

From Airgap to Zero Trust–A Systematic Review of Operational Technology Cybersecurity Technologies for Critical Infrastructure in the Era of ICS–Specific Malware

Dr.A.Shaji George¹, Dr.T.Baskar², Dr.P.Balaji Srikaanth³, Dr. Digvijay Pandey⁴

¹Independent Researcher, Chennai, Tamil Nadu, India.

²Professor, Department of Physics, Shree Sathyam College of Engineering and Technology, Sankari Taluk, Tamil Nadu, India.

³Associate Professor, Dept of Networking and Communications, School of Computing, SRM Institute of Science and Technology, Kattankulathur, Tamil Nadu, India.

⁴Department of Technical, Education, Lucknow, Uttar Pradesh, India.

Abstract – Traditionally, Operational Technology (OT) environments were comprised of programmable logic controllers (PLCs), distributed control systems (DCSs), safety instrumented systems, and the industrial networks that connect them, which were protected by physical isolation and obscurity. Today, with the merging of information technology (IT) and operational technology (OT) in the era of Industry 4.0, the proliferation of remote access and the increasing number of cloud-connected industrial IoT, that isolation has been broken. At the same time, the threat landscape has evolved, with Dragos reporting 1,693 ransomware attacks against industrial organisations in 2024, representing an 87% increase from the previous year, and the first-ever weaponization of Modbus TCP in a real district-heating system with the emergence of the FrostyGoop malware. To assess the state of OT cybersecurity technology today, this review systematically combines and summarizes peer-reviewed literature, standards documents ISA/IEC 62443, NIST SP 800–82 Rev. 3, NIST SP 800–207, and government advisories CISA, ENISA and vendor threat intelligence published between 2015 and 2026 across five domains asset visibility and passive network monitoring, network segmentation and zero-trust architectures, anomaly detection using artificial intelligence and machine learning, secure remote access and identity management, and resilience engineering including digital twins and consequence-driven design. We discover that detection and visibility technologies have come a long way, while patch management, cryptographic protection of legacy protocols and standardised resilience metrics are still in its infancy. Practitioners and researchers distill five key messages. We define labeled OT datasets research gaps, explainable anomaly detection for safety-critical loops, supply-chain assurance for firmware and quantitative cyber-physical risk models. The review's conclusion is that OT security needs to be rethought as a problem of consequence management, where technology choices are made based on the physical impact, rather than IT-centric measures of confidentiality.

Keywords: Operational Technology, Industrial Control Systems, ICS malware, Zero Trust Architecture, IEC 62443, Anomaly detection, Cyber-physical resilience, Critical infrastructure, IT/OT convergence, FrostyGoop.

1. INTRODUCTION

Operational Technology is the technology that monitors and controls physical processes such as turbines, pumps, valves, breakers, robotic arms and chemical reactors in energy, water, manufacturing, transportation, and healthcare. Whereas enterprise IT has a security triad where the focus is on confidentiality, OT has the security triad inverted availability and physical safety are most important, and a mis-timed reboot can be more critical than a data leak. This inversion is very significant for the design of technologies. Equipment life cycles are 15 to 25 years, controllers often are unable to host software agents, and industrial protocols like Modbus, DNP3, PROFINET, and EtherNet/IP were developed when the network was considered a trusted one and therefore do not have built-in authentication or encryption.

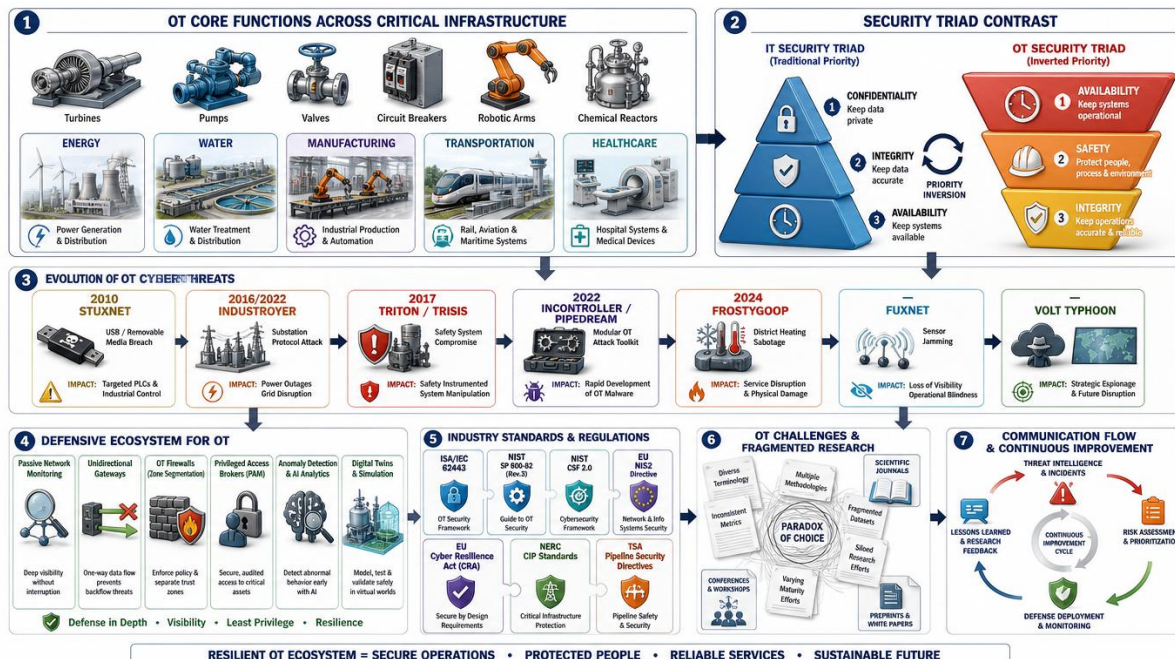


Fig -1: OT Core Functions Across Critical Infrastructure

The implicit security model for decades has been the air gap. There was a physical separation between control networks and corporate networks and the internet and specialist knowledge to manipulate a PLC was deemed to be sufficient. Stuxnet 2010 showed that an air gap could be bridged with removable media and that attackers could get a very detailed knowledge of vendors. Industroyer 2016 and Industroyer2 2022 demonstrated how to directly manipulate substation protocols to de-energize parts of the Ukrainian grid. Triton/TRISIS 2017 attacked a safety instrumented system which is the final line of defence against catastrophic physical failure. INCONTROLLER/PIPEDREAM 2022 developed a modular and vendor independent toolkit that can communicate with a few controller families. Every time there was an incident, it took away the notion that OT was too obscure or too isolated to attack.

