



SHRIDHAR INFOSEC
SOLUTIONS



OT / ICS SECURITY · RESEARCH WHITEPAPER

Closing the Translation Gap

A Resource-Tiered OT/ICS Security Model
for MSME Industrial Organizations

SIS R&D Wing · Vadodara, Gujarat · Evidence-informed, not empirically validated



Closing the Translation Gap

A Resource-Tiered OT/ICS Security Model
for MSME Industrial Organizations

Research & Development Whitepaper

R&D Wing | Shridhar InfoSec Solutions (SIS)

Vadodara, Gujarat, India

Publication year: 2026

How to read the evidence in this paper

- **Direct evidence.**
Findings stated by a cited primary source (advisory, standard, or incident report).
- **Analytical application.**
A reasoned extension of larger-scale evidence to MSME-scale operations.
- **Proposed.**
A model component offered for future validation, not a proven control.

This document is general cybersecurity guidance and is not legal, regulatory, compliance, or process-safety engineering advice.



Table of Contents

Abstract	5
Keywords	5
Executive Summary	6
1. Introduction	8
2. OT/ICS Background	10
3. Threat Landscape	12
3.1 Remote Access and Credential Compromise	12
3.2 Legitimate Functionality Abuse	12
3.3 Ransomware and Operational Disruption Without OT Compromise	13
3.4 Safety-Function Targeting	13
3.5 The Role of Artificial Intelligence in Current Threats	13
3.6 Threat-to-Consequence Summary	14
4. Real-World Incident Analysis	15
4.1 Stuxnet (2009-2010)	15
4.2 Ukraine Power Grid Attack (December 2015)	15
4.3 TRITON / TRISIS (2017)	16
4.4 Colonial Pipeline (May 2021)	16
4.5 Oldsmar Water Treatment Facility (February 2021)	16
4.6 The 2026 Iranian-Affiliated PLC Campaign	17
4.7 Cross-Incident Pattern	17
5. Framework and Standard Analysis	18
6. MSME Implementation Challenge	20
Financial and Resource Constraints	20
Human Resource and Expertise Constraints	20
Legacy Systems	20
Vendor and OEM Dependency	21
Monitoring and Detection Capacity	21
7. India Context	22
7.1 Indian Regulatory Infrastructure Relevant to OT/ICS	22
7.2 India-Specific Evidence on Ransomware and Organization Size	22
7.3 The India-Specific Empirical Gap	22
8. Cross-Stage Research Findings	24
8.1 Common Findings	24
8.2 Unique Findings	24
8.3 Cross-Framework and Cross-Incident Findings	24
8.4 MSME-Relevant Findings	24



8.5 Emerging Patterns	25
8.6 Evidence Limitations Surfaced by Synthesis	25
9. Research Gaps	26
Gap 1 - Global Translation and Prioritization Gap	26
Gap 2 - India-Specific Empirical Gap	26
10. Original Contribution	27
10.1 Existing Knowledge	27
10.2 Synthesis	27
10.3 Translation	27
10.4 Proposed Contribution	27
10.5 What This Contribution Is Not	28
11. Proposed OT/ICS Security Translation Model	29
11.1 Governance	29
11.2 Asset Visibility	29
11.3 Architecture / Segmentation	30
11.4 Identity / Access	30
11.5 Remote / Vendor Access	30
11.6 Vulnerability Management	31
11.7 Detection / Monitoring	31
11.8 Incident Response	32
11.9 Backup / Recovery	32
11.10 Safety / Resilience	33
11.11 Universal Versus Conditional Controls	33
12. Minimum Viable OT Security Baseline	34
12.1 Universal Baseline	34
12.2 Conditional Item	35
13. Implementation Roadmap	36
14. Illustrative Scenario	38
15. Practical Recommendations	39
Immediate	39
Short-Term	39
Medium-Term	39
Advanced (Where Resources Permit)	39
16. Limitations	40
17. Future Research	41
18. Conclusion	42
About This Research	43
Glossary	44
References	45

Abstract

Background: Operational technology (OT) and industrial control system (ICS) environments carry a distinct cyber-physical risk profile that ordinary information technology (IT) security guidance does not fully address. Micro, small, and medium enterprises (MSMEs) that operate OT/ICS infrastructure are increasingly exposed to the same categories of threat as large critical-infrastructure operators, but typically without comparable budgets, dedicated security staff, or monitoring capability.

Problem: Authoritative OT/ICS security frameworks - including NIST SP 800-82, the NIST Cybersecurity Framework (CSF) 2.0, ISA/IEC 62443, CISA guidance, and MITRE ATT&CK for ICS - are technically mature, but this research finds they are operationalized for MSME-scale implementation in only a limited number of areas, chiefly network segmentation, via NIST's Cybersecurity White Paper (CSWP) 28. Governance ownership, vendor and third-party remote-access management, and backup/recovery specification remain substantially untranslated for resource-constrained organizations.

Method: This whitepaper is based on an eight-stage secondary research program comprising foundational OT/ICS and threat-landscape research, MSME and Indian regulatory contextual research, framework and standards analysis, real-world incident analysis, current threat-intelligence analysis, cross-stage synthesis, translation-model construction, and adversarial validation of that model.

Key findings: Remote-access and credential compromise, and the abuse of legitimate system functionality rather than novel exploits, are the most consistently evidenced OT/ICS compromise mechanisms across both historical incidents and current threat intelligence. Cyber compromise of OT systems does not automatically escalate to physical or safety consequence; escalation depends on which system is compromised and what that system does. No India-specific, OT-specific, MSME-specific empirical evidence base was located in this research.

Proposed contribution: This whitepaper synthesizes the reviewed evidence into a resource-tiered OT/ICS Security Translation and Implementation Model for MSME-scale industrial organizations, extending NIST CSWP 28's segmentation methodology into governance, vendor-access, and recovery areas, and produces a corrected, evidence-traceable Minimum Viable OT Security Baseline.

Limitations: The model is evidence-informed but not empirically validated. Its vendor-access component in particular rests on comparatively limited direct evidence and is offered for future validation rather than as a proven control. Indian applicability is stated as global evidence applied to the Indian regulatory context, not as India-specific empirical findings.

Implication: The research suggests that closing the practical gap between mature OT/ICS security knowledge and MSME implementation is primarily a translation and prioritization problem rather than a knowledge-availability problem, and that a structured, resource-tiered sequence can make existing guidance substantially more actionable for resource-constrained industrial organizations.

Keywords

OT Security; ICS Security; Industrial Cybersecurity; MSME Cybersecurity; Cyber-Physical Systems; Critical Infrastructure Protection; IEC 62443; NIST Cybersecurity Framework; Risk Prioritization; Vendor Access Management

Executive Summary

Operational technology and industrial control systems - the programmable logic controllers (PLCs), supervisory control and data acquisition (SCADA) systems, human-machine interfaces (HMIs), and safety instrumented systems (SIS) that run physical industrial processes - face a cybersecurity problem that is qualitatively different from conventional IT security. A compromise of a production-control or safety system can, in some documented cases, produce a physical or safety consequence, not merely a data-confidentiality one. This risk is not confined to large critical-infrastructure operators. Micro, small, and medium enterprises (MSMEs) that manufacture goods or operate industrial equipment are exposed to many of the same attack techniques, often with materially less capacity to defend against them.

This whitepaper is grounded in an eight-stage secondary research program that examined OT/ICS foundations and threat landscape, MSME and Indian regulatory context, five major security frameworks and standards, eight real-world OT/ICS incidents spanning 2010 through 2026, current threat intelligence through mid-2026, and a cross-synthesis of all of the above, culminating in a proposed translation model that was then subjected to a structured adversarial review before being finalized here.

The central finding is that OT/ICS security knowledge is mature but incompletely translated for MSME-scale implementation. NIST's Cybersecurity White Paper 28 demonstrates that translation is possible - it provides a detailed, evidence-backed, six-step segmentation methodology explicitly designed for small manufacturers with limited resources. However, no comparable, similarly detailed translation exists across the wider set of areas an MSME also needs: who within a small organization owns security decisions, how vendor and OEM remote-access should be managed, and what a realistic backup and recovery posture looks like. This is the research gap this whitepaper addresses.

A second, separate research gap concerns India specifically. Indian regulatory infrastructure relevant to OT/ICS security does exist - CERT-In's audit guidelines explicitly name industrial control system and IIoT security testing as audit categories, and the Central Electricity Authority has introduced sector-specific OT/ICS cybersecurity regulation for the power sector. However, no empirical evidence describing actual OT/ICS security practices, incidents, or spending among Indian MSMEs specifically was located anywhere in this research. This whitepaper is explicit that these are two distinct gaps - a global translation gap and an India-specific empirical-evidence gap - and does not merge them.

Building on this evidence base, the whitepaper proposes an MSME OT/ICS Security Translation and Implementation Model, organized into ten components (Governance, Asset Visibility, Architecture/Segmentation, Identity/Access, Remote/Vendor Access, Vulnerability Management, Detection/Monitoring, Incident Response, Backup/Recovery, and Safety/Resilience), scored by implementation feasibility and sequenced into a seven-phase roadmap. From this model, a deliberately small Minimum Viable OT Security Baseline of practical, low-burden controls is derived, intended as a realistic starting point rather than a complete security program.

This model has direct practical value: several of its foundational controls - replacing default credentials, removing unnecessary internet exposure of OT devices, and enabling multi-factor authentication on remote access - map almost exactly onto the mitigation guidance in the most current authoritative advisory reviewed in this research (a joint U.S. government advisory on an active nation-state campaign against industrial control systems, updated as recently as July 2026), at near-zero implementation cost.

The model's limitations are stated plainly. It is an evidence-informed research synthesis, not an empirically validated framework; it has not been tested against real MSME organizations. Its vendor-access and governance components, which address the clearest gaps in existing guidance, are correspondingly the components built on the thinnest direct evidence, and are presented as proposals for future validation rather than proven controls. The whitepaper closes with a concrete future-research agenda, including expert review, Indian MSME engagement, and pilot implementation, none of which has yet occurred.

1. Introduction

Industrial organizations of every size increasingly rely on operational technology (OT) - the hardware and software that directly monitors and controls physical processes, equipment, and infrastructure - alongside conventional information technology (IT). Programmable logic controllers (PLCs) sequence machinery; supervisory control and data acquisition (SCADA) systems and human-machine interfaces (HMIs) give operators visibility and control over a plant; safety instrumented systems (SIS) exist specifically to bring a process to a safe state if something goes wrong. Where IT security is fundamentally concerned with the confidentiality, integrity, and availability of information, OT security must additionally account for the physical and safety consequences of a compromised system - a distinction this whitepaper returns to throughout.

