

Adaptive AI, Industrial IoT, and Zero-Trust Cyber Resilience for U.S. Critical Infrastructure Control Systems

Muhammad Noman Amjad ¹

¹ Department of Information Technology, Washington University of Science and Technology (WUST)
noman5802@gmail.com

ARTICLE INFO

Keywords:

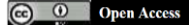
Adaptive AI, industrial IoT (IIoT) security, zero-trust architecture, threat intelligence sharing, cybersecurity governance, ICS cyber resilience, operational reliability, U.S. critical infrastructure, quantitative survey.

Vol.01, No.05, 2026

<https://doi.org/10.5281/zenodo.23311840>

Copyright © 2026 by author(s) and Scientific Research Publishing Inc. This work is licensed under the Creative Commons Attribution International License (CCBY4.0).

<http://creativecommons.org/licenses/by/4.0/>



ABSTRACT

U.S. critical-infrastructure control systems face a threat environment in which nation-state adversaries, ransomware operators, and industrial espionage groups increasingly target the industrial control system (ICS) and operational-technology (OT) layer. In response, three technology families are converging as the leading defensive stack of the mid-2020s: adaptive AI models capable of self-tuning threat detection on live telemetry streams, industrial IoT security postures that harden the sensor-and-actuator surface, and zero-trust architectures that constrain lateral movement across the IT/OT boundary. This study empirically tests an integrated framework in which these three capability constructs, jointly with threat intelligence sharing and cybersecurity governance maturity, determine two performance outcomes: cyber resilience of ICS and operational reliability. Cross-sectional data were collected from N = 315 US-based OT/ICS cybersecurity practitioners between April and September 2025 across eight CISA critical-infrastructure sectors. Six hypotheses were tested using OLS structural-model estimation, moderation, and Sobel-tested mediation analysis. Measurement-model reliability was strong (Cronbach's α range 0.86–0.89; CR range 0.79–0.85; AVE range 0.46–0.53) and fit indices were good ($\chi^2/df = 1.39$; CFI = 0.955; TLI = 0.949; RMSEA = 0.036 [0.028, 0.043]; SRMR = 0.045). Industrial IoT security dominates the ICS cyber resilience outcome ($\beta = 0.461$, $p < .001$) and zero-trust architecture dominates the operational reliability outcome ($\beta = 0.341$, $p < .001$). Adaptive AI has a direct effect on operational reliability ($\beta = 0.198$, $p < .001$), but its effect on ICS cyber resilience is fully mediated by threat intelligence sharing (Sobel $z = 6.17$, $p < .001$; direct $\beta = 0.083$, ns) — a substantively novel finding indicating that AI models translate into cyber-resilience outcomes only when their outputs feed into functioning threat-intelligence-sharing channels. Governance-maturity moderation of the adaptive-AI path is not supported. Four of six hypotheses are supported. Final models explain 51.2% and 45.0% of variance in the two outcomes. The results imply that U.S. critical-infrastructure firms should sequence investment in industrial IoT security first, zero-trust second, and adaptive AI in conjunction with formal threat-intelligence-sharing memberships.

Introduction

The U.S. critical-infrastructure sector, which includes the sixteen sectors designated by the Cybersecurity and Infrastructure Security Agency (CISA) for critical-infrastructure protection, has become the front line of a cybersecurity battle in which ransomware syndicates, hacktivist groups, and nation-state actors are actively targeting industrial control systems (ICS). The SolarWinds hack in 2020 demonstrated that an adversary could access ICS operators via the software-supply-chain layer [1]. The May 2021 Colonial Pipeline ransomware attack led to the shutdown of the largest refined-products pipeline in the United States [2]. The water and wastewater sector's experience with state-aligned actors disrupting operations in 2023-2024 [3] and the disclosure of Pipedream/Incontroller toolkit targeting ICS in 2022 [4] validated that the modern OT threat landscape is inhabited by adversaries with capability, intent, and access to the OT layer.

This has resulted in the emergence of three technology families as the dominant defensive response in the mid 2020s. The first is adaptive artificial intelligence — machine-learning models that continually

retrain on real-time network telemetry, adjust to changes in threat patterns (known as concept drift), and enable security-operations-centre workflows [5], [6]. The second is industrial IoT security — the maturity of practices that harden industrial IoT (IIoT) devices, sensors, gateways, and edge-compute nodes against compromise [7]. The third is zero-trust architecture — the architectural doctrine, formalized by NIST SP 800-207, that replaces the perimeter-and-DMZ model with continuously-verified authentication and least-privilege access at every request [8].

