

THE CONVERGENCE OF FUNCTIONAL SAFETY (IEC 61511) AND OT CYBERSECURITY (IEC 62443): TOWARD AN INTEGRATED CYBER HAZOP FRAMEWORK FOR SECURE AND SAFE INDUSTRIAL CONTROL SYSTEMS

Alfred Basta^{*1}, Rebecca Basta^{*2}, Stavros Basta^{*3}

^{*1}PhD, LCCA, C|CISCO, CRISC, CISM, CISA, CGEIT, PMP, CHFI, ESCA, USA.

^{*2}CAP, PCAD, PMP, CIPP/US, AIGP, CDPPM, Six Sigma Master Black Belt, USA.

^{*3}GISCP, LPTM, CPENT, GSLC, CISM, PMP, CIPP/US, CompTIA Security+, USA.

DOI: <https://www.doi.org/10.56726/IRJMETs92937>

ABSTRACT

The rapidly advancing digitalization of critical infrastructure has fundamentally transformed the operational landscape of industrial control systems (ICS). Where once these systems operated in relative isolation, they now exist at the intersection of Information Technology (IT) and Operational Technology (OT), creating unprecedented opportunities for efficiency while simultaneously introducing novel and cascading risk vectors (Tarek & Hasan, 2024). The historical separation between functional safety engineering and cybersecurity has become operationally untenable; a compromised safety system through cyberattack poses identical physical consequences to a failed safety device through mechanical degradation (Deconinck et al., 2025). This convergence represents a critical inflection point in industrial systems management, where organizational structures, regulatory frameworks, and technical architectures must fundamentally recalibrate to address dual-domain threats from first principles.

The fundamental challenge lies in the philosophical divergence between these two disciplines. Traditional functional safety, governed by standards such as IEC 61508 and IEC 61511, adopts a deterministic, fault-based risk paradigm focused on accidental failures and probabilistic hardware degradation. Conversely, cybersecurity frameworks operating under IEC 62443 embrace an adversarial threat model rooted in intentional, multi-stage attack scenarios that exploit both logical and physical vulnerabilities (Hollerer et al., 2021). The intersection of these domains creates a complex threat landscape wherein malicious actors can deliberately induce unsafe control actions, transforming safety systems themselves into attack vectors (Friedberg et al., 2016).

The emerging Cyber HAZOP (CHAZOP) framework represents a methodological breakthrough in addressing this convergence. By extending the traditional Hazard and Operability Study with threat modeling principles specific to cybersecurity, CHAZOP enables organizations to systematically identify scenarios where cyber-attacks result in safety-critical failures and to implement unified protection strategies grounded in established risk governance frameworks (Heluany & GALVAO, 2023). This research paper provides a comprehensive treatment of the theoretical foundations, practical methodologies, and implementation blueprints for architects, engineers, and plant managers tasked with designing, deploying, and maintaining industrial systems that are simultaneously Safety Integrity Level (SIL) certified and Target Security Level (SL-T) capable.

I. INTRODUCTION

Functional Safety Foundations: IEC 61511 and the HAZOP-LOPA-SIL Paradigm

The HAZOP Methodology and Its Application to Process Safety

Hazard and Operability Studies (HAZOP) have served as the cornerstone of process safety analysis for more than four decades, providing a systematic, structured approach to identifying potential hazards and operability issues across all phases of a system's lifecycle (Rehail et al., 2024). The methodology employs specialized guide words, including "more," "less," "none," "reverse," "part of," and "other than," as cognitive prompts to systematically explore deviations from intended design parameters across all nodes or functions within a system. Each deviation is then examined to determine potential causes, consequences, and existing safeguards (Hu et al., 2023).

The HAZOP process unfolds through sequential, disciplined phases. First, the system boundary is rigorously defined, and the process flow is represented through piping and instrumentation diagrams (P&ID). A multidisciplinary team, comprising process engineers, control system specialists, operations personnel, and safety practitioners, conducts a workshop-based analysis in which each process section and parameter is systematically interrogated. For each identified hazard, the team documents the cause, consequence, existing protective layers, and risk category (Ye et al., 2025). This qualitative foundation provides the essential input for downstream quantitative assessments, particularly Layer of Protection Analysis (LOPA), which determines the required Safety Integrity Levels for instrumented safety functions.

The deterministic, accident-focused paradigm of HAZOP reflects its origins in an era when industrial systems operated in closed, air-gapped networks where the primary threat model centered on random hardware failures, design defects, and operator error. Traditional HAZOP, however, lacks explicit mechanisms to model adversarial scenarios, multi-stage attack chains, or scenarios wherein safety systems are deliberately circumvented or compromised through digital means (Choi & Byeon, 2020). This limitation becomes critically apparent in modern Industry 4.0 environments where IT systems, remote access capabilities, and interconnected networks expose safety logic controllers to cyber-attacks that would be nonsensical in a pre-connected era.

Safety Integrity Level (SIL) Determination and Allocation

The Safety Integrity Level framework, formalized in IEC 61508 and adopted domain-specifically in IEC 61511 for the process industries, quantifies the probability that a safety instrumented function (SIF) will fail to perform its protective action on demand (Kim et al., 2025). The SIL scale ranges from 1 to 4, with SIL 1 representing the lowest level of integrity (typical tolerable failure probability range of 10^{-2} to 10^{-1} per demand) and SIL 4 representing the highest (10^{-5} to 10^{-4} per demand). For each SIL level, IEC 61508 and 61511 specify architectural requirements, diagnostic coverage targets, proof-test intervals, and hardware fault-tolerance mandates (Julserccwong & Thepmanee, 2018).

The process of determining the required SIL entails several methodological streams. The first is risk-based SIL allocation, wherein the tolerable risk criterion, often expressed as an annual fatality or economic loss threshold, is established through a combination of regulatory guidance, societal consensus, and company-specific risk appetite (Park et al., 2023). The risk graph method, represented through a calibrated matrix encompassing consequence severity, exposure frequency, and system fail-safe design, provides a semi-quantitative pathway to initial SIL recommendations. However, the LOPA approach has emerged as the predominant quantitative methodology in process industries (Rehail et al., 2024).

LOPA fundamentally assesses the risk reduction factor (RRF) required to bring an identified hazardous event from its current frequency to a tolerable level. The analysis begins by establishing an initiating event frequency (e.g., loss of cooling water at 0.1 events per year), defines the consequence if unmitigated (e.g., reactor overpressure leading to rupture), and catalogs all independent protective layers (IPLs) currently in place (Dan et al., 2015). Each IPL is assigned a probability of failure on demand (PFD), and the combined effectiveness across all layers determines the residual risk. If the residual risk exceeds organizational tolerance, additional layers, typically embodied as Safety Instrumented Systems (SIS) with specific SIL requirements, are mandated (Gholami et al., 2024).

