

Cyber Resilience for Industrial Control Systems in Saudi Arabia: An Asset-Specific Framework for SCADA, PLC, DCS and HMI Protection and Trusted Recovery

Ishaq Siddiqui Mohammed^{1*} 

¹Independent Researcher

***Corresponding Author**
Ishaq Siddiqui Mohammed
Independent Researcher

Article History

Received: 27.07.2026

Accepted: 21.09.2026

Published: 25.09.2026

Abstract: Industrial Control Systems (ICS) are increasingly connected to enterprise networks, cloud platforms, remote engineering services, and industrial Internet of Things devices. Saudi Arabia is a particularly relevant setting because NCA OTCC-1:2022 establishes minimum cybersecurity requirements for relevant government organizations and private-sector organizations owning, operating or hosting Critical National Infrastructures, while other organizations are encouraged to use the controls as guidance (NCA, 2022). This review synthesizes evidence published between 2020 and 2025 with emphasis on the ability to anticipate, withstand, detect and contain, recover from, and adapt after cyber incidents while preserving safety, availability, integrity, and deterministic operational requirements. Across the retained evidence set, recurring resilience practices include current asset and dependency visibility, segmentation, least privilege, controlled remote access, process-aware monitoring, disciplined engineering change control, safety-centered response, and verified restoration. These are evidence-supported findings from the reviewed literature and authoritative guidance. Building on that evidence, this study proposes a Saudi-oriented, asset-specific resilience framework that maps NCA OTCC/ECC requirements and complementary NIST and IEC guidance to SCADA, PLC, DCS, and HMI resilience functions, and extends the synthesis with recovery engineering, exercise-based validation, and a Proposed Saudi OT Cyber Resilience Measurement Set.

Keywords: Industrial Control Systems (ICS); Operational Technology (OT); Cyber Resilience; SCADA; Programmable Logic Controllers (PLC); Distributed Control Systems (DCS).

Copyright © 2026 The Author(s): This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY-NC 4.0) which permits unrestricted use, distribution, and reproduction in any medium for non-commercial use provided the original author and source are credited.

INTRODUCTION

Industrial Control Systems (ICS) monitor physical conditions, execute control logic and coordinate production through field devices, controllers, supervisory servers, engineering workstations and operator interfaces. Here, SCADA denotes geographically distributed supervision and control; PLCs execute deterministic local logic; DCSs

coordinate integrated plant control; and HMIs provide operator visualization and commands. Enterprise analytics, remote support, virtualization and cloud connectivity have weakened assumptions of natural isolation (Yadav & Paul, 2021; Kayan *et al.*, 2022).

Citation: Mohammed, I. S. (2026). Cyber Resilience for Industrial Control Systems in Saudi Arabia: An Asset-Specific Framework for SCADA, PLC, DCS and HMI Protection and Trusted Recovery. *Glob Acad J Econ Buss*, 8(5), 1425-1447. <https://doi.org/10.36348/gajeb.2026.v08i05.033>

OT security differs from conventional IT because availability, integrity, safety, deterministic timing and stable process behaviour are critical. A control that introduces delay, forced reboot or blocked engineering traffic can itself create operational risk. Cyber resilience therefore asks whether essential functions can withstand attack, contain compromise and recover a trusted state (Alrumaih *et al.*, 2023). This creates a cybersecurity-safety-production balance: the most restrictive technical action is not necessarily the safest operational action.

Saudi Arabia provides a relevant regulatory context. NCA OTCC-1:2022 establishes minimum requirements for relevant government organizations and private-sector organizations owning, operating or hosting Critical National Infrastructures; other organizations are encouraged to use it as guidance (NCA, 2022). ECC 2-2024 supplies the broader national baseline (NCA, 2024a). This paper uses OTCC as its principal Saudi OT reference without implying identical scope for every organization. Compliance addresses required controls; resilience additionally requires evidence that critical functions withstand disruption, contain effects and return to a verified safe, trusted state.

Recent literature covers several dimensions of ICS cybersecurity, including SCADA architecture and vulnerabilities (Upadhyay & Sampalli, 2020; Yadav & Paul, 2021; Alanazi *et al.*, 2023), industrial cyber-physical security (Kayani *et al.*, 2022; Canonico & Sperli, 2023; Harkat *et al.*, 2024), machine-learning-based detection and its limitations (Anthi *et al.*, 2021; Umer *et al.*, 2022; Koay *et al.*, 2023; Kravchik *et al.*, 2022), threat modeling and process-aware monitoring (Khalil *et al.*, 2024; Rehman & Bahsi, 2024), and incident response and recovery (Etchezarreta *et al.*, 2023; Staves *et al.*, 2022). Alrumaih *et al.* (2023) explicitly review cyber resilience in industrial networks. The relevant gap is therefore not an absence of resilience research, but fragmentation across asset classes, regulatory settings, recovery engineering, and operational measurement. The comparison set in Table 1 was drawn from retained 2020–2025 reviews that were directly comparable because they addressed one or more of these core dimensions; within that comparison set, no identified review combines all four asset-specific views, Saudi NCA operationalization, trusted recovery engineering, and a formal operational measurement taxonomy.

Research questions. RQ1 asks which recurring technical, organizational, response and recovery capabilities support cyber resilience across

ICS environments. RQ2 asks how resilience requirements differ among SCADA, PLC, DCS and HMI assets. RQ3 asks how those capabilities can be operationalized under Saudi NCA OTCC/ECC through auditable evidence and measurable outcomes. RQ4 asks which trusted-recovery outcomes and validation gaps remain insufficiently measured or empirically tested. The result chain is explicit: RQ1 is answered by the control strategy and thematic evidence matrix; RQ2 by the asset-specific threat and recovery analysis; RQ3 by the NCA alignment, traceability mapping and measurement set; and RQ4 by the trusted-state protocol, limitations and proposed validation agenda. The study is a structured synthesis and framework proposal, not a comparative efficacy experiment.

Safety and protocol precision. Safety instrumented systems, safety PLCs, emergency shutdown and fire-and-gas functions are treated as distinct safety layers rather than ordinary IT/OT assets. Cyber actions must preserve functional safety, defined trip logic and operator authority. Industrial protocol weakness is deployment-dependent: not every site uses insecure Modbus/TCP, and direct encryption or MFA may be infeasible at Level 1/2. Compensating controls therefore include IEC 62443 zones and conduits, segmentation, secure gateways, allowlisting, passive monitoring, controlled engineering paths and MFA at jump hosts, PAM systems, remote-access gateways and engineering workstations where technically feasible.

Table 1 provides explicit evidence for the novelty claim. It does not support a blanket assertion that prior reviews are predominantly detection-focused; instead, it shows heterogeneous coverage. Some reviews address resilience broadly, whereas others focus on SCADA, threat modelling, machine learning, process-aware monitoring, or intrusion response. Within the reviewed comparison set, no identified prior review simultaneously combines (i) SCADA, PLC, DCS, and HMI as distinct resilience objects, (ii) explicit mapping to Saudi NCA OTCC/ECC requirements, (iii) recovery engineering as a first-class outcome, and (iv) a proposed operational resilience measurement taxonomy. This integrated combination is the specific contribution of the present study.

The objectives are to: O1 compare asset-specific exposure and consequences; O2 synthesize preventive, absorptive, response and recovery practices; O3 map evidence to NCA OTCC/ECC, NIST and IEC 62443; and O4 identify gaps in measurement, trustworthy detection, safe recovery and human-machine coordination.

Table 1A: Comparative coverage of existing ICS resilience reviews

Review	ICS Resilience	SCADA	PLC	DCS	HMI	Saudi/NCA
Yadav & Paul (2021)	Partial	Yes	Partial	Partial	Partial	No
Kayan et al. (2022)	Partial	Partial	Partial	Partial	Partial	No
Umer et al. (2022)	Detection focus	Partial	Partial	Partial	Partial	No
Alrumaih et al. (2023)	Yes	Cross-cutting	Cross-cutting	Cross-cutting	Cross-cutting	No explicit NCA mapping
Alanazi et al. (2023)	Partial	Yes	Limited	Limited	Limited	No
Canonico & Sperli (2023)	Partial	Cross-cutting	Cross-cutting	Cross-cutting	Cross-cutting	No
Etxezarreta et al. (2023)	Partial-response	Cross-cutting	Cross-cutting	Cross-cutting	Cross-cutting	No
Khalil et al. (2024)	Partial threat modeling	Cross-cutting	Cross-cutting	Cross-cutting	Cross-cutting	No
Rehman & Bahşi (2024)	Partial monitoring	Cross-cutting	Cross-cutting	Cross-cutting	Cross-cutting	No
Bajwa et al. (2025)	No – AI detection focus	Yes	Limited	Limited	Limited	No
Present Review (author-coded)	Yes	Yes	Yes	Yes	Yes	Yes – OTCC/ECC

Table 1B: Coverage of recovery engineering, resilience metrics and evidence basis

Review	Recovery Engineering	Resilience Metrics	Review-level evidence / present-framework status
Yadav & Paul (2021)	No	No	Narrative review scope
Kayan et al. (2022)	Limited	Partial	Review scope
Umer et al. (2022)	No	Detection metrics	Detection review
Alrumaih et al. (2023)	Partial	Yes – identifies needs	State-of-art review
Alanazi et al. (2023)	No	Limited	SCADA review
Canonico & Sperli (2023)	Limited	Limited	Methodological review
Etxezarreta et al. (2023)	Limited	Response-oriented	Response survey
Khalil et al. (2024)	No	Validation gaps	Threat-model review
Rehman & Bahşi (2024)	No	Detection/monitoring	Monitoring review
Bajwa et al. (2025)	No	Detection metrics	AI detection review
Present Review (author-coded)	Yes	Yes – formal set	Integrated author synthesis; proposed and validation-ready, not empirically validated

Interpretation: “Partial” means a topic is discussed but is not the organizing scope; “cross-cutting” means ICS-level treatment without separate asset synthesis. All labels, including the Present Review row, are

author-coded from reported scope, were not independently re-coded, and do not constitute a systematic quality appraisal.

