Applied Human Factors and Ergonomics (AHFE2025), Vol. 199, 2025, 2334–2344
https://doi.org/10.54941/ahfe1007046

Empirical Study of Information Sharing and Decision-Making in IT/OT Incident Response

Kenta Nakayama[1,2], Ichiro Koshijima[2], and Kenji Watanabe[1]

[1]Nagoya Institute of Technology, Gokiso-cho, Showa, Nagoya, Japan
[2]Manufacturing and Innovation DX Laboratory, Nagoya Institute of Technology, Gokiso-cho, Showa, Nagoya, Japan

ABSTRACT

In recent years, cyberattacks have grown increasingly advanced and sophisticated, requiring organizations to build comprehensive defenses that extend beyond technical controls to include human factors. For critical infrastructure facing IT/OT convergence risks, the establishment of rapid and accurate information-sharing mechanisms is central to strengthening resilience. As part of a human-centered approach, this study designed and conducted a Tabletop Exercise (TTX) with 119 frontline and managerial participants from Japanese critical-infrastructure firms. Using communication logs recorded during the exercise, the analysis examined actual information flows and assessed how differences in security-education levels affect command structures and network dynamics. The results indicate that more advanced education promotes the formation of flexible network structures and can support faster, more autonomous judgment at the operational edge. These findings offer actionable guidance for improving TTX design, concretizing information-sharing protocols, and standardizing incident-response procedures, thereby contributing to enhanced organizational security preparedness and resilience.

Keywords: Cyber security, Tabletop exercise (TTX), Operational technology (OT), Critical infrastructure (CI), Human factor, Communication network analysis (CNA)

INTRODUCTION

In recent years, cyberattacks targeting Operational Technology (OT) environments have become a growing concern, as they directly threaten physical infrastructure and industrial operations. High-profile incidents such as the 2015 Ukraine blackout (CISA, 2021) and the 2019 production halt at Norsk Hydro in Norway have demonstrated that cyber threats have expanded beyond IT systems to impact essential services and manufacturing (Hydro, 2024). Japan has also experienced significant OT-related cybersecurity incidents. In 2021, a ransomware attack on a regional hospital disabled its electronic medical record system for nearly two months, severely affecting healthcare delivery (Handa, 2022). In 2022, a cyberattack targeting a major port system disrupted logistics nationwide, underscoring the vulnerability of critical infrastructure (Meikokyo, 2023).

© 2025. Published by AHFE Open Access. All rights reserved.

These cases illustrate a shift toward a persistent threat landscape in which any organization may become a target, regardless of sector or scale. The convergence of IT and OT systems further complicates cybersecurity strategies, as it requires coordinated responses that consider the distinct priorities of each domain, such as confidentiality for IT versus availability and safety for OT.

To address these challenges, enhancing organizational resilience is essential. This involves not only implementing technical safeguards but also fostering the capacity for rapid information sharing, cross-functional decision-making, and seamless coordination between frontline operations and executive leadership in times of crisis.

RESEARCH GAP AND CONTRIBUTION

Although diverse Tabletop Exercise (TTX) designs have been empirically demonstrated across various domains, the methodology for evaluating their effectiveness remains underdeveloped. This deficiency stems from three critical gaps in antecedent literature, which this study directly addresses.

Firstly, a significant lack of objectivity persists in TTX evaluation. While TTX is effective in cultivating higher-order cognitive skills, such as judgment and information integration (Kolb, 1984), assessments largely depend on self-reporting and subjective judgments, resulting in a critical deficiency in standardized metrics (Skryabina, 2017). The potential for cognitive biases like the Dunning-Kruger effect (Kruger, 1999) further necessitates a shift toward objective evaluation. Objectively assessing decision-making processes, which depend on rapid and accurate information sharing, is paramount.

Secondly, the literature contains a substantial empirical gap regarding TTXs explicitly simulating IT/OT environments in critical infrastructure. In these settings, a fundamental divergence in security priorities exists: IT emphasizes Confidentiality, while OT prioritizes Availability and Safety. Cultivating hybrid personnel capable of knowledge bridging between these two cultures is essential (Haddouch, 2024). However, within the scope of this review, there are no studies that analytically examine the communication structures through which such personnel exercise their capabilities during incidents.

