Proceedings of the 2025 SICE Festival with Annual Conference
September 9-12, 2025, Chiang Mai, Thailand

Preliminary Study on Incident Response in Production Control Systems

Kousei Sakata[1†] and Takayuki Arai[2]

[1]Security & Trust Research Dept., Hitachi Ltd. R&D Group, Yokohama, Japan
(E-mail: kosei.sakata.ky@hitachi.com)
[2]Marketing Headquarters External Affairs & Technology MK Center, Yokogawa Electric Corporation, Tokyo, Japan
(E-mail:Takayuki.Arai@yokogama.com)

Abstract: Digitalisation and increased connectivity have improved the productivity of industrial control systems (ICS) but have also broadened their cyber-attack surface. Existing guidelines such as NIST SP 800-61 and NISTIR 8428 presume the availability of expert-level CSIRTs, a requirement that can be difficult to satisfy for manufacturing sites facing staff and budget constraints. To bridge this gap, the SICE/JEITA/JEMIMA Joint Security Working Group (Joint Security WG) is developing lightweight incident-response documentation that complements the preventive J-CLICS toolset. The proposed concept emphasises operational continuity, clearly defined roles for plant operators and vendors, and procedures that can be executed by non-experts. A comparative analysis with current standards clarifies the unique requirements of production environments. Scenario-based validation and stakeholder feedback will guide further refinement.

Keywords: ICS Security, J-CLICS, Incident Responce

1. INTRODUCTION

The increasing integration of digital technology and networking in control systems has significantly enhanced operational efficiency and productivity[1][2]. However, this integration also exposes control systems to heightened cybersecurity risks, making the development and implementation of robust security measures essential citeICSsecurity. The SICE/JEITA/JEMIMA Joint Security Working Group (Joint Security WG), in which the authors participate, actively engages in research and outreach activities aimed at strengthening control system security.

Recognizing the necessity for practical tools, the Joint Security WG developed security self-assessment tools tailored specifically for control system users: “J-CLICS STEP1/STEP2” [3] (Fig. 1) and “J-CLICS Based on Attack Surface Analysis” [4][5]. Released in 2014, “J-CLICS STEP1/STEP2” primarily aims to prevent information security incidents by providing effective and easily implementable recommended practices for on-site application.

Fig. 1 J-CLICS STEP1/STEP2

† Kousei Sakata is the presenter of this paper.

Building upon this foundation, ”J-CLICS Based on Attack Surface Analysis,” published in 2023, focuses on halting external cyberattacks as early as possible by detailing recommended measures for four primary attack pathways anticipated in control systems. Both tools mainly emphasize preventive strategies, resulting in limited coverage of measures for preparing responses to incidents.

To address this gap, since 2024, the Joint Security WG has been developing practical and understandable measures designed to prepare control system users to effectively respond to information security incidents. This new initiative prioritizes broad applicability and ease of implementation in diverse operational environments.

This paper introduces the background, objectives, and progress of the Joint Security WG’s recent activities on incident response preparation in control systems, aiming to enhance overall cybersecurity resilience.

2. BACKGROUND AND OBJECTIVES

2.1. Objectives

To effectively address incident response in production control systems, we have established the following objectives:

- To develop documentation that outlines preparations, procedures, and relevant information for responding to incidents in production control systems.
- To aim to make sure the content and volume of the documentation are comprehensible and feasible for on-site personnel in production control environments.
- To contribute to the widespread adoption of recommended countermeasures by disseminating practical guidance.

2.2. Target Audience and Systems

The documentation produced through this study is intended to serve as a supplementary resource to the J-CLICS STEP1/STEP2 and the J-CLICS Based on Attack

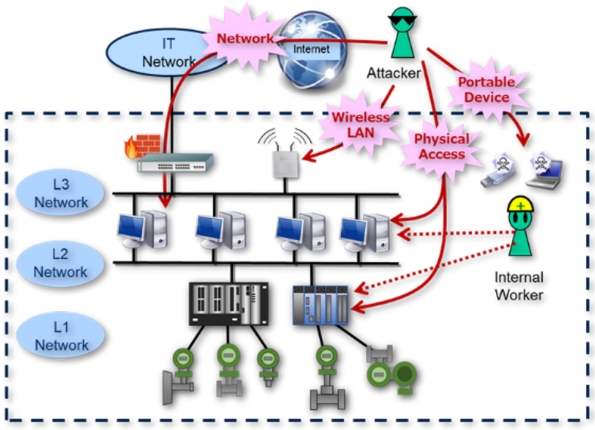

Fig. 2 ISA95 Purdue Model

Surface Analysis. Therefore, the target audience and systems are aligned with those assumed in the J-CLICS series.