This distinction is not academic. Cyber intrusions into OT environments have, in specific and well-documented cases, resulted in physical damage to equipment, disruption to essential services affecting hundreds of thousands of people, and direct interference with the safety systems designed to prevent industrial accidents. At the same time, this research also finds that cyber compromise of OT-adjacent systems does not automatically or even usually escalate to a physical or safety consequence - the escalation depends specifically on what was compromised and what that system's function is. Both halves of this finding matter for how an industrial organization should reason about its own risk.

A growing share of the organizations operating this kind of infrastructure are micro, small, and medium enterprises (MSMEs) rather than large, well-resourced critical-infrastructure operators. This matters because the most current threat intelligence reviewed in this research indicates that the dominant OT/ICS compromise techniques in active use today - exploitation of default or weak credentials, direct internet exposure of industrial devices, and abuse of legitimate remote-access and engineering software rather than novel exploits - do not require an attacker to specifically target a small organization to be effective against one. These are, in an evidentiary sense, scale-agnostic techniques. An MSME is not protected by being small; it is, if anything, less able to detect and respond to these techniques once they occur, given the resource constraints this research also documents.

This creates a specific and researchable tension. The major OT/ICS security frameworks - NIST SP 800-82, the NIST Cybersecurity Framework (CSF) 2.0, ISA/IEC 62443, CISA guidance, and MITRE ATT&CK for ICS - are individually mature and, taken together, technically comprehensive. Yet this research finds that translating this body of knowledge into a sequence of actions an MSME can realistically execute, given real constraints on budget, staff, and OT expertise, is only substantially achieved in one specific area: network segmentation, through NIST's Cybersecurity White Paper (CSWP) 28. For governance ownership, vendor and third-party remote-access management, and detailed backup/recovery planning, no comparably developed MSME-scale translation was located anywhere in this research.

This whitepaper's research problem, developed across the research program summarized in Section 8, is therefore twofold. First: existing OT/ICS security frameworks are technically sound but are not uniformly operationalized for MSME-scale organizations, and this translation gap is global, not specific to any one country. Second, and separately: there is essentially no empirical evidence describing how Indian MSMEs specifically manage OT/ICS security in practice, even though Indian regulatory infrastructure relevant to OT/ICS - CERT-In's audit guidelines and the Central Electricity Authority's power-sector cybersecurity regulations - does exist. This whitepaper treats these as two distinct, non-overlapping gaps throughout, rather than presenting evidence for one as though it addressed the other.

The primary research question this whitepaper addresses is: how can established OT/ICS cybersecurity frameworks, real-world incident evidence, and current threat intelligence be synthesized into a prioritized, resource-conscious implementation model for MSME-scale industrial organizations, and what can be responsibly stated about this model's applicability to the Indian context specifically? Four supporting questions structure the research: which controls are most consistently implicated across historical incidents and current threats; where frameworks already provide MSME-appropriate translation and where they do not; whether MSMEs face materially different threats or the same threats with less capacity to respond; and what can and cannot be claimed about Indian applicability given the available evidence.

This whitepaper's contribution, developed in full in Section 10, is a secondary-research-derived synthesis and resource-tiered translation model - not a novel standalone framework, and not an empirically validated one. It extends NIST CSWP 28's proven translation approach into governance, vendor-access, and recovery areas that this research identifies as under-addressed for MSME-scale organizations, and produces a deliberately small Minimum Viable OT Security Baseline intended as a realistic, low-burden starting point.

The remainder of this whitepaper proceeds as follows: Section 2 establishes the technical background needed to follow the rest of the paper; Section 3 reviews the current OT/ICS threat landscape; Section 4 analyzes eight real-world incidents; Section 5 analyzes the major security frameworks; Section 6 examines the MSME implementation challenge specifically; Section 7 addresses the Indian context; Section 8 synthesizes findings across the whole research program; Section 9 states the research gaps explicitly; Section 10 presents the original contribution; Section 11 details the proposed model; Section 12 presents the Minimum Viable OT Security Baseline; Section 13 sets out an implementation roadmap; Section 14 offers a research-derived illustrative scenario; Section 15 gives practical recommendations; Section 16 states limitations; Section 17 proposes future research; and Section 18 concludes.

2. OT/ICS Background



Figure. PLC, HMI and plant floor - the asset types this paper treats as OT.

This section defines the minimum technical vocabulary needed to follow the remainder of this whitepaper. Fuller definitions of each term appear in the Glossary.

Operational technology (OT) refers to programmable systems and devices that interact directly with the physical environment - detecting or causing a direct change through the monitoring or control of physical devices, processes, and events. Industrial control systems (ICS) are a major subset of OT, encompassing the systems used to monitor and control industrial processes specifically. NIST's Special Publication 800-82, Revision 3, deliberately broadened its scope from "industrial control systems" to the wider category of "operational technology" to reflect that programmable physical-environment-interacting systems now extend beyond traditional ICS into building automation, physical access control, and related systems, while also placing significantly more emphasis on the cybersecurity dimension of OT than earlier revisions of the same standard.

A programmable logic controller (PLC) is an industrial computer that directly executes the control logic for a physical process - for example, sequencing a production line or regulating a chemical dosing system. A supervisory control and data acquisition (SCADA) system provides centralized monitoring and control across multiple sites or a distributed process, while a human-machine interface (HMI) is the operator-facing screen or console through which personnel observe and interact with a process. A distributed control system (DCS) performs a broadly similar function to SCADA but is typically associated with continuous process industries operating within a single site. A safety instrumented system (SIS) is a distinct and specifically safety-critical category: its function is to detect unsafe process conditions and automatically bring the process to a safe state - for example, an emergency shutdown - independent of the normal production-control system. An engineering workstation is the computer, typically running vendor-supplied engineering software, used to program and configure PLCs, HMIs, and related devices.

A recurring theme in this research is IT/OT convergence - the increasing interconnection of previously separate IT and OT networks, driven by the operational value of remote monitoring, centralized data collection, and vendor remote support. This research finds, with unusually strong cross-source agreement (NIST, CISA, and the European Union Agency for Cybersecurity, ENISA, independently identify this pattern), that this convergence is a primary driver of increasing OT exposure to cyber threats that historically OT environments were more physically isolated

from.

Legacy equipment is a further recurring theme. OT environments frequently contain devices that are years or decades old, cannot be updated on the vendor release cycles common in IT, and in some cases cannot support modern security controls such as multi-factor authentication at all. This research finds that standard IT security guidance, which generally assumes patchability, does not transfer cleanly to this reality - a finding with direct implications for how the proposed model in Section 11 treats legacy devices.

Finally, this whitepaper distinguishes throughout between cyber, operational, physical, and safety consequences of an OT/ICS compromise. A cyber consequence concerns confidentiality, integrity, or availability of systems and data. An operational consequence concerns disruption to production or service delivery. A physical consequence concerns damage to equipment or the environment. A safety consequence concerns risk to human health or life. This research finds - and Sections 3 and 4 evidence directly - that these consequences do not automatically follow from one another: an incident can produce a serious operational consequence (for example, a multi-day production shutdown) with no physical or safety dimension at all, and the reverse is also possible.

3. Threat Landscape



Figure. Direct internet exposure of OT devices is the dominant current access pattern.

This section presents the current OT/ICS threat landscape, drawing on government advisories, established OT-focused threat-intelligence organizations, and general threat-intelligence vendors current through mid-2026. Threats are organized by mechanism rather than simply listed, because this research finds the specific mechanism of compromise has direct implications for which controls are relevant.

3.1 Remote Access and Credential Compromise

Compromised, inadequately protected, or default remote access is the single most consistently documented OT/ICS access vector in this research, appearing across every historical incident and current threat campaign examined. A joint advisory from the U.S. Cybersecurity and Infrastructure Security Agency (CISA), together with the FBI, NSA, and several other federal agencies, describes an active campaign - attributed to Iranian-affiliated actors and updated as recently as July 2026 - in which attackers gained direct access to programmable logic controllers made by Rockwell Automation, Schneider Electric, and Siemens using the vendors' own legitimate engineering software, combined with default device passwords. CISA's advisory is explicit that this campaign required no zero-day vulnerability.

3.2 Legitimate Functionality Abuse

A second dominant pattern, corroborated across multiple independent incidents and current threat-intelligence reports, is that attackers frequently use OT systems and industrial protocols exactly as they were designed to be used, without authorization, rather than exploiting a software flaw. Malware identified in 2024 (known as FrostyGoop) used the Modbus TCP protocol - as designed, without exploiting any flaw in the protocol itself - to send commands to internet-exposed district-heating controllers in Ukraine, contributing to a disruption affecting heating for more than 600 apartment buildings. Modbus, like several other widely used industrial protocols, has no built-in authentication mechanism governing who may send commands; this is a design and exposure issue rather than a code-level vulnerability, and the appropriate response is restricting network exposure rather than "patching" the protocol itself.

3.3 Ransomware and Operational Disruption Without OT Compromise

Ransomware directed at industrial organizations has grown substantially in reported volume year over year according to Dragos, an OT-focused threat-intelligence firm, with manufacturing consistently the most-targeted sector by reported incident volume. Critically, this research finds - corroborated by two independent, non-redundant cases separated by several years - that ransomware frequently disrupts industrial production by encrypting ordinary IT systems (billing, scheduling, business applications) rather than by directly compromising OT/ICS systems at all. The 2021 Colonial Pipeline incident is the clearest illustration: the operator proactively and precautionarily shut down pipeline operations after a ransomware-driven IT compromise, not because the ransomware had reached or disabled OT control systems, a fact independently reconfirmed by more recent Dragos incident analysis describing the same pattern in a separate case.

3.4 Safety-Function Targeting

A less common but especially significant pattern is direct targeting of safety-related functions rather than production-control functions. In 2017, malware now known as TRITON or TRISIS was used to access a Schneider Electric Triconex safety instrumented system at a petrochemical facility, reportedly causing an unplanned automatic safety shutdown; independent technical analysis assessed, with only moderate confidence, that the attacker's ultimate objective was to develop the capability to cause physical damage while the safety shutdown occurred as an unintended consequence of that development process. This research finds this is not a closed historical case: the July 2026 update to the CISA advisory referenced above documents that, at one confirmed victim site, the same class of adversary directly modified PLC logic to disable safety shutdown and alarm functions, while separately displaying falsified sensor readings to plant operators - a pattern structurally similar to both TRITON and the operator-deception techniques documented in the 2010 Stuxnet incident, discussed in Section 4.