Thirdly, there is a lack of analysis regarding the dynamic shift in communication structures during cybersecurity incidents. While evidence from the disaster domain indicates that organizational communication dynamically shifts from centralized to distributed forms as incidents unfold (Brown, 2021), this insight has not been applied empirically to the IT/OT context. Understanding how communication structures emerge and evolve constitutes a key research agenda for informing optimal deployment strategies for hybrid personnel.

Against this backdrop, this study employs Communication Network Analysis (CNA) to achieve objective evaluation and structural understanding, thereby filling these three crucial gaps.

RESEARCH QUESTION AND OBJECTIVES

This study reconstructs interactions among participants in TTX as communication networks and applies CAN based on "who communicated what to whom" to achieve objective evaluation and structural understanding. Building on prior literature that highlights (1) a lack of objectivity due to overreliance on subjective feedback and (2) limited empirical investigation of incident-time communication structures in IT/OT environments, the following research questions (RQs) are posed.

RQ1 (Objectivity of Evaluation): Can CNA metrics identify statistically significant structural differences between groups, such as those defined by prior education level or professional function (IT/OT)?

RQ2 (Temporal Dynamics): As phases shift from security-priority to safety-priority, how are network centralization, the affiliation of major hubs, and the centrality of field nodes reconfigured?

RQ3 (Link to Outcomes): To what extent do CNA metrics serve as predictors of response speed (escalation/decision latency) and accuracy (error rate and prioritization consistency)?

By addressing these research questions, the study advances a data-driven approach to TTX evaluation and offers practical and strategic implications for the development, deployment, and coordination design of hybrid personnel in complex IT/OT settings, while also advancing an objective, structure-oriented framework for TTX assessment in the academic domain.

RESEARCH METHOD

This study uses TTX and CNA for solving research questions. The TTX employed in this study is based on a virtual company with an IT/OT environment whose educational effectiveness has been demonstrated in the same author's prior work (Nakayama, 2024). The node set used for CNA is identical to that in the prior study; only the role labels are listed in Table 1.

Table 1: Nodes (characters and their roles in the virtual company).

Location	Nodes (Role Name)	Location	Nodes (Role Name)
Head office	Management	Plant1	Plant Manager
	Sales Div.		Operation Sec.
	CSIRT		Equipment Sec.
	Back Office Div.		Safety Sec.
	IT Div.		IT Sec.
	Manufacturing Div.	Others	Others

Behavioral data for analysis are drawn from the chronology records. Particular attention is given to three phases in which a security incident unfolds and tangible impacts arise in the OT environment; behavioral outcomes are analyzed within and across these phases. The focal scenarios and the relative priorities of Security and Safety in each phase are summarized in Table 2.

Table 2: Incident response exercise scenario focused on this study.

Scenario	Priority	Events
1	**Security**	Threats are found on office terminals in Back Office Div.
2	**Security/Safety**	Threats are found on SCADA terminals in Plant 1
3	**Safety**	SCADA terminal will no longer be able to control the plant

To elucidate decision-making processes during IT/OT incidents, this study additionally defines the expected actions for the present scenario (Table 3). Using the chronology, the analysis identifies who executed each predefined expected action and compares decision-making processes across groups with differing levels of prior education (knowledge). These observations are then discussed alongside CNA results, with reference to response speed and content accuracy as reflected in the recorded actions.

Table 3: Expected actions in the decision-making process.

No.	Action	Reason
1	**Isolation of Inter-site Networks**	Containment measures based on the potential or confirmed spread of infection
2	**Manual Degradation or Shutdown of Plant Operations**	A safety-priority response in the event of potential or actual impact from a security incident on plant operation

The participants for this exercise will be drawn from the trainees of the IPA Industrial Cybersecurity Center's "Core Human Resource Development Program" (IPA, 2023). Eligibility for this program requires either an IT Passport certification or at least one year of professional experience in IT or OT domains. Furthermore, the trainees are composed of personnel seconded from Critical Infrastructure companies, such as electric power and railway operators, as well as manufacturers.

In addition, the initial two months of the ICSCoE program include lectures to provide a fundamental foundation in IT/OT knowledge. This study was conducted within the ICSCoE program. To enable more granular analysis, participants were grouped according to the education they had completed before the TTX (shown in Table 4), and these differences in prior education (knowledge) were subsequently used to inform the interpretation of results.