The mathematical framework for SIL verification requires reliability modeling of all components comprising the SIF, including sensors, logic solvers, and final elements. The fault tree analysis and Markov modeling techniques enable quantification of probability of failure on demand (PFDavg), accounting for random hardware failures, diagnostic coverage limitations, proof test effectiveness, and common cause failure mechanisms (Demichela & Pirani, 2013). This quantitative rigor ensures that implemented safety systems meet their design specifications under real-world operating conditions, accounting for component degradation, wear-out, and proof testing cycles (Jeong et al., 2025).

Design, Implementation, and Verification of Safety Instrumented Systems

Once SIL requirements are established, the design phase translates safety requirements into specific hardware architectures, sensor selections, logic solver configurations, and final element specifications. The IEC

61508/61511 standards prescribe several canonical architectures: 1oo1 (single-channel), 1oo2 (single-channel with manual override), 2oo2 (two-channel series), 2oo3 (two-out-of-three voting), and redundant configurations with cross-monitoring; each with defined diagnostic coverage and hardware fault tolerance capabilities (Riad et al., 2018). The designer must ensure that the selected architecture meets the required SIL while respecting operational constraints (e.g., proof test intervals, maintenance windows, and diagnostic latency requirements).

Commissioning and validation of SIS demand comprehensive testing protocols encompassing factory acceptance testing (FAT), site acceptance testing (SAT), and full operational validation. The as-built system must be proven, through a combination of functional testing, failure injection, and quantitative verification, to meet or exceed its specified SIL. Crucially, this verification addresses only the functional safety dimension; the cybersecurity posture of the SIS is typically secondary at this stage or entirely absent in legacy installations (Chen et al., 2025). This represents a critical gap in the convergence landscape: a system may be certified to SIL 3 in terms of random hardware failure rates while possessing trivial cyber vulnerabilities that any moderately skilled attacker could exploit to induce unsafe control actions.

OT Cybersecurity Fundamentals: IEC 62443 and the Threat Modeling Paradigm

The IEC 62443 Standard Series: Zones, Conduits, and Security Levels

The IEC 62443 standard series, jointly developed by the International Electrotechnical Commission and the International Society of Automation (ISA), establishes a comprehensive framework for securing industrial automation and control systems across their entire lifecycle (Ramdass & Balaraman, 2025). Unlike IEC 61508, which focuses on functional safety through probabilistic hardware reliability, IEC 62443 adopts a systems-based, defense-in-depth approach that compartmentalizes systems into security zones and regulates inter-zone communications through secure conduits (Tarek & Hasan, 2024).

A security zone, as defined in IEC 62443-3-3, represents a logical grouping of assets possessing similar security requirements and trust relationships. Zones are populated with devices performing supervisory, control, or sensing functions; the zone boundary is defined as the perimeter within which a particular security policy applies (Swain & Venkatraman, 2024). Conduits are the communication channels, whether wired, wireless, or logical/virtual, that convey information between zones. Each conduit must be protected through architectural measures (air-gapping, network segmentation), cryptographic controls (encryption, authentication), and monitoring mechanisms to ensure that communications conform to permitted protocols and are free from tampering (Cindrić et al., 2025).

Target Security Levels (SL-T), arranged on a scale from SL 0 (no specific security requirement) to SL 4 (maximum security requirement), analogously represent the security assurance level required for specific assets or processes (Wang et al., 2023). However, unlike SIL determination, which is primarily driven by hazard severity and probability, SL-T determination incorporates threat modeling, vulnerability assessment, and the likely sophistication and motivation of potential adversaries (Iturbe et al., 2023). A water treatment facility, for instance, might assign SL 3 to sensors directly controlling chemical dosing (reflecting both the criticality of the function and the likely threat sophistication), while assigning SL 1 to non-critical parameter monitoring.

Threat Modeling and Vulnerability Analysis in ICS Environments

Unlike safety analysis, which proceeds from a base assumption of random failures, cybersecurity threat modeling begins with an adversarial posture: what capabilities would an attacker need, what are their likely objectives, and what vulnerabilities exist that could be exploited to achieve those objectives (Hollerer et al., 2021)? The MITRE ATT&CK framework for ICS provides a structured taxonomy of adversary tactics, techniques, and procedures (TTPs) observed in real-world attacks against industrial systems, enabling organizations to benchmark their threat landscape against known attack patterns (Bhosale et al., 2024).

Common attack vectors against ICS environments include supply chain compromise (malware embedded in firmware or software updates), credential theft and privilege escalation, exploitation of unpatched vulnerabilities in legacy systems, and false data injection attacks wherein malicious data is inserted into control loops to induce unsafe operating states without triggering safety interlocks (Zhou et al., 2021). A particularly

insidious class of attack targets the safety systems themselves; an attacker who gains access to the logic solver executing safety functions can disable alarms, delete historical records of unsafe states, or reprogram the safety logic to permit dangerous operating conditions while appearing to the operator to be functioning normally (Xin, 2023).

Vulnerability assessment in ICS is methodologically distinct from IT-focused vulnerability scanning. Many industrial devices lack operating systems amenable to traditional patching; they may run firmware that is proprietary, poorly documented, and difficult to update without disrupting continuous process operations (Ramdass & Balaraman, 2025). Consequently, IEC 62443 emphasizes the identification of vulnerabilities through threat modeling and architectural analysis rather than reliance on automated vulnerability scanning tools. The standard's risk assessment methodology (IEC 62443-3-2) guides practitioners to identify the protected assets within each security zone, catalog the threats plausible against those assets given the threat environment, and systematically evaluate whether implemented controls reduce threat exploitability to acceptable levels (M. Silva et al., 2025).

Security by Design and the Lifecycle Approach

IEC 62443 mandates a security-by-design paradigm wherein security requirements are established during the specification phase and are integrated throughout design, implementation, testing, and operational phases (Parekh et al., 2021). Unlike functional safety, where verification can often be deferred to the commissioning phase through comprehensive testing, security cannot be "tested in"; a system that is secure only due to the difficulty of exploitation remains vulnerable to determined adversaries with sufficient resources or insider knowledge. Therefore, security must be architected into the system from its conception.

The IEC 62443 lifecycle encompasses ten phases: concept, specification, implementation, integration, verification, validation, deployment, operations, maintenance, and decommissioning (Alawi, 2025). At each phase, specific security controls are mandated, including secure coding practices (to minimize software vulnerabilities), secure configuration management (to prevent security policies from being weakened during maintenance), and secure disposal of decommissioned equipment (to prevent sensitive data extraction). Importantly, IEC 62443 recognizes that security is not a static state but must be continuously evaluated and adapted as new threats emerge; the standard explicitly requires ongoing monitoring, threat intelligence gathering, and risk re-assessment (Hanssen et al., 2023).

The Convergence Challenge: Conflicts, Complementarities, and Dual-Domain Threats

Philosophical and Methodological Differences Between Safety and Security Disciplines

The fundamental philosophical divergence between functional safety and cybersecurity creates significant organizational and technical challenges. Functional safety operates within a probabilistic, random-failure paradigm wherein component failures are modeled using exponential distributions with constant hazard rates and are assumed to be independent except for common cause mechanisms. This framework, derived from reliability engineering, assumes that with sufficient redundancy, diagnostic coverage, and proof testing, a safety system can achieve arbitrarily high assurance (Linnoosmaa et al., 2022).