- Target Audience: Personnel responsible for considering cybersecurity measures for control systems (e.g., users, system integrators, vendors)
- Target Systems: Control systems based on the three-layer ISA95 Purdue model (Fig. 2)

3. ISSUE IDENTIFICATION

To explore incident response for production control systems, we began by reviewing existing literature and evaluating its applicability from the perspective of ease of understanding and implementation in real-world control environments.

3.1. Literature Review

We conducted a comprehensive literature review to identify prior work on incident response for control systems. To ensure credibility, we limited our search to publications from public institutions and prioritized sources that are freely accessible online. Among the documents examined, we reviewed both **NIST SP 800-61** (IT-oriented) and **NISTIR 8428 (NIST DFIR: Digital Foensics and Incident Rsponce)** (OT-oriented) [6]. While SP 800-61 provides a valuable IT baseline, we selected **NISTIR 8428** [7] for detailed analysis because it specifies operational-technology requirements that more closely align with industrial control environments.

3.2. Key Challenges

Based on the literature review, we identified the following key challenges in applying existing guidelines to production control systems:

1. **Human Resource Constraints:** Existing literature assumes the presence of dedicated incident response teams with specialized expertise. However, in the manufacturing sector, aging workforce and personnel shortages are growing concerns, and such resources may not always be available. The documentation should therefore be understandable and actionable by staff without deep cybersecurity expertise.
2. **Scope of Responsibilities:** Many guidelines assume that the internal response team will handle a wide range of actions including detection, analysis, and digital forensics. In practice, control system vendors are often expected to manage technical investigations and system-specific responses. Thus, clear delineation of responsibilities between on-site staff and vendors should be emphasized.
3. **Operational Continuity:** Typical guidance recommends isolating potentially compromised systems, which may degrade system availability. However, in production control environments, availability is critical to maintaining operational safety and preventing significant damage to plants or the environment. Therefore, the documentation should prioritize strategies that enable continued operation where feasible.

4. APPROACH TO KEY CHALLENGES

We use table 1 to juxtapose our *Proposed Document* with NIST SP 800-61 and NISTIR 8248. Since our proposal remains at the conceptual stage, we organize the following discussion according to the same five row headers—*Target Audience, Primary Objective, Goal, Focus, Response*— and describe what we currently *envision* rather than what has already been implemented.

4.1. Target Audience

We envisage a dual readership consisting of **plant operators** and **vendor engineers**. This operator–vendor split mirrors day-to-day responsibility across Purdue Levels 0–3 and differs from SP 800-61 (government CSIRTs) and DFIR (OT/ICS incident-response teams).

4.2. Primary Objective

In addition to the Safety & Availability emphasis already explicit in NISTIR 8248, we explicitly add the notion of **downtime minimisation**. During Working-Group discussions, we agreed that line-stop penalties in discrete manufacturing make downtime a first-order metric that deserves its own wording.

4.3. Goal

Rather than building a full in-house DFIR unit, the goal is to provide a **lightweight operator–vendor workflow** that any plant can adopt without adding head-count. The idea is compatible with existing maintenance contracts and reflects human-resource constraints identified in Section 3.

4.4. Focus

We discuss to condense DFIR's six life-cycle phases into a continuity-centric chain:
Operator Triage → Vendor Escalation → Safety-conscious Recovery → Continuity Resume → Lessons Learned.