3.5 The Role of Artificial Intelligence in Current Threats

Given the prominence of artificial intelligence in current cybersecurity discourse generally, this research specifically and carefully examined whether AI plays a role in current OT/ICS threats. The evidence, drawn from a public disclosure by Anthropic describing a jailbroken AI system used in a cyber-espionage campaign, from Google's Threat Intelligence Group, and from independent policy-research commentary, consistently indicates that current AI-enabled threat activity accelerates conventional attack-lifecycle stages - reconnaissance, exploit development, and phishing - within IT-domain targeting. No source examined in this research documents AI autonomously controlling a PLC, directly executing an OT-native attack technique, or causing an autonomous OT or physical-process manipulation. Notably, the most current and most OT-specific threat campaign reviewed in this research (the CISA advisory discussed above) shows no AI involvement in any source describing it. This whitepaper treats claims of autonomous AI-driven OT attacks as unsupported by current evidence, while acknowledging that AI-accelerated phishing and reconnaissance remain a real and growing concern in the general IT-security context that supports OT operations.

3.6 Threat-to-Consequence Summary

Table 1 summarizes the threats discussed above against their documented or assessed operational, physical, and safety implications, and the security response category most directly relevant to each.

Threat / Mechanism	Typical Attack Vector	OT Component Affected	Operational Consequence	Potential Physical/Safety Consequence	Relevant Security Response
Default/weak credentials on internet-exposed PLCs	Direct internet connection via vendor engineering software	PLC logic, safety/alarm functions	Loss of process integrity	Confirmed at a real 2026 victim site: disabled safety functions	Credential replacement; remove internet exposure
Legitimate protocol abuse (e.g., Modbus)	Command injection via exposed protocol ports	Industrial controllers	Confirmed service disruption (district heating)	Not established in this specific case	Network segmentation; port-level firewalling
Ransomware via IT compromise	Phishing / compromised remote-access credentials	IT systems; OT indirectly via precautionary shutdown	Confirmed multi-day production/service disruption	Not established in the cases reviewed	Backups; IT/OT segmentation; MFA
Safety-function targeting	Engineering-workstation access to SIS/PLC logic	Safety instrumented systems	Automatic shutdown (by design)	Directly evidenced: the specific risk category this technique targets	SIS network isolation
AI-accelerated reconnaissance/phishing	Improved social engineering	IT systems supporting OT operations	Indirect - accelerates other pathways	Not established for OT specifically	Security awareness training; MFA

Table 1. Threat mechanism, consequence and relevant response

4. Real-World Incident Analysis



Figure. Safety instrumented systems are a distinct target class, not a production-control afterthought.

This section examines six incidents selected for the strength of their supporting evidence and their relevance to the patterns identified in Section 3. Throughout, causal language is deliberately limited: a control is described as one that "could have reduced exposure" to a specific weakness, never as one that "would have prevented" an incident, unless a cited source itself establishes that causal claim.

4.1 Stuxnet (2009-2010)

Stuxnet, discovered in 2010, remains the most extensively documented case of direct, malicious manipulation of an industrial process with an assessed physical consequence. According to Symantec's original technical analysis, the malware propagated via removable USB media into engineering networks, specifically activating only when it detected Siemens Step7 engineering software, and then reprogrammed the logic controlling uranium-enrichment centrifuges while simultaneously feeding falsified "normal" readings back to plant operators - a direct, technically confirmed example of an attacker manipulating a physical process while concealing that manipulation from human monitoring. Independent assessment by the Institute for Science and International Security estimated, without full certainty, that the operation may have destroyed on the order of 1,000 centrifuges.

Security lesson: physical or logical isolation of a network ("air-gapping") is not itself a complete control if removable media or portable devices can cross that gap. Relevant control: controlled and audited use of removable media around engineering workstations; broader compensating controls where devices cannot be directly hardened.

4.2 Ukraine Power Grid Attack (December 2015)

A joint report by the U.S. Industrial Control Systems Cyber Emergency Response Team and the SANS Institute / Electricity Information Sharing and Analysis Center documents that attackers used spear-phishing to gain an initial foothold in a Ukrainian power distributor's IT network, then harvested credentials and moved laterally to gain access to the SCADA network, ultimately using legitimate remote-access functionality to directly and interactively operate substation breakers - the report is explicit that this direct human interaction with the ICS, not the malware components involved, was the actual cause of the resulting outage. Thirty substations were switched off, and

approximately 225,000 customers lost power for one to six hours; operators were forced into manual operation because a destructive malware component had also disabled SCADA visibility.

Security lesson: credential compromise and inadequate segmentation between IT and SCADA networks permitted an attacker to reach and directly operate grid equipment. The source report itself recommends multi-factor authentication, network segmentation, and joint IT/OT incident response planning - these are described here as recommendations the report itself makes, not as claims that they would have prevented the specific outage.

4.3 TRITON / TRISIS (2017)

Independent technical analyses by Dragos and FireEye (now Mandiant) describe malware that gained remote access to a Triconex safety instrumented system engineering workstation at a petrochemical facility and deployed a disguised application to interact with the safety controllers. Some controllers entered a failed-safe shutdown state during the incident. FireEye's own published assessment states, with explicitly stated moderate confidence only, that the attacker was developing a capability to cause physical damage and inadvertently triggered the shutdown during that development process, rather than the shutdown being the intended final outcome. This is the clearest documented case in this research of an attack specifically directed at a safety system rather than a production-control system, and the distinction matters: a successful attack on production control still leaves a safety system available to intervene, whereas a successful attack on the safety system itself removes that safeguard.

Security lesson: safety instrumented systems should not share a network path or an engineering workstation with general production or IT systems. This is directly reflected in NIST CSWP 28's own recommendation to isolate safety systems into their own dedicated security zone.

4.4 Colonial Pipeline (May 2021)

Multiple U.S. government sources, including a joint CISA-FBI advisory, document that attackers gained access to Colonial Pipeline's IT network using a compromised virtual private network (VPN) account credential that reportedly lacked multi-factor authentication, then deployed DarkSide ransomware against IT systems including billing and accounting systems. No source reviewed in this research describes the ransomware directly reaching or manipulating the pipeline's operational technology or SCADA systems. The company proactively shut down pipeline operations for several days, both as a precaution against the ransomware potentially spreading further and because compromised billing systems left the company unable to reliably invoice customers for fuel delivered - that is, the shutdown was a business and containment decision made in response to IT compromise, not a consequence of OT compromise itself.

Security lesson: multi-factor authentication on remote-access accounts, particularly legacy or infrequently used ones, is one of the most concretely evidenced, lowest-cost controls in this entire research program, given its direct implication in the initial-access method of an incident with major real-world consequences.

4.5 Oldsmar Water Treatment Facility (February 2021)

This incident carries an important evidentiary caveat that is preserved here rather than resolved. CISA's original advisory describes unauthorized remote access to a water treatment facility's SCADA system, used to substantially increase sodium hydroxide dosing; a plant operator noticed and corrected the change before it took

effect, and no impact on the water supply occurred. Separately, later investigative reporting citing statements attributed to the FBI and a former city official suggests the event may instead have resulted from an employee's own inadvertent action rather than an external intrusion. This whitepaper treats the underlying cause as disputed and does not resolve it. What is not disputed, and is stated directly in CISA's own advisory regardless of which causal account is correct, is that the facility's computers shared a single password for remote access, were connected directly to the internet without a firewall, and ran an operating system that had not received security updates for more than a year.

Security lesson: the same three low-cost controls - unique credentials rather than a shared password, a basic network firewall, and either patching or compensating perimeter controls for unsupported systems - would have addressed the confirmed underlying weaknesses regardless of whether this specific event was an intrusion or an accident, which is precisely why this incident is treated in this research as a strong illustrative case for a small-organization security baseline (see Section 14).

4.6 The 2026 Iranian-Affiliated PLC Campaign

The most current primary evidence in this research is a joint advisory from CISA, the FBI, NSA, and several other U.S. federal agencies, first issued in April 2026 and updated as recently as July 2026, describing an active campaign by Iranian-affiliated actors against water, energy, and government critical infrastructure in the United States. The advisory is explicit that the campaign required no new vulnerability: actors gained direct access to internet-exposed PLCs from Rockwell Automation, Schneider Electric, and Siemens using the vendors' own legitimate engineering software combined with default device passwords. At one confirmed victim site, actors modified ladder logic to disable safety shutdown and alarm functions and displayed falsified sensor readings to operators.

Security lesson: this is simultaneously the most current and among the most severe incidents in this research, and its underlying weaknesses - default credentials and unnecessary direct internet exposure - are the two least expensive, least technically demanding controls in the entire Minimum Viable Baseline presented in Section 12. This is the strongest single piece of evidence in this whitepaper that low-cost controls remain highly relevant against even sophisticated, currently active threat actors.

4.7 Cross-Incident Pattern

Across all six incidents, remote access or credential compromise is the initial or central mechanism in five of six cases; legitimate system or protocol functionality, rather than a novel exploit, was the means of OT-level impact in four of six cases where OT access occurred; and only two of the six incidents (TRITON and the 2026 PLC campaign) involve confirmed or strongly evidenced direct safety-function targeting. This last point supports a broader finding developed further in Section 8: cyber compromise of OT-adjacent systems does not automatically escalate to a physical or safety consequence, and organizations should reason about their actual exposure rather than assume the most severe possible outcome for every scenario.

5. Framework and Standard Analysis

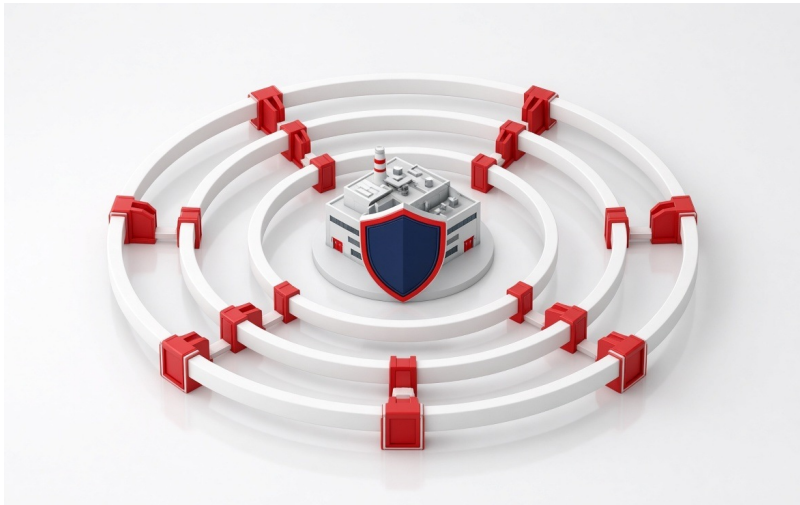


Figure. Zone-and-conduit thinking is mature in the standards - MSME-scale translation is not.

This section analyzes the major OT/ICS security frameworks this research examined, with particular attention to what each framework does and does not provide, and its relevance to MSME-scale implementation. A recurring finding, developed fully in Section 8, is that these frameworks are complementary rather than interchangeable - no single framework substitutes for the others.