Saudi-Oriented Resilient ICS Architecture

Simplified security zones and recovery

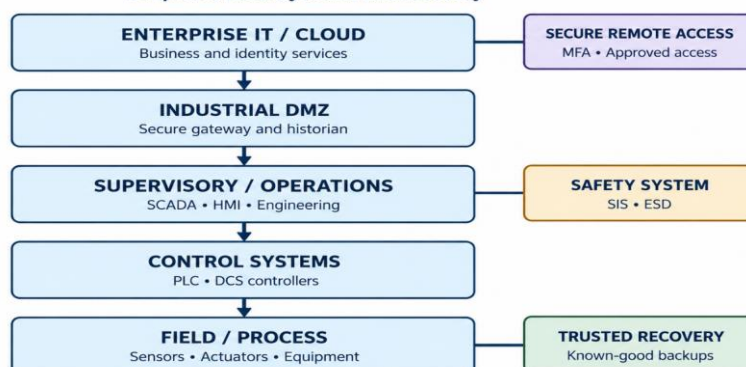


Figure 1: Saudi-oriented resilient ICS architecture with explicit enterprise, industrial DMZ, supervisory/control, independent safety, remote-access, monitoring/management, and trusted-recovery zones and conduits.

Threat Landscape across SCADA, PLC, DCS and HMI Environments

SCADA attack paths include remote telemetry, protocol gateways, historians, engineering workstations, wireless links, vendor access and enterprise integration. Geographic dispersion and legacy protocols complicate visibility and trust. Vulnerability arises from software defects, insecure configuration, flat networks, exposed services and weak access control (Upadhyay & Sampalli, 2020; Yadav & Paul, 2021; Alanazi *et al.*, 2023).

PLC compromise can modify logic, set points, firmware, memory, communications or operating mode, directly affecting physical outputs (Hui *et al.*, 2021; Ocaka *et al.*, 2024). A controller may communicate normally while executing malicious logic, so network-only detection is insufficient.

DCS environments typically integrate controllers, process servers, engineering stations, operator consoles, historians, batch systems, and safety-related interfaces in a plant-wide architecture. Redundancy and integration can improve availability, but the same integration can create routes for correlated or cascading failures. Canonico and Sperli (2023) emphasize that industrial cyber-physical protection must account for both cyber pathways and physical consequences.

HMIs and operator stations occupy a critical human-machine boundary. The risk is cognitive as well as technical because altered displays may induce unsafe operator decisions. Miller *et al.* (2021) show that major ICS incidents commonly involve multi-

stage attack chains, while Kumar *et al.* (2022) model advanced persistent threats through linked attack-tree sequences.

Across all four asset classes, protocol capability and deployment choices remain important. Modbus/TCP, for example, was designed for trusted environments and does not provide modern authentication or confidentiality by default; however, the resulting exposure depends on how the protocol is deployed and what compensating controls surround it. Rahman *et al.* (2022) demonstrate denial-of-service risks and evaluate protection mechanisms. Where protocol security cannot be added directly, segmentation, secure gateways, application allowlisting, passive monitoring, and tightly controlled conduits can reduce exposure. Monitoring should therefore consider expected roles, commands, timing, and process context rather than IP addresses and ports alone.

Machine-learning-based defences also introduce resilience considerations. Koay *et al.* (2023) and Umer *et al.* (2022) identify dataset limitations and challenges in generalizing across plants. Anthi *et al.* (2021) show that adversarial examples can reduce classifier performance, and Kravchik *et al.* (2022) demonstrate poisoning attacks against online anomaly detectors. AI should therefore be treated as an assisting detection layer rather than an infallible authority, with protected training pipelines, drift monitoring, interpretable alerts, fallback rules, and independent process-safety checks.

Table 2: Asset-specific threat exposure and resilience priorities.

Asset class	Primary resilience concern	Representative attack paths	Priority resilience controls
SCADA	Loss or manipulation of supervisory visibility and remote control	Remote access compromise; protocol abuse; gateway/historian pivot; ransomware	IT/OT segmentation; protocol-aware monitoring; redundant communications; trusted historian/HMI recovery
PLC	Integrity of deterministic control logic and field outputs	Logic injection; firmware abuse; MITM; DoS; unauthorized mode change	Restricted engineering paths; logic baselines; secure change control; controller backups; physical/process interlocks
DCS	Plant-wide propagation and coordinated process disruption	Engineering workstation compromise; privileged misuse; malicious configuration distribution	Zone separation; redundant servers/controllers; privileged access management; staged restoration; configuration integrity
HMI	Trusted operator perception, alarms, and commands	Credential theft; ransomware; alarm suppression; screen/data manipulation	Application whitelisting; least privilege; trusted images; alarm validation; local/manual fallback procedures

Cyber Resilience Architecture and Control Strategy

Cyber resilience assumes some prevention will fail. It therefore limits blast radius, sustains safe functions, accelerates detection and supports trusted recovery. NIST SP 800-82 Rev. 3 and Saudi OTCC emphasize OT-specific performance, safety,

segmentation, access control, monitoring, incident handling, backup and third-party governance (NIST, 2023; NCA, 2022; NCA, 2024b).

The first resilience measure is accurate visibility of assets and dependencies. Organizations cannot protect or restore systems they do not

understand. NCA implementation guidance further emphasizes evidence and periodic effectiveness measurement rather than purely documentary control existence (NCA, 2024b).

Segmentation separates enterprise IT, industrial DMZs, supervisory and control networks, safety areas and remote-access routes. Gateways permit only necessary traffic, while IEC 62443-2-1:2024 embeds zones, conduits and compensating measures within the asset-owner lifecycle (IEC, 2024).

The third layer concerns identity and privileged access. Shared engineering accounts, default passwords, uncontrolled vendor access, and excessive administrator rights weaken accountability and complicate recovery. CISA cross-sector performance goals likewise emphasize strong identity controls and IT/OT coordination (CISA, 2025).

Change management requires authorization, version control, integrity checks, testing, rollback and post-change verification. Known-good packages and baseline comparison support Trusted Configuration Coverage and reveal unexpected controller changes (Khalil *et al.*, 2024; Rehman & Bahşi, 2024).

The fifth layer is continuous, passive, and process-aware monitoring. Packet visibility alone is insufficient for stealthy process manipulation; resilience improves when network telemetry is correlated with controller state, engineering changes,

alarm behaviour, historian data, and physical process constraints. Lightweight methods may be useful where resources are limited (Kravchik & Shabtai, 2022).

The sixth layer is response centred on both security and continuity. Staves *et al.* (2022) show that ICS response and recovery require frameworks adapted to operational constraints.

The seventh layer is recovery engineering. Backups provide limited assurance if they are incomplete, unprotected, outdated, or untested. Recovery must use known-good configurations and firmware and follow operational dependencies. Restoring HMI visibility before verifying controller integrity, for example, may recover observation without restoring trust. The recovery endpoint used in this study is a trusted OT state: controller logic and configuration are integrity-verified and authorized, privileged identities are validated, no known persistence remains, communications conform to approved paths, and the physical process operates within its validated safe envelope. Exercises should demonstrate that essential control functions can be reconstructed with available software, hardware, credentials, documentation, and safety authority.

Learning and adaptation use operational evidence such as containment time, verified recovery time, backup coverage, privileged-session assurance, unauthorized-change detection and exercise results (Alrumaih *et al.*, 2023; Harkat *et al.*, 2024).



Figure 2: Cyber resilience lifecycle for industrial control systems: asset discovery, risk assessment, segmentation, continuous monitoring, incident response, recovery, and continuous improvement.

METHODOLOGY

This structured integrative literature review uses PRISMA 2020-informed reporting (Page *et al.*, 2021) and combines scholarly research with authoritative guidance. It asks which practices support resilience across SCADA, PLC, DCS and HMI environments and how they can be operationalized for Saudi critical infrastructure. The evidence window was January 2020-December 2025.