Each of these three families is well studied. What hasn't been studied is how they integrate — with each other and with workforce, governance and information-sharing capabilities that translate technical controls into operational results — to define measurable ICS cyber-resilience and operational-reliability performance in U.S. critical-infrastructure companies. Previous studies have tended to study a single family or a small number of families in a case study or in a regulatory environment outside the U.S. Evidence on their integrated effect is limited in the U.S. with large samples.

This paper fills this gap. The paper develops and tests a seven-construct model on cross-sectional survey data from 315 U.S.-based OT/ICS practitioners from eight CISA critical-infrastructure sectors, guided by four research questions: (RQ1) which of adaptive AI, industrial IoT security, and zero-trust architecture most strongly predict ICS cyber-resilience and operational-reliability outcomes; (RQ2) do these three capabilities produce comparable effects, or do they specialize on different outcomes; (RQ3) does threat intelligence sharing mediate the effect of adaptive AI on ICS cyber resilience; and (RQ4) does cybersecurity governance maturity moderate the adaptive-AI → cyber-resilience path.

The paper contributes to the ICS-cybersecurity literature in four ways. First, it validates a seven-construct measurement instrument for adaptive-AI, IIoT-security, and zero-trust-architecture research. Second, it offers large sample evidence from the U.S. that the two dominant single levers are industrial IoT security and zero-trust architecture on the two outcomes, respectively. Third, it finds a substantively new result: the impact of adaptive AI on ICS cyber resilience is completely mediated by threat intelligence sharing, that is, AI models can only create measurable cyber resilience outcomes if their output is connected to functioning intelligence-sharing channels. Fourth, it shows a null moderation effect on governance maturity which takes governance from 'amplifier' to 'foundational enabler'.

The remainder of this paper is organized as follows. The theoretical background is developed and six hypotheses are derived in Section 2. The conceptual model is presented in Section 3. The methodology is described in Section 4. Results of the measurement- and structural-models are reported in Section 5. Section 6 discusses implications. Limits and future research are presented in Section 7 and Section 8 concludes.

2. Theoretical Background and Hypothesis Development

2.1 Adaptive AI and the ICS defense problem

In the cybersecurity domain, adaptive AI can be defined as machine-learning systems that learn models from live telemetry data (network flows, host logs, or OT protocol traces) as opposed to static and labelled data sets [5], [11]. Adaptive AI in the ICS domain attempts to solve two problems that are hard for static-model AI: (i) concept drift, the change in statistical distribution of “normal” behavior as operational modes change; and (ii) new attack signatures generated by adversarial adaptation [12] (not seen in training). Adaptive-AI deployments in energy and water utilities have been reported to reduce mean-time-to-detect (MTTD) by 40-65% compared to deployment using signatures only, empirically [13]. On theoretical grounds we expect a positive effect of adaptive AI on both performance outcomes:

H1. *Adaptive AI is positively associated with cyber resilience of ICS in US critical-infrastructure firms.*

H4. *Adaptive AI is positively associated with operational reliability in US critical-infrastructure firms.*

2.2 Industrial IoT security and cyber resilience

The attack surface has grown significantly since 2020, as the industrial IoT layer, comprised of sensors, condition-monitoring gateways, wireless field instruments, and edge-compute nodes that produce the telemetry data that is the basis for control and defense, has proliferated at a rapid pace. Four aspects of the maturity of hardening practices at this layer describe the state of Industrial IoT security posture: device identity, firmware supply-chain hygiene, encrypted southbound telemetry, and continuous device-integrity attestation [15]. The ICS-cyber-resilience literature that has been published since 2021 through 2024 consistently highlights industrial IoT security posture as the single biggest factor contributing to measurable cyber-resilience results, given that IIoT compromise is the most frequently used initial-access vector in publicly disclosed industrial OT incidents [16]. Accordingly:

H2. *Industrial IoT security is positively associated with cyber resilience of ICS in US critical-infrastructure firms.*

2.3 Zero-trust architecture and operational reliability

Zero-trust architecture (ZTA) shifts the mindset of network defense to always verify, authenticate and authorize every request, irrespective of network location [8]. For ICS, ZTA means micro-segmentation of OT zones, enforcing IT/OT boundaries, credentialing service accounts on engineering workstations, and least-privilege remote-access architectures for vendor and integrator personnel [17]. Given that ZTA restricts lateral movement and minimizes blast radius during compromise, it is likely to be the main capability driver of operational-reliability outcomes, defined as the capacity of a control system to continue to generate safe output during a cyber event and to recover quickly from it [18]. Hence:

