo, A., Smarra, F., Malavolta, I., & Di Benedetto, M. D. (2019). State of the art of cyber-physical systems security: An automatic control perspective. *Journal of Systems and Software*, *149*, 174–216. https://doi.org/10.1016/j.jss.2018.12.006

[94]. Maglaras, L. A., Kim, K.-H., Janicke, H., Ferrag, M. A., Rallis, S., Fragkou, P., Maglaras, A., & Cruz, T. J. (2018). Cyber security of critical infrastructures. *ICT Express*, *4*(1), 42–45. https://doi.org/10.1016/j.icte.2018.02.001

[95]. Mathur, A. P., & Tippenhauer, N. O. (2016). SWaT: A water treatment testbed for research and training on ICS security. In *2016 International Workshop on Cyber-physical Systems for Smart Water Networks (CySWater)* (pp. 31–36). IEEE. https://doi.org/10.1109/CySWater.2016.7469060

[96]. McLaughlin, S., & McDaniel, P. (2012). SABOT: Specification-based payload generation for programmable logic controllers. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security* (pp. 439–449). ACM. https://doi.org/10.1145/2382196.2382244

[97]. McLaughlin, S., Konstantinou, C., Wang, X., Davi, L., Sadeghi, A.-R., Maniatakos, M., & Karri, R. (2016). The cybersecurity landscape in industrial control systems. *Proceedings of the IEEE*, *104*(5), 1039–1057. https://doi.org/10.1109/JPROC.2015.2512235

[98]. Miller, T., Staves, A., Maesschalck, S., Sturdee, M., & Green, B. (2021). Looking back to look forward: Lessons learnt from cyber-attacks on industrial control systems. *International Journal of Critical Infrastructure Protection*, *35*, 100464. https://doi.org/10.1016/j.ijcip.2021.100464

[99]. Mo, Y., Kim, T. H.-J., Brancik, K., Dickinson, D., Lee, H., Perrig, A., & Sinopoli, B. (2012). Cyber–physical security of a smart grid infrastructure. *Proceedings of the IEEE*, *100*(1), 195–209. https://doi.org/10.1109/JPROC.2011.2161428

[100]. National Institute of Standards and Technology. (2024a). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29

[101]. National Institute of Standards and Technology. (2024b). *Module-lattice-based key-encapsulation mechanism standard* (FIPS 203). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.FIPS.203

[102]. Nicholson, A., Webber, S., Dyer, S., Patel, T., & Janicke, H. (2012). SCADA security in the light of cyber-warfare. *Computers & Security*, *31*(4), 418–436. https://doi.org/10.1016/j.cose.2012.02.009

[103]. North American Electric Reliability Corporation. (2024). *CIP standards*. North American Electric Reliability Corporation. https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

[104]. Nourian, A., & Madnick, S. (2018). A systems theoretic approach to the security threats in cyber physical systems applied to Stuxnet. *IEEE Transactions on Dependable and Secure Computing*, *15*(1), 2–13. https://doi.org/10.1109/TDSC.2015.2509994

[105]. Ouyang, M. (2014). Review on modeling and simulation of interdependent critical infrastructure systems. *Reliability Engineering & System Safety*, *121*, 43–60. https://doi.org/10.1016/j.ress.2013.06.040

[106]. Oz, H., Aris, A., Levi, A., & Uluagac, A. S. (2022). A survey on ransomware: Evolution, taxonomy, and defense solutions. *ACM Computing Surveys*, *54*(11s), Article 238. https://doi.org/10.1145/3514229

[107]. Parfomak, P. W., & Jaikaran, C. (2021). *Colonial Pipeline: The DarkSide strikes* (CRS Insight IN11667). Congressional Research Service. https://crsreports.congress.gov/product/pdf/IN/IN11667

[108]. Piggin, R. S. H. (2013). Development of industrial cyber security standards: IEC 62443 for SCADA and industrial control system security. *IET Conference on Control and Automation 2013: Uniting Problems and Solutions*, 1–6. https://doi.org/10.1049/cp.2013.0001

[109]. Powell, M., Brule, J., Pease, M., Stouffer, K., Tang, C., Zimmerman, T., Deane, C., Hoyt, J., Raguso, M., Sherule, A., Zheng, K., & Zopf, M. (2022). *Protecting information and system integrity in industrial control system environments: Cybersecurity for the manufacturing sector* (NIST Special Publication 1800-10). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.1800-10

[110]. Progoulakis, I., Nikitakos, N., Rohmeyer, P., Bunin, B., Dalaklis, D., & Karamperidis, S. (2021). Perspectives on cyber security for offshore oil and gas assets. *Journal of Marine Science and Engineering*, *9*(2), 112. https://doi.org/10.3390/jmse9020112

[111]. Ralston, P. A. S., Graham, J. H., & Hieb, J. L. (2007). Cyber security risk assessment for SCADA and DCS networks. *ISA Transactions*, *46*(4), 583–594. https://doi.org/10.1016/j.isatra.2007.04.003