2024-2026 is a qualitative change. In April 2024, Dragos discovered FrostyGoop and it was deployed in January 2024 against the Lviv district heating system, which directly sent Modbus TCP commands resulting in over 600 apartment buildings being left without heat for two days in subzero temperatures. When Dragos scanned again, it found more than 46,000 Modbus-speaking devices that were connected to the Internet. The Blackjack group is believed to have jammed tens of thousands of sensors in the city of Moscow's monitoring system with Fuxnet. In the meantime, state-sponsored groups like Volt Typhoon also

known as VOLTZITE by Dragos have been seen pre-positioning in North American utilities, stealing GIS data, network diagrams, and operating procedures, which are all essential ingredients for future disruptive operations. In 2024, Dragos analysed a total of 75% of industrial ransomware cases, which are largely IT-borne, but resulted in OT consequences, including 25% of cases that saw a full shutdown of an OT site. According to Dragos' tracking, the trend is accelerating, as 1,211 industrial ransomware incidents have been seen in Q4 2025 alone.

In response to this threat landscape, a significant OT defensive technology ecosystem has developed passive OT network monitoring platforms, unidirectional gateways, OT-aware firewalls, privileged remote-access brokers, AI-driven anomaly detection, and digital twins to simulate attacks. Standards have also all evolved in parallel, with ISA/IEC 62443 adding a new 62443-2-1 2025 and new parts covering IIoT devices, supplier evaluation, and industry profiles, NIST SP 800-82 moving to Revision 3, and NIST CSF 2.0 adding a Govern function. The EU NIS2 Directive, Cyber Resilience Act, NERC CIP, and TSA pipeline directives have increased the rigor of requirements for regulators.

However, research on these technologies is spread out in engineering journals, computer science conferences, standards organizations, and commercial threat reports, and it uses varying terminology and lacks independent studies of effectiveness. A paradox of choice exists for practitioners, and researchers do not have a clear overview of the areas of strong and weak evidence. The aim of this review is to bridge that gap.

2. OBJECTIVE

The main goal of this review is to critically synthesize the current state of the art of OT cybersecurity technology and assess the evidence of its effectiveness against the current threats, including ICS-specific malware and the spillover from IT to OT ransomware.

Specific objectives are:

- Identify the key types of OT defense technology and align them to the phases of the attack that they defend against, based on the taxonomy of MITRE ATT&CK for ICS.
- Evaluate the maturity of each category based on peer evaluated, standards-aligned, and documented field deployed.
- Discuss the impact of governance frameworks such as IEC 62443, NIST SP 800-82 Rev. 3, NIST SP 800-207 and NIS2 on technology selection and implementation.
- Summarize 5 key messages, based on evidence, for asset owners, integrators, and researchers.
- Determine research areas that have not been explored and suggest areas for future research.

3. METHODOLOGY

This review used a structured narrative approach, modified for a field where much authoritative evidence is found in non-publication sources government advisories, standards, and incident reports, among others as well as peer-reviewed journals.

Search strategy. Publications between January 2015 and mid-2026 were searched in IEEE Xplore, ACM Digital Library, ScienceDirect, SpringerLink, arXiv and Google Scholar. The search strings used included

controlled terms operational technology, industrial control system, SCADA, ICS security, and cyber-physical system security, plus the technology terms anomaly detection, intrusion detection, zero trust, segmentation, unidirectional gateway, digital twin, remote access, asset inventory, and IEC 62443. The sources of the grey literature included the CISA ICS advisories and joint cybersecurity advisories, ENISA threat landscape reports, the Dragos OT/ICS Cybersecurity Year in Review series 2018-2025, Dragos quarterly ransomware analyses, Claroty, Nozomi Networks and Fortinet state-of-OT reports, and standards texts from ISA/IEC and NIST.

Inclusion criteria. Sources were only included if they were related to defensive technology or architecture in an OT/ICS context if they were the result of empirical evaluation, documented deployment, or normative guidance from a recognised standards body and if they were accessible in English. Theoretical proposals, that were not evaluated, marketing material without technical detail and IT only security studies were excluded unless they specifically discussed the effects at the IT/OT boundary.

Screening and synthesis. After title and abstract screening, an initial corpus of about 640 items was obtained which was further narrowed down to 187 items after full-text assessment. All the resources retained were scored on a framework that included technology category, MITRE ATT&CK for ICS tactic(s) addressed, evaluation type testbed, simulation, field deployment, expert consensus, sector, and standards alignment. The incident record was triangulated by using recent comprehensive surveys, such as the 2025-2026 arXiv tutorial survey cataloguing 69 cross-validated incidents from 2010 to 2025.

Quality appraisal. Peer-reviewed studies were evaluated with respect to testbed realism whether the testbed was physical or purely simulated, provenance of the datasets, and their reproducibility. Grey literature was evaluated, based on the transparency of methodology and freedom from product promotion. With vendor data e.g. ransomware counts figures have been cross-checked with at least one independent source.

Limitations. There's survivorship bias and report bias as only publicly disclosed incidents are reported. Vendor telemetry is not a random sample, but rather customer bases. The limitations are recognised when making quantitative claims.

4. ASSET VISIBILITY IS THE NON-NEGOTIABLE FOUNDATION, AND MOST ORGANISATIONS STILL LACK IT

All security programs start with knowing what you have, but asset inventory is the most common gap in security benchmark assessments, especially when it comes to OT assets. Dragos's 2025 Year in Review has also found that most of the organisations they have assessed lacked visibility or had limited visibility into their OT networks, and CISA's ICS guidance repeatedly mentions how brownfield environments legacy controllers with modern IIoT devices often have undocumented assets, forgotten engineering workstations, and dual-homed devices connecting zones that were thought to be separated.

The technological answer has been passive network monitoring, sensors placed on SPAN or TAP ports that are able to decode the industrial protocols (Modbus, DNP3, IEC 61850, S7comm, CIP) without sending traffic. This is a very important design requirement. Active scanning tools used on IT networks have resulted in controller failures and process disruptions, while passive discovery doesn't pose the same threat and provides a listing of devices, firmware, communications, and logical zones. Now, platforms in this category are mature enough to have transitioned from proof-of-concept to comparative field

evaluation and the ISA/IEC 62443-2-1 update has taken the best practice of inventory and turned it into an organisational cybersecurity management requirement.

There are 3 downstream functions of visibility. Firstly, it allows prioritizing vulnerabilities. Only 6% of OT vulnerabilities were categorized by Dragos as Now meaning they need to be addressed immediately for operational impact, 63% were categorized as Next these vulnerabilities may have an impact on operations but are mitigated by architecture and 31% were categorized as Never these vulnerabilities are unlikely to have direct impact on operations. If an organisation doesn't have an accurate inventory and knowledge of network exposure it cannot make that triage and will either patch indiscriminately with the risk of downtime or not at all. Second, to detect it, it must be visible the odd network activity that indicates VOLTZITE reconnaissance can only be identified in the context of normal network activity. Third, segmentation design is based on inventory, you can't draw zones and conduits around unknown assets.