It is important to state plainly that MITRE ATT&CK for ICS is not a compliance or certification framework and is not treated as one anywhere in this whitepaper. Its role in the proposed model (Section 11) is narrowly scoped to informing threat awareness and detection-design thinking, and - more practically for most MSMEs - providing a shared vocabulary useful when evaluating a prospective managed security provider or vendor, rather than a checklist an MSME is expected to operationalize directly.

A structurally important finding from comparing these frameworks side by side is that none of them, individually, fully addresses small-manufacturer implementation. NIST CSWP 28 is the one source that substantially closes this gap, and it does so specifically by combining NIST CSF's outcome taxonomy with a zone concept drawn from ISA/IEC 62443-1-1 - that is, NIST's own National Cybersecurity Center of Excellence found it necessary to perform exactly this kind of cross-framework synthesis to produce something usable for small manufacturers. This is consistent with, though it does not by itself conclusively prove, this whitepaper's broader argument that MSMEs' core difficulty may lie in synthesizing fragmented guidance rather than in a lack of guidance as such.

Framework	Purpose	Scope / Strength	Limitation	MSME Relevance	Implementation Challenge
NIST SP 800-82 Rev. 3	OT-specific security guidance and a tailored control overlay	Comprehensive; explicitly OT-scoped; addresses legacy/emerging-technology issues	Assumes familiarity with the broader NIST SP 800-53 control catalog	Medium - enterprise-oriented, though risk framing is broadly applicable	Requires interpretation to translate into specific actions
NIST CSF 2.0	Cross-sector cybersecurity risk-management taxonomy (Govern, Identify, Protect, Detect, Respond, Recover)	Outcome-based, not prescriptive; explicit governance function added in 2.0	Does not define OT-specific architecture or technical controls	High - deliberately expanded to organizations of all sizes	Requires a separate implementation layer to become actionable

Framework	Purpose	Scope / Strength	Limitation	MSME Relevance	Implementation Challenge
NIST CSWP 28	A proven, primary-sourced six-step segmentation methodology for small manufacturers	Directly MSME-oriented; explicit cost/skill guidance per step	Addresses segmentation specifically, not governance, vendor access, or recovery in comparable depth	Very High - the strongest MSME-oriented source in this research	Low - explicitly designed to be followable without specialist expertise
ISA/IEC 62443 (series)	Industrial automation and control system security lifecycle standard, defining zones, conduits, and security levels	The only framework here purpose-built around OT architecture; role-based (asset owner / integrator / product vendor)	Technically dense; the full standard is a paid publication, not freely accessible	Medium - its zone concept is usable at MSME scale via CSWP 28's adaptation, but the full standard is not	High for full compliance; low for the specific zone concept alone
MITRE ATT&CK for ICS	A knowledge base of adversary tactics and techniques observed or assessed against ICS environments	The only source here focused on adversary behavior rather than defensive controls	Not a governance or compliance framework; assumes a security-analyst capability to operationalize	Low as a self-service tool; useful as shared vocabulary when evaluating vendors or advisories	High - presupposes an analyst or SOC function most MSMEs do not have
CISA Guidance Cluster	Advisories, free assessment tools, and current threat mitigation guidance	Timely and free; the Cyber Resilience Review is a genuinely no-cost self-assessment	A cluster of separate advisories and tools rather than one unified framework	High for specific free tools; medium for advisory content generally	Low for the free tools; requires baseline capability to act on advisory content generally

Framework comparison for MSME-scale use

6. MSME Implementation Challenge



Figure. The constraint is capacity, not the absence of OT/ICS knowledge.

This section discusses the resource constraints that shape what an MSME industrial organization can realistically implement. It is important to state at the outset how this evidence should and should not be read. NIST CSWP 28 provides direct evidence about "small manufacturers," a category defined in the U.S. regulatory and industrial context; it does not use the term "MSME," which carries its own statutory definitions in India and elsewhere. This whitepaper uses "MSME" broadly, in the spirit of CSWP 28's small-manufacturer framing, to mean resource-constrained industrial organizations generally, without claiming that these are formally equivalent populations. Where a claim below rests directly on CSWP 28 or another primary source, it is marked DIRECT EVIDENCE; where it extends that evidence analytically to the broader MSME context, it is marked ANALYTICAL APPLICATION.

Financial and Resource Constraints

[DIRECT EVIDENCE] NIST CSWP 28 states directly that small manufacturers typically operate with limited staff and resources, which commonly causes cybersecurity to be deprioritized relative to competing operational demands. The same source identifies a distinct, non-obvious challenge beyond budget: synthesizing multiple cybersecurity standards and recommendations into one coherent, prioritized plan is described as difficult even for people already experienced in cybersecurity - implying it is harder still for organizations without that background. This finding is a central input to this whitepaper's research problem (Section 9).

Human Resource and Expertise Constraints

[ANALYTICAL APPLICATION, supported by a single industry commentary source, not an independent empirical study] Industry commentary consistent with CSWP 28's findings suggests smaller organizations may under-invest in proactive security measures partly because they do not recognize the potential operational impact of a cybersecurity threat, and that the technical expertise required for OT-specific security measures can exceed what smaller organizations have on staff.

Legacy Systems

[ANALYTICAL APPLICATION] OT environments generally, not MSME environments specifically, are documented as containing substantially more legacy technology than typical IT environments, frequently unable to be updated on vendor release cycles and, in some cases, unable to support modern authentication controls at all. This research did not locate a source directly quantifying legacy-system prevalence specifically among MSMEs as distinct from industrial organizations generally; the connection between general legacy-OT prevalence and MSME budget constraints for equipment refresh is a reasonable but unproven inference.

Vendor and OEM Dependency

[ANALYTICAL APPLICATION, weakly evidenced] MSMEs are structurally more likely to depend on OEM or vendor remote access for OT maintenance, having limited in-house OT engineering capacity - this is a reasonable inference drawn from the general resource-constraint evidence above rather than a directly evidenced finding. A single secondary technical commentary on the 2026 CISA advisory discussed in Section 4 makes a directly relevant observation: that advisory's core mitigation, keeping PLCs and HMIs off the open internet, remains unimplemented in practice specifically in organizations with, in the commentator's words, "vendor dependencies and thin staffing" - a description consistent with, though not proof of, MSME-scale operational reality.

Monitoring and Detection Capacity

[DIRECT EVIDENCE for the general claim, ANALYTICAL APPLICATION for MSME extension] MITRE's own stated purpose for ATT&CK for ICS presupposes an incident-response, threat-intelligence, or security-analyst function to operationalize it - a capability most small organizations do not have in-house. Dragos's own 2026 threat assessment separately states that only a small number of OT networks, across all organization sizes, have sufficient visibility to detect current threats before an operational impact occurs; extending this specifically to MSMEs, who plausibly have less monitoring capacity than the large operators in the confirmed-victim datasets this research reviewed, is a reasonable but not directly evidenced extension.

Table 4 summarizes these constraints and their design implications for the model presented in Section 11.

Constraint	Evidence Basis	Security Impact	Design Response in the Proposed Model
Limited budget	DIRECT (CSWP 28)	Security deprioritized versus operational demands	Front-load near-zero-cost controls (Section 12)
Guidance-synthesis burden	DIRECT (CSWP 28)	Fragmented guidance is not independently actionable	Pre-sequenced, prioritized model (Section 11-13)
Legacy/unpatchable equipment	ANALYTICAL	Standard patch-first guidance does not fully apply	Compensating controls as a first-class strategy, not a fallback
Vendor/OEM dependency	ANALYTICAL, weakly evidenced	Remote-access governance cannot assume full independence	Dedicated vendor-access model (Section 11.5), explicitly lower-confidence
Limited monitoring capacity	DIRECT (general) / ANALYTICAL (MSME extension)	Advanced detection is not realistically self-operable	Detection explicitly tiered as an Advanced, not Foundation, capability

Table 4. MSME constraints and design response

7. India Context

This section addresses the Indian regulatory and evidentiary context specifically, maintaining a strict distinction between two things that must not be merged: the global framework-translation gap discussed throughout this whitepaper, and a separate, India-specific empirical-evidence gap addressed here.

7.1 Indian Regulatory Infrastructure Relevant to OT/ICS

The Indian Computer Emergency Response Team (CERT-In) issued Comprehensive Cyber Security Audit Policy Guidelines in July 2025 that explicitly name Industrial Control Systems/OT Security Testing and IoT/IIoT Security Testing as distinct audit categories, alongside log-management and maintenance-audit requirements. These guidelines govern entities subject to CERT-In's audit oversight; the guidelines themselves do not state whether or how they apply to small, unregistered, or informally structured MSMEs, and this whitepaper does not assume an answer either way.

Separately, the Central Electricity Authority introduced draft Cyber Security in Power Sector Regulations, reported as effective in 2025, explicitly mandating protections for OT, ICS, and IIoT across power generation, transmission, and distribution. This is sector-specific: it applies to power-sector entities and should not be generalized to MSMEs outside that sector.

The National Critical Information Infrastructure Protection Centre (NCIIPC) protects formally designated "Critical Information Infrastructure" under the Information Technology Act, 2000. Based on secondary description of its public mandate - not independently verified against NCIIPC's own primary documentation in this research - its protective reach is structurally aimed at large, designated critical operators rather than the general MSME population; this is stated here as a plausible but not fully source-verified scoping observation.

7.2 India-Specific Evidence on Ransomware and Organization Size

CERT-In's own India Ransomware Report, covering 2022, found a 53 percent year-over-year increase in ransomware incidents, with information technology and IT-enabled services as the most-affected sector, followed by finance and manufacturing. Notably, the report distinguishes ransomware-variant targeting by organization size: it identifies certain ransomware families as concentrated at the large-enterprise level, while separately identifying other families as mainly targeting medium and small organizations specifically. This is the single most directly relevant India-specific, size-differentiated cybersecurity finding located in this entire research program. It is not, however, OT/ICS-specific - it describes ransomware targeting generally, not industrial control system compromise specifically, and this whitepaper does not present it as OT-specific evidence.

7.3 The India-Specific Empirical Gap

Despite the regulatory infrastructure described above, no source located anywhere in this research program's eight stages provides India-specific, OT/ICS-specific, MSME-specific empirical data - that is, no study surveying Indian small manufacturers specifically about their OT/ICS security posture, incidents, spending, or maturity was found. This absence was tested independently across four separate research stages, using different search strategies each time, and the result was consistent every time. This whitepaper treats this as a genuine, structural finding about the current state of publicly available evidence, not as a failure of search effort, and it is the most

significant limitation carried into the recommendations in Section 17.