Cybersecurity, conversely, operates within a worst-case adversarial paradigm wherein an attacker is assumed to possess knowledge of system design, sufficient time and resources to craft exploit code, and motivation to succeed. From this perspective, the only sustainable defense is cryptographic assurance: mathematical proofs that certain attacks are computationally infeasible given contemporary computational resources, combined with the diversity of mechanisms (ensuring that exploiting one attack surface does not automatically compromise the system) (Khan & Madnick, 2021).

These paradigmatic differences manifest in practical conflicts. A safety engineer designing a control system for a refinery distillation column might specify a standardized, commercially available programmable logic controller (PLC) to minimize design cost and leverage extensive operational experience. The cybersecurity architect, however, recognizes that the widely deployed PLC model has known vulnerabilities documented in public exploit databases and that any defender deploying that specific device is immediately vulnerable to publicly available attack tools. The tension between standardization (which aids reliable operation and maintenance)

and diversity (which impedes broad-scale attacks) exemplifies the fundamental conflict between safety and security optimization.

Another critical divergence concerns the treatment of human operators. Functional safety theory treats operators as a protective layer, with well-defined detection times and error probabilities that can be incorporated into LOPA calculations (Demichela & Pirani, 2013). Cybersecurity, however, recognizes operators as a primary attack surface: social engineering, phishing, and credential theft targeting operators are among the most successful attack vectors against industrial systems (Ramdass & Balaraman, 2025). The safe staffing practices recommended by safety engineering, operators with deep system knowledge, stable employment, and strong institutional loyalty, can paradoxically increase security risk if those same highly knowledgeable operators are targeted with sophisticated social engineering attacks.

Common Threat Vectors and Dual-Domain Risk Scenarios

While safety and security disciplines address distinct hazard sources, their consequences can be identical. A loss of coolant in a chemical reactor can result from either a mechanical pipe rupture (a traditional safety concern) or a cybersecurity compromise wherein an attacker manipulates pump speed setpoints through compromised control logic (a cybersecurity concern). From the perspective of protective design, both scenarios must result in an equivalent safe state; typically, emergency cooling activation and reactor shutdown.

The attack surface of modern ICS encompasses multiple pathways by which an adversary can induce unsafe control actions (Bhole et al., 2025). Remote access capabilities required for predictive maintenance and remote diagnostics create direct pathways for attackers to reach critical control logic without needing physical proximity to the facility. Software updates and patches, while essential for fixing security vulnerabilities, introduce a vulnerability window during which systems are at elevated risk if the update process itself is not rigorously secured (Edeh et al., 2025). The integration of non-safety-critical IT systems (e.g., enterprise resource planning, data analytics) with operational technology creates "bridges" whereby a successful attack on the business system can cascade to compromise the control system (Yu et al., 2023).

A particularly insidious attack vector is the compromise of sensors or field instrumentation. Safety systems rely on sensor inputs to monitor process conditions and determine when protective actions should be activated. An attacker who can manipulate sensor readings can induce false alarms (driving unnecessary protective actions that increase wear on safety devices and potentially damage the process), can suppress true alarms (preventing protective actions when they are actually needed), or can induce unsafe control actions by providing misleading process state information to control logic (Ma et al., 2024). Modern cybersecurity attacks on critical infrastructure, including the Stuxnet attack on uranium enrichment centrifuges and the Triton/TRISIS malware targeting safety systems in petrochemical facilities, demonstrate the sophisticated capability of well-resourced adversaries to specifically target safety systems with the intent of inducing unsafe states that bypass traditional protective measures (Khan & Madnick, 2021).

Integration Challenges and Organizational Barriers

Beyond the technical divergence between safety and security disciplines lies a significant organizational challenge: most industrial enterprises have historically segregated these functions within distinct organizational silos. Safety departments, often reporting through environmental health and safety (EHS) chains, focus on compliance with OSHA, EPA, and process safety management regulations. Cybersecurity departments, often nascent in industrial organizations, are sometimes embedded within IT and inherit frameworks designed for office network security rather than OT-specific threats (Link et al., 2018). This organizational segregation means that when convergence challenges arise, such as determining whether a particular control system should prioritize operator alertness (a safety concern) or encryption of remote access credentials (a security concern), there is often no established governance mechanism to make integrated decisions.

The technical expertise required for integrated safety-security assessment is uncommon. A traditional safety engineer possesses deep knowledge of process chemistry, failure mechanisms, and probabilistic risk assessment, but may lack cryptographic literacy or understanding of attack patterns. Conversely, a cybersecurity architect may be conversant with threat modeling and zero-trust architecture but lack understanding of process control loops, fail-safe design principles, or the specific operational constraints of

continuous process operations. The creation of integrated teams requires not merely adding security personnel to safety teams, but rather fostering a culture of mutual education and collaborative decision-making (Linnoosmaa et al., 2022).

From HAZOP to Cyber HAZOP (CHAZOP): Integrating Threat Modeling with Process Safety Analysis

Conceptual Evolution: Extending HAZOP Guide Words for Cybersecurity Deviations

The Cyber HAZOP (CHAZOP) methodology represents a conceptual bridge between traditional HAZOP's process-centric hazard identification and the adversarial threat modeling paradigm of cybersecurity (Heluany & GALVAO, 2023). Rather than replacing traditional HAZOP, CHAZOP extends the existing framework by introducing guide words and analytical lenses specifically designed to expose cyber-induced deviations from intended process operation.

Traditional HAZOP guide words (more, less, none, reverse, etc.) are primarily suited for continuous process parameters: temperature, pressure, flow rate, concentration. These guide words readily generate plausible process deviations; "more pressure" clearly represents an identifiable hazard scenario. However, when applied to digital control systems, these guide words must be augmented with cyber-specific variations. For example, a traditional analysis might identify that "failure of level control valve to close" (a mechanical failure) represents a hazard. The cyber-specific extension would recognize that the level control valve could also fail to close if:

- The valve control signal is intercepted and modified by an attacker before reaching the valve.
- The firmware controlling the valve actuator is compromised and ignores legitimate close commands.
- The sensor providing level feedback is spoofed to indicate a lower level than actual, preventing the control logic from recognizing that the valve should be closed.
- The safety interlock preventing the valve from remaining open indefinitely is disabled through logic manipulation.

By systematically applying cyber-specific guide word extensions across all nodes and functions in a process flow, CHAZOP enables identification of scenarios wherein cyber-attacks induce the same unsafe states as traditional hardware failures (Elleman et al., 2026). Importantly, this is not merely an additive exercise; CHAZOP must also evaluate whether the causal pathways for cyber-induced deviations differ from traditional pathways in ways that affect protective layer effectiveness (Hollerer et al., 2021).