Search terms combined ICS/OT asset terms with cyber resilience, incident response, recovery, process-aware monitoring, ransomware and anomaly detection. Eligible scholarly sources were peer-reviewed reviews, experiments, frameworks or methods relevant to ICS security and recovery; authoritative standards and government guidance were also eligible. Because the exact final execution date was not preserved, the December 2025

boundary is reported as a deliberate evidence cutoff, not proof that the evidence is current through 2026.

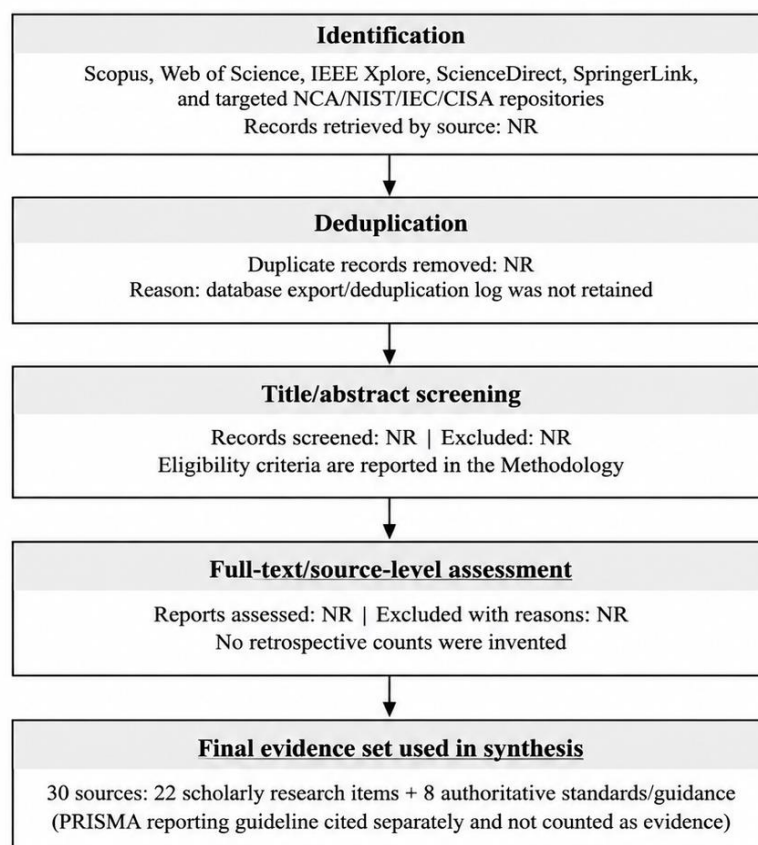
The review is not presented as a fully reproducible systematic review because raw exports, deduplication records, complete exclusion logs and the final search date were not retained. The intended sources were Scopus, Web of Science, IEEE Xplore, ScienceDirect, SpringerLink and NCA, NIST, IEC and CISA repositories. The bibliography contains 30 evidence sources plus Page *et al.* (2021) as reporting guidance. Appraisal was qualitative and no retrospective numeric score was invented.

Search-log integrity and PRISMA reporting

Unsupported intermediate screening counts from an earlier draft were removed. Figure 3 and Table 3 therefore use NR where records were not preserved. Complete PRISMA reproducibility would require raw exports, deduplication records, dated searches and full-text exclusion reasons.

PRISMA 2020-Aligned Evidence Accounting

Reconstructed from the retained manuscript record; unrecorded intermediate counts are marked NR.



NR = not recorded in the retained audit trail. This transparent limitation replaces the unsupported 214 → 181 → 89 → 47 → 30 sequence.

Figure 3: Partial/reconstructed PRISMA 2020-informed evidence accounting based on the retained manuscript record. NR denotes an intermediate count that was not recorded and therefore was not retrospectively invented; the figure is not a complete historical screening audit.

Table 3: Reproducibility status of the retained search record

Source / stage	Records retrieved	Duplicates	Title/abstract exclusions	Full-text exclusions (reasons)	Quality-assessment result	Final included
Scopus	NR	NR	NR	NR - no retained exclusion log	No source-specific score retained	Not attributable by database
Web of Science	NR	NR	NR	NR - no retained exclusion log	No source-specific score retained	Not attributable by database
IEEE Xplore	NR	NR	NR	NR - no retained exclusion log	No source-specific score retained	Not attributable by database
ScienceDirect	NR	NR	NR	NR - no retained exclusion log	No source-specific score retained	Not attributable by database
SpringerLink	NR	NR	NR	NR - no retained exclusion log	No source-specific score retained	Not attributable by database
NCA / NIST / IEC / CISA targeted repositories	NR	Not applicable/ NR	NR	NR - no retained exclusion log	Authority/provenance verified	8 authoritative sources in final set
Final evidence set	—	—	—	—	Eligibility and metadata verified for cited sources	30 evidence sources (22 scholarly + 8 authoritative)

Because source-level provenance was not retained for each scholarly record, assigning the 22 scholarly sources back to a specific discovery database would be speculative. A future update should preserve raw exports, automated and manual deduplication records, reasons for each full-text exclusion, and a dated search strategy for every database.

Data extraction, coding, and reviewer process

The synthesis codes each included source by publication year, asset focus, threat or problem type, resilience phase, control mechanism, evidence type, and practical limitation. Findings are organized into

five resilience functions: anticipate, withstand, detect and contain, recover, and adapt. A second coding layer distinguishes SCADA, PLC, DCS, HMI, and cross-cutting OT controls. The evidence is then compared with NCA OTCC-1:2022 and ECC 2-2024, NIST SP 800-82 Rev. 3, and IEC 62443 asset-owner and service-provider program requirements.

The retained review materials do not document independent double screening or an inter-reviewer adjudication process. The review is therefore conservatively reported as a single-reviewer screening and extraction exercise. No disagreement-resolution procedure is implied.

Table 4: Data-extraction and coding template used for thematic synthesis and future reproducibility.

Field	Operational definition	Permitted coding / examples	Purpose in synthesis
Bibliographic identity	Verified author, year, title, venue, DOI/official URL	Publisher/DOI or official issuing-body record	Traceability and reference integrity
Source class	Nature of evidence	Peer-reviewed research; conference proceedings; government guidance; international standard	Separates empirical/scholarly evidence from authoritative requirements
Asset focus	ICS component explicitly addressed	SCADA; PLC; DCS; HMI; cross-cutting OT/ICS	Supports asset-specific synthesis
Threat/problem type	Primary security or resilience problem studied	Ransomware; protocol abuse; malicious logic; APT; anomaly detection; remote access; recovery	Links threats to operational consequences
Resilience phase	Primary lifecycle function addressed	Anticipate; withstand; detect & contain; recover; adapt; multi-phase	Organizes evidence by resilience function
Control mechanism	Technical/organizational mechanism evaluated or recommended	Segmentation; identity; monitoring; change control; backup; incident response; recovery	Maps evidence to controls
Evidence type	Basis of the source claim	Systematic review; survey; experiment/testbed; incident	Qualifies strength and transferability

Field	Operational definition	Permitted coding / examples	Purpose in synthesis
		analysis; framework; authoritative control/standard	
Outcome/metric	Reported or inferable assessment dimension	Accuracy; latency; availability; response time; recovery; continuity; qualitative requirement	Separates detection metrics from operational resilience outcomes
Saudi/NCA relevance	Whether the source directly maps to Saudi requirements	Direct NCA source; indirect international guidance; no Saudi-specific mapping	Supports the Saudi-oriented synthesis
Limitation	Constraint affecting interpretation	Dataset specificity; simulation; limited asset scope; no recovery validation; guidance rather than empirical evidence	Prevents over-generalization
Verification status	Reference-integrity check	DOI/publisher verified; official issuing-body source verified	Ensures cited metadata and provenance are traceable

Quality assessment was intentionally non-numeric because the original screening record did not preserve a validated scoring instrument. Authoritative sources were retained only when verified against the issuing organization. No retrospective quality scores were invented.

FINDINGS

A recurring thematic pattern across the included evidence is that resilience depends on architecture and operational discipline as well as on detection technology. This statement is derived from convergent support across authoritative lifecycle

guidance (NCA, 2022; NIST, 2023; IEC, 2023; IEC, 2024) and scholarly reviews of industrial cybersecurity, resilience, threat modelling, incident experience, and response/recovery (Kayan *et al.*, 2022; Alrumaih *et al.*, 2023; Khalil *et al.*, 2024; Miller *et al.*, 2021; Staves *et al.*, 2022). It is not a quantitative finding that architecture is statistically “more influential” than another determinant. Rather, the evidence matrix in Table 5 shows that architecture, operational discipline, detection, response, and recovery recur with different emphasis across the literature, supporting a multi-determinant resilience model.

Table 5: Thematic evidence matrix showing which included sources substantively support major resilience determinants.