Table 4: TTX participants.

Group	Attendance	Remarks
1	38	7 teams that have fundamental IT/OT knowledge
2	41	9 teams that have fundamental IT/OT knowledge and IT security education
3	40	9 teams that have fundamental IT/OT knowledge and IT/OT security education
Total	119	-

Please note that due to ICSCoE curriculum, it's not possible to adjust the participants who have completed the "Fundamental IT/OT Knowledge" and "OT Security Education" modules.

RESULTS AND DISCUSSION

In this analysis, three groups with differing levels of security education were examined to assess how decision-making routes and information-sharing structures change when a security incident occurs.

Scenario 1: Security-Priority Phase

In the scenario that prioritized security, clear differences attributable to education were observed in the speed of the initial response and the ability to escalate to the appropriate decision makers. The communication network in this scenario is shown in Figure 1.

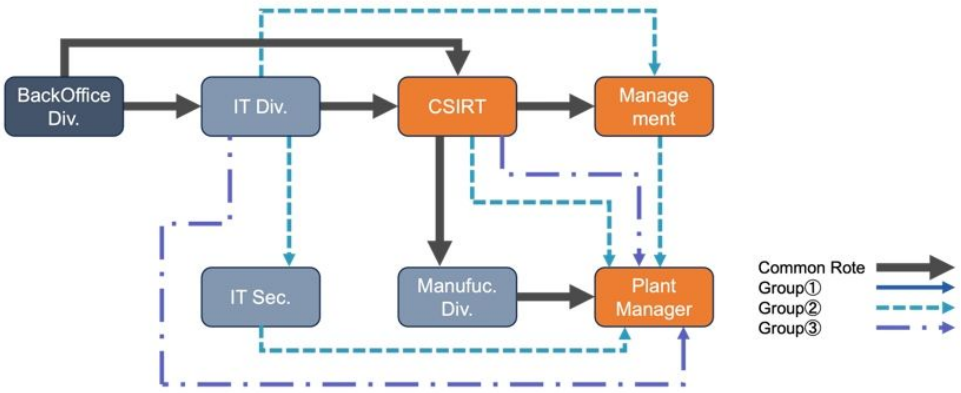

Figure 1: Scenario 1 (security-priority)'s communication network.

Group 1 generally adhered to templated reporting routes and tended to rely on a hierarchical network. This behavior suggests insufficient consideration of the incident's potential enterprise-wide impact.

Group 2 established a systematic flow in which the corporate IT department contacted the plant IT section, which then notified the plant manager. This pattern indicates recognition of propagation risk and an

attempt to involve corporate functions. However, because the path traversed intermediate units, responsiveness with respect to OT impacts remained limited.

Group 3 exhibited "skip communication," whereby the corporate IT department contacted the plant manager directly. This action indicates that IT/OT education had fostered an integrated assessment of technical effects and managerial risk, enabling immediate escalation by shortening the OODA loop. Accordingly, Group 3 appeared to possess an advantage in strategic judgment that takes an enterprise-wide risk perspective.

Scenario 2: Security/Safety-Priority Complexed Phase

In this scenario, where security and safety considerations intersected, all groups shared information with the plant manager, CSIRT, and executive leadership. However, differences emerged in sensemaking, specifically recognizing the event as a security incident and routing it to the appropriate point of contact. The communication network in this scenario is shown in Figure 2.

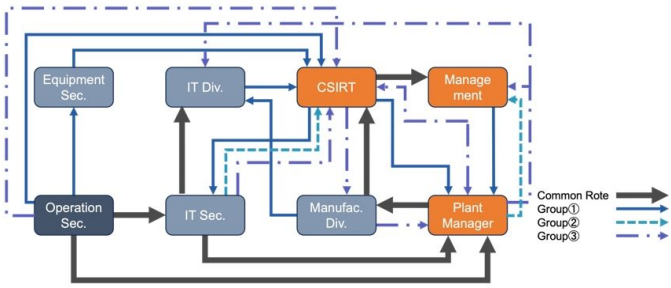

Figure 2: Scenario 2 (security/safety priority complexed)'s communication network.