This chain retains the detection–analysis–recovery logic of SP 800-61 but re-orders tasks so that production

Table 1 Comparison of SP 800-61, NISTIR 8428, and the Proposed Concept

Item	NIST SP 800-61 Rev.2[6]	NISTIR 8428[7]	Proposed Concept
Target Audience	Federal civilian / agency CSIRTs	OT/ICS Incident Response Team	Plant operators & OEM vendors
Primary Objective	Protect Confidentiality, Integrity, Availability (CIA)	Ensure safety and availability of OT operations	Minimise downtime while safeguarding Safety & Availability
Goal	Establish and maintain an organizational incident-response capability	Develop organic OT DFIR capability and expedite safe restoration	Provide lightweight operator–vendor workflow enabling rapid, safe recovery
Focus	Preparation, Detection & Analysis, Containment, Eradication, Recovery, Post-Incident Activity	Routine, Identification, Technical Event Handling, Cyber Incident Analysis& Response, End-of-Incident /Post-Incident	Operator Triage, Vendor Escalation, Safety-conscious Recovery, Continuity, Resume, Lessons Learned
Response	Single CSIRT executes detection→ analysis → containment → recovery	Escalation path: SOC → FCR → IRT → Management	Operator triage → Vendor investigation → Safety-conscious recovery (degraded mode if required)

can continue in a degraded yet safe mode. We also debated incorporating *regulatory reporting and insurance claims* as auxiliary steps; these will be revisited in future drafts.

4.5. Response

At concept level, first-tier triage is performed by the operator, deep technical investigation by the vendor, and recovery proceeds under a **safety-first degraded mode** when a full shutdown would jeopardise availability. Criteria that trigger a switch between normal, degraded, and halted states are still under discussion and scheduled for scenario-based validation.

In summary, the Joint Security WG's draft framework extends NIST guidance with downtime-aware objectives and explicit operator–vendor role sharing while remaining lightweight enough for resource-constrained sites. Ongoing tabletop exercises will determine whether the concept can be promoted to a formal supplement to the J-CLICS toolset in a future release.

5. FUTURE WORK

We will validate the framework with case studies and tabletop exercises—such as an HMI ransomware scenario—to measure how clear operator-vendor role separation reduces downtime and preserves safety. Feedback from field engineers and workshops with vendors and asset owners will be incorporated to address remaining edge cases and polish the documentation for real-world deployment.

6. CONCLUSION

This study presented an initiative by the Joint Security Working Group to develop practical incident response documentation for ICS. By identifying limitations in existing guidelines (e.g., NIST SP800-61, NISTIR 8428), we proposed a context-aware framework suited to industrial environments, focusing on lightweight procedures, vendor coordination, and operational continuity.

Unlike conventional CSIRT-centric models, our approach reflects on-site constraints and is designed for practical adoption, even in resource-limited settings. Although still under review, future work includes scenario-based validation and stakeholder collaboration to enhance applicability and completeness.

This initiative contributes to advancing ICS cyber resilience with response strategies grounded in operational reality.

REFERENCES

[1] M. M. U. Aslam, A. Tufail, R. A. A. H. M. Apong, L. C. De Silva, and M. T. Raza, "Scrutinizing Security in Industrial Control Systems: An Architectural Vulnerabilities and Communication Network Perspective," *IEEE Access*, vol. 11, pp. 1–20, 2023.

[2] W. Knowles, D. Prince, D. Hutchison, J. F. P. Disso, and K. Jones, "A survey of cyber security management in industrial control systems," *International Journal of Critical Infrastructure Protection*, vol. 9, pp. 52–80, 2015.

[3] JPCERT/CC, "J-CLICS STEP1/STEP2: ICS Security Self-Assessment Tool," https://www.jpcert.or.jp/ics/jclics.html, (accessed May 7, 2025).

[4] JPCERT/CC, "J-CLICS Based on Attack Surface Analysis", https://www.jpcert.or.jp/ics/jclics-attack-path-countermeasures.html, (accessed May 7, 2025).

[5] H. Murakami, R. Nagasaku, H. Endo, and K. Sakata, "Cybersecurity in Industrial Control Systems," *Keisou (Instrumentation Control)*, vol. 66, no. 12, pp. 38–43, 2023.

[6] A. Nelson, S. Rekhi, M. Souppaya, and K. Scarfone, "Computer Security Incident Handling Guide," *NIST Special Publication (SP) 800-61 Revision 3*, National Institute of Standards and Technology, Gaithersburg, MD, 2024.

[7] E. Salfati and M. Pease, "Digital Forensics and Incident Response () Framework for Operational Technology (OT)," *NIST Interagency/Internal Report (NISTIR) 8428*, National Institute of Standards and Technology, Gaithersburg, MD, 2022.