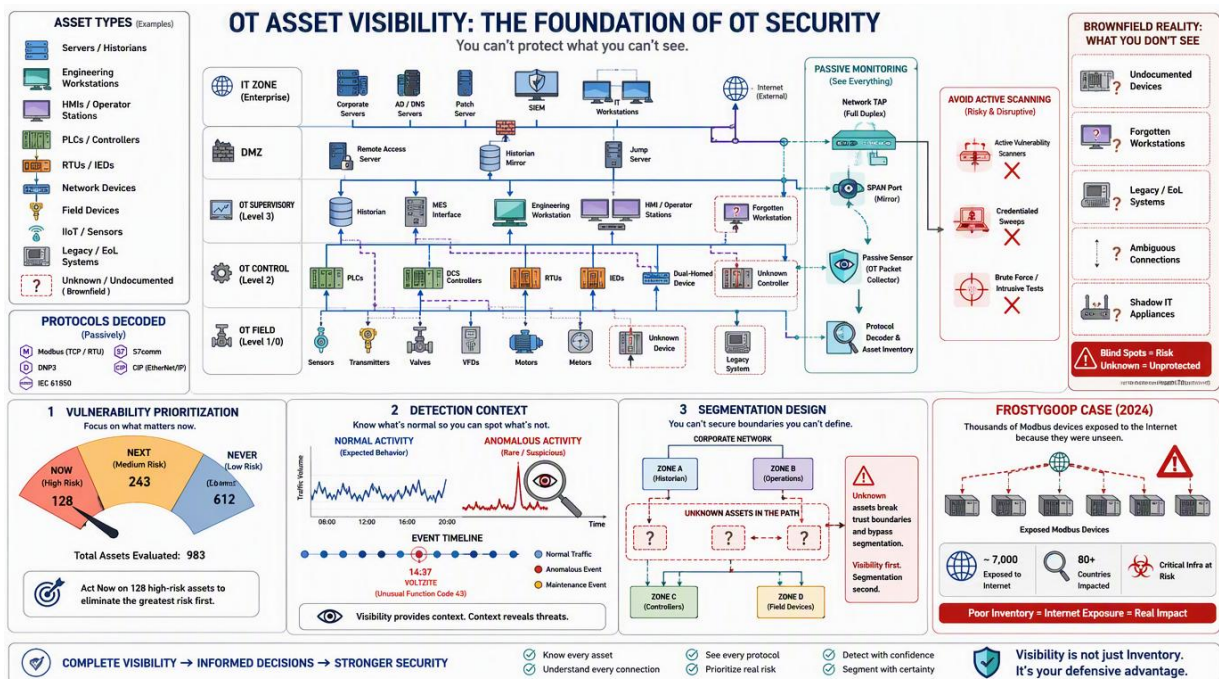


Fig -2: OT Asset Visibility the foundation of OT Security

The FrostyGoop case is a case in point. The 46,000 Modbus devices Dragos found online are not necessarily high-tech attacks, but rather simply an oversight of inventory, meaning that operators either didn't know they were exposed or that they didn't know they existed. Fuxnet's purported effectiveness against Moscollector was based on the use of systems that are accessible via the internet and have default credentials. Evidence gaps remain. There are limited independent studies that quantify inventory accuracy on the various platforms and coverage of serial, wireless, and proprietary protocols is inconsistent. However, the message in the peer-reviewed literature, standards and threat intelligence is clear Asset visibility is the greatest bang for your buck when it comes to OT security investments, and it should come first.

4.1 Segmentation is evolving from static zones to identity-aware zero trust, but the Purdue model is not obsolete

The Purdue Enterprise Reference Architecture (PERA), which has been the main paradigm for OT segmentation for 20 years, is part of ISA-95 and has been adopted by the zone-and-conduit model of IEC 62443. It has a hierarchical structure, from field devices (Level 0) to control (Levels 1-2), to site operations (Level 3), to a demilitarised zone (Level 3.5), to enterprise IT (Levels 4-5) and has firewalls that control the traffic between the levels. Cloud connectivity, IIoT sensors directly reporting to analytics platforms and vendor remote access have made the hierarchy porous, critics say. The idea of the model was not to be strictly topological, but to establish trust boundaries and to regulate conduits between them, proponents respond.

Based on the literature reviewed, a synthesis of the model is that the Purdue model is still useful as a conceptual model for consequence based zoning however, its enforcement mechanisms need to change. Three technology advances show that.