Group 1 issued an initial report to CSIRT but also contacted the instrumentation section. This pattern suggests incomplete cognitive linkage of the event to a security problem, resulting in ambiguity in the choice of recipients.

Group 2 coordinated efficiently from the on-site IT section to CSIRT and correctly identified the event as a security risk. The behavior implies that IT security education improved the precision of information classification and prioritization.

Group 3 linked the event to a security incident immediately after its occurrence and contacted CSIRT, while the plant manager formed a dynamic command structure to coordinate multiple departments. As a result, the end-to-end process from initial response to information sharing was streamlined, indicating that education enhanced the autonomy of field-level judgment.

Scenario 3: Safety-Priority Phase

In this scenario, where safeguarding production equipment is paramount, clear education-related differences were observed in vertical and horizontal information-sharing structures and in field-level autonomy.

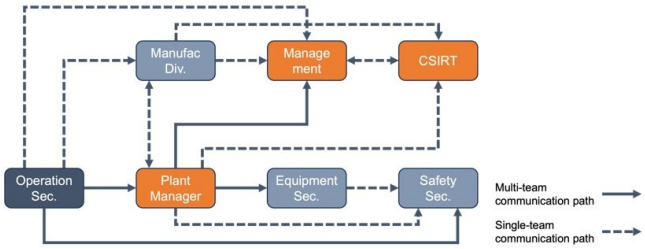

Figure 3: Scenario 3 (safety-priority) Group 1.

Group 1 (shown in Figure 3) maintains a vertical flow from the plant manager to executive leadership, but shows weak linkage with CSIRT, indicating limited attention to latent security risks. Group 1 also exhibits occasional horizontal communication on the corporate side, suggesting uncertainty about appropriate coordination partners and potential inefficiencies in information sharing.

Group 2 (shown in Figure 4) forms an efficient command structure centered on the plant manager and demonstrates economical communications. However, Group 2 continues horizontal dissemination within corporate units, reflecting ongoing reliance on the corporate IT department and deference to its judgment from an IT-security perspective, which indicates an incomplete shift away from headquarters-dependent leadership under safety-priority conditions.

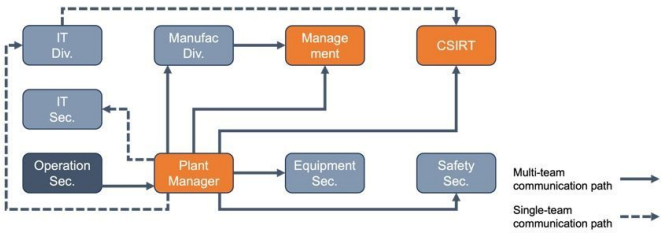

Figure 4: Scenario 3 (safety-priority) Group 2.

Group 3 (shown in Figure 5) centers information dissemination on the plant manager while also activating coordination among frontline personnel. Group 3 routes information to the corporate side directly from field operators and limits corporate-side horizontal dissemination compared with Groups 1 and 2, implying that corporate units primarily receive reports or are contacted selectively as decision makers. This pattern suggests that IT/OT security education has strengthened autonomous field judgment and fostered a decentralized, self-directed information-sharing structure that avoids unnecessary headquarters-centric consultation.

The results of the CNA indicate that more advanced education and knowledge are associated with qualitative and quantitative shifts in intra-organizational communication structures. In Group 1, reporting relied on fixed, vertical hierarchical pathways, revealing a centralized tendency in which information accumulated at upper layers. In Group 2, a systematic network emerged with the corporate IT department as a hub,

reflecting coordination attentive to enterprise-wide risk; however, decision concentration and response latency persisted. By contrast, Group 3 built an autonomous, decentralized network in which frontline personnel and the plant manager coordinated bidirectionally and, when necessary, contacted corporate decision makers directly. This configuration coincided with shorter information paths and the emergence of spontaneous field leadership.

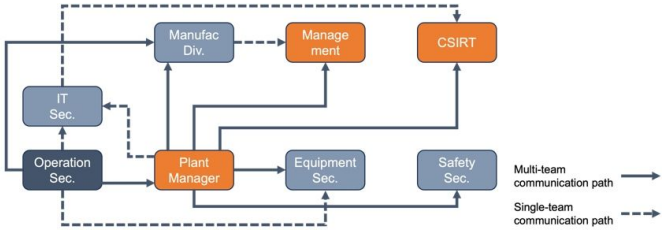

Figure 5: Scenario 3 (safety-priority) Group 3.