[112]. Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, *21*(6), 11–25. https://doi.org/10.1109/37.969131

[113]. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture* (NIST Special Publication 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

[114]. Sadeghi, A.-R., Wachsmann, C., & Waidner, M. (2015). Security and privacy challenges in industrial Internet of Things. *Proceedings of the 52nd Annual Design Automation Conference*, Article 54. https://doi.org/10.1145/2744769.2747942

[115]. Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). AI-driven cybersecurity: An overview, security intelligence modeling and research directions. *SN Computer Science*, *2*(3), 173. https://doi.org/10.1007/s42979-021-00557-0

[116]. Slowik, J. (2019). Evolution of ICS attacks and the prospects for future disruptive events. In *Dragos, Inc.*. https://www.dragos.com/wp-content/uploads/Evolution-of-ICS-Attacks-and-the-Prospects-for-Future-Disruptive-Events-Joseph-Slowik-1.pdf

[117]. Sridhar, S., Hahn, A., & Govindarasu, M. (2012). Cyber–physical system security for the electric power grid. *Proceedings of the IEEE*, *100*(1), 210–224. https://doi.org/10.1109/JPROC.2011.2165269

[118]. Stergiopoulos, G., Gritzalis, D. A., & Limnaios, E. (2020). Cyber-attacks on the oil & gas sector: A survey on incident assessment and attack patterns. *IEEE Access*, *8*, 128440–128475. https://doi.org/10.1109/ACCESS.2020.3007960

[119]. Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., Lightman, S., Hahn, A., Saravia, S., Sherule, A., & Thompson, M. (2023). *Guide to operational technology (OT) security* (NIST Special Publication 800-82 Rev. 3). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-82r3

[120]. Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2015). *Guide to industrial control systems (ICS) security* (NIST Special Publication 800-82 Rev. 2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-82r2

[121]. Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. B. (2018). *MITRE ATT&CK: Design and philosophy*. The MITRE Corporation. https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf

[122]. Sullivan, J. E., & Kamensky, D. (2017). How cyber-attacks in Ukraine show the vulnerability of the U.S. power grid. *The Electricity Journal*, *30*(3), 30–35. https://doi.org/10.1016/j.tej.2017.02.006

[123]. Ten, C.-W., Manimaran, G., & Liu, C.-C. (2010). Cybersecurity for critical infrastructures: Attack and defense modeling. *IEEE Transactions on Systems, Man, and Cybernetics – Part A: Systems and Humans*, *40*(4), 853–865. https://doi.org/10.1109/TSMCA.2010.2048028

[124]. Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & Security*, *72*, 212–233. https://doi.org/10.1016/j.cose.2017.09.001

[125]. U.S. Government Accountability Office. (2018). *Critical infrastructure protection: Actions needed to address significant weaknesses in TSA's pipeline security program management* (GAO-19-48). U.S. Government Accountability Office. https://www.gao.gov/products/gao-19-48

[126]. U.S. Government Accountability Office. (2021). *Critical infrastructure protection: TSA is taking steps to address some pipeline security program weaknesses* (GAO-21-105263). U.S. Government Accountability Office. https://www.gao.gov/products/gao-21-105263

[127]. Urbina, D. I., Giraldo, J. A., Cardenas, A. A., Tippenhauer, N. O., Valente, J., Faisal, M., Ruths, J., Candell, R., & Sandberg, H. (2016). Limiting the impact of stealthy attacks on industrial control systems. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1092–1105). ACM. https://doi.org/10.1145/2976749.2978388

[128]. Wang, W., & Lu, Z. (2013). Cyber security in the smart grid: Survey and challenges. *Computer Networks*, *57*(5), 1344–1371. https://doi.org/10.1016/j.comnet.2012.12.017

[129]. Whitehead, D. E., Owens, K., Gammel, D., & Smith, J. (2017). Ukraine cyber-induced power outage: Analysis and practical mitigation strategies. *2017 70th Annual Conference for Protective Relay Engineers (CPRE)*, 1–8. https://doi.org/10.1109/CPRE.2017.8090056

[130]. Williams, T. J. (1994). The Purdue enterprise reference architecture. *Computers in Industry*, *24*(2–3), 141–158. https://doi.org/10.1016/0166-3615(94)90017-5

[131]. Yadav, G., & Paul, K. (2021). Architecture and security of SCADA systems: A review. *International Journal of Critical Infrastructure Protection*, *34*, 100433. https://doi.org/10.1016/j.ijcip.2021.100433

[132]. Young, W., & Leveson, N. G. (2014). An integrated approach to safety and security based on systems theory. *Communications of the ACM*, *57*(2), 31–35. https://doi.org/10.1145/2556938

[133]. Zetter, K. (2014). *Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon*. Crown.

[134]. Zhu, B., Joseph, A., & Sastry, S. (2011). A taxonomy of cyber attacks on SCADA systems. In *2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing* (pp. 380–388). IEEE. https://doi.org/10.1109/iThings/CPSCom.2011.34