Integration of Threat Modeling Frameworks: STRIDE, MITRE ATT&CK, and Attack Trees

CHAZOP achieves full rigor through systematic integration of established threat modeling frameworks. The STRIDE methodology, encompassing Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege, provides a structured vocabulary for characterizing cyber attacks (M. D. Silva et al., 2023). Each STRIDE category maps to specific attack vectors that could induce unsafe control actions:

- Spoofing of sensor data or control signals (e.g., an attacker impersonates a legitimate control command)
- Tampering with setpoints, alarm thresholds, or safety logic (e.g., modifying the maximum allowable pressure setpoint)
- Denial of Service to critical control functions (e.g., rendering communication channels unavailable so that control commands cannot reach actuators)
- Elevation of Privilege to access safety-related functions (e.g., an attacker gains administrative access to reprogram the safety logic controller)
- Information Disclosure of sensitive process parameters (e.g., an attacker learns the precise timing and logic of safety shutdown sequences)
- Repudiation of control commands (e.g., an attacker causes legitimate safety shutdown commands to be rejected as unauthorized)

The MITRE ATT&CK for ICS framework provides an empirical grounding for threat modeling by cataloging tactics and techniques observed in real-world attacks against industrial systems (Alawi, 2025). Rather than speculating about hypothetical attack scenarios, practitioners can reference documented instances wherein specific techniques have been successfully deployed, lending credibility to threat assessments and helping to prioritize defensive investments toward the most likely attack scenarios.

Attack tree analysis provides a visual and quantitative methodology for decomposing complex attack scenarios into constituent steps (Guzman et al., 2021). An attack tree for "compromise safety shutdown logic" might decompose into two parallel attack paths: (1) remote exploitation of a network-accessible vulnerability in the safety logic controller, and (2) insider compromise wherein an authorized user with legitimate access to the controller is socially engineered or coerced into installing malware. By quantifying the effort, skill requirements, and likelihood of success for each path, practitioners can identify which attack vectors represent the most plausible routes and therefore merit the most robust defensive measures.

CHAZOP Execution: Practical Methodology and Deliverables

The execution of CHAZOP follows an enhanced HAZOP process structure but with explicit cybersecurity focus integrated throughout. The preparation phase identifies not only the process boundaries (as in traditional HAZOP) but also the system boundaries encompassing IT systems, network connectivity, remote access points, and cybersecurity control infrastructure. The multidisciplinary team is enlarged to include cybersecurity specialists capable of articulating threat scenarios alongside process engineers who can evaluate consequences and identify protective measures.

For each process node and parameter, the traditional HAZOP analysis proceeds conventionally, identifying cause-consequence-safeguard chains for hardware-based failures. However, at the conclusion of each node analysis, a structured augmentation introduces cyber-specific deviations. Analysts ask: "For each identified hazard scenario, what cyber-attacks could induce the same unsafe state?" This is not merely a theoretical exercise; it must be grounded in plausible threat scenarios derived from the threat modeling analysis. For example, if CHAZOP identifies that high reactor pressure represents a hazard, and traditional HAZOP identifies "pressure relief valve sticks closed" as a cause, CHAZOP then systematically explores whether an attacker could induce high pressure through cyber means: manipulation of inlet flow control, modification of relief valve opening setpoint, spoofing of pressure sensor data to prevent relief valve actuation, or disabling of high-pressure alarm notifications.

The output of CHAZOP includes:

1. Hazard-Threat Mappings: Documentation of which identified hazard scenarios can be induced through both traditional failure mechanisms and cyber-attacks
2. Unified Risk Assessment: Quantification of the combined frequency of each hazard scenario across both accidental and intentional causal pathways
3. Protective Layer Adequacy: Evaluation of whether existing safety instrumented systems are resilient to cyber compromise of their own components
4. Cyber-Safety Requirements: Specification of additional cybersecurity controls (beyond traditional SIS requirements) needed to mitigate cyber-induced hazards
5. Integrated SIL-SL-T Requirements: Allocation of both Safety Integrity Levels and Target Security Levels to control systems, recognizing the interdependencies

Integrated Risk Assessment Methodology: From Specification through Commissioning

Dual-Risk Assessment Framework and Requirements Specification

The translation of CHAZOP outputs into actionable system requirements demands a rigorous integrated assessment framework that recognizes both the independence of some safety and security requirements and their critical interdependencies (Piesik et al., 2024). The specification phase must articulate requirements in a manner that permits independent design tracks (safety engineers designing SIS architecture, cybersecurity architects designing secure networks) while ensuring that downstream design decisions do not introduce vulnerabilities in either domain.

A dual-risk assessment framework structures requirements into four categories:

- Pure Safety Requirements: Specifications derived from functional safety analysis that are not materially affected by cybersecurity considerations (e.g., the safety shutdown valve must withstand process conditions and fail closed on loss of power)

- **Pure Security Requirements:** Specifications derived from cybersecurity analysis that do not impact process safety (e.g., user access logs must be protected from tampering for compliance and forensics purposes)
- **Dual-Domain Requirements:** Specifications that address both safety and security simultaneously (e.g., the safety logic controller must authenticate all incoming control commands to prevent injection attacks, while maintaining deterministic response times to ensure safe shutdown can occur within specified time horizons)
- **Trade-off Resolution Requirements:** Specifications that explicitly acknowledge conflicts between safety and security optimization and establish policy-level decisions about prioritization (e.g., "In the event of cybersecurity incident detection, safety interlocks shall remain functional and shall not be automatically disabled, even if disablement is requested by command from a potentially compromised source")

The specification document must be sufficiently precise to enable independent verification. For pure safety requirements, traditional IEC 61508/61511 specification methodologies apply. For pure security requirements, standard ISA/IEC 62443 specification guidance applies. For dual-domain requirements and trade-off resolutions, specification writers must employ structured language and formal requirements notation to eliminate ambiguity. Consider the requirement "the safety logic controller shall be protected against unauthorized modification." In a safety-only specification, this might be interpreted to mean protection against accidental corruption or damage. In an integrated specification, this must be explicitly clarified to mean protection against both accidental corruption AND intentional modification by unauthorized actors, including scenarios wherein an attacker with partial system access attempts to reprogram safety logic (M. Silva et al., 2025).

II. DESIGN METHODOLOGY

Safety-Security Co-Design and Architectural Patterns

The design phase translates integrated requirements into specific architecture, hardware selections, software designs, and operational procedures. Traditional design processes often proceed sequentially: safety engineers design the safety instrumented system to meet SIL requirements, and subsequently cybersecurity architects are tasked with "hardening" the design against attack. This waterfall approach is fundamentally flawed because cybersecurity measures (such as encryption, authentication, and network segmentation) must be designed into systems from the outset; retrofitting security often introduces new failure modes or reduces the determinism required for safety assurance (Shang et al., 2025).