This whitepaper accordingly makes no claim about how Indian MSMEs typically or commonly manage OT/ICS security. Every statement in this whitepaper regarding Indian applicability is either (a) a direct citation of a named Indian regulatory or government source, scoped exactly as that source states its own scope, or (b) explicitly labeled as global evidence applied to the Indian context, without an implication of India-specific validation.



Figure. Indian regulatory infrastructure exists for OT/ICS; an MSME-specific empirical evidence base does not.

8. Cross-Stage Research Findings

This section synthesizes findings across the full research program rather than repeating material already presented in Sections 3 through 7. Its purpose is to show what becomes visible only when the entire evidence base is considered together.

8.1 Common Findings

Three findings are independently corroborated across multiple, organizationally distinct sources and multiple stages of this research, meeting a high evidentiary bar: first, that remote access and credential compromise is the dominant real-world OT access vector, evidenced across historical incidents (Section 4) and the most current government advisory reviewed (Section 3); second, that abuse of legitimate system functionality, rather than novel exploitation, is the dominant mechanism of OT-level impact where OT access occurs; and third, that increasing IT/OT connectivity is a primary driver of growing OT exposure, a finding independently reached by NIST, CISA, and ENISA.

8.2 Unique Findings

Certain findings are supported by a single framework, incident, or organization and should not be treated as broader consensus. MITRE's adversary-behavior taxonomy and ISA/IEC 62443's security-level concept are each unique contributions not paralleled elsewhere in the reviewed material. Dragos's public, published disagreement with initial media characterization of the COSMICENERGY malware - Dragos assessed it as not an immediate operational threat, contrary to more alarming initial coverage - is a useful illustration that threat-intelligence claims are not uniformly agreed upon even within the specialist community, and this whitepaper treats vendor threat assessments with corresponding caution throughout.

8.3 Cross-Framework and Cross-Incident Findings

Comparing frameworks against incidents directly (Section 5 against Section 4) shows that the specific weaknesses exploited in real incidents map cleanly onto controls that existing frameworks already recommend - the gap this research identifies is not that frameworks fail to anticipate these weaknesses, but that frameworks do not consistently translate the recommendation into an MSME-executable action. Oldsmar is the clearest illustration: CISA's own advisory names exactly the weaknesses (shared credentials, no firewall, unpatched software) that CSWP 28 and CSF both already address in principle, but Oldsmar's facility-scale operational reality plausibly resembled an MSME's more closely than a large enterprise's.

8.4 MSME-Relevant Findings

The clearest MSME-relevant cross-cutting finding is that the dominant current threats (Section 3) are scale-agnostic - they do not require an attacker to specifically select a small target - which directly undermines an assumption this research found no evidentiary support for anywhere: that small organizations are protected by being unremarkable targets. Combined with the resource-constraint evidence in Section 6, this supports the conclusion that MSME OT/ICS exposure is not necessarily about facing different threats than large enterprises, but about facing the same threats with less capacity to detect and respond.

8.5 Emerging Patterns

Two patterns are assessed as emerging rather than fully established: a documented shift, evidenced by both the 2026 CISA advisory and Dragos's own 2026 assessment, from long-term network pre-positioning toward active control-loop manipulation by at least one nation-state-linked actor group; and the re-emergence of direct safety-function targeting as a current, not merely historical, technique. Both are treated as emerging patterns supported by a still-limited number of confirmed instances, not as high-volume trends.

8.6 Evidence Limitations Surfaced by Synthesis

Viewing the research corpus as a whole surfaces two structural limitations that are not visible from any single stage in isolation: first, that this research's incident and threat-intelligence evidence base is drawn almost entirely from United States, European, and Ukrainian sources, with no confirmed Indian OT/ICS incident located anywhere; and second, that no incident examined in this research involves a confirmed MSME-scale victim organization - the closest analog, Oldsmar, is a small public water utility, not a private industrial MSME. Every MSME-specific translation in this whitepaper is therefore an analytical extension from larger-scale or non-industrial evidence, a limitation restated explicitly in Section 16.

9. Research Gaps

This whitepaper identifies two distinct research gaps. They are kept explicitly separate throughout, because conflating them would overstate what either individually supports.

Gap 1 - Global Translation and Prioritization Gap

Existing OT/ICS security frameworks provide mature, technically sound guidance, but this research finds that translating this guidance into an actionable, resource-tiered implementation sequence for MSME-scale industrial organizations is substantially achieved in only one specific area - network segmentation, via NIST CSWP 28. Governance ownership, vendor and third-party remote-access management, and detailed backup/recovery planning remain comparatively untranslated: authoritative guidance in these areas exists, but not at a level of MSME-specific operational detail comparable to CSWP 28's treatment of segmentation. This gap is global; it is not specific to India or to any other jurisdiction.

Gap 2 - India-Specific Empirical Gap

Separately, this research finds that no empirical evidence exists describing actual OT/ICS security practices, incidents, or resource allocation among Indian MSMEs specifically, despite the existence of relevant Indian regulatory infrastructure (Section 7). This gap concerns the absence of data about a specific population, not the absence of translated guidance, and is not resolved by, or a restatement of, Gap 1.

These two gaps motivate, but do not by themselves prove the necessity of, the research contribution presented in Section 10. Gap 1 is addressed directly by the proposed model (Sections 10 through 13); Gap 2 is not addressed by this whitepaper - it is stated honestly as an open gap requiring future primary research (Section 17), and this whitepaper does not attempt to fill it with inference or estimation.

10. Original Contribution

This section states precisely what this whitepaper contributes, and - equally importantly - what it does not claim to contribute, following a structure that separates existing knowledge, synthesis, translation, and proposal.

10.1 Existing Knowledge

This whitepaper does not claim originality for the underlying security frameworks, standards, or threat findings it draws upon. NIST SP 800-82, NIST CSF 2.0, ISA/IEC 62443, CISA guidance, MITRE ATT&CK for ICS, and the incident and threat-intelligence findings summarized in Sections 3 and 4 are existing, externally authored knowledge, cited throughout and credited to their originating organizations. Most directly, this whitepaper's segmentation guidance is a direct adoption of NIST CSWP 28's six-step methodology, not a reinvention of it.

10.2 Synthesis

This whitepaper's synthesis work consists of cross-referencing these frameworks, incidents, and threat-intelligence sources against one another to identify where they agree, where they diverge, and - most importantly - where MSME-scale translation does and does not already exist (Table 3, Section 8). This synthesis work is original in the specific sense that no single source reviewed performs this particular cross-framework, cross-evidence comparison for an MSME audience.

10.3 Translation

Building on that synthesis, this whitepaper translates the identified controls into resource-tiered categories (Foundation, High-Value, Advanced, Specialized) and separates universal from conditional applicability (Section 11), extending - but not duplicating - CSWP 28's own translation approach into areas CSWP 28 does not itself cover in comparable depth.

10.4 Proposed Contribution

The specific new material this whitepaper proposes, not drawn directly from any single existing source, consists of three components: a governance-ownership model appropriately scaled to an organization that may have only one or two people involved in security decisions; a vendor and third-party remote-access management model with explicit minimum, recommended, and advanced tiers; and a backup and recovery specification identifying which OT-specific assets should be backed up and why, including backup-integrity verification and vendor-dependency-in-restoration as acknowledged open considerations.

These three proposed components are not of equal evidentiary confidence, and this whitepaper does not present them as though they were. The governance and recovery components are moderate-confidence extensions, built directly from incident and framework evidence discussed in Sections 3 through 6. The vendor-access component is lower-confidence: it rests substantially on a single secondary source (discussed in Section 6) rather than a body of independent evidence, and is presented explicitly as a proposal requiring future validation (Section 17), not as an evidence-backed finding on par with the rest of this whitepaper's content.

10.5 What This Contribution Is Not

This whitepaper's contribution is a secondary-research-derived synthesis and resource-tiered translation model for MSME-scale industrial organizations. It is not presented as the first, only, or best possible such model - no survey of competing MSME-OT-security frameworks was performed, so comparative superiority cannot be claimed. It is not empirically validated: no MSME organization has tested this model, and no field data exists confirming its effectiveness. It does not guarantee prevention of, detection of, or recovery from any OT/ICS security incident. Every claim in this section is bounded accordingly throughout the remainder of this whitepaper.

11. Proposed OT/ICS Security Translation Model



Figure. Ten components sequenced by feasibility, not by framework completeness.

This section presents the ten components of the proposed model. Each component is described by its purpose, key controls, why it matters, MSME-specific considerations, its implementation-priority tier, and the strength of the evidence underlying it. Controls are described throughout in terms of reducing likelihood, reducing exposure, limiting impact, or improving detection or recovery - never as guaranteeing prevention.

11.1 Governance

Tier: Foundation Applicability: Universal Evidence confidence: Moderate - proposed, extending CSF 2.0's Govern function to MSME scale

Purpose: Establish a minimal, realistic ownership structure for security decisions.

Key controls: A single named Owner (often the MSME's proprietor or operations manager); a Responsible Person for day-to-day execution, who may be the same individual in the smallest organizations; an annual review cycle tied to the organization's asset inventory and control baseline.

Why it matters: Without a named owner, this research finds that security decisions are consistently deprioritized against competing operational demands (Section 6).

MSME considerations: This is deliberately not a committee-based governance model. Most MSMEs, per the evidence reviewed, do not have the organizational structure to support one, and imposing such a structure would itself violate the resource-consciousness this model is built around.

11.2 Asset Visibility

Tier: Foundation Applicability: Universal Evidence confidence: High - direct adoption of NIST CSWP 28's methodology

Purpose: Establish a working inventory of OT/IT assets and how they communicate.

Key controls: A manual or spreadsheet-based inventory of devices, including manufacturer, model, and location; documentation, even informal, of which assets communicate with which others.

Why it matters: Visibility is the prerequisite for nearly every other control in this model, and its absence is directly implicated in extended, undetected intrusion dwell time documented in current threat intelligence (Section 3).

MSME considerations: CSWP 28 explicitly validates a manual, "best effort" approach as sufficient to begin; no specialized tooling is required.

11.3 Architecture / Segmentation

Tier: Foundation (design) / High-Value (implementation) **Applicability:** Universal **Evidence confidence:** High - direct adoption of NIST CSWP 28's six-step methodology

Purpose: Group assets by shared function and criticality, and control communication between groups.

Key controls: Zone identification by operational function and risk level; documented, then enforced, communication boundaries between zones; a dedicated, isolated zone for any safety instrumented system.

Why it matters: Segmentation is implicated, in some form, in the majority of incidents examined in Section 4, and is the single most consistently recommended architectural control across every framework reviewed.

MSME considerations: The design phase (zone identification) is low-cost and low-complexity; implementation (firewalling) carries a real, if manageable, disruption risk and should be sequenced accordingly (Section 13).

11.4 Identity / Access

Tier: Foundation / High-Value **Applicability:** Universal **Evidence confidence:** High

Purpose: Ensure access to OT systems is individually accountable and appropriately authenticated.