On the quantitative side, an increase in node-to-node connectivity density was observed; on the qualitative side, a more flexible decision-making process adapted to situational shifts was identified. Taken together, these findings show, both quantitatively and qualitatively via CNA, that education can shift an organization's information architecture from centralized control to distributed collaboration, thereby enhancing command flexibility and frontline resilience.

Complements the CNA-derived differences in decision-making structures by analyzing, for each scenario, whether the expected actions were executed and who served as the decision-making principal.

Network isolation was executed by roughly half of the teams across all groups, and in every group, the CSIRT emerged as the largest decision-making principal (Group 1: 28.6%, Group 2: 44.4%, Group 3: 33.3%), as shown in Table 5.

Table 5: Isolation of the inter-site networks decision-maker and phase.

	S1	S2	S3				Total
	C	C	M	C	PM	Others	
Group 1	14.3%	14.3%	14.3%	-	-	-	42.9%
Group 2	-	33.3%	-	11.1%	-	22.2%	66.7%
Group 3	11.1%	11.1%	-	11.1%	11.1%	11.1%	55.6%

M: Management, C: CSIRT, PM: Plant Manager, O: Others

This result aligns with the high betweenness centrality of the CSIRT node observed in CNA during the early scenario stages, reflecting that network isolation is a containment action requiring enterprise-level authority and technical expertise. In other words, regardless of education level, CSIRT consistently functioned as the technical decision hub in the initial response.

Regarding manual plant derating or shutdown, all Group 2 and 3 teams executed the decision. Notably, a subset of Group 3 teams made the

manual operation decision during the initial security-priority phase (shown in Table 6). This suggests that the teams evaluated managerial risks to the OT environment and business continuity early on, resulting in a safety-priority stance. This early decision aligns with CNA observations of field-led response and skip communication, showing that network flexibility led to faster, concrete actions.

Table 6: Manual degradation or shutdown of the plant operations decision-maker and phase.

	S1	S2			S3			Total
	PM	C	PM	Others	M	PM	Others	
Group 1	-	-	14.3%	-	28.6%	28.6%	14.3%	85.7%
Group 2	-	-	22.2%	11.1%	22.2%	44.4%	-	100%
Group 3	11.1%	11.1%	11.1%	-	11.1%	44.4%	11.1%	100%

M: Management, C: CSIRT, PM: Plant Manager, O: Others

The current analysis focused only on coarse-grained indicators (action execution and principal identification) to reinforce structural insights from CNA. It does not yet quantitatively test the causal link between structural flexibility and decision quality or latency. Future work will require more detailed analysis, including examining decision nodes based on educational differences, explaining decision divergence, and qualitatively analyzing communication content.

RESEARCH QUESTION (RQ) RESPONSES

The present study addressed the empirical and structural gaps in antecedent literature regarding cybersecurity training by conducting a comprehensive analysis of IT/OT integrated TTX using CNA. By quantifying the communication structures that emerged during simulated incidents, we aimed to overcome the prevailing issue of subjective evaluation and gain structural insights into cross-functional decision-making. Based on the results of the CNA applied across different educational groups and temporal phases, the following conclusions can be drawn for the posed Research Questions.

RQ1 (Objectivity of Evaluation)

Consistent differences were observed in communication structures based on the level of prior education. Notably, Group 3 (Advanced Education) exhibited a relatively higher frequency of Skip Communication (defined as direct contact bypassing middle management), resulting in a communication structure characterized by a reduced number of nodes and edges, and shorter primary communication paths. Group 2 (IT Security Education), in contrast, formed hierarchical paths following organizational order (e.g., Headquarters IT → IT Section → Plant Manager) during Scenario 1 (Security Priority), leading to high Betweenness Centrality for Headquarters IT-related nodes. Meanwhile, Group 1 (Basic Education) showed mixed patterns, including inaccurate recipient selection and redundant pathways. These findings support the utility of CNA as an objective metric for TTX evaluation.