Effective integrated design requires concurrent engineering, wherein safety and cybersecurity requirements simultaneously drive architectural decisions. Several design patterns have emerged as particularly effective:

Functional Isolation and Compartmentalization: Safety-critical control logic is isolated into dedicated, hardened platforms with minimal attack surface, rather than executing on general-purpose computers alongside non-critical functions. This principle aligns with the IEC 62443 concept of security zones: the safety logic controller resides in a zone with stringent access controls, limited inter-zone connectivity, and rigorous authentication for any commands traversing zone boundaries (Alawi, 2025).

Defense-in-Depth Through Architectural Layering: Multiple protective layers are implemented such that compromise of any single layer does not render the system unsafe. This principle is common to both safety and security but manifests differently in each domain. In safety, defense-in-depth might include primary control logic, redundant sensors with cross-checking, and independent alarm logic. In security, defense-in-depth might include network firewalls, application-level authentication, encrypted inter-system communications, and end-point intrusion detection (Wai & Lee, 2023).

Deterministic, Measurable Communication: All communications between control zones are explicitly enumerated, authenticated, and subject to strict latency requirements. Rather than permitting arbitrary TCP/IP traffic between zones (which is flexible but creates unbounded attack surface), architects specify precise message formats, response times, and allowable command repertoires. This enables both verification that communications are proceeding nominally and rapid detection of anomalous patterns (Tarek & Hasan, 2024).

Fail-Safe Default Behavior: When system security cannot be assured (e.g., during a cyber-attack or security incident), the system defaults to a safe state rather than attempting to continue normal operation under

potentially compromised control. This principle is fundamental to safety engineering, but is sometimes violated in security design that prioritizes system availability over safety. The integration principle is clear: availability of unsafe operation is not a desirable outcome (Khan & Madnick, 2021).

Verification and Validation: Integrated Assurance Approach

The verification and validation phase confirms that the designed system meets its specified requirements for both safety and security. Traditionally, these have been separate activities: safety engineers conduct functional testing to verify that safety interlocks activate correctly under fault conditions, and cybersecurity testers conduct penetration testing to identify security vulnerabilities. Integrated V&V must demonstrate that the system simultaneously meets its safety and security requirements and that security measures do not introduce failures that violate safety objectives.

Verification activities for integrated systems include:

- **Functional Safety Verification:** Traditional verification that all Safety Instrumented Functions meet their specified SILs, including: - Proof of correct sensor reading under nominal and fault conditions - Verification of safety logic correctness under normal, degraded, and failed states - Confirmation that final elements (e.g., shutdown valves) respond correctly to logic commands - Quantitative verification that Probability of Failure on Demand meets SIL requirements
- **Cybersecurity Verification:** Confirmation that all security controls function as designed and provide intended protection: - Testing of authentication and authorization mechanisms under simulated attack scenarios - Verification of encryption and data integrity protection under communication network disruption - Evaluation of firewall and network segmentation effectiveness against injection and lateral movement attacks - Assessment of monitoring and alerting systems' capability to detect security anomalies
- **Dual-Domain Verification:** Confirmation that security measures do not degrade safety and that safety assurance is maintained even under active cyber-attack conditions: - Testing of safety functions under conditions of partial cybersecurity compromise (e.g., attacker-controlled network segments) - Verification that safety shutdown can occur despite communications interference or network segmentation - Confirmation that authentication delays or certificate validation do not prevent timely safety responses - Assessment of operator situational awareness under scenarios where cybersecurity monitoring is consuming system resources

Commissioning Phase: Integrated Assurance and Transition to Operations

The commissioning phase represents the transition from factory testing to actual operational deployment. At this phase, the system must be proven to function correctly in the actual operational environment through comprehensive on-site testing and validation, which typically introduces complexity not fully replicated in factory testing. Traditional commissioning focuses on verifying that the system can be started safely, responds correctly to operator input, and maintains stable control of the process under normal operating conditions (Kim et al., 2025).

Integrated commissioning adds a cybersecurity dimension that demands formal security acceptance testing. This includes:

- **Network Segmentation Verification:** Confirmation that the implemented network architecture achieves intended isolation between security zones, that firewall rules enforce the specified policies, and that no unintended pathways exist for lateral movement between critical zones.
- **Access Control Validation:** Testing that authentication mechanisms function reliably, that authorized users can access only their assigned functions, and that audit trails accurately record all access and modifications to safety-critical systems.
- **Intrusion Detection Commissioning:** Calibration of anomaly detection systems to understand normal operational patterns, tuning of alert thresholds to minimize both false alarms (which erode operator confidence) and missed detections (which leave system vulnerable), and verification that detected anomalies trigger appropriate response procedures.

- Integrated Response Procedures: Verification that security incident response procedures, including procedures for disabling controls that may be compromised, isolating affected systems, and reverting to safe operation, can be executed quickly and effectively during actual incidents.

Secure Safety System Architecture: Achieving Simultaneous SIL and SL-T Certification

Defense-in-Depth Architecture for ICS Resilience

The architectural implementation of a system that is simultaneously Safety Integrity Level certified and Target Security Level capable demands a defense-in-depth strategy that integrates multiple protective layers across network, platform, application, and operational dimensions (Ramdass & Balaraman, 2025). Unlike traditional sequential defense (whereby each layer is expected to fail before the next layer engages), defense-in-depth for critical infrastructure must assume that every layer may be compromised and that the system must maintain functional safety assurance even under partial compromise.

The architectural framework commonly known as the "three-layer" or "three-frontier" model provides a practical structure for defense-in-depth implementation:

- Frontier 1 - Perimeter Defense: The first defensive layer establishes the boundary between the industrial control system and the broader enterprise IT network (and the Internet beyond). Firewalls at this frontier enforce the principle of "deny unless explicitly permitted," blocking all inbound connections except those explicitly required for authorized applications. Industrial-specific firewalls (such as those designed to understand Modbus, OPC-UA, and other industrial protocols) provide detection of anomalous commands that fall within the firewall's permitted traffic categories but represent suspicious patterns. Intrusion prevention systems at this frontier detect and block known attack signatures.
- Frontier 2 - Intra-Domain Defense: Within the trusted zone (industrial control network), security zones are created through internal network segmentation. Critical devices such as programmable logic controllers, safety instrumented systems, and human-machine interfaces reside in zones with restricted intra-zone traffic and strict controls on inter-zone communications. A compromised device in one security zone cannot easily propagate attacks to other zones. Endpoint protection on each device includes whitelisting of executable code (only explicitly approved software is permitted to execute), host-based firewalls, and intrusion detection agents that monitor for suspicious process behavior (Wai & Lee, 2023).
- Frontier 3 - Process Control Assurance: Even if an attacker bypasses perimeter and intra-domain defenses and gains access to control systems, the safety architecture itself provides assurance that unsafe control actions cannot occur. This is achieved through architectural means rather than purely cybersecurity means: redundant sensors, cross-checking logic that detects inconsistencies in control commands, fail-safe final elements that default to safe states, and independent safety shutdown systems that cannot be disabled through normal control logic (but can execute independently if their trigger conditions are met).