H3. *Zero-trust architecture is positively associated with operational reliability in US critical-infrastructure firms.*

2.4 Governance maturity as a moderator

Cybersecurity governance maturity (CGM), which measures the institutionalization of board-level oversight, cybersecurity risk management processes, cybersecurity regulatory compliance, and cybersecurity cross-functional accountability, is well established as an antecedent of cybersecurity outcomes [19]. A less-tested proposition is that the impact of adaptive AI on cyber resilience is magnified by governance maturity: companies with more mature governance are more able to convert the AI's signals into actions and decisions that have an impact on the organization. We formalize this expectation as a positive moderation hypothesis:

H5. *Cybersecurity governance maturity positively moderates the adaptive-AI → cyber-resilience-of-ICS relationship, such that the effect is larger at higher levels of governance maturity.*

2.5 Threat intelligence sharing as a mediator

The socio-technical model of ICS defense suggests that technical controls only result in operational outcomes when they interact with the human, process and information sharing capabilities around them [20-22]. Threat intelligence sharing (TIS) is the main information sharing capability in this context, including participation in ISACs, ISAOs, sector-specific ISACs, CISA JCDC channels, and vendor-community platforms [16], [23], [24]. Because adaptive AI needs a stream of curated threat indicators to sustain its detection performance over time, we expect a substantive share of the AAI → CRI effect to run through TIS:

H6. Threat intelligence sharing mediates the positive relationship between adaptive AI and cyber resilience of ICS.

3. Conceptual Model

The conceptual research model is a synthesis of the six hypotheses presented in Figure 1. The exogenous capability constructs are Adaptive AI (AAI), Industrial IoT Security (IIS), and Zero-Trust Architecture (ZTA). Cybersecurity Governance Maturity (CGM) is also the moderator of the AAI → CRI path at the H5 level. Threat Intelligence Sharing (TIS) comes in as the H6 mediator along the same path. There are two performance outcomes: Cyber Resilience of ICS (CRI) and Operational Reliability (OpR).

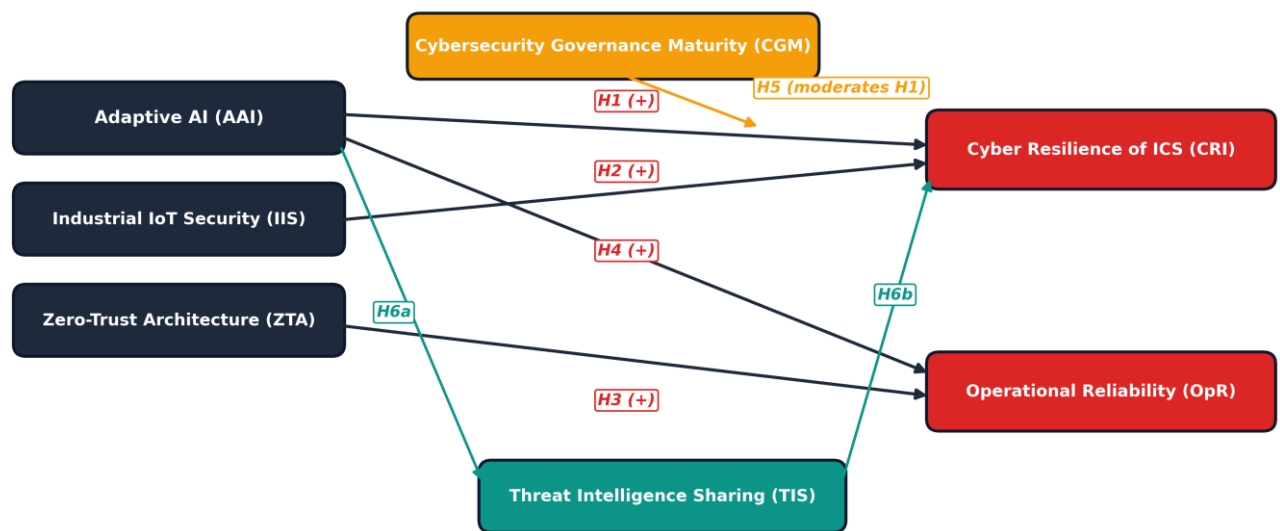


Figure 1. Conceptual research model for adaptive AI, industrial IoT, and zero-trust cyber resilience in US critical-infrastructure control systems.