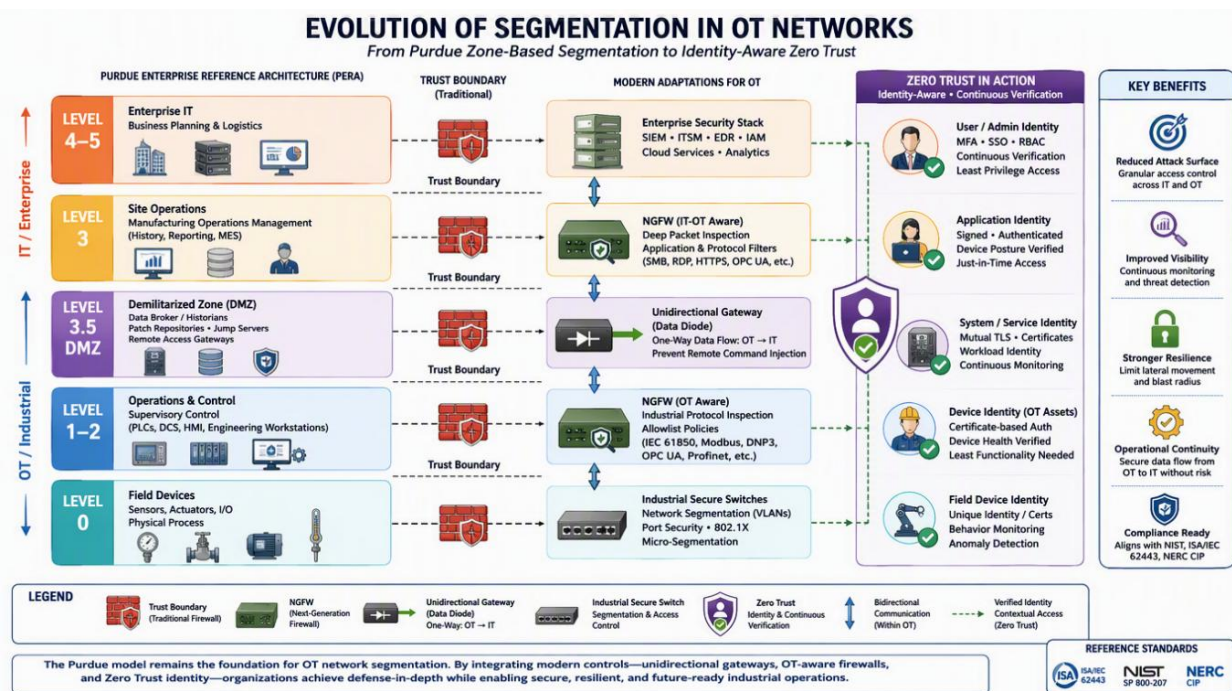


Fig -3: Evolution of Segmentation In OT Networks

1. First, unidirectional security gateways data diodes ensure that the data flows in one direction only from OT to IT, and that there is no path back for ransomware and remote attackers to go. They are proven, in use at nuclear and power plants, and are becoming more affordable for mid-tier applications, but they make it more difficult to have legitimate bidirectional requirements like remote maintenance.
2. Second, next-generation firewalls that are OT aware can do deep packet inspection of industrial protocols and enforce policies at the function-code level, such as allowing Modbus reads, but blocking writes from unauthorized sources. If they had existed at the conduit at the time of the write commands, they would have directly limited the write commands of FrostyGoop.
3. Third and most importantly, is the adaptation of Zero Trust Architecture (NIST SP 800-207) to OT. CISA released a guide for adopting a zero-trust approach to OT environments, and the Cloud

Security Alliance (CSA) released manufacturing-specific analysis. With a zero trust approach, trust in the network location is eliminated and replaced with continuous verification of identity, device posture, and context. The literature in OT suggests that the most promising insertion points are IT-OT border and engineering network, and that it is not possible to rely on agent-based endpoint enforcement as most controllers cannot support this. There is still a lack of empirical research and the evidence reviewed suggested that zero trust on OT is currently a path of maturity and not a deployed end state.

The takeaway is that segmentation should be multi-layered physically at the highest consequence boundaries, protocol aware policy at conduits and identity centric controls for human and machine access. Security levels (IEC 62443-3-3) allow them to correlate the enforcement level with the criticality of the zone.

4.2 AI-driven anomaly detection outperforms signatures for novel ICS threats, but explainability and dataset scarcity limit trust in safety-critical settings

In OT, the biggest problem with signature-based intrusion detection Snort, Suricata, YARA is that it relies on a known signature, and at the time of deployment, the most significant ICS malware Signature Triton, Signature INCONTROLLER, Signature FrostyGoop was new. Furthermore, rule sets are IT-centric, and do not have a lot of built-in support for the semantics of industrial protocols. All the surveys reviewed come to the same conclusion Signature-based tools are needed for known threats but are not enough by themselves.

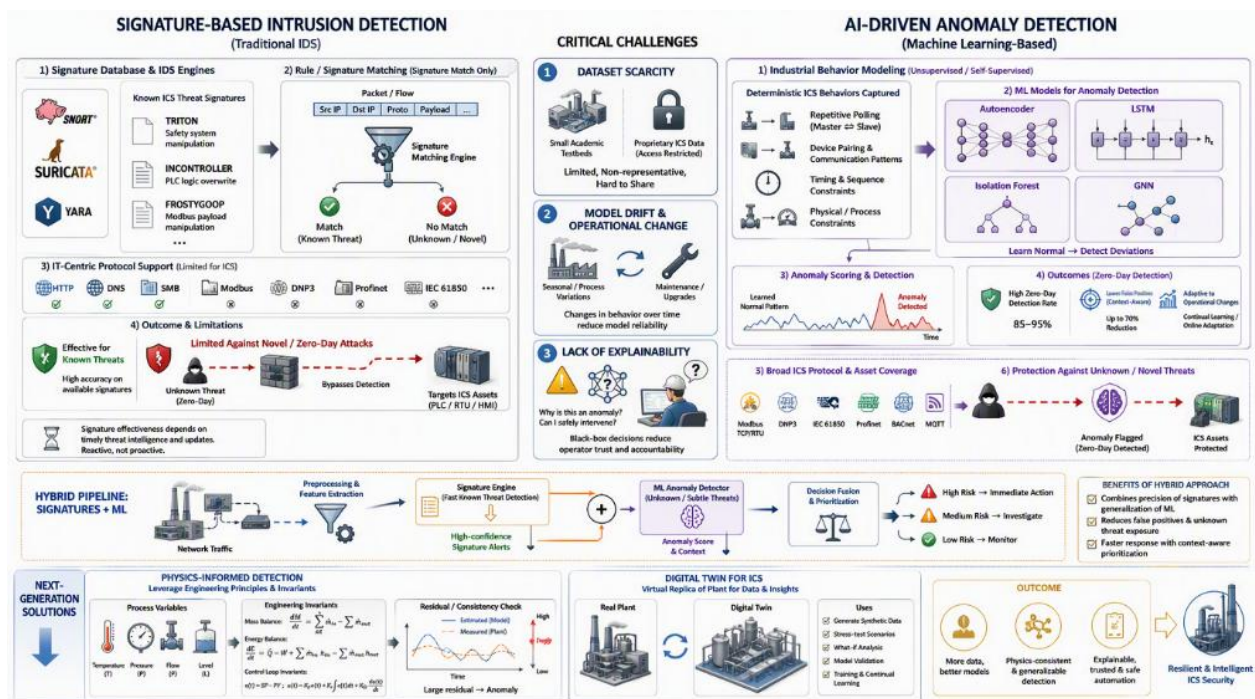


Fig -4: Signature Based Intrusion and AI Driven Anomaly Detection

Machine learning-based anomaly detection fills this void by learning and modelling the normal process and network behavior and alerting anomalies. In principle, OT is very suitable for this approach industrial traffic is very deterministic with repetitive polling cycles, fixed device pairings, and physically constrained

process variables. Unsupervised and semi-supervised models autoencoders, LSTM-based sequence models, isolation forests, and graph neural networks that model device relationships have been shown to have higher detection rates and lower false-positive rates than signature approaches for zero-day and process-manipulation attacks on testbeds like SWaT Secure Water Treatment and WADI. The combination of signatures for known threats and ML for novel behaviour hybrid pipelines always perform better than either approach on its own.

Three caveats are found throughout the literature, however.