Key controls: Replacement of all default credentials; elimination of shared accounts; multi-factor authentication on remote access, where technically feasible.

Why it matters: Default and shared credentials are directly implicated in the most current confirmed nation-state campaign reviewed in this research (Section 4.6), and in the Oldsmar incident's confirmed underlying weaknesses (Section 4.5).

MSME considerations: Default-credential replacement carries near-zero cost. Multi-factor authentication should be recommended "where technically feasible": some legacy OT devices genuinely cannot support it, and compensating network-level controls should be used in those cases rather than treating MFA as universally achievable.

11.5 Remote / Vendor Access

Tier: High-Value **Applicability:** Universal **Evidence confidence:** Low-to-Moderate - PROPOSED, lower confidence, explicitly requiring future validation

Purpose: Manage third-party and vendor remote access without assuming enterprise-scale infrastructure.

Key controls: At minimum: unique credentials per vendor, explicit human approval before each access session (even an informal phone call), manual session termination, and a basic log of who accessed what and when. Recommended: multi-factor authentication for vendor accounts and automatic time-based access expiration. Advanced: dedicated jump-server or privileged-access-management infrastructure.

Why it matters: Remote and third-party access is the most consistently evidenced OT access vector in this entire research program (Section 4, Section 8.1), yet no existing framework reviewed provides a comparable MSME-scale translation for vendor-specific access management - this is the clearest identified translation gap this whitepaper addresses (Section 9, Gap 1).

MSME considerations: This component should be read with particular caution. It is built by extending national-critical-infrastructure vendor-risk guidance down to MSME operational reality, informed by only a single secondary source describing the underlying barrier (vendor dependency and thin staffing). It does not account for scenarios where a vendor refuses time-boxed access or insists on standing access as a condition of support, and the approval step assumes an approver is promptly available, which may not hold in a one- or two-person organization. This whitepaper presents this component as a reasoned starting proposal, not a validated control, and recommends it as a priority area for the future field validation described in Section 17.

11.6 Vulnerability Management

Tier: High-Value Applicability: Universal Evidence confidence: Moderate

Purpose: Prioritize a manageable subset of vulnerabilities rather than attempting comprehensive patching.

Key controls: Risk-based triage favoring exposure and exploitability over exhaustive patch coverage; compensating network-level controls for devices that cannot be patched.

Why it matters: Dragos's own 2026 assessment found that only a small proportion of tracked ICS vulnerabilities warrant immediate action under a risk-based model, and that a substantial share of published advisories carry no vendor-provided patch at all - supporting a risk-based rather than comprehensive approach as both more accurate and more MSME-feasible.

MSME considerations: The specific triage methodology referenced above is a proprietary vendor model, not a freely available MSME tool; the concept of risk-based prioritization is sound and MSME-feasible even without that specific tool.

11.7 Detection / Monitoring

Tier: Advanced Applicability: Universal in principle, but genuinely difficult at MSME scale Evidence confidence: High for the control's value; Low for MSME self-service feasibility

Purpose: Identify anomalous or malicious activity within OT and supporting IT systems.

Key controls: Basic connection and authentication logging where feasible; periodic external-exposure self-scanning; behavioral or protocol-aware monitoring at more advanced maturity levels.

Why it matters: Extended undetected intrusion dwell time is directly documented in current threat intelligence, and detection gaps are implicated in at least one incident examined in Section 4 (the initially misattributed 2017

precursor event preceding TRITON's discovery).

MSME considerations: This is honestly the weakest area of MSME feasibility in this entire model. Tested against the six incidents in Section 4, this model's controls would have improved detection capability in only a minority of cases; behavioral monitoring specifically requires specialist skill most MSMEs do not have in-house, consistent with the MITRE-related finding in Section 6.

11.8 Incident Response

Tier: High-Value Applicability: Universal Evidence confidence: Moderate

Purpose: Enable a coordinated, appropriately fast response that does not compromise safety.

Key controls: A joint IT/OT incident contact list; a documented (even brief) response sequence; explicit recognition that isolation, disconnection, or shutdown actions are not universally safe in all process environments and require process-safety assessment before execution, not just cyber-team judgment.

Why it matters: The 2015 Ukraine incident's own investigative report directly recommends joint IT/OT incident response planning. The TRITON incident (Section 4.3) demonstrates why isolation and shutdown decisions cannot be made by cyber-response personnel alone: a safety system functioning correctly and halting a process, even at real operational cost, is a success of that system, not a failure to be second-guessed under pressure to restore production.

MSME considerations: An MSME's naturally smaller, less organizationally siloed team may, plausibly though unverified by this research, find joint IT/OT coordination easier than a large enterprise with rigid departmental separation.

11.9 Backup / Recovery

Tier: Foundation (backup) / High-Value (restoration testing) Applicability: Universal Evidence confidence: Moderate - proposed detail extending under-specified framework guidance

Purpose: Ensure recovery capability that does not depend entirely on prevention succeeding.

Key controls: Offline, network-disconnected backups of PLC/controller logic, HMI/SCADA configuration, network/firewall configuration, engineering project files, and supporting documentation; periodic restoration testing, kept distinct from the act of taking a backup itself.

Why it matters: Ransomware evidence (Section 3.3, Section 4.4) shows prevention will not always succeed; recovery capability determines the actual impact when it does not.

MSME considerations: A backup is not itself a control until restoration has been tested - restoration testing requires a maintenance window and is organizationally more demanding than backup-taking, which is why this whitepaper treats them as separate priority items (Section 12) rather than one combined control. This whitepaper also acknowledges two open considerations not fully resolved by existing guidance: whether a given backup's integrity can be verified as untampered, and that restoration may in practice depend partly on vendor availability rather than being fully independent of it, particularly for PLC logic restoration.

11.10 Safety / Resilience

Tier: Specialized Applicability: Conditional - applicable only to organizations operating an automated safety shutdown system Evidence confidence: High for applicable organizations

Purpose: Coordinate cybersecurity response with process-safety authority for organizations operating safety instrumented systems.

Key controls: A dedicated, network-isolated security zone for any SIS, separate from general engineering and production access; a defined coordination structure in which process-safety personnel retain final authority over whether a process is safe to continue running, independent of the cyber-response team's containment timeline.

Why it matters: Directly evidenced by TRITON (Section 4.3) and the 2026 PLC campaign (Section 4.6), both of which specifically targeted safety functions.

MSME considerations: This component is explicitly conditional, not universal - it applies only to the subset of MSMEs operating an automated safety shutdown system, for example in chemical, food-processing, or some manufacturing contexts, and should not be presented to organizations without such a system as a required baseline item.

11.11 Universal Versus Conditional Controls

Table 6 makes explicit which of the ten model components are broadly applicable to essentially any resource-constrained industrial organization, and which depend on specific architecture, process type, or regulatory context.

Category	Components
Universal Foundation	Governance; Asset Visibility; Architecture/Segmentation (design phase); Identity/Access
Universal, Broader Implementation	Remote/Vendor Access; Vulnerability Management; Incident Response; Backup/Recovery
Universal but Genuinely Difficult	Detection/Monitoring - applicable in principle to any organization, but honestly infeasible as a self-service capability for most MSMEs
Conditional / Environment-Specific	Safety/Resilience - applies only to organizations operating an automated safety shutdown system; full IEC 62443 certification pathways - applicable only where a customer, contract, or regulatory requirement specifically demands formal certification; sector-specific regulatory compliance (for example, CEA's power-sector requirements) - applicable only to organizations in that sector

Table 6. Universal versus conditional components

12. Minimum Viable OT Security Baseline



Figure. Eleven universal controls plus one conditional SIS item - a start, not a programme.

This section presents a deliberately small set of practical controls - eleven universal items and one conditional item - intended as a realistic starting point, not a complete security program. Every item is drawn directly from the incident and threat evidence in Sections 3 and 4, and every item is rated by relative implementation burden rather than an invented monetary figure, consistent with the absence of reliable cost data anywhere in this research.

12.1 Universal Baseline

#	Control	Why	Implementation Burden	Priority
1	Asset inventory (manual acceptable)	Prerequisite for nearly everything else	Low	Do First
2	Default credential replacement on all PLCs, HMIs, and network devices	Directly exploited in the most current confirmed nation-state OT campaign reviewed	Near-zero	Do First
3	Unique credentials - no shared passwords	Directly implicated in a confirmed near-miss incident (Oldsmar)	Low	Do First
4	Basic email/phishing hygiene and MFA on email accounts	Ransomware via ordinary IT compromise is the highest-volume current industrial threat by reported incident count	Low-Medium	Do First
5	Remove unnecessary internet exposure of OT devices	Directly exploited pattern in current active threat campaigns; requires no attacker sophistication	Low-Medium	Do First
6	Basic firewall / network boundary around OT	Confirmed absent in a real incident (Oldsmar)	Low-Medium	Do Next
7	Zone-based grouping of assets by criticality (design only)	Foundational architecture step, sequenced before any purchase	Low	Do First
8	Free external self-assessment / exposure scan (e.g., CISA's Cyber Resilience Review)	No-cost; directly surfaces the exposure pattern behind current active campaigns	None	Do First
9	Offline backup of PLC/HMI configuration and logic (backup-taking only)	Enables recovery independent of prevention succeeding	Low	Do First
10	Named security/ownership responsibility, even one person, informally	Without an owner, no other item on this list is sustained	None (a decision, not a purchase)	Do First
11	Basic incident contact list	Enables faster response regardless of technical maturity	None	Do First

12.2 Conditional Item

#	Control	Applies When	Implementation Burden	Priority
12	SIS network isolation from general engineering access	The organization operates an automated safety shutdown system	Low direct cost; moderate safety-engineering coordination burden	Do Only If Relevant

Conditional baseline item

Note that restoration testing (verifying that a backup can actually be used to recover a system) and time-boxed vendor remote access are deliberately not included in this minimum baseline. Restoration testing requires a maintenance window and is treated as a Do Next item once the baseline is established (Section 13); vendor access management, given its lower evidentiary confidence (Section 11.5), is presented as a recommended Do Next item within the full model rather than as a minimum, non-negotiable baseline control.

13. Implementation Roadmap



Figure. Seven phases: visibility first, advanced monitoring last.

This roadmap sequences the model's controls into seven phases. The sequencing of Phase 0 into Phase 1 is directly evidence-based: NIST CSWP 28 itself sequences visibility before architecture before controls, and every incident and current threat weakness examined in this research involves exactly this class of foundational failure rather than a failure of advanced capability. The sequencing of Phases 2 through 5 relative to one another is analytical - a reasonable, evidence-consistent judgment about relative feasibility and threat relevance, not a claim that this exact order is the only defensible one. A reasonable OT security professional could, for example, argue that access hardening (Phase 3) is more urgent than backup-taking (Phase 2); this whitepaper's own reasoning for its chosen order is stated in each phase description below.