Source	Architecture / segmentation	Operational discipline / governance	Detection / monitoring	Response / containment	Recovery / restoration	Evidence class / validation basis
Upadhyay & Sampalli (2020)	Yes	Partial	Partial	Limited	Limited	Review
Yadav & Paul (2021)	Yes	Partial	Yes	Limited	Limited	Review
Miller <i>et al.</i> (2021)	Partial	Yes	Partial	Yes	Partial	Incident analysis / lessons
Kayan <i>et al.</i> (2022)	Yes	Yes	Yes	Partial	Partial	Review
Umer <i>et al.</i> (2022)	Limited	Limited	Yes	No	No	Review
Staves <i>et al.</i> (2022)	Partial	Yes	Partial	Yes	Yes	Framework + stakeholder evidence
Alrumaih <i>et al.</i> (2023)	Yes	Yes	Yes	Yes	Yes	State-of-art review
Canonico & Sperli (2023)	Yes	Partial	Yes	Partial	Limited	Methodological review
Etchezarreta <i>et al.</i> (2023)	Yes	Partial	Yes	Yes	Limited	Response survey/review
Khalil <i>et al.</i> (2024)	Yes	Yes	Partial	Partial	Limited	Systematic review
Rehman & Bahsi (2024)	Partial	Partial	Yes	Partial	No	Systematic review
NCA OTCC / implementation guidance	Yes	Yes	Yes	Yes	Yes	Authoritative Saudi guidance

Source	Architecture / segmentation	Operational discipline / governance	Detection / monitoring	Response / containment	Recovery / restoration	Evidence class / validation basis
NIST SP 800-82r3	Yes	Yes	Yes	Yes	Yes	Authoritative international guidance
IEC 62443-2-1/-2-4	Yes	Yes	Partial	Partial	Partial	International standards/guidance

Note. Yes, Partial and Limited describe substantive coverage in the cited source; they do not establish empirical effectiveness of the control or validate the present framework.

Asset needs differ. SCADA emphasizes distributed communications, remote access and supervisory visibility; PLCs emphasize logic and firmware integrity; DCSs emphasize configuration governance and propagation control; and HMIs emphasize trusted visualization, alarm integrity and operator fallback. A generic hardening checklist is therefore insufficient.

Process-aware attacks challenge conventional monitoring assumptions. Rehman and Bahşi (2024) demonstrate the value of incorporating process behaviour and physical relationships, while Etxezarreta et al. (2023) show that programmable network response can support rapid containment, subject to industrial safety constraints.

Machine learning can detect multivariate anomalies but remains constrained by plant specificity, class imbalance, explainability and adversarial risk (Anthi *et al.*, 2021; Koay *et al.*, 2023; Kravchik *et al.*, 2022). High-consequence facilities should retain deterministic safety protections and expert judgment.

Recovery is less consistently evaluated than detection performance. Staves et al. (2022) explicitly

address response and recovery. A resilient facility therefore needs evidence that backups can reconstruct controllers and supervisory systems, that teams know dependency-aware restoration sequences, and that compromised persistence mechanisms or credentials are not reintroduced. Verified Recovery Time (VRT) is defined here as a post-recognition recovery metric: the elapsed time, reported in minutes or hours, from the first auditable incident-recognition timestamp to authorized approval of verified trusted safe operation. VRT does not measure attacker dwell time or the period between initial compromise and recognition. The stop event requires completion of the trusted-state checklist: authorized and integrity-verified logic/configuration, validated privileged identities, no known persistence, approved communication paths, and stable process operation within the accepted safe envelope. Server or application availability alone does not stop the VRT clock.

OTCC-1:2022 provides the Saudi OT control basis, supported by its implementation guidance and the enterprise-level ECC 2-2024 baseline (NCA, 2022; NCA, 2024a; NCA, 2024b). Table 6 maps synthesized resilience practices to these requirements and international guidance.

Table 6: Resilience practices aligned with Saudi NCA and international OT guidance

Resilience practice	Saudi NCA alignment	Complementary guidance	Operational evidence artifact	Source status
OT asset/dependency inventory	OTCC asset management; ECC asset governance	NIST SP 800-82r3	Current inventory, owners, firmware, dependencies, automated change alerts	NCA + author traceability
Segmentation and controlled conduits	OTCC network security and segregation	IEC 62443 program controls; NIST OT architecture	Documented zones, allowed flows, firewall reviews, blocked unauthorized paths	NCA + international guidance
Privileged and remote access control	OTCC identity/access and third-party requirements	IEC 62443-2-1:2024; IEC 62443-2-4:2023	Named accounts, MFA where feasible, jump hosts, time-limited vendor access, session logs	NCA + international guidance
Monitoring and process-aware detection	OTCC monitoring, logging, incident detection	NIST SP 800-82r3; CISA CPGs	Passive OT sensors, protocol alerts, engineering-change alerts, process correlation	NCA + research synthesis

Resilience practice	Saudi NCA alignment	Complementary guidance	Operational evidence artifact	Source status
Backup, response and recovery	OTCC incident, continuity, and recovery expectations; ECC continuity controls	NIST SP 800-82r3; IEC program requirements	Offline controller/HMI/DCS backups, tested restoration, verified recovery time, exercise reports	NCA + recovery synthesis

Trusted-state and resilience model. Operational resilience is represented conceptually as $OR = f(A, W, DC, R, AD)$. A (anticipate) means identifying critical functions, assets, dependencies and credible threats and preparing controls; W (withstand) means sustaining or safely degrading essential functions under disruption; DC (detect/contain) means identifying abnormal cyber/process behaviour and limiting adverse effects without creating unsafe process consequences; R (recover) means restoring an authorized, integrity-verified and process-safe trusted state; and AD (adapt) means converting incident/exercise evidence into improved architecture, controls, procedures and training. This expression is an organizing synthesis, not a statistically validated causal or predictive equation. A trusted OT state requires authorized controller logic and configuration, verified firmware/configuration integrity, validated privileged identities, absence of known persistence, communications consistent with approved architecture, process variables within safe envelopes and successful validation of critical control and safety functions. Recovery time therefore ends at verified

safe operation, not simple server availability. These functions overlap and operate iteratively rather than as a strictly linear sequence; evidence from detection, containment and recovery feeds renewed anticipation and adaptation.

Monitoring and safe containment. The intended evidence chain is sensor and process telemetry to passive OT monitoring, correlation/analytics, SOC/OT analyst review and engineering/process validation. Process-aware detection asks whether commands, timing, states and physical relationships are plausible, not merely whether packets are unusual. Containment follows a safety-first decision rule: cyber confidence and consequence are evaluated with current process state; low-risk logging, evidence collection and credential restriction may be automated, while actions capable of changing a physical process, removing safety visibility or interrupting an essential service require pre-authorized operational and process-safety approval unless an engineered fail-safe condition has been explicitly validated.

Table 6A: Asset-specific Purdue/ISA-95 overlay and trusted recovery

Asset	Typical level	Critical function	Dominant consequence	Recovery package	Trusted-state endpoint
SCADA	L3	Supervisory visibility/control	Loss/manipulation of remote operations	Server/config/historian backups	Validated view, commands and communications
PLC	L2	Deterministic control logic	Unsafe/incorrect field outputs	Known-good logic, firmware, parameters	Logic hash/version and safe process response
DCS	L2-L3	Plant-wide coordinated control	Propagation across process units	Controllers, servers, engineering repository	Configuration integrity and staged process verification
HMI	L3	Operator view and commands	False perception/alarm loss	HMI image, graphics, alarm database	Trusted displays, alarms and operator access
SIS/ESD	L1-L2 safety boundary	Independent protective action	Loss of functional safety	Approved safety logic/configuration	Safety validation under authorized procedure

Note. Purdue/ISA-95 level labels are used only as typical functional references, not as a universal physical architecture. Real plants may use hybrid or vendor-specific layouts; IEC 62443-style zones and conduits are logical security boundaries that can span or subdivide nominal Purdue levels.

Discussion: Consequences for Saudi Critical Infrastructure

The findings support moving from documentary compliance toward evidence of operational resilience: demonstrable safe continuity,

controlled degradation, containment and trusted recovery. NCA, NIST and IEC provide requirements and guidance; the author-proposed contribution integrates these with four asset views, recovery verification, exercises and measurement.