RQ2 (Temporal Dynamics)

Tracking the phase transition revealed a repeated structural reconfiguration: during the Security Priority phase, CSIRT's Betweenness Centrality and the overall network centralization degree were high. However, during the Safety Priority phase, centralization decreased, and the Plant Manager became the primary point of communication. Group 2 effectively positioned the incident as security-driven, forming a less redundant hierarchical route during the initial response. Group 3 demonstrated the ability to rapidly assess both IT/OT impacts, swiftly establishing a field-centric, decentralized structure. These findings are consistent with the structural reorganization expected when the priority shifts from security to safety in an IT/OT environment.

RQ3 (Link to Outcomes)

Response: The high frequency of Skip Communication observed in Group 3, along with the less redundant hierarchical routes in Group 2, structurally suggests a potential for faster escalation and greater consistency in decision-making. However, we do not make causal claims. Since this study's scope was limited to the structural measurement of communication networks, we did not directly measure the actual response time or the accuracy of communication content. The quantitative verification of the correlation between these CNA metrics and outcome variables (response speed and accuracy) is, therefore, reserved for future research.

CONCLUSION

To overcome the inherent subjectivity in TTX assessment, this study leveraged CNA to extract objective, structural metrics from simulated IT/OT incidents. The analysis confirmed that higher education directly correlates with a more decentralized and adaptive communication structure. Key findings, such as Skip Communication and the formation of field-centric pathways in Group 3, prove the utility of these metrics in quantifying command flexibility and frontline autonomy. These structural changes indicate personnel capable of swiftly assessing converged IT/OT risks and making self-directed decisions.

Consequently, this research validates CNA as a vital methodology for future TTX evaluation, providing a strategic roadmap for designing effective coordination protocols and optimizing hybrid personnel placement. Moving forward, the critical next step is the quantitative verification of the correlation between these measured CNA structural metrics (e.g., centrality, destinations) and performance outcomes, specifically decision latency and error rates.

ACKNOWLEDGMENT

This work has been partially supported by Information-Technology Promotion Agency (IPA), Japan, however all remaining errors belong to the authors.

REFERENCES

Brown, O. et al. (2021). Communication and coordination across event phases: A multiteam system emergency response. J. Occup. Organ. Psychol. 94, 591–615. doi.org/10.1111/joop.12349.

CISA. (July 20, 2021) Cyber-Attack Against Ukrainian Critical Infrastructure. https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16–056-01.

Haddouch, R. et al. (2024). Strengthening Incident Response: Lessons from Cybersecurity Tabletop Exercises for Rural Critical Infrastructure. 2024 Proceedings of the ISCAP Conference, 10 (6201), Baltimore, MD. ISSN 2473–4901.

Handa Hospital. (June 7, 2022). Expert Panel Report on the Computer Virus Incident. https://www.handa-hospital.jp/topics/2022/0616/index.html.

Hydro. (May 14, 2024). Cyber-attack on Hydro. https://www.hydro.com/en/global/media/on-the-agenda/cyber-attack/.

IPA, Japan. (Oct 11, 2023). Human Resource Development Program. https://www.ipa.go.jp/en/it-talents/ics/humandev.html.

Kolb, D. A. (1984). Experiential learning : Experience as the source of learning and development. Prentice-Hall.

Kruger, J. & Dunning, D. (1999). Unskilled and unaware of it: How difficulties in recognizing one's own incompetence lead to inflated self-assessments. Journal of Personality and Social Psychology, 77(6), 1121–1134. doi.org/10.1037/0022–3514.77.6.1121.

Meikokyo. (July 26, 2023). MUTS system failure report. https://meikoukyo.com/wp-content/uploads/2023/07/0bb9d9907568e832da8f400e529efc99.pdf.

Nakayama, K. (2024). Analyzing important factors in cybersecurity incidents using table-top exercise, AHFE (2024) International Conference, vol 127, Jul. 2024, doi.org/10.54941/ahfe1004770.

Skryabina, E. et al. (2017). What is the value of health emergency preparedness exercises? A scoping review study, International Journal of Disaster Risk Reduction, Volume 21, 2017, Pages 274–283, ISSN2212–4209. doi.org/10.1016/j.ijdrr.2016.12.010.