1. First is the lack of datasets that are few, small, and publicly available labelled OT attack datasets exist, and they are based on academic testbeds which may not capture the level of heterogeneity found in industry. Proprietary data in the field is not readily available to train models on, and models trained on them have poor generalisations.
2. Second, model drift and operational change Alert fatigue for under-resourced OT security teams is caused by legitimate process changes, maintenance activities, and seasonal variations, which are not attacks.
3. Third, and most importantly, explainability if an alert issued by a controller is that its behaviour is anomalous, and the operator must decide whether to intervene in a live physical process or not. In safety critical decision making, interpretable evidence, i.e. which variable, which device, how far from expected, is required, is only partially given by the current deep-learning approaches.

One new response is called physics informed detection. These approaches incorporate engineering reality, known process dynamics mass balance, thermodynamic constraints, control loop invariants, which reduces false positives and provides explanations based on engineering reality and not statistical distance. Digital twins further take this one step further by creating synthetic attack data to train. The takeaway for practitioners is that AI-driven detection is a powerful and evolving capability that is most defensible today when used to detect network-level anomalies at the IT-OT boundary and engineering network, and process-level variables with proper human in the loop protections. Realistic, shared data sets and physics aware models that explain the data are the most valuable inputs for researchers.

4.3 Remote access and identity are the dominant initial-access vector secure them first

If you look at the incident record, you'll see a pattern Most OT compromises start with a non-exotic controller exploit. They start by either gaining credentials, remote-access services, or an IT foothold which is pivoted to OT. Many of the intrusions Dragos saw in 2025 were due to known vulnerabilities, weak remote access configurations, and exposed OT assets, according to the company's 2025 review, which details brute-force attacks against Cisco, Fortinet, and Palo Alto VPN appliances used to guard electric, oil and gas, water, and manufacturing networks in North America. APT28 GRAPHITE used compromised Ubiquiti Edge Routers to harvest credentials and for command and control. Volt Typhoon's living off the land tradecraft relies on legitimate administrative tools and valid credentials instead of malware. With the normalization of remote engineering, vendor support and integrator access after the pandemic, these avenues have increased many times over. Workstations with direct access to the controllers are accessible through VPNs, jump hosts and all too frequently directly exposed remote desktop services. The exposure is exacerbated by shared vendor accounts, default credentials on controllers and HMIs and flat authentication domains that cover both IT and OT.

The technology world has reacted with a few capabilities that are now coming together. Privileged remote access brokers, also known as Secure Remote Access (SRA) platforms in the OT market, provide a

hardened intermediary to mediate all external sessions, which enforces multi-factor authentication, time-bound access approvals, session recording and protocol restrictions, and enables a vendor engineer to connect to a specific HMI for a specific window without ever having network-level access. In an OT setting, where it was common to have shared operator logins, identity governance adds the concept of named accounts, role-based access, and periodic review. we talked about the identity centric model and how it applies to the network, but ZTNA takes that to remote users. There are unidirectional gateways with controlled reverse flow remote screen view which give monitoring without command capability. Although less common than for detection technologies, there is a compelling incident evidence base for peer-reviewed evaluations of these controls. In incidents where SRA and MFA were deployed, the adversaries either were unable to reach OT or were detected at the broker. Where they did not exist, the classic example is the compromised legacy VPN account of Colonial Pipeline without MFA IT compromise meant operational shutdown.

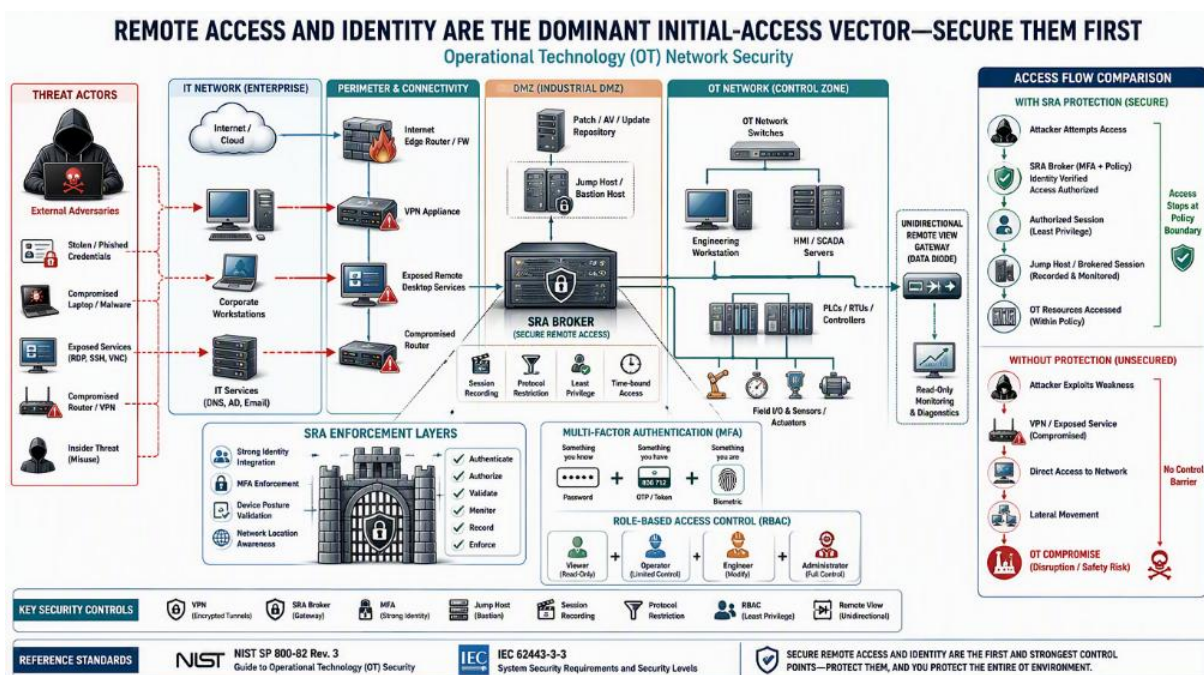


Fig -5: Remote Access and Identity are the Dominant Initial Access Vector

The bottom line is Prioritise. Hardening remote access and identity provides more risk reduction per dollar spent than most investments in detection, which is the vector that the adversary is using. IEC 62443-3-3 Foundational Requirements 1 Identification and Authentication Control and 2 Use Control, and NIST SP 800-82 Rev. 3, offer a pathway to implementation in the form of CISA's zero-trust guidance for OT.

4.4 Resilience engineering consequence-driven design, digital twins, and recovery rehearsal is the frontier

Prevention and detection are important but, with so many adversaries and legacy assets that can't be patched, they're not enough. The literature surveyed indicates an increase in the focus on resilience, the ability to remain safe in operation when attacked and to recover quickly. This frontier is determined by three technology and method clusters.