Saudi OT Cyber Resilience Framework

Authoritative control mappings + asset-specific resilience + measurable recovery outcomes

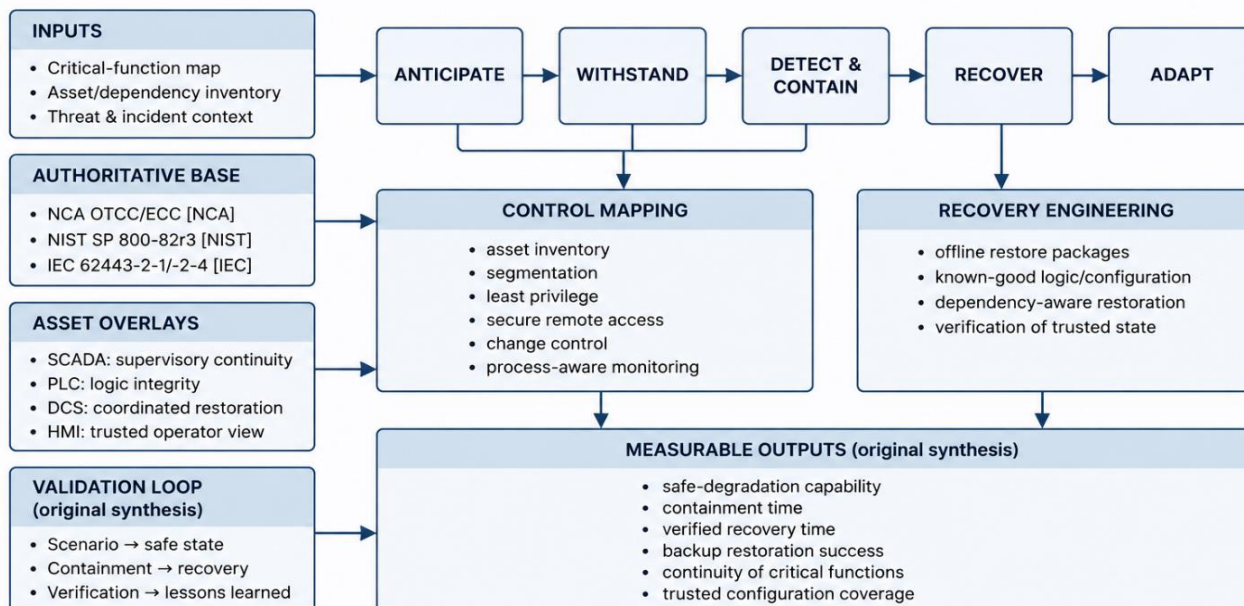


Figure 4: Proposed Saudi OT Cyber Resilience Framework. NCA, NIST, and IEC components are authoritative inputs; the integrated asset-specific mapping, recovery-oriented outputs, validation loop, and measurement taxonomy are the author-proposed synthesis and require empirical validation.

Figure 4 presents an author-proposed staged framework linking authoritative inputs, asset overlays, recovery engineering and measurable

outcomes. Regulatory alignment supports traceability but does not prove effectiveness; exercises and field studies are required.

Table 6B: Framework traceability from authoritative controls to asset focus, operational evidence artifacts, and proposed metrics

Framework stage	Authoritative requirement/guidance	Asset focus	Operational evidence artifact	Linked metric(s)
Anticipate	NCA OTCC asset/risk management; NIST OT security	All assets/dependencies	Critical-function map; asset/dependency inventory; approved baseline	TCC
Withstand	NCA OTCC segregation/access; IEC 62443 zones/conduits	SCADA, PLC, DCS, HMI, remote access	Approved zone/conduit diagram; firewall rules; PAM/session records	PSAR; CFR
Detect & contain	NCA OTCC monitoring/incident; NIST/CISA guidance	All assets; supervisory/engineering paths	Passive sensor logs; process correlation; incident timeline	MCT; UCDE
Recover	NCA OTCC continuity/recovery; NIST/IEC program guidance	SCADA, PLC, DCS, HMI; SIS under safety authority	Known-good restore package; logic/config hashes; restore test; trusted-state checklist	VRT; BRSR; TCC
Adapt	NCA effectiveness review; lifecycle improvement	Cross-cutting	Exercise report; corrective-action register; updated baselines/procedures	Trend across all metrics

The scale and complexity of Saudi industry also make third-party and remote access particularly important. Equipment manufacturers, integrators, maintenance contractors, and original equipment manufacturers often require specialized access. IEC 62443-2-4:2023 specifies security-program requirements for IACS service providers, complementing asset-owner requirements in IEC 62443-2-1:2024. Saudi operators can align these principles with OTCC contracting requirements by defining approved personnel, access windows, managed jump hosts, session recording, malware controls, and rapid revocation capability. Vendor remote access should be revocable, time-bounded, monitored, and disabled by default where technically feasible. Remote access should also be designed so that loss of enterprise connectivity does not prevent safe local operation. Emergency vendor access should follow a documented exceptional-access procedure with named approval authority, time-bounded credentials, complete logging and a post-session review.

Engineering truth must also be protected. Recoverable engineering truth includes approved PLC logic and parameters, DCS configuration, HMI

graphics and alarm databases, firmware, network-device configuration, certificates or cryptographic keys where applicable, and the approved baseline/version evidence that establishes authorization. These repositories should be integrity-protected, independently backed up, and compared with running systems. TCC measures whether critical assets possess an approved, integrity-verified, restorable package, while VRT is not complete until those artifacts have been used to verify the restored trusted state. Cryptographic keys and certificates require separate secure key-management, escrow where authorized, rotation and recovery procedures; they should not simply be copied into ordinary configuration-backup repositories.

Exercise-validation model

Exercises should define the scenario, safe state, containment authority, restoration dependencies, safety criteria, evidence and pass/fail rules. Governance must record approval, production classification, safety observer, stop conditions, abort authority and post-exercise restoration. Operations or process-safety authority may immediately terminate production tests.

Table 7: Exercise-validation model for testing the Saudi OT cyber resilience framework

Scenario	Expected safe state	Containment action	Recovery sequence	Pass/fail and trusted-state criteria	Primary measures	Lessons / improvement output
Ransomware on HMI/engineering workstation	Local control preserved; unsafe commands prevented	Isolate affected workstation/HMI; preserve controller operation where safe	Clean HMI image → trusted application/configuration → credential reset → reconnect after validation	PASS if no malware persistence remains; alarms/trends match field state; operator commands are validated; safe envelope preserved. Acceptance: operations + OT engineering + process safety/HSE.	Containment time; verified recovery time; HMI restore success	Image quality, access controls, response decision rights
Malicious PLC logic modification	Process held within predefined safe envelope	Restrict engineering path; move controller/process to approved safe mode if required	Verify logic hash/baseline → restore known-good program → validate I/O and interlocks	PASS if logic matches approved baseline; I/O/interlocks validate; process response remains within limits. Acceptance: control engineering + operations + process safety/HSE.	Safe-degradation success; PLC restore success; trusted-state verification time	Change-control gaps, baseline integrity, engineering access

Scenario	Expected safe state	Containment action	Recovery sequence	Pass/fail and trusted-state criteria	Primary measures	Lessons / improvement output
Loss/manipulation of SCADA visibility	Local/field control remains safe; critical alarms available by fallback	Segment compromised supervisory path; enable alternate/local visibility	Restore trusted SCADA/HMI services → historian/gateway validation → reconnect conduits	PASS if telemetry consistency and alarm correctness are verified; no unauthorized flows remain; fallback maintained safety. Acceptance: operations + OT engineering.	Maximum loss-of-view duration; continuity of critical function	Redundancy, operator fallback, telemetry validation
Compromised remote vendor session	Vendor path revoked without disrupting safe local operation	Terminate session; disable account/token; isolate jump host if needed	Rebuild/validate jump host → credential rotation → controlled reauthorization	PASS if session trail is complete; credentials/tokens are revoked; no residual unauthorized change exists; safe local operation is preserved. Acceptance: OT security + operations.	Containment time; session assurance rate	Vendor governance, logging, time-bound access
False process data / adversarial analytics	Deterministic protections remain authoritative; operators receive trusted fallback	Quarantine suspect analytics/data source; maintain rule/process-safety controls	Validate sensors/data path → restore model only after integrity and drift checks	PASS if physical consistency checks pass; deterministic safety controls remain authoritative; model/data integrity and operator fallback are validated. Acceptance: operations + process safety/HSE + OT security.	Detection latency; false-alarm burden; safe-degradation success	Model governance, explainability, maintenance-mode testing

Table 7A: Validation evidence requirements by exercise environment

Scenario	Test environment	Evidence artifact	Success criterion	Observed result (future test)	Test date / version	Environment / configuration ID
Ransomware on engineering workstation	Digital twin or cyber range	Containment timeline; HMI/DCS restore log; access-control record	Affected zone isolated without unsafe process effect; trusted HMI/DCS state restored	To be recorded during validation	To be recorded	To be recorded
Malicious PLC logic change	Hardware-in-the-loop or controlled testbed	Logic baseline/hash; controller backup; process historian trace	Unauthorized logic detected; safe fallback maintained; verified known-good logic restored	To be recorded during validation	To be recorded	To be recorded
Compromised remote vendor session	Tabletop plus technical	PAM/jump-host logs; revocation	Access revoked within site target while safe local	To be recorded	To be recorded	To be recorded

Scenario	Test environment	Evidence artifact	Success criterion	Observed result (future test)	Test date / version	Environment / configuration ID
	remote-access test	evidence; session recording	operation remains available	during validation		
False process data / adversarial analytics	Digital twin	Sensor/historian comparison; model explanation; operator decision record	Anomaly identified without unsafe automatic isolation and with acceptable false-positive burden	To be recorded during validation	To be recorded	To be recorded

Proposed Saudi OT Cyber Resilience Measurement Set

The proposed metrics connect controls to auditable outcomes using site-specific targets rather

than universal national thresholds. Provenance distinguishes established or adapted concepts from measures proposed or redefined in this study.

Table 8: Proposed Saudi OT Cyber Resilience Measurement Set.