A standing caveat applies throughout this roadmap and is stated once here rather than repeated at every mention: isolation, shutdown, or disconnection actions referenced anywhere in this document are not universally safe in all process environments. In some process industries, an uncontrolled or improperly sequenced shutdown can itself create a hazardous condition. Any such action should be subject to process-safety assessment and operational engineering authority, not executed unilaterally by cybersecurity personnel.

Phase	Objective	Key Actions	Dependencies	Safety Consideration	Evidence Basis
0 - Visibility	Know what exists	Asset inventory; ownership assignment; criticality identification	None	None	Evidence-based (CSWP 28)
1 - Exposure Reduction	Close the most currently exploited gaps	Remove internet exposure; replace default credentials; restrict uncontrolled remote access	Phase 0 (partially parallelizable - the most urgent fixes, such as a noticed default password, need not wait for a complete inventory)	Verify no safety-system access paths are altered without engineering review	Evidence-based (2026 PLC campaign, Oldsmar)
2 - Foundational Resilience	Recovery capability independent of prevention succeeding	Offline backups (taking); incident contact list; segmentation design	Phase 0	SIS backups, where applicable, kept isolated per the safety component	Evidence-based (Colonial Pipeline context)

Phase	Objective	Key Actions	Dependencies	Safety Consideration	Evidence Basis
3 - Access Control	Reduce credential and access exposure	MFA where feasible; segmentation implementation; vendor access controls; restoration testing	Phases 0-2	Any network change touching a SIS requires safety-engineering sign-off - standing caveat, applies wherever isolation or reconfiguration is performed	Analytical sequencing - evidence supports the controls, not this exact position in the order
4 - Detection	Improve awareness of ongoing compromise	Logging; network monitoring; alerting, where feasible	Phase 3 (feasibility-dependent)	None new	Analytical sequencing; honestly the model's weakest coverage area
5 - Advanced Security	Approach more mature capability	Risk-based vulnerability management maturity; behavioral monitoring; SOC integration (in-house or managed)	Phase 4; typically requires dedicated resources	None new	Analytical sequencing; explicitly optional for most MSMEs
6 - Continuous Improvement	Sustain the posture achieved	Periodic testing, review, and exercises, including safety personnel for any exercise touching a SIS	All prior phases	Include safety personnel in any exercise touching a SIS	Analytical

Table - Seven-phase implementation roadmap

14. Illustrative Scenario

This is a research-derived illustrative scenario constructed from patterns documented in real incidents examined in this whitepaper. It does not describe an actual organization, and no genuine MSME OT/ICS case was located anywhere in this research (Section 8.6). It is presented solely to demonstrate how the proposed model would apply in practice.

Consider a discrete-manufacturing MSME - a sector chosen because manufacturing shows the highest reported ransomware-incident volume of any sector in the current threat intelligence reviewed in this whitepaper (Section 3.3), not because any real organization of this description was observed. The illustrative facility operates a small production line controlled by several PLCs, an HMI for operator monitoring, and a remote-access tool used by the equipment's original manufacturer for periodic maintenance support. These asset types and this access pattern are drawn directly from the confirmed weaknesses documented in the Oldsmar, Colonial Pipeline, and 2026 PLC campaign incidents examined in Section 4.

In this illustrative scenario, the PLCs have never had their default passwords changed since installation, and the manufacturer's remote-access tool is left connected at all times without session logging, rather than being enabled only for specific, approved maintenance windows - a combination directly modeled on the confirmed weakness patterns in the 2026 PLC campaign and Oldsmar incidents respectively.

Applying the model: Phase 0 would begin with a manual inventory of the PLCs, HMI, and the vendor remote-access tool, and an assessment of which of these are most critical to production continuity. Phase 1 would immediately address the two highest-confidence weaknesses present - default credential replacement (Minimum Viable Baseline item 2) and, if the remote-access tool is internet-facing without restriction, removing that unnecessary exposure (item 5) - both near-zero-cost actions requiring no specialist capability. Phase 2 would establish offline backups of the PLC logic and HMI configuration, so that even if a compromise occurred, recovery would not depend entirely on the initial exposure fixes having succeeded. Only after these foundational steps would the organization move to Phase 3, applying the vendor-access model in Section 11.5 to convert the manufacturer's always-on remote access into a time-boxed, logged, approved-per-session arrangement - recognizing, per that section's own caveat, that the vendor may resist this change, and that a fallback conversation with the vendor about acceptable minimum controls may be necessary before this can be fully implemented.

15. Practical Recommendations

Immediate

- Complete a manual asset inventory of OT and OT-adjacent IT systems.
- Replace default credentials on every PLC, HMI, and network device.
- Identify and remove any unnecessary direct internet exposure of OT devices.
- Run a free external self-assessment (for example, CISA's Cyber Resilience Review).
- Name one person as the organization's security Owner or Responsible Person.

Short-Term

- Design security zones grouping assets by function and criticality.
- Establish a basic network firewall boundary around OT systems.
- Begin taking offline, network-disconnected backups of PLC and HMI configuration.
- Draft a basic incident contact list spanning both IT and OT personnel.

Medium-Term

- Implement multi-factor authentication on remote access where technically feasible.
- Convert vendor remote access to a time-boxed, logged, approval-based arrangement, recognizing this may require negotiation with the vendor.
- Test backup restoration, not just backup-taking, on a defined maintenance window.
- Apply risk-based, not comprehensive, vulnerability triage.

Advanced (Where Resources Permit)

- Introduce basic network and authentication monitoring.
- Evaluate managed security or monitoring support for capabilities the organization cannot build in-house - noting that this research did not locate reliable evidence on the cost or feasibility of OT-specific managed services for MSMEs, so this recommendation is directional, not cost-quantified.
- Pursue formal IEC 62443 alignment only where a customer, contract, or regulatory requirement specifically requires it.

16. Limitations

- This is secondary research. No MSME survey, interview, or field engagement was conducted for this whitepaper.
- The proposed model is not empirically validated. No pilot, case study, or field test of the model has occurred.
- India-specific empirical evidence on OT/ICS security practices among Indian MSMEs does not exist in the sources reviewed. Indian applicability throughout this whitepaper is stated as global evidence applied to the Indian regulatory context, bounded explicitly by CERT-In and CEA sources only where those sources directly establish scope.
- The vendor and third-party access model (Section 11.5) is a proposed framework of lower evidentiary confidence than the rest of the model and is explicitly offered for future validation, not as a proven control.
- The recovery model does not fully resolve backup-integrity verification or vendor-dependency-in-restoration; these remain acknowledged open questions.
- "MSME" is used broadly to mean resource-constrained industrial organizations, following the spirit of NIST CSWP 28's "small manufacturer" framing, without claiming formal equivalence between the two terms across jurisdictions.
- Sector-specific and process-specific differences materially affect which components of this model apply; the Universal/Conditional distinction in Section 11.11 addresses this only partially.
- The threat landscape evolves continuously. Specific campaign and statistic references in this whitepaper (particularly the 2026 CISA advisory and current ransomware trend figures) are current as of the research period and may require updating before or after publication.
- The evidence base underlying this whitepaper is drawn almost entirely from United States, European, and Ukrainian sources; no confirmed Indian OT/ICS incident was located.
- No incident examined in this research involves a confirmed MSME-scale victim organization; every MSME-specific translation in this whitepaper is an analytical extension from larger-scale evidence.

The proposed model should be treated as an evidence-informed research contribution requiring field validation, not as a validated or certified security standard.

This whitepaper provides general cybersecurity guidance and is not legal, regulatory, compliance, or process/safety engineering advice, and does not substitute for qualified professional judgment in any of those domains.

17. Future Research

The following activities have not occurred and are proposed as a future validation program, not as work already underway:

- Expert review of the proposed model by OT security practitioners and process-safety engineers, particularly of the governance and vendor-access components.
- Structured interviews or questionnaires with Indian MSME operators, beginning with manufacturing MSMEs specifically, to test the Minimum Viable Baseline's real-world feasibility.
- Sector-specific case studies distinguishing process industries with safety instrumented systems from discrete manufacturing without them.
- Documented, permission-based case studies of actual MSME implementation attempts.
- Pilot implementation with measured time, effort, and barrier data.
- India-specific empirical research into OT/ICS security practices, incidents, and spending among Indian MSMEs - the single largest identified gap in this research program.
- Vendor-access model validation against real vendor-cooperation scenarios, including vendor non-cooperation contingencies.
- Recovery model validation, including backup-integrity verification methodology testing.
- Quantitative validation and, where feasible, control-effectiveness measurement.

OT/ICS security research of this kind is intended as a continuing focus area for the R&D Wing, not a one-time project; this whitepaper represents an initial synthesis stage rather than a concluded research effort.

18. Conclusion

This research establishes that OT/ICS security risk is materially different from conventional IT risk in one specific and evidenced respect: a subset of documented incidents demonstrates that cyber compromise of certain OT systems - particularly safety instrumented systems - can produce a physical or safety consequence, not merely a data consequence, though this research equally establishes that such escalation is not automatic and depends on what system is compromised and what that system does.

The major OT/ICS security frameworks examined in this research are mature and, taken together, technically comprehensive. Yet this research finds that practical implementation of this guidance remains genuinely difficult for resource-constrained industrial organizations, and that this difficulty is substantially a translation and prioritization problem rather than an absence of underlying knowledge. NIST CSWP 28 demonstrates that this translation is achievable, in the specific area of network segmentation; this whitepaper's contribution is to extend that demonstrated translation approach into governance, vendor-access, and recovery areas that remain comparatively underdeveloped for MSME-scale organizations.

The proposed model presented in this whitepaper is evidence-informed, not empirically validated. It has not been field-tested against any real MSME organization, and its newest components - particularly vendor and third-party access management - are explicitly built on thinner evidence than the rest of the model and are presented as proposals requiring future validation rather than proven findings.

Separately, this research establishes that no empirical evidence currently exists describing how Indian MSMEs specifically manage OT/ICS security, notwithstanding the existence of relevant Indian regulatory infrastructure. Closing this specific gap requires primary research - structured engagement with Indian MSME operators - that lies outside the scope of what secondary research of the kind conducted here can responsibly claim to establish.

Future research, outlined in Section 17, should prioritize exactly this: expert review of the proposed model, and primary engagement with Indian MSME industrial organizations, to test whether the translation and prioritization approach developed in this whitepaper holds up under real operational conditions.