The integration of these three frontiers is essential; no single frontier can be solely relied upon. A perimeter firewall, while essential, cannot defend against insider attacks or advanced persistent threats that slowly establish footholds and exfiltrate data over time. Intra-domain defenses improve isolation but introduce operational complexity and may impact determinism of control systems. Process control assurance provides the ultimate safeguard but may impose constraints on operational efficiency. The three-frontier model recognizes that sustainable cybersecurity and safety assurance emerge from the combination of all three layers working synergistically (Tarek & Hasan, 2024).

Network Segmentation and Secure Inter-Zone Communication

Network segmentation, often referred to as "zero trust architecture" in the cybersecurity literature, reverses the default assumption in many industrial networks. Historically, systems connected to the same physical network (e.g., all devices on the control system LAN) were implicitly trusted to communicate with one another freely. Zero trust architecture assumes that every system requesting communication must authenticate its identity and authorization for the specific requested action, regardless of whether source and destination are on the same physical network.

Implementing zero trust in industrial control systems demands specific mechanisms:

- Demilitarized Zones (DMZs): Server clusters providing specific functions (e.g., secure gateway to enterprise network, historian database, SCADA master servers) are isolated in dedicated security zones accessible only through controlled entry points. This prevents a compromise in a less-critical system from providing a bridge to safety-critical systems (Alawi, 2025).
- Industrial Protocol Analysis: Firewalls and monitoring systems that understand industrial protocols (Modbus, OPC-UA, Profibus, HART) can distinguish between legitimate and anomalous command sequences. For example, a normal operator might issue multiple setpoint adjustment commands, but an attacker attempting to induce an unsafe state might issue a rapid sequence of setpoint changes that would be unusual from an operational perspective (Almulla & Rahman, 2025).
- Cryptographic Identity and Encryption: All inter-zone communications employ cryptographically authenticated protocols (such as TLS for network communications, digital signatures for control commands), ensuring that devices are communicating with intended counterparts and that messages have not been modified in transit. The requirement for cryptographic validation imposes latency and computational overhead that must be carefully managed to ensure that safety response times are not degraded (Ramdass & Balaraman, 2025).

The practical implementation of network segmentation in industrial environments confronts legacy system constraints. Many devices deployed decades ago lack cryptographic capabilities or have firmware that cannot be updated to support modern security protocols. The segmentation strategy must accommodate these legacy systems while protecting them from attack. Common approaches include:

- Unidirectional Data Diodes: Physical devices that permit information flow in only one direction, preventing any reverse-channel attack
- Secured Serial Communications: Encryption and authentication applied at the application layer above Modbus Serial or other serial protocols
- Industrial Gateways: Devices that translate between legacy protocols (non-encrypted, non-authenticated) in isolated zones and modern secure protocols in adjacent zones, with explicit validation that commands crossing the gateway comply with established safety policies (Boeding et al., 2025)

Monitoring, Detection, and Adaptive Response

Intrusion detection in industrial environments faces specific constraints absent from IT security contexts. In IT networks, behavioral anomaly detection can afford high false alarm rates because the cost of a false alarm (a brief degradation of service) is typically acceptable. In industrial control networks, a false alarm might trigger a protective shutdown, interrupting production and creating safety implications (e.g., a reactor batch ruined, production equipment thermally stressed by emergency cooling). Consequently, anomaly detection systems for ICS must achieve both high sensitivity (detecting true intrusions) and high specificity (avoiding false alarms).

Modern detection approaches integrate multiple data sources:

- Network Traffic Analysis: Characterization of normal network flows (which devices communicate with which, at what frequency, with what payload sizes and patterns) enables identification of anomalous traffic patterns suggesting lateral movement, data exfiltration, or new command patterns (Tarek & Hasan, 2024).
- Endpoint Behavioral monitoring: Tracking process control parameters, alarm history, and operator actions enables detection of anomalous control sequences or device states that suggest compromise. For instance, if a control valve that normally cycles predictably suddenly enters a state requiring manual operator intervention, this might indicate cyber interference in the valve's control logic (Lu et al., 2024).
- Event Log Correlation: Aggregation and analysis of security logs, system logs, and process history from multiple sources enables identification of attack patterns that would be invisible in individual log streams. A sophisticated attacker attempting to disable a safety alarm might create a pattern of multiple small, individually plausible events that collectively indicate malicious intent (Tarek & Hasan, 2024).

The integration of detection systems with adaptive response mechanisms enables organizations to maintain both safety and security assurance even under active attack. When anomalies are detected, response procedures must distinguish between true positives (actual security compromises requiring containment) and

false positives (operational transients or sensor noise). The response strategy must support graduated escalation:

- Level 1 - Enhanced Monitoring: When initial anomalies are detected, monitoring intensity increases, and alert thresholds are tightened to catch follow-on indicators of attack progression.
- Level 2 - Isolation and Segmentation: If anomalies persist or escalate, affected systems are isolated from critical control zones while non-critical functions are maintained.
- Level 3 - Controlled Shutdown and Safe State: If attack indicators suggest imminent compromise of safety-critical systems, procedurally controlled shutdown to safe state is initiated, preserving system integrity while ensuring physical process safety (Alawi, 2025).

Lifecycle Integration and Continuous Vulnerability Management

Operational Phase: Continuous Risk Assessment and Adaptive Controls

The transition to operations marks a fundamental shift in risk management philosophy. During design, risk assessment focuses on known threats and specified requirements. During operations, emerging threats, including zero-day vulnerabilities, novel attack techniques demonstrated against similar systems in other industries, and evolving capabilities of threat actors, create a continuously shifting risk landscape (Alawi, 2025).

The Evergreen OT Security Assurance Model provides a framework for continuous security assessment aligned with IEC 62443 principles. Rather than conducting security audits at discrete intervals (which may reveal vulnerabilities weeks or months after they have emerged), evergreen security integrates continuous monitoring, threat intelligence gathering, and risk re-assessment into operational processes. Organizations implementing evergreen security:

- Monitor real-time security metrics (intrusion attempts, blocked suspicious traffic, failed authentication attempts) to detect emerging patterns indicative of sophisticated, sustained attack campaigns.
- Subscribe to threat intelligence feeds providing information about newly discovered vulnerabilities affecting deployed equipment models.
- Conduct periodic risk re-assessments (typically annually or when significant system changes occur) to evaluate whether identified control gaps require remediation.
- Maintain backlogs of security improvement initiatives, prioritized by risk and feasibility, for systematic implementation during maintenance windows.

The integration of vulnerability management with functional safety assurance demands rigor absent from typical IT vulnerability management. In an enterprise IT environment, patching decisions are often made based primarily on vulnerability severity and asset criticality, with implementation constrained mainly by system availability requirements. In industrial control systems, patch decisions must additionally consider:

- Safety Impact Assessment: Does the patch change software behavior in ways that could affect determinism, response times, or failure modes? Some patches, while fixing security vulnerabilities, also modify control system algorithms, creating risk that the patch could itself induce unsafe states.
- Proof-Testing Requirements: IEC 61508/61511 typically mandate proof-testing of safety systems at prescribed intervals (often annually for SIL 2-3 systems). A patch applied to safety-critical software may invalidate previous proof-test results, requiring re-testing before the system can be returned to service.
- Change Management Procedures: Industrial plants typically maintain stringent change control procedures requiring documented approval, documented testing, scheduled implementation windows (often only during planned maintenance shutdowns), and documented verification post-implementation. Security vulnerability remediation must flow through these same procedures, which can create delays in applying critical patches (Ramdass & Balaraman, 2025).