Metric	Definition / formula + unit / endpoint	Measurement source	Target logic + known limitation	Frequency	Responsible owner	Provenance class
Safe-degradation success rate (SDSR)	Successful degradation events within predefined safe envelope ÷ total degradation events × 100. Unit: %. Endpoint: end of incident/exercise . Population: all formally declared degradation incidents/exercises in scope. Exclude only pre-approved aborted tests; zero events = N/A.	Historian; SIS/process records; exercise report	Target: site risk-based. Limitation: depends on scenario selection and definition of the safe envelope.	Each exercise; quarterly trend	Operations + process safety/HSE + OT security	Proposed in this study
Mean containment time (MCT)	$\Sigma(\text{effective containment time} - \text{incident confirmation time}) \div \text{incidents}$. Unit: minutes/hours. Endpoint: effective containment. Population: confirmed in-scope incidents with auditable confirmation and effective-containment timestamps; zero incidents = N/A.	SOC/OT monitoring logs; incident timeline	Target: site-defined by consequence and segmentation design. Limitation: confirmation and containment timestamps may vary by workflow.	Per incident; monthly/quarterly trend	OT security / incident commander	Established/adapted
Verified recovery time (VRT)	Verified trusted safe operation time – incident-recognition time. Unit: minutes/hours.	Recovery logs; engineering verification; historian/process validation	Target: ≤ site-defined maximum tolerable disruption. Limitation:	Per restoration exercise/incident	OT engineering + operations + process safety/HSE	Redefined for this study

Metric	Definition / formula + unit / endpoint	Measurement source	Target logic + known limitation	Frequency	Responsible owner	Provenance class
	Endpoint: completion of trusted-state checklist. Population: every in-scope restoration incident/exercise. Start: incident recognition. Stop: authorized trusted-state approval; zero restorations = N/A.		verification scope/checklist is site- and process-dependent.			
Backup restoration success rate (BRSR)	Successful verified restores ÷ attempted restore tests × 100. Unit: %. Endpoint: trusted restore validation. Population: all scheduled or incident-driven restore attempts for designated critical assets; zero attempts = N/A.	Backup system; restore test records; engineering validation	Target: site-approved critical-asset success criteria. Limitation: test success may not reproduce compromised -incident conditions.	Quarterly or after major changes	OT engineering / backup owner	Established/adapted
Critical-function continuity ratio (CFCR)	Time critical function remained available within safe operating envelope ÷ incident/exercise duration × 100. Unit: %. Population: all defined critical functions during each in-scope event; zero-duration events = N/A.	Historian; operations log; continuity record	Target: derived from function criticality and tolerable interruption. Limitation: requires reliable synchronized process records and an agreed safe envelope.	Per event; quarterly trend	Operations / business continuity	Proposed in this study
Trusted configuration coverage (TCC)	Critical OT assets with approved, integrity-verified baseline and restorable package ÷ critical OT assets × 100. Unit: %. Population: the approved, version-controlled register of critical OT assets for the period; zero registered assets = N/A and requires	CMDB/asset inventory; version control; backup repository	Target: site-defined, approaching full coverage for designated critical assets. Limitation: coverage does not prove baseline correctness or recovery speed.	Monthly/quarterly	OT asset owner / engineering	Proposed in this study

Metric	Definition / formula + unit / endpoint	Measurement source	Target logic + known limitation	Frequency	Responsible owner	Provenance class
	governance review.					
Privileged/remote session assurance rate (PSAR)	Authorized privileged/vendor sessions with required approval and logging ÷ total privileged/vendor sessions × 100. Unit: %. Population: all privileged/vendor sessions, including documented approved exceptions; zero sessions = N/A.	PAM; jump-host; VPN; session logs	Target: site policy. Limitation: incomplete logging or approved exceptions can distort the denominator.	Monthly	IAM/PAM owner + OT security	Established/adapted
Unauthorized-change detection effectiveness (UCDE)	Confirmed or seeded unauthorized engineering changes detected within defined monitoring window ÷ total confirmed/seeded changes × 100. Unit: %. Population: confirmed incident changes plus formally seeded tests with retained evidence and a defined window; zero changes = N/A.	Change monitoring; version control; exercise records	Target: asset-criticality based. Limitation: seeded tests may not represent stealthy real changes and the monitoring window is site-specific.	Each test; quarterly trend	OT engineering + SOC	Proposed in this study

In an HMI ransomware exercise recognized at 09:00, system availability at 09:42 does not end recovery if controller integrity, alarms and privileged identities remain unverified. If trusted-state validation completes at 10:12, VRT is 72 minutes. CFCR should be calculated separately for each defined critical function and reported with an approved aggregation method where a combined value is required. This prevents one highly available function from masking loss of another critical function. Timestamps must be synchronized and auditable.

Detection accuracy alone does not show safe degradation, continuity, containment speed or recovery trust. The taxonomy therefore links cyber controls to physical continuity and restoration assurance without claiming every underlying concept is new.

The framework and metrics are validation-ready but have not been benchmarked across Saudi facilities. Future tests should record environment, scenario, evidence, success criteria and observed results. Thresholds are site-specific, and the proposed five-level maturity model is not an NCA standard.

Table 8A: Metric taxonomy and validation status

Category	Metrics	Validation requirement	Provenance classification
Safety/continuity	SDSR; CFCR	Representative degradation exercises and safe-envelope evidence	Proposed in this study
Recovery	VRT; BRSR	Trusted-state protocol and verified restore tests	VRT redefined; BRSR established/adapted

Category	Metrics	Validation requirement	Provenance classification
Integrity/configuration	TCC; UCDE	Complete inventory plus known/seeded unauthorized-change tests	Proposed in this study
Access/containment	MCT; PSAR	Incident timelines, approved session logs and site-specific consequence thresholds	Established/adapted

Table 8B: Proposed five-level OT cyber resilience maturity model for Saudi application

Level	Observable characteristics	Representative evidence artifacts
1 Reactive	Ad hoc response; incomplete asset/dependency visibility; recovery largely assumed	Incident records; gap register
2 Managed	Documented controls, roles, backups and basic segmentation; periodic exercises	Approved policies; asset register; backup and exercise records
3 Resilient	Asset-specific containment, process-aware monitoring, tested recovery and safety gates	Zone/conduit evidence; process-aware alerts; trusted restore tests
4 Measured	Outcome metrics trended; trusted-state verification; evidence-based corrective action	Metric register; signed trusted-state checklists; corrective actions
5 Adaptive	Threat-led improvement, cross-site learning, adversarial testing and continuous revalidation	Threat-led test reports; cross-site lessons; revalidation records

Note. The five maturity levels are an author-proposed interpretive model for Saudi application and are not an NCA maturity standard or formally adopted national scale. Evidence artifacts and thresholds require site-specific calibration and empirical validation.

Limitations

The framework has not been validated in live Saudi plants and lacks national benchmark distributions. Evidence types are heterogeneous and the final set is relatively small; screening was performed by one reviewer and historical search records are incomplete. Database, English-language and publication-selection bias, proprietary data and legacy constraints further limit replication. Findings are therefore an evidence-informed synthesis, not causal proof or nationally exhaustive sector guidance.

Research Gaps and Future Directions

Evidence-grounded gaps

Operational resilience measures remain weakly standardized and empirically validated. Detection studies often report accuracy or latency but do not capture safe degradation, critical-function continuity, containment time or trusted engineering recovery (Alrumaih *et al.*, 2023; Harkat *et al.*, 2024; Umer *et al.*, 2022). The proposed measures address these under-standardized outcomes.

Research on recovery from process-aware compromise remains limited. Priorities include forensic validation of PLC logic, trusted DCS rebuilds, compromised recovery repositories, credential compromise and manipulated supervisory visibility. Success must be judged by restored engineering and

process trust rather than restart alone (Staves *et al.*, 2022).

Cross-vendor interoperability is another persistent challenge. Research is needed on compensating controls and normalized evidence models that can provide comparable resilience assurance across mixed legacy and modern estates without disrupting deterministic operations.

Human factors also require deeper investigation. Research should evaluate interface designs that communicate cyber confidence, process risk, and recommended actions without overwhelming operators. HMI resilience is therefore both a software-hardening problem and a decision-support problem.

Proposed research agenda and validation environments

Future validation should combine Delphi consensus, digital twins, hardware-in-the-loop, cyber ranges, incident histories and controlled exercises. Tests should cover ransomware, malicious logic, false data, maintenance modes, mixed vendors and cross-sector process profiles. Outcomes should include detection and containment time, VRT, false-positive burden, production loss, safe degradation, safety impact and operator decision quality. This agenda is proposed validation work, not established evidence.

Table 9: Proposed representative Saudi-sector applicability mapping for the OT resilience framework.