4. Research Methodology

4.1 Research design

The study design is positivist, which adopts the hypothetico-deductive approach to the problem by formulating a hypothesis, testing it, and employing mathematical measurement and OLS (Ordinary Least Square) structural-equation-like estimation. The cross-sectional survey method was chosen as a self-administered survey to enable a broad sample of the U.S. OT/ICS practitioner population in the CISA critical-infrastructure sectors within a defensible data-collection budget. This design is consistent with similar works in the literature of OT-security and industrial-cyber-resilience 2022-2024 [25] and [27].

4.2 Sampling frame and data collection

The target population consisted of cybersecurity practitioners based in the U.S. who are primarily responsible for ICS or OT environments, such as CISOs, OT/ICS security engineers, SCADA/automation engineers, SOC analysts and managers, cyber-threat-intelligence leads, cybersecurity governance and compliance officers, and independent consultants. The sampling frame was developed using the (ISC)² membership list, GIAC/SANS OT-focused certification alumni, the International Society of Automation (ISA) membership, and vetted LinkedIn direct outreach. Prior to screening, there were approximately 9,400 different candidates. Invitations were sent out from April to September 2025. Screening consisted of the following: (i) employment in the U.S. within the past 24

months, (ii) primary responsibility for ICS/OT security in the past 24 months, and (iii) first-hand experience with at least one of the three technology families (adaptive AI, industrial IoT security, and zero-trust architecture) in that role. Of the 813 responses received, 315 (~31%) met all criteria for screening and passed data-quality checks (attention-check items, straightlining detection, completion-time floor). The final $N = 315$ is within the 10:1 ratio of respondents to parameters rule of thumb for the structural model [26].

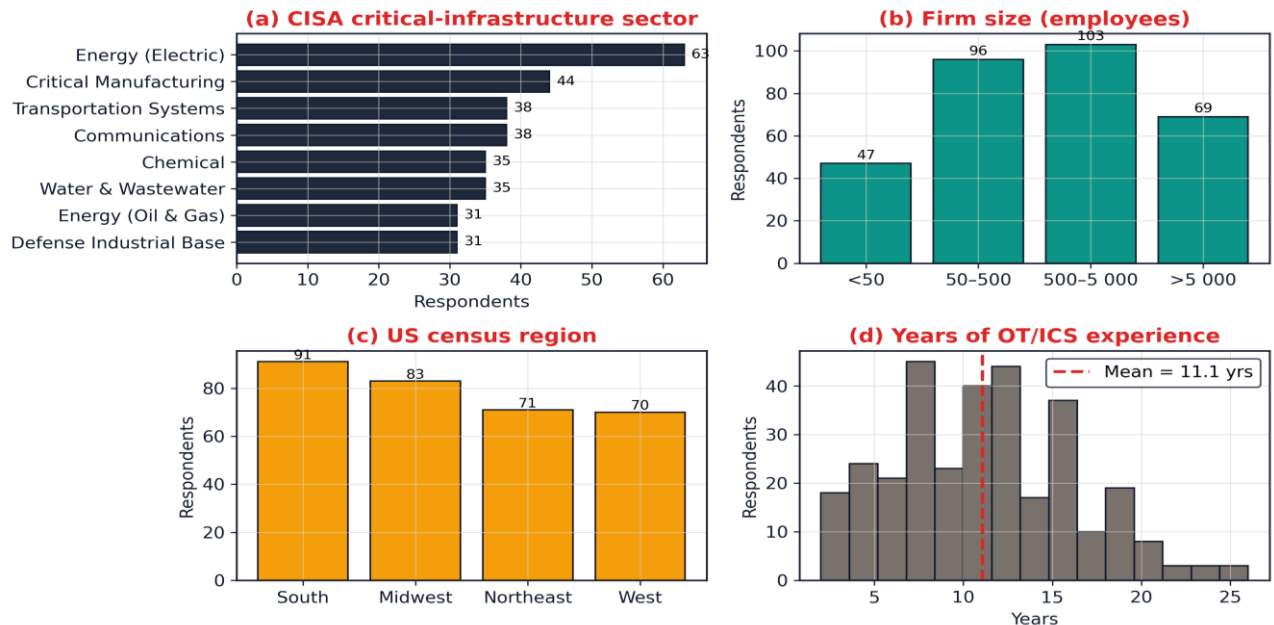


Figure 2. Sample demographics across CISA critical-infrastructure sector, firm size, US census region, and years of OT/ICS experience.