Vulnerability Disclosure, Patch Timing, and Supply Chain Security

A particularly acute challenge emerges when critical vulnerabilities are discovered in deployed systems. Responsible vulnerability disclosure practices (whereby the discovering researcher provides advance notice to affected vendors before public disclosure) create a window during which organizations know they are vulnerable but do not have patches available. The typical window, 30 to 90 days from disclosure to patch

availability, can stretch months in industrial settings where vendor development and testing processes are slower than in IT-focused companies (Edeh et al., 2025).

During this vulnerability window, risk mitigation becomes critical. Temporary controls might include:

- Enhanced Compensating Controls: Increased network monitoring, air-gapping of vulnerable systems, or temporary restriction of remote access
- Risk Acceptance Documentation: Formal acknowledgment and documentation that the organization is accepting residual cyber risk for the vulnerable system until a patch becomes available
- Prioritized Patch Testing: Accelerated testing in lab environments to enable rapid deployment when patches become available

Supply chain security introduces additional complexity. Modern industrial equipment often contains software components from multiple vendors embedded within single devices. A vulnerability in a third-party library (such as an open-source cryptography library) might affect safety equipment from dozens of equipment manufacturers. Coordinating vulnerability disclosure, patch development, testing, and deployment across this fragmented ecosystem creates significant delay. Organizations must establish relationships with equipment vendors and maintain updated inventories of deployed software component versions to enable rapid assessment when vulnerabilities are disclosed (Heinl et al., 2025).

Decommissioning and Lifecycle Closure

The final phase of the system lifecycle, decommissioning of aging equipment, presents often-overlooked cybersecurity and safety risks. Legacy equipment that has reached end-of-life may contain sensitive data (historical operating records, equipment calibration data, security credentials stored in firmware). Improper decommissioning (discarding equipment without data destruction, or selling decommissioned equipment to third parties without removing sensitive data) can create pathways for attackers to extract information useful for compromise of remaining systems (Kosmowski et al., 2022).

Secure decommissioning requires:

- Data Identification and Classification: Determination of what sensitive information is stored on decommissioned equipment (memory, flash storage, or even mechanical state data in some devices)
- Secure Data Destruction: Verified destruction of all sensitive data, with documented evidence of destruction maintained for compliance purposes
- Device Disposition: Secure reuse, refurbishment, or destruction procedures that prevent sensitive information leakage

III. CONCLUSION

Toward Integrated Secure-Safe Industrial Systems

The convergence of functional safety and cybersecurity represents both an exceptional challenge and a profound opportunity for industrial enterprises. The CHAZOP framework, grounded in the established rigor of HAZOP and enriched with threat modeling discipline, provides a practical methodology for systematically identifying scenarios wherein cyber-attacks induce unsafe control actions and for designing unified protections that achieve both SIL certification and SL-T capability.

Successful implementation demands more than technical methodology; it requires organizational commitment to breaking down traditional silos between safety and cybersecurity disciplines, investment in cross-disciplinary team expertise, and recognition that security, unlike traditional safety assurance, demands continuous vigilance and adaptation as threat landscapes evolve (Linnosmaa et al., 2022). Industrial enterprises that navigate this convergence successfully will achieve systems that are simultaneously more resilient to both accidental failures and malicious attacks, protecting their workforce, assets, and critical societal functions against an increasingly sophisticated and determined adversarial threat environment (Zhou et al., 2021).

IV. REFERENCES

- [1] Alawi, N. A. (2025). Evergreen OT security assurance: A sustainable approach to OT cybersecurity risk management. SPE Conference at Oman Petroleum Energy Show.

- [2] Almulla, Z., & Rahman, H. (2025). The role of network segmentation and micro-segmentation in operational technology security. Digital Signal Processing and Signal Processing Education Workshop.
- [3] Bhole, M., Sauter, T., & Kastner, W. (2025). Enhancing industrial cybersecurity: Insights from analyzing threat groups and strategies in operational technology environments. IEEE Open Journal of the Industrial Electronics Society.
- [4] Bhosale, P., Kastner, W., & Sauter, T. (2024). Mapping ICS vulnerabilities: Prioritization and risk propagation analysis with MITRE ATT&CK framework and bayesian belief networks. IEEE International Conference on Emerging Technologies and Factory Automation.
- [5] Boeding, M., Hempel, M., & Sharif, H. (2025). End-to-end framework for identifying vulnerabilities of operational technology protocols and their implementations in industrial IoT. Future Internet.
- [6] Chen, Y., Jin, P., Wu, H., & Zhao, J. (2025). A novel lightweight CAN-based functional safety protocol for low-performance embedded systems. IEEE Sensors Journal.
- [7] Choi, J.-Y., & Byeon, S. (2020). HAZOP methodology based on the health, safety, and environment engineering. International Journal of Environmental Research and Public Health.
- [8] Cindrić, I., Jurčević, M., & Hadjina, T. (2025). Mapping of industrial IoT to IEC 62443 standards. Italian National Conference on Sensors.
- [9] Dan, S., Kim, J., Kim, I. H., Cho, S., Yoon, E. S., & Shin, D. (2015). Integrated framework for determining safety integrity level for improved process safety. Society of Chemical Engineers, Japan.
- [10] Deconinck, G., Luyts, J., & Boogaerts, G. (2025). Exploring complementarity between functional safety and cybersecurity in the chemical process industry. 2025 20th European Dependable Computing Conference Companion Proceedings (EDCC-C).
- [11] Demichela, M., & Pirani, R. S. (2013). Human factor analysis embedded in risk assessment of industrial machines: Effects on the safety integrity level. None.
- [12] Edeh, N., Öztürk, E., & Waedt, K. (2025). Adapting IEC 62443 for steganographic threat detection in ICS environments. Annual Conference of the IEEE Industrial Electronics Society.
- [13] Elleman, D., Christian, A. A., & Hale, J. (2026). LLM-assisted CPSTRIDE threat modeling for critical water infrastructure. International Conference on Cyber Warfare and Security.
- [14] Friedberg, I., McLaughlin, K., Smith, P., Laverty, D., & Sezer, S. (2016). STPA-SafeSec: Safety and security analysis for cyber-physical systems. Elsevier BV.
- [15] Gholami, B., Jabbari, M., & Eskandari, D. (2024). Safety integrity level (SIL) determination and verification for gas turbine and generator in a combined cycle power plant. Journal of Health and Safety at Work.
- [16] Guzman, N. H. C., Kozine, I., & Lundteigen, M. A. (2021). An integrated safety and security analysis for cyber-physical harm scenarios. Elsevier BV.
- [17] Hanssen, G., Thieme, C., Bjarkø, A. V., Lundteigen, M., Bernsmed, K., & Jaatun, M. (2023). A continuous OT cybersecurity risk analysis and mitigation process. Proceeding of the 33rd European Safety and Reliability Conference.
- [18] Heinl, M. P., Reuter, A., Peters, S. N., & Bever, M. (2025). Leveraging BRSKI to protect the hardware supply chain of operational technology: Opportunities and challenges. ACM Symposium on Applied Computing.
- [19] Heluany, J. B., & GALVAO, R. C. (2023). IEC 62443 standard for hydro power plants. Multidisciplinary Digital Publishing Institute.
- [20] Hollerer, S., Kastner, W., & Sauter, T. (2021). Towards a threat modeling approach addressing security and safety in OT environments. IEEE International Workshop on Factory Communication Systems.
- [21] Hu, Y., Su, Z., Wang, Z., & Wang, H. (2023). Research on safety integrity level assessment for stage machinery of temporary performance site. 2023 International Conference on Culture-Oriented Science and Technology (CoST).
- [22] Iturbe, E., Rios, E., Mansell, J., & Toledo, N. (2023). Information security risk assessment methodology for industrial systems supporting ISA/IEC 62443 compliance. 2023 International Conference on Electrical, Computer and Energy Technologies (ICECET).