Sector	Dominant OT assets	Critical function	Representative consequence	Priority capability	Guidance / evidence basis
Oil and gas	PLC, DCS, SCADA, SIS	Process control and containment	Unsafe shutdown, loss of containment or prolonged outage	Segmentation, engineering integrity, SIS-aware containment, trusted recovery	NCA OTCC/ECC; NIST SP 800-82r3; IEC 62443
Petrochemical	DCS, PLC, SIS, HMI	Continuous/batch process control	Cascading unit disruption or unsafe process state	Zone isolation, change control, process-aware monitoring	NCA OTCC/ECC; IEC 62443
Power	SCADA, PLC/IED, HMI	Generation/transmission continuity	Loss of control visibility or service interruption	Redundant communications, identity control, recovery sequencing	NCA OTCC/ECC; NIST OT guidance
Water/desalination	SCADA, PLC, HMI	Treatment, pumping and distribution	Service interruption or unsafe process quality	Remote-access control, monitoring, verified configuration recovery	NCA OTCC/ECC; NIST/IEC guidance
Manufacturing	PLC, DCS, robots, HMI	Production and safety interlocks	Quality loss, equipment damage, downtime	Asset visibility, logic integrity, safe degradation	NCA OTCC/ECC; IEC 62443
Transportation	SCADA, PLC, HMI	Signaling, facilities and operational services	Loss of availability or unsafe operational decisions	Segmentation, resilient communications, tested recovery	NCA OTCC/ECC; NIST/IEC guidance

Note. This is an author-proposed representative mapping, not an official NCA sector classification. Asset priorities and metric thresholds must be calibrated through site-specific hazard/consequence analysis, process dynamics, tolerable downtime, safety requirements, and actual architecture; they should not be interpreted as universal Saudi limits.

CONCLUSION

ICS resilience requires operations to anticipate, withstand, contain, recover and adapt when prevention fails. SCADA, PLC, DCS and HMI assets share convergence risks but differ in consequences and restoration dependencies. Effective resilience combines visibility, segmentation, least privilege, change control, process-aware monitoring, safety-centred response and verified recovery. Full availability is not always correct: controlled safe degradation followed by trusted recovery can also demonstrate resilience.

For Saudi Arabia, OTCC-1:2022 and ECC 2-2024 provide the control foundation, complemented by NIST and IEC 62443. This review integrates those sources with asset-specific resilience, recovery engineering, exercises and a Proposed Saudi OT Cyber Resilience Measurement Set. Facilities should map critical functions and dependencies, define safe degradation and containment authority, protect recovery sources, rehearse restoration and retain trusted-state evidence. Targets remain site-specific and require empirical validation. Assurance ownership should include operations, OT

engineering, process safety/HSE, cybersecurity, maintenance and management.

Validation should compare brownfield and greenfield environments using digital twins, hardware-in-the-loop, cyber ranges and safely governed plant tests. Studies should report both successful and unsuccessful trials, continuity, false positives, containment latency, trusted recovery and operator decisions, including supplier, remote-access and supply-chain scenarios.

Human factors should be measured through decision quality, alarm burden, escalation timing and coordination among operations, engineering, cybersecurity, safety/HSE, maintenance, vendors and management. Repeated exercises should convert lessons into revised baselines, access rules, detection logic, recovery packages and training.

REFERENCES

1. Alanazi, M., Mahmood, A., & Chowdhury, M. J. M. (2023). SCADA vulnerabilities and attacks: A review of the state-of-the-art and open issues. *Computers & Security*, 125,

- 103028.<https://doi.org/10.1016/j.cose.2022.103028>
2. Alrumaih, T. N. I., Alenazi, M. J. F., AlSowaygh, N. A., Humayed, A. A., & AlAblani, I. A. (2023). Cyber resilience in industrial networks: A state of the art, challenges, and future directions. *Journal of King Saud University - Computer and Information Sciences*, 35(9), 101781.<https://doi.org/10.1016/j.jksuci.2023.101781>
3. Anthi, E., Williams, L., Rhode, M., Burnap, P., & Wedgbury, A. (2021). Adversarial attacks on machine learning cybersecurity defences in Industrial Control Systems. *Journal of Information Security and Applications*, 58, 102717.
<https://doi.org/10.1016/j.jisa.2020.102717>
4. Canonico, R., & Sperli, G. (2023). Industrial cyber-physical systems protection: A methodological review. *Computers & Security*, 135, 103531.<https://doi.org/10.1016/j.cose.2023.103531>
5. Etchezarreta, X., Garitano, I., Iturbe, M., & Zurutuza, U. (2023). Software-defined networking approaches for intrusion response in Industrial Control Systems: A survey. *International Journal of Critical Infrastructure Protection*, 42, 100615.
<https://doi.org/10.1016/j.ijcip.2023.100615>
6. Harkat, H., Camarinha-Matos, L. M., Goes, J. C., & Ahmed, H. F. T. (2024). Cyber-physical systems security: A systematic review. *Computers & Industrial Engineering*, 188, 109891.<https://doi.org/10.1016/j.cie.2024.109891>
7. Hui, H., McLaughlin, K., & Sezer, S. (2021). Vulnerability analysis of S7 PLCs: Manipulating the security mechanism. *International Journal of Critical Infrastructure Protection*, 35, 100470.<https://doi.org/10.1016/j.ijcip.2021.100470>
8. Kayan, H., Nunes, M., Rana, O., Burnap, P., & Perera, C. (2022). Cybersecurity of Industrial Cyber-Physical Systems: A review. *ACM Computing Surveys*, 54(11s), Article 229.<https://doi.org/10.1145/3510410>
9. Khalil, S. M., Bahşi, H., & Korötko, T. (2024). Threat modeling of industrial control systems: A systematic literature review. *Computers & Security*, 136, 103543.<https://doi.org/10.1016/j.cose.2023.103543>
10. Koay, A. M. Y., Ko, R. K. L., Hettema, H., & Radke, K. (2023). Machine learning in industrial control system (ICS) security: Current landscape, opportunities and challenges. *Journal of Intelligent Information Systems*, 60, 377–405.
<https://doi.org/10.1007/s10844-022-00753-1>
11. Kravchik, M., Demetrio, L., Biggio, B., & Shabtai, A. (2022). Practical evaluation of poisoning attacks on online anomaly detectors in industrial control systems. *Computers & Security*, 122, 102901.<https://doi.org/10.1016/j.cose.2022.102901>
12. Kravchik, M., & Shabtai, A. (2022). Efficient cyber attack detection in industrial control systems using lightweight neural networks and PCA. *IEEE Transactions on Dependable and Secure Computing*, 19(4), 2179–2197.
<https://doi.org/10.1109/TDSC.2021.3050101>
13. Kumar, R., Kela, R., Singh, S., & Trujillo-Rasua, R. (2022). APT attacks on industrial control systems: A tale of three incidents. *International Journal of Critical Infrastructure Protection*, 37, 100521.
<https://doi.org/10.1016/j.ijcip.2022.100521>
14. Miller, T., Staves, A., Maesschalck, S., Sturdee, M., & Green, B. (2021). Looking back to look forward: Lessons learnt from cyber-attacks on Industrial Control Systems. *International Journal of Critical Infrastructure Protection*, 35, 100464.
<https://doi.org/10.1016/j.ijcip.2021.100464>
15. Rahman, A., Mustafa, G., Khan, A. Q., Abid, M., & Durad, M. H. (2022). Launch of denial-of-service attacks on the Modbus/TCP protocol and development of its protection mechanisms. *International Journal of Critical Infrastructure Protection*, 39, 100568.<https://doi.org/10.1016/j.ijcip.2022.100568>
16. Rehman, M. U., & Bahşi, H. (2024). Process-aware security monitoring in industrial control systems: A systematic review and future directions. *International Journal of Critical Infrastructure Protection*, 47, 100719.
<https://doi.org/10.1016/j.ijcip.2024.100719>
17. Staves, A., Anderson, T., Balderstone, H., Green, B., Gougliadis, A., & Hutchison, D. (2022). A cyber incident response and recovery framework to support operators of industrial control systems. *International Journal of Critical Infrastructure Protection*, 37, 100505.<https://doi.org/10.1016/j.ijcip.2021.100505>
18. Umer, M. A., Junejo, K. N., Jilani, M. T., & Mathur, A. P. (2022). Machine learning for intrusion detection in industrial control systems: Applications, challenges, and recommendations. *International Journal of Critical Infrastructure Protection*, 38, 100516.<https://doi.org/10.1016/j.ijcip.2022.100516>
19. Upadhyay, D., & Sampalli, S. (2020). SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations. *Computers & Security*, 89,