Idaho National Laboratory's consequence driven, cyber-informed engineering (CCE) turns the traditional risk assessment process on its head. CCE starts with the physical events that would have the greatest impact on an organisation's operations and asks the question what are the digital pathways that could cause these events rather than enumerating vulnerabilities and asking how they could be exploited. Then, engineered, non-digital safeguards mechanical relief valves, hard-wired interlocks, manual fallback procedures are used to disconnect those pathways. The targeting of a safety instrumented system by Triton is a good illustration of why this is important. If the digital safety layer can be compromised, then the real last line of defense is non-digital protection. The Cyber-Informed Engineering principles are now included in the U.S. Department of Energy guidance and are in keeping with the risk-based security level assignment of IEC 62443.

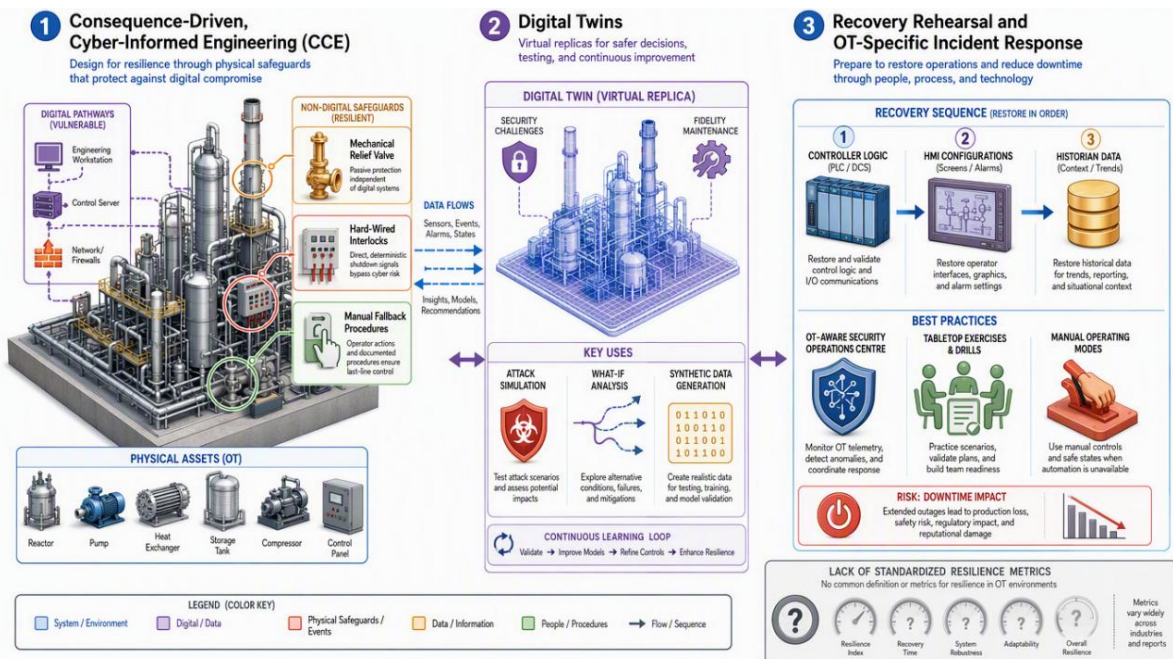


Fig -6: Consequence Driven Cyber Informed Engineering

Digital twins are virtual copies of physical OT systems, which reflect the real-time state of the physical systems. Their cybersecurity applications are increasingly documented in peer-reviewed studies, and include attack simulation without touching production, what-if analysis of segmentation or patch changes, and generation of synthetic datasets to help overcome the ML training-data shortage mentioned, among others. The drawbacks are that the cost and complexity of maintaining the twin fidelity as the physical plant evolves, and the security of the twin itself, a high-value target, containing complete process knowledge.

Recovery rehearsal and OT-specific incident response are two key solutions that tackle the fact that 25% of industrial ransomware incidents in 2024 resulted in full site shutdown. Unlike IT, the logic of controllers, HMI configurations and historian data must be restored in a specific order, which must consider process safety PLC program golden image backups are often not available or are out of date. The literature highlights practices that are most correlated to a reduction in downtime, such as OT-aware Security Operations Centres, tabletop exercises with operations and engineering staff, and pre-negotiated

manual operating modes. However, there is not yet any problem solved when it comes to resilience metrics. As per the survey reviewed, there are no consistent or comparable measures of OT cyber resilience time to safe state, recovery time under cyber conditions, or tolerable degradation, and it is hard to justify investment in these measures. The message is that resilience needs to be designed, not hoped for, and that engineering, not just digital, safeguards should be the backbone of the highest consequence functions.

5. DISCUSSION

The five key messages together constitute a field that is moving away from thinking in the periphery to thinking in terms of consequences. There are three themes that are cross cutting.

There is an uneven maturity gradient. Visibility and detection technology has progressed greatly, due to a deterministic traffic environment, and commercial competition, which favours anomaly modelling. Segmentation is maturing with protocol awareness and identity centric enforcement. Patch management for OT, on the other hand, is nearly impossible literature reviewed indicates that there is not much more than compensating controls or risk based triage, and IEC 62443-2-3 patch management is one of the least implemented sections of the standard. Legacy protocols like IEC 62351 for power systems, or Modbus/TCP Security, are cryptographically protected, but are not widely used due to the need to replace devices that may have a life cycle of decades. In short, the tech industry has become adept at seeing and detecting but has yet to learn to harden.

Exposed sectors are not keeping up with threat evolution and governance adoption. The marginal victim is not the IEC 62443 programme utility with significant resources, it is the mid-tier utility without a programme that is the target of FrostyGoop's attacks, Fuxnet's use of default credentials, and the rise of ransomware in the water, energy, and smaller manufacturers sectors. This is the target of the expansion of regulated entities in NIS2 and the product-security obligations in the EU Cyber Resilience Act and compliance capacity is a constraint. The extension of IEC 62443 to security for IoT devices in the industrial sector (62443-1-6), supplier conformity assessment (62443-6-2) and industry-specific profiles (62443-1-5) is good news and at the same time complicates things for organisations that still struggle with the basics of inventory.

The IT/OT split is a practical reality that is a strategic fiction. The ransomware data indicate that the majority of OT disruption comes from the IT world 75% of the industrial ransomware cases in 2024 resulted in a disruption of operations without necessarily involving a controller. However, there is a disconnect in the security cultures, tooling, and reporting lines in most organisations. The evidence reviewed supports converged governance, which is a single accountable executive, an OT-aware SOC and shared identity infrastructure, while maintaining the engineering driven risk methodology consequence first, availability first that OT requires. In fact, zero trust is not really a product but a governance decision to cease trusting network location, and it's the adaptation of zero trust to OT where IT and OT security practices most productively converge. There is a need for caution about the evidence base. Most of the attack prevalence information comes from vendor telemetry data or incidents that have been disclosed, both of which have selection bias. There are very few independent and peer-reviewed field evaluations of the efficacy of defensive technology, and most evaluations are testbed studies. The conclusions of this review are thus more on the direction than on the magnitude.