- [23] Jeong, D., Kwon, G., & Kwon, R. (2025). Probabilistic SIL verification of a synthesized fault-tolerant model for reliable safety assessment. IEEE Access.
- [24] Julserccwong, A., & Thepmanee, T. (2018). Design and implementation of functional safety for repairable systems. Annual Conference of the Society of Instrument and Control Engineers of Japan.
- [25] Khan, S., & Madnick, S. (2021). Cybersafety: A system-theoretic approach to identify cyber-vulnerabilities mitigation requirements in industrial control systems. IEEE Computer Society.
- [26] Kim, Y., Han, S., Song, H., & Jung, S. (2025). Risk assessment of an off-site hydrogen refueling station: A hybrid IEC 61511-CCPS LOPA framework. Energies.
- [27] Kosmowski, K., Piesik, E., Piesik, J., & Śliwiński, M. (2022). Integrated functional safety and cybersecurity evaluation in a framework for business continuity management. Multidisciplinary Digital Publishing Institute.
- [28] Link, J., Waedt, K., Zid, I. B., & Lou, X. (2018). Current challenges of the joint consideration of functional safety & cyber security, their interoperability and impact on organizations: How to manage RAMS + s (reliability availability maintainability safety + security). International Conference on Reliability, Maintainability and Safety.
- [29] Linnosmaa, J., Papakonstantinou, N., Malm, T., Kotelba, A., & Pärssinen, J. (2022). Security and safety integration for the nuclear instrumentation and control systems. IEEE International Conference on Emerging Technologies and Factory Automation.
- [30] Lu, X., Wu, K., & Chen, Y. (2024). Enhancing situational awareness in industrial automation and cybersecurity through an integrated framework that leverages both machine learning and deep learning technologies. 2024 IEEE 5th International Conference on Pattern Recognition and Machine Learning (PRML).
- [31] Ma, R., Hu, Z., Yang, H., Jiang, Y., Huo, M., Luo, H., & Yang, R. (2024). Adversarial FDI attack monitoring: Toward secure defense of industrial electronics. IEEE Industrial Electronics Magazine.
- [32] Parekh, M., Waedt, K., & Tellabi, A. (2021). 28. September - 2. Oktober 2020. None.
- [33] Park, S., Lee, T. H., Kang, K., Noh, H., Kim, H., Oh, J., Kim, K.-H., & Cho, S. (2023). Risk assessment of solid desiccant dehydration package system using safety integrity level-based safety instrumented system design approach. Process Safety Progress.
- [34] Piesik, E., Śliwiński, M., Subramanian, N., & Zalewski, J. (2024). Concept of multifactor method and non-functional requirements solution to increase resilience through functional safety with cybersecurity analysis. Eksploatacja i Niezawodność – Maintenance and Reliability.
- [35] Ramdass, K., & Balaraman, N. K. (2025). Securing industrial control systems: PLC, SCADA, and HMI protection. IEEE Conference on Systems, Process and Control.
- [36] Rehail, Y., Zennir, Y., Larit, K., & Tchouar, N. (2024). Evaluation of safety instrumented system using “HAZOP-LOPA-FTA” methodology. Algerian Journal of Signals and Systems.
- [37] Riad, B., Hamid, B., Hind, R., & Youcef, Z. (2018). Design of an integration frame HAZOP-SIL for safety optimization of a fired heater. International Conference on Electrical Sciences and Technologies in Maghreb.
- [38] Shang, W., Lu, J., Cao, Z., Ding, L., Zhang, M., & Huan, S. (2025). A tree-based scheme to assess the safety and security for industrial control systems. IEEE Transactions on Dependable and Secure Computing.
- [39] Silva, M. D., Puys, M., Thevenon, P.-H., Mocanu, S., & Nkawa, N. (2023). Automated ICS template for STRIDE microsoft threat modeling tool. ARES.
- [40] Silva, M., Mocanu, S., Puys, M., & Thevenon, P.-H. (2025). Safety-security convergence: Automation of IEC 62443-3-2. Computers & Security.
- [41] Swain, K., & Venkatraman, K. (2024). Application of cybersecurity policies and standards in indian power sector. National Power Systems Conference.
- [42] Tarek, J. H., & Hasan, Z. (2024). ADAPTING PLC/SCADA SYSTEMS TO MITIGATE INDUSTRIAL IOT CYBERSECURITY RISKS IN GLOBAL MANUFACTURING. American Journal of Interdisciplinary Studies.
- [43] Wai, E., & Lee, C. K. M. (2023). Seamless industry 4.0 integration: A multilayered cyber-security framework for resilient SCADA deployments in CPPS. Applied Sciences.

-
- [44] Wang, J.-H., Huang, C.-Y., Chou, H., Wang, C.-Y., Kuo, H., & Ting, V. (2023). Security service architecture design based on IEC 62443 standard. 2023 IEEE 3rd International Conference on Electronic Communications, Internet of Things and Big Data (ICEIB).
- [45] Xin, Y. (2023). Protection architecture of endogenous safety and security for industrial control systems. Secur. Saf.
- [46] Ye, W., Wang, J., Wei, Z., Wang, Z., & Zhang, L. (2025). SIL assessment of safety instrumented systems in oil and gas stations based on STPA-bow-tie. Elsevier BV.
- [47] Yu, Z., Gao, H., Cong, X., Wu, N., & Song, H. (2023). A survey on cyber-physical systems security. IEEE Internet of Things Journal.
- [48] Zhou, C., Hu, B., Shi, Y., Tian, Y.-C., Li, X., & Zhao, Y. (2021). A unified architectural approach for cyberattack-resilient industrial control systems. Proceedings of the IEEE.