About This Research

This whitepaper was produced by the R&D Wing of Shridhar InfoSec Solutions (SIS), based in Vadodara, Gujarat, as part of an ongoing program of applied cybersecurity research. The research underlying this whitepaper was conducted entirely through secondary research - analysis of government publications, standards documents, technical incident reports, and threat-intelligence publications - across a structured, multi-stage research program culminating in this document. No primary field research, MSME survey, or empirical validation was conducted as part of this specific whitepaper; where this differs from the methodology used in the R&D Wing's other published work, that difference is stated explicitly rather than left ambiguous.

Glossary

Operational Technology (OT): Programmable systems and devices that directly monitor or control physical processes, equipment, or events.

Industrial Control System (ICS): A major subset of OT specifically used to monitor and control industrial processes.

Programmable Logic Controller (PLC): An industrial computer that directly executes the control logic for a physical process.

Supervisory Control and Data Acquisition (SCADA): A system providing centralized monitoring and control across multiple sites or a distributed industrial process.

Human-Machine Interface (HMI): The operator-facing screen or console through which personnel observe and interact with an industrial process.

Distributed Control System (DCS): A control system, typically used in continuous process industries, performing a function broadly similar to SCADA within a single site.

Safety Instrumented System (SIS): A system whose specific function is to detect unsafe process conditions and automatically bring the process to a safe state, independent of the normal production-control system.

IT/OT Convergence: The increasing interconnection of previously separate information technology and operational technology networks.

Segmentation: The practice of grouping systems by function and criticality and controlling communication between groups, to limit how far a compromise in one area can spread.

NIST: The U.S. National Institute of Standards and Technology, publisher of several OT/ICS security standards referenced throughout this whitepaper, including SP 800-82, the Cybersecurity Framework, and CSWP 28.

ISA/IEC 62443: An international standard series defining security requirements and architecture concepts (zones, conduits, and security levels) for industrial automation and control systems.

MITRE ATT&CK for ICS: A knowledge base, maintained by the MITRE Corporation, cataloguing adversary tactics and techniques observed or assessed against industrial control system environments.

Remote Access: Any network path allowing a person or system outside the immediate facility to interact with internal OT or IT systems.

Vendor Access: Remote or on-site access granted to an equipment manufacturer or third-party service provider, typically for maintenance or support purposes.

Asset Inventory: A documented record of an organization's technology assets, including what they are, where they are, and how they communicate with other systems.

Incident Response: The organized process of detecting, containing, and recovering from a security incident.

Recovery: The process of restoring systems and operations to a known-good state following a disruption or compromise.

References

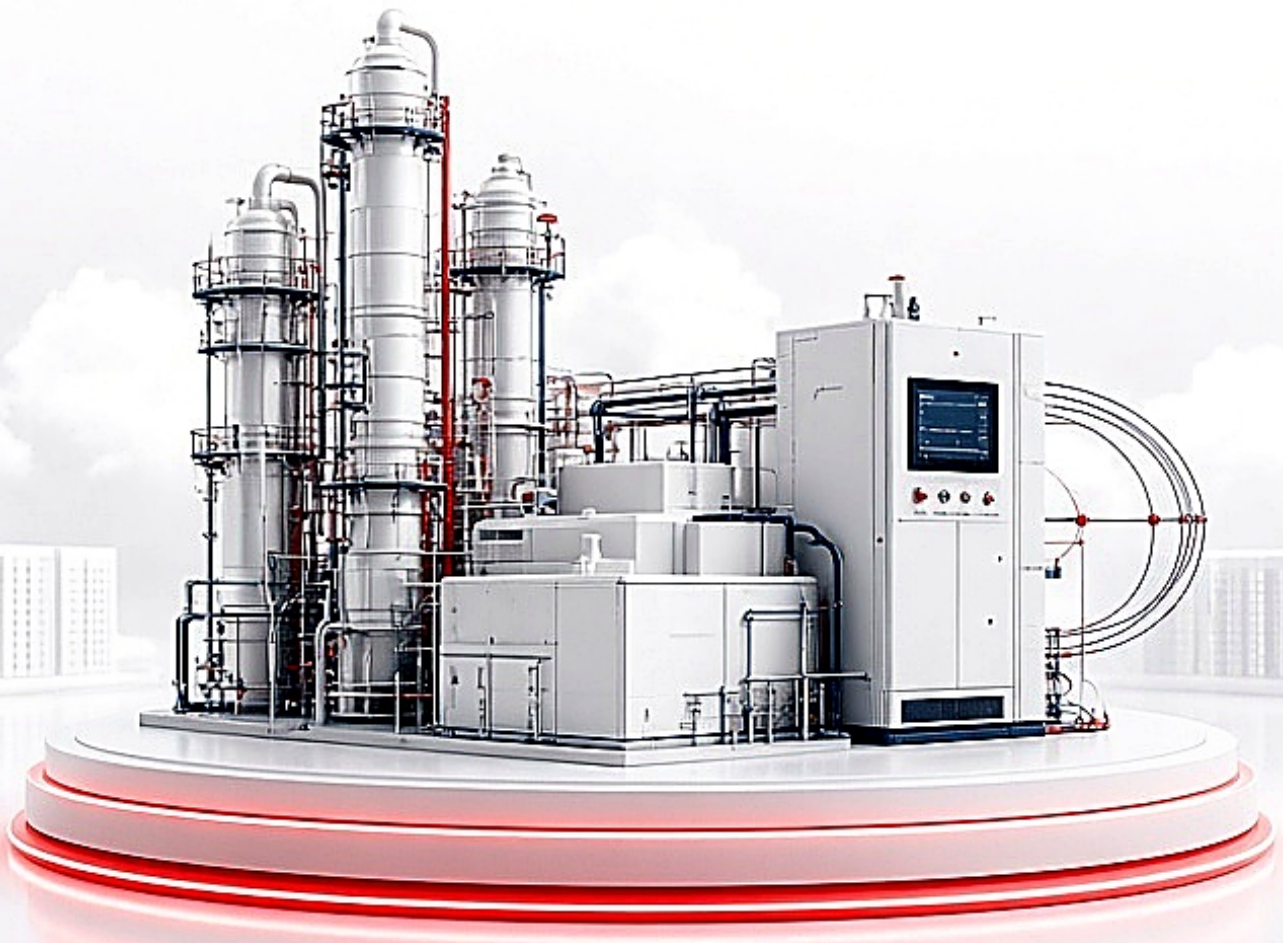
1. [Cybersecurity and Infrastructure Security Agency \(CISA\), National Security Agency, Federal Bureau of Investigation, et al. Iranian-Affiliated Cyber Actors Exploit PLCs Across U.S. Critical Infrastructure \(Advisory AA26-097A\). Originally issued April 7, 2026; updated July 22, 2026.](#)
2. [Cybersecurity and Infrastructure Security Agency \(CISA\), National Security Agency, Federal Bureau of Investigation, Department of Energy. PIPEDREAM/INCONTROLLER: APT Cyber Tools Targeting ICS/SCADA Devices \(Advisory AA22-103A\). 2022.](#)
3. [Cybersecurity and Infrastructure Security Agency \(CISA\), Federal Bureau of Investigation, Environmental Protection Agency, Multi-State Information Sharing and Analysis Center. Compromise of U.S. Water Treatment Facility \(Advisory AA21-042A\). February 2021.](#)
4. [Cybersecurity and Infrastructure Security Agency \(CISA\), Federal Bureau of Investigation. DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks. May 11, 2021.](#)
5. [Cybersecurity and Infrastructure Security Agency \(CISA\), National Security Agency, Federal Bureau of Investigation, and international partners. PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure \(Advisory AA24-038A, Volt Typhoon\). February 7, 2024.](#)
6. [Electricity Information Sharing and Analysis Center \(E-ISAC\), SANS Industrial Control Systems. Analysis of the Cyber Attack on the Ukrainian Power Grid. March 2016.](#)
7. [National Institute of Standards and Technology. Guide to Operational Technology \(OT\) Security, NIST Special Publication 800-82, Revision 3. September 2023.](#)
8. [National Institute of Standards and Technology. The NIST Cybersecurity Framework \(CSF\) 2.0. February 2024.](#)
9. [National Institute of Standards and Technology, National Cybersecurity Center of Excellence. Security Segmentation in a Small Manufacturing Environment, NIST Cybersecurity White Paper \(CSWP\) 28. April 6, 2023.](#)
10. [National Institute of Standards and Technology. Cybersecurity Framework Version 1.1 Manufacturing Profile, NIST Internal Report 8183, Revision 1. 2020.](#)
11. [MITRE Corporation. ATT&CK for ICS: Philosophy and Design Considerations. March 2020.](#)
12. [Dragos, Inc. TRISIS Malware: Analysis of Safety System Targeted Malware. 2017.](#)
13. [FireEye \(Mandiant\). Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure. 2017.](#)
14. [ESET. Win32/Industroyer: A New Threat for Industrial Control Systems. 2017.](#)
15. [Dragos, Inc. CRASHOVERRIDE: Analyzing the Malware that Attacks Power Grids. 2017.](#)
16. [Symantec. W32.Stuxnet Dossier. 2011.](#)
17. [Institute for Science and International Security. Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? 2010.](#)
18. [Dragos, Inc. FrostyGoop: First Malware to Directly Use Modbus TCP to Sabotage Critical Infrastructure. 2024.](#)
19. [Mandiant \(Google\). COSMICENERGY: New OT Malware Possibly Related to Russian Emergency Response Exercises. 2023.](#)
20. [Dragos, Inc. 8th Annual OT/ICS Cybersecurity Year in Review. 2025; and 2026 OT/ICS Cybersecurity Year in Review. 2026.](#)

21. [Anthropic. Disrupting the First Reported AI-Orchestrated Cyber Espionage Campaign. November 2025.](#)
22. [Google Threat Intelligence Group. Reporting on AI-Enabled Attack Lifecycle Integration. 2025-2026.](#)
23. [Indian Computer Emergency Response Team \(CERT-In\), Ministry of Electronics and Information Technology. Comprehensive Cyber Security Audit Policy Guidelines, Version 1.0. July 25, 2025.](#)
24. [Indian Computer Emergency Response Team \(CERT-In\). India Ransomware Report 2022. 2023.](#)
25. [Central Electricity Authority \(India\). Draft Cyber Security in Power Sector Regulations. 2024.](#)
26. [CUTS International / CUTS Centre for Competition, Investment & Economic Regulation. Briefing Paper: Cybersecurity Challenges for Indian MSMEs.](#)
27. [European Union Agency for Cybersecurity \(ENISA\). ENISA Threat Landscape 2025.](#)



SHRIDHAR INFOSEC
S O L U T I O N S

DEFENDING YOUR DATA, SECURING YOUR SUCCESS



Ready to take the next step?

Talk to our OT/ICS experts about a readiness conversation.



+91 93286 67642



info@shridharinfosec.com



www.shridharinfosec.com