6. RESEARCH GAPS

Seven gaps are identified in the synthesis which limit progress.

1. Realistic, common OT data sets. The available public datasets are academic, small, and homogeneous. Little work has been done on privacy preserving approaches for sharing industrial telemetry data across operators federated learning, synthetic generation using digital twins, differential privacy.
2. Explainable & Physics-informed Anomaly Detection for Safety critical Loops. Operators require explanations, based on engineering principles and causality, not statistical anomaly scores. The use of control theoretic invariants is still in the nascent stages with learning models.
3. Quantitative cyber-physical risk and resilience measures. There is no consistent model that connects cyber events to the probability and magnitude of physical consequences, and that can be used to help make investment decisions or insurance pricing. financial-risk modelling of the impact of a \$329.5 billion severe scenario is indicative, but not yet a standardised methodology.
4. Firmware and supply chain assurances. There is no mature tooling or empirical evaluation of the integrity of the controller firmware, software bill of materials of OT products or detection of supply chain implants. Requirements are set by IEC 62443-4-1/4-2 and the EU Cyber Resilience Act, but there is no measurement of efficacy of compliance.
5. Zero Trust in restricted environments. Architectural innovation for proxy-based attestation, network-layer identity, is proposed for devices that cannot run agents, don't have cryptographic capability, or are on a deterministic real-time network, but is not validated at scale.
6. Patch & life cycle management for multi decade assets. Virtual patching, protocol-aware compensating controls, and risk-based deferral frameworks must be tested and evaluated in the real world in terms of actual exploit activity.
7. Human factors workforce. It is widely recognised that there is a lack of staff with a control engineering background who are also cybersecurity experts, and little research has been done on this. There is limited research on the effectiveness of cross-training, OT-aware SOC design, and operator decision making while facing process anomalies caused by cyber-attacks.

7. ETHICAL, LEGAL, AND EQUITY CONSIDERATIONS

The difference between OT and enterprise cybersecurity is that if it fails, it can have physical and even life threatening consequences. This introduces moral responsibilities which are not always stated in the technology literature.

Dual-use research. Digital twins, attack simulation techniques and public PoCs for industrial protocols not only help the research work on the defense side, but also reduce the efforts required by the attackers. If network access is obtained, it would be easy for someone to manipulate Modbus, such as Fuxnet and FrostyGoop show. In OT, researchers and journals should be more aligned with coordinated-disclosure norms that are more suited to the multi-year patch cycles, as well as the restraint of publishing weaponizable detail of unpatched safety-relevant systems. There is a baseline in the ICS-CERT/CISA coordinated vulnerability disclosure process and IEC 62443-4-1 vulnerability-handling requirements.

Attribution and Framing of geopolitical events. Much of the threat intelligence regarding OT attacks is generated by vendors and governments in a few countries and the attribution of attacks is often an intelligence assessment, not a forensics fact. Academic publications should identify attributions as statements by named actors and avoid attributing the actions of a criminal or hacktivist group to a state, and recognize that civilian infrastructure in Ukraine, as well as Russia, has been attacked. Technical scholarship can be vulnerable to uncritical repetition of contested attributions, which can risk the incorporation of geopolitical narratives.

Equality of defence capability. The reviewed technologies assume that water utilities, district-heating providers and small manufacturers have access to budgets, staff, vendors etc., which is often not the case. The cost of passive monitoring platforms, SRA brokers and OT-aware SOC's are geared towards large enterprises. There are obligations that are imposed on regulatory regimes without commensurate funding, like NIS2 and TSA directives. Low cost, open source, and shared-service models e.g., sector ISACs, state-level SOC's, and free CISA vulnerability scanning need to be considered and evaluated equally to commercial products as part of an ethical technology agenda.

Balancing safety and security. Correct controls in IT Forced Re-authentication, Automatic Session Termination, Aggressive Blocking can cause hazards in OT when they lock out the operators during upsets. Human-factors assessment should be part of technology evaluation and the principle that security measures should not compromise safety-instrumented functions is part of IEC 61511 and IEC 62443.

Workforce and responsibility. Putting security responsibility on control engineers who are not trained in security or on IT people who don't know the process leads to a spreading of responsibilities. Good governance, accountable executive and documented OT specific competency requirements is a requirement both for ethics and operation.

These considerations are brought together to make the review go beyond a technology catalogue and towards a socially responsible research agenda.

8. CONCLUSION

As the air-gap era has ended, the protocol-native attack of physical processes using ICS has arrived and is now a reality. The fact that FrostyGoop used Modbus to freeze a city's heating, Volt Typhoon patiently pre-positioned itself in utilities, and ransomware's rampage has extended to over 1,200 industrial incidents in a quarter alone, are all testament to the fact that OT is a mainstream target and is often attacked using the simplest of means, exposed devices, default credentials, and unsecured remote access. This review reveals that OT cybersecurity technology has come a long way in terms of visibility, detection, and segmentation, and is progressing in identity-centric access control and resilience engineering. It also discovers that the core disciplines understanding assets, hardening remote access, and implementing protocol-aware segmentation continue to be the best bang for buck, and are often the most overlooked. Detection and digital twins could be very promising using AI, but they need to be explainable and realistic with data to be trusted in safety critical applications. There are still no structural solutions to patch management and legacy protocol protection.

The bottom line OT security needs to be governed by consequence and not by IT derived metrics. The choice and stacking of technology should be based on the physical consequences to be prevented, with non-digital engineering safeguards underpinning the functions which may not be allowed to fail. The

scaffolding is given by standards like IEC 62443 and NIST SP 800-82 Rev. 3, and the direction is provided by zero-trust principles, while the discipline comes from consequence driven engineering. The ability of defenders to keep up with adversaries' speed at which they are turning reconnaissance into disruption will depend on closing the research gaps identified here, especially in the areas of shared datasets, explainable detection, and quantitative resilience metrics.