101666.
<https://doi.org/10.1016/j.cose.2019.101666>
20. Yadav, G., & Paul, K. (2021). Architecture and security of SCADA systems: A review. *International Journal of Critical Infrastructure Protection*, 34, 100433.<https://doi.org/10.1016/j.ijcip.2021.100433>
 21. Bhamare, D., Zolanvari, M., Erbad, A., Jain, R., Khan, K., & Meskin, N. (2020). Cybersecurity for Industrial Control Systems: A survey. *Computers & Security*, 89, 101677. <https://doi.org/10.1016/j.cose.2019.101677>
 22. Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computers & Security*, 56, 1–27. <https://doi.org/10.1016/j.cose.2015.09.009>
 23. Genge, B., Kiss, I., & Haller, P. (2015). A system dynamics approach for assessing the impact of cyber-attacks on critical infrastructures. *International Journal of Critical Infrastructure Protection*, 10, 3–17. <https://doi.org/10.1016/j.ijcip.2015.04.001>
 24. Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-Physical Systems Security—A Survey. *IEEE Internet of Things Journal*, 4(6), 1802–1831.<https://doi.org/10.1109/JIOT.2017.2703172>
 25. Kriaa, S., Bouissou, M., & Piètre-Cambacédès, L. (2015). Modeling the security of industrial control systems: A survey. *Computers & Security*, 53, <https://doi.org/10.1016/j.cose.2015.05.003>
 26. National Cybersecurity Authority. (2022). *Operational Technology Cybersecurity Controls (OTCC-1:2022)*. Kingdom of Saudi Arabia.Official document: <https://nca.gov.sa>
 27. National Cybersecurity Authority. (2024). *Essential Cybersecurity Controls (ECC 2-2024)*. Kingdom of Saudi Arabia. Official document: <https://nca.gov.sa>
 28. National Cybersecurity Authority. (2024). *Guide to Operational Technology Cybersecurity Controls (OTCC) Implementation*. Kingdom of Saudi Arabia.Official document: <https://nca.gov.sa>
 29. National Institute of Standards and Technology. (2023). *Guide to Operational Technology (OT) Security (NIST SP 800-82 Rev.3)*.<https://doi.org/10.6028/NIST.SP.800-82r3>
 30. International Electrotechnical Commission. (2024). *IEC 62443-2-1:2024 Security for industrial automation and control systems – Security program requirements for IACS asset owners*.Official standard: <https://www.iec.ch>

Appendix A. Operational metric calculation notes

VRT begins at the first auditable incident-recognition timestamp and ends only when authorized reviewers approve verified trusted safe operation. The numbered trusted-state protocol is: (1) operations and identity/PAM owners validate privileged identities and revoke suspect access; (2) OT engineering verifies approved PLC/DCS/HMI logic, firmware and configuration integrity; (3) OT cybersecurity confirms that no known persistence remains; (4) network and OT engineering confirm approved communication paths and segmentation; (5) operations and process safety/HSE confirm that process variables remain inside the accepted safe envelope; and (6) control engineering and process safety/HSE validate critical control, interlock and safety functions. Site procedures must use synchronized clocks, record timezone, define an event-source hierarchy, document missing timestamps and excluded incidents, and identify

approval authority. Rate metrics use a fixed, version-controlled population and denominator. When the denominator is zero, the result is reported as not applicable rather than 0% or 100%. Approved exceptions must be documented before the measurement period; a confirmed/seeded change must have a retained test or incident record and defined monitoring window. Incident-recognition and trusted-state validation timestamps must be synchronized and auditable.

Appendix B. Reusable data-extraction and coding template

The following reusable fields operationalize the source → evidence type → asset → resilience phase → control → outcome traceability used in the synthesis. The template is intended for future update searches and independent quality checks; it does not reconstruct missing historical database exports.

Field	Required entry	Permitted coding / examples
Bibliographic identity	Author, year, title, venue, DOI/official URL	Publisher/DOI or issuing-body record
Source class	Nature of evidence	Empirical study; review; incident analysis; framework; government guidance; international standard
Asset focus	ICS component addressed	SCADA; PLC; DCS; HMI; SIS/ESD; cross-cutting OT
Threat/problem type	Primary security/resilience problem	Ransomware; malicious logic; protocol abuse; remote access; process manipulation; recovery

Field	Required entry	Permitted coding / examples
Resilience phase	Primary lifecycle function	Anticipate; withstand; detect/contain; recover; adapt; multi-phase
Control mechanism	Technical/organizational mechanism	Segmentation; identity; monitoring; change control; backup; response; recovery
Evidence type / validation basis	Basis of source claim	Experiment/testbed; survey; review; incident evidence; authoritative requirement; author synthesis
Outcome / metric	Reported or inferable outcome	Detection latency; continuity; recovery; VRT; BRSR; qualitative requirement
Saudi/NCA relevance	Directness of Saudi mapping	Direct NCA; indirect international guidance; no Saudi-specific mapping
Limitation	Constraint affecting interpretation	Simulation; dataset specificity; limited asset scope; no recovery validation; guidance not empirical
Verification status	Reference-integrity check	DOI/publisher verified; official issuing-body source verified
Discovery database/platform	Database or repository used	Scopus; Web of Science; IEEE Xplore; official repository
Search execution	Search date, exact query and fields	Date; Boolean string; title/abstract/keyword or full-text fields
Search result count	Unmodified result count at execution	Integer with saved export identifier
Selection decision	Inclusion/exclusion decision and reason	Included; duplicate; out of scope; unavailable full text; other coded reason

Appendix C. Revision-stage reproducible search protocol

The retained historical record does not contain the exact original execution date or raw exports. Accordingly, this appendix supplies a revision-stage protocol for the next update and does

not reconstruct unsupported historical counts. The review evidence remains intentionally frozen at 31 December 2025. Each future run must record the actual execution date, raw export, unmodified result count, deduplication record and exclusion reasons.

Platform	Revision-stage Boolean string	Fields	Language	Document types / filters	Execution record
Scopus	TITLE-ABS-KEY ("industrial control system*" OR "operational technology" OR SCADA OR PLC OR DCS OR HMI) AND ("cyber resilience" OR cybersecurity OR "incident response" OR recovery OR "process-aware" OR ransomware OR "anomaly detection")	Title, abstract, keywords	English	2020 onward; article, review, conference paper	Date/result count/export ID: record at run
Web of Science	TS=("industrial control system*" OR "operational technology" OR SCADA OR PLC OR DCS OR HMI) AND ("cyber resilience" OR cybersecurity OR "incident response" OR recovery OR "process-aware" OR ransomware OR "anomaly detection")	Topic	English	2020 onward; article, review, proceedings paper	Date/result count/export ID: record at run
IEEE Xplore	("industrial control system*" OR "operational technology" OR SCADA OR PLC OR DCS OR	All metadata	English	2020 onward; journals and conferences	Date/result count/export ID: record at run

Platform	Revision-stage Boolean string	Fields	Language	Document types / filters	Execution record
	HMI) AND ("cyber resilience" OR cybersecurity OR "incident response" OR recovery OR "process-aware" OR ransomware OR "anomaly detection")				
ScienceDirect	("industrial control system*" OR "operational technology" OR SCADA OR PLC OR DCS OR HMI) AND ("cyber resilience" OR cybersecurity OR "incident response" OR recovery OR "process-aware" OR ransomware OR "anomaly detection")	Title/abstract/keywords where supported	English	2020 onward; research and review articles	Date/result count/export ID: record at run
SpringerLink	("industrial control system*" OR "operational technology" OR SCADA OR PLC OR DCS OR HMI) AND ("cyber resilience" OR cybersecurity OR "incident response" OR recovery OR "process-aware" OR ransomware OR "anomaly detection")	Title/abstract/full text as supported	English	2020 onward; article and chapter results screened	Date/result count/export ID: record at run
NCA/NIST/IEC/CISA	OT OR ICS combined with controls, guidance, incident response, recovery and resilience	Official-site search/catalogue	English	Current authoritative documents; retain version/date	Date, URL/version and result path: record at run

Appendix D. Author-proposed control evidence and metric traceability

This crosswalk is an author-proposed operationalization, not an NCA-endorsed equivalence. Control identifiers and wording must be

verified against the controlled versions of OTCC-1:2022 and ECC 2-2024 used by the submitting organization. Evidence artifacts and metric targets require site-specific calibration.

Control objective	NCA source family	NIST / IEC guidance	Evidence artifact	Metric	Bidirectional audit test
Asset and dependency governance	OTCC asset/cyber-risk controls; ECC asset management	NIST SP 800-82r3; IEC 62443-2-1	Approved critical-asset and dependency register; versioned baseline	TCC	Sample metric numerator/denominator back to assets and each asset back to approval evidence
Segmentation and controlled conduits	OTCC network security/segregation; ECC protection	NIST OT architecture; IEC 62443 zones/conduits	Approved zone/conduit diagram; firewall review; blocked-path test	CFCR; PSAR	Trace each allowed flow to approval and each exception to owner, expiry and review

Control objective	NCA source family	NIST / IEC guidance	Evidence artifact	Metric	Bidirectional audit test
Privileged and remote access	OTCC access and third-party controls; ECC IAM	NIST SP 800-82r3; IEC 62443-2-1/-2-4	Named account; MFA feasibility decision; PAM/jump-host record; session log	PSAR; MCT	Reconcile all sessions to approvals, logs, exceptions and revocation evidence
Monitoring and change detection	OTCC monitoring/logging/incident controls; ECC detection	NIST SP 800-82r3; CISA CPGs	Passive sensor record; process correlation; version-control alert	UCDE; MCT	Trace every seeded/confirmed change to detection record and monitoring-window definition
Continuity, backup and trusted recovery	OTCC continuity/recovery controls; ECC continuity	NIST SP 800-82r3; IEC 62443 program guidance	Known-good package; restore log; signed trusted-state checklist	VRT; BRSR; SDSR	Trace each recovery result to evidence and each evidence item to an authorized requirement and acceptance owner