REFERENCES

- [1] 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
- [2] Bochman, A. A., & Freeman, S. G. (2021). Countering cyber sabotage: Introducing consequence-driven, cyber-informed engineering (CCE). CRC Press. ISBN 978-0-367-67371-0
- [3] Cybersecurity and Infrastructure Security Agency. (2024, February 7). PRC state-sponsored actors compromise and maintain persistent access to U.S. critical infrastructure (Cybersecurity Advisory AA24-038A). U.S. Department of Homeland Security. from <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a>
- [4] Dragos, Inc. (2024, July). Impact of FrostyGoop ICS malware on connected OT systems (Intelligence brief). from <https://hub.dragos.com/report/frostygoop-ics-malware-impacting-operational-technology>
- [5] Dragos, Inc. (2025). Dragos 2025 OT/ICS cybersecurity report: 8th annual year in review. from <https://www.dragos.com/ot-cybersecurity-year-in-review/>
- [6] European Parliament & Council of the European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). Official Journal of the European Union, L 333, 80–152. <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>
- [7] European Union Agency for Cybersecurity. (2024). ENISA threat landscape 2024. from <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024>
- [8] Goh, J., Adepu, S., Junejo, K. N., & Mathur, A. (2017). A dataset to support research in the design of secure water treatment systems. In G. Havarneanu, R. Setola, H. Nassopoulos, & S. Wolthusen (Eds.), Critical information infrastructures security: CRITIS 2016 (Lecture Notes in Computer Science, Vol. 10242, pp. 88–99). Springer. https://doi.org/10.1007/978-3-319-71368-7_8
- [9] International Electrotechnical Commission. (2024). IEC 62443-2-1:2024 Security for industrial automation and control systems Part 2-1: Security program requirements for IACS asset owners (Edition 2.0). IEC. Available from <https://webstore.iec.ch/>
- [10] Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. IEEE Security & Privacy, 9(3), 49–51. <https://doi.org/10.1109/MSP.2011.67>
- [11] National Institute of Standards and Technology. (2024). The NIST cybersecurity framework (CSF) 2.0 (NIST CSWP 29). U.S. Department of Commerce. <https://doi.org/10.6028/NIST.CSWP.29>
- [12] 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>
- [13] George, D. (2026b). IEC 62443 Wireless Security: Deploying OT wireless controllers in industrial factory networks. Zenodo (CERN European Organization for Nuclear Research). <https://doi.org/10.5281/zenodo.19428491>
- [14] 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>
- [15] George, D. (2026a). Architectural Convergence in Security Operations: a technical framework for AI-Augmented Threat Detection, Automated response, and Organizational cyber resilience. Zenodo (CERN European Organization for Nuclear Research). <https://doi.org/10.5281/zenodo.19986642>
- [16] Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, U.S. Department of Commerce. (n.d.). Operational Technology – NIST Risk Management Framework | CSRC | CSRC. <https://csrc.nist.gov/projects/risk-management/sp800-53-controls/overlay-repository/nist-developed-overlay-submissions/operational-technology>

- [17] Dragos, Inc. (2026, January 8). Dragos's 8th annual OT Cybersecurity Year in Review is now available. <https://www.dragos.com/blog/dragos-8th-annual-ot-cybersecurity-year-in-review-is-now-available>
- [18] George, D. (2025). Cyber resilience in an AI-Driven world: a Strategic framework. Zenodo (CERN European Organization for Nuclear Research). <https://doi.org/10.5281/zenodo.18002783>
- [19] Dragos reports OT/ICS cyber threats escalate amid geopolitical conflicts and increasing ransomware attacks. (2025, September 18). <https://www.dragos.com/resources/press-release/dragos-reports-ot-ics-cyber-threats-escalate-amid-geopolitical-conflicts-and-increasing-ransomware-attacks>
- [20] George, D. (2024). The impact of IT/OT convergence on digital transformation in manufacturing. Zenodo (CERN European Organization for Nuclear Research). <https://doi.org/10.5281/zenodo.10895704>
- [21] FrostyGoop: Reassessing the Lviiv heating attack. (2026, August 1). Trout Software. <https://www.trout.software/resources/frostygoop-malware-analysis>
- [22] Intel Brief: Impact of FrostyGoop ICS malware on connected OT systems | Dragos. (n.d.). <https://hub.dragos.com/report/frostygoop-ics-malware-impacting-operational-technology>
- [23] George, D., Dr.T.Baskar, & Srikaanth, P. B. (2026). Beyond the perimeter Rethinking enterprise network security in an age of distributed threats. Zenodo (CERN European Organization for Nuclear Research). <https://doi.org/10.5281/zenodo.20329717>
- [24] ISA OT Cybersecurity Summit. (n.d.). <https://otcs.isa.org/>
- [25] George, D., Dr.T.Baskar, & Dr.M.M.Karthikeyan. (2026). Driving Cybersecurity transformation through Managed Extended Detection and Response (MXDR): a framework for unified threat visibility and operational resilience. Zenodo (CERN European Organization for Nuclear Research). <https://doi.org/10.5281/zenodo.20341639>
- [26] ISA Self-Paced, Modular training. (n.d.). <https://programs.isa.org/free-training>
- [27] George, D. (2026d). Skills to level up Operational Technology (OT) Cybersecurity: A Quadrant-Based analysis of workforce capabilities, demand trajectories, and strategic development pathways. Zenodo (CERN European Organization for Nuclear Research). <https://doi.org/10.5281/zenodo.20433334>
- [28] Ribeiro, A. (2025, February 25). Dragos finds ransomware attacks on industrial sector surge 87%, manufacturing hit hardest as OT targeting rises. Industrial Cyber. <https://industrialcyber.co/reports/dragos-finds-ransomware-attacks-on-industrial-sector-surge-87-manufacturing-hit-hardest-as-ot-targeting-rises/>
- [29] George, D. (2026c). Multi-Vendor firewall strategy: IT, OT, and edge networks. Zenodo (CERN European Organization for Nuclear Research). <https://doi.org/10.5281/zenodo.19630402>
- [30] Sharma, D. a. K. (2026). AI-Powered Cybersecurity for OT and the IoT: A review of convergence, risk, and resilience in industrial environments. Zenodo (CERN European Organization for Nuclear Research). <https://doi.org/10.5281/zenodo.20156819>
- [31] Stevens, S. (2026, August 14). Breaking down the Dragos 2025 OT/ICS Cybersecurity Report: What Houston Energy & manufacturing companies need to know. CinchOps, LLC. <https://cinchops.com/dragos-2025-ot-ics/>
- [32] 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. <https://doi.org/10.6028/nist.sp.800-82r3>
- [33] The Hacker News. (n.d.). New ICS malware "FrostyGoop" targeting critical infrastructure. <https://thehackernews.com/2024/07/new-ics-malware-frostygoop-targeting.html?ref=blog.netmanageit.com>
- [34] Using the Palo Alto Network Security platform to help Owner-Operators of Cyber-Physical systems achieve IEC 62443. (n.d.). Palo Alto Networks. <https://www.paloaltonetworks.com/resources/whitepapers/using-the-palo-alto-network-security-platform-to-help-owner-operators-of-cyber-physical-systems-achieve-iec-62443>
- [35] Wikipedia contributors. (2025, October 17). IEC 62443. Wikipedia. https://en.wikipedia.org/wiki/IEC_62443