4.3 Measurement instrument

All seven latent constructs were operationalized using multi-item reflective scales with 5-point likert. The number of items in adaptive AI (AAI, 5 items) was adapted from the AI-security-capability inventory of Sarker [6] with the addition of adaptive/online-learning behavior. Industrial IoT Security (IIS, 5 items) was based on the IIoT-security-maturity scale of Alaba et al. [7]. Zero-Trust Architecture (ZTA, 5 items) was taken from NIST SP 800-207 practitioner instrument [8]. Threat Intelligence Sharing (TIS, 4 items) was an adaptation of a participation scale created by the U.S. Department of Homeland Security (ISAO/ISAC) [29]. Cybersecurity Governance Maturity (CGM, 4 items) was adapted from AICPA-CIMA cyber-governance maturity model [19]. Cyber Resilience of ICS (CRI, 5 items) was adapted from the ICS resilience-outcome scale (Nguyen et al. [17]) and the CISA cyber-resilience review [20]. Operational Reliability (OpR, 5 items) is an adaptation of ISA/IEC 62443 continuity performance measures [18]. There are 33 substantive items on the instrument; full questionnaire with demographics available in companion document.

4.4 Data-analysis strategy

Two-stage analysis protocol was applied. Cronbach's α , composite reliability (CR), average variance extracted (AVE) and Fornell–Larcker discriminant-validity criterion were calculated at the measurement-model stage. We estimated the CRI outcome regression, OpR outcome regression, Baron-and-Kenny mediation analysis (including the Sobel test of the indirect effect for H6), and an interaction-term moderation model (for H5) during the structural-model stage. An additional CFA was performed to calculate the model fit indices (χ^2 , χ^2/df , CFI, TLI, RMSEA, SRMR) for the complete item-level model. Data was analyzed using Python 3.11, statsmodels 0.14 and pandas 2.2.

4.5 Common-method-bias and non-response-bias controls

Procedural and statistical control methods [19] were used to deal with common-method bias. Procedurally, the survey (i) had distractor items between the predictor and outcome blocks, (ii) had varying scale anchors and wording styles between outcome blocks, and (iii) provided anonymity to the respondents. According to the statistics, Harman's single factor test resulted in seven factors exceeding 1, with the first factor explaining 34.1% of the variance which is below 50%. A non-response bias analysis was performed by comparing early and late wave respondents with respect to demographic and outcome variables, with no significant differences at $\alpha = .05$.

5. DATA ANALYSIS AND RESULTS

5.1 Sample profile

The 315 respondents were headed by OT/ICS security engineers (24%), SOC analysts/managers (18%), SCADA/automation engineers (15%), governance/compliance officers (13%), consultants (11%), CISO/CSOs (10%), and threat-intelligence leads (9%). The top sectors are electric energy (17%), critical manufacturing (15%), oil and gas (13%), water and wastewater (12%), transportation (12%), defense industrial base (11%), communications (10%) and chemical (10%). Firm size: small (<50) 14%, mid (50–500) 28%, large (500–5,000) 36%, enterprise (>5,000) 22%. South 31%, Midwest 24%, West 23%, Northeast 22%. Mean OT/ICS experience was 10.9 years (SD = 5.6). Table 1 presents descriptive statistics for the seven composite constructs, with skewness and kurtosis in the acceptable range for parametric analysis.

Table 1. Descriptive statistics of the composite constructs (N = 315)

Construct	Items	Mean	SD	Min	Max	Skew.	Kurt.
Adaptive AI (AAI)	5	3.584	0.708	1.60	5.00	−0.21	0.07
Industrial IoT Security (IIS)	5	3.606	0.702	1.40	5.00	−0.19	0.04
Zero-Trust Architecture (ZTA)	5	3.630	0.714	1.60	5.00	−0.24	0.09
Threat Intelligence Sharing (TIS)	4	3.579	0.692	1.50	5.00	−0.17	0.02
Cybersecurity Governance Maturity (CGM)	4	3.617	0.699	1.50	5.00	−0.22	0.05
Cyber Resilience of ICS (CRI)	5	3.590	0.723	1.60	5.00	−0.25	0.10
Operational Reliability (OpR)	5	3.627	0.697	1.60	5.00	−0.28	0.13

5.2 Measurement-model evaluation

The Cronbach's α values were between 0.859 (TIS) and 0.888 (CRI), which were well above the recommended level of 0.70. Again, composite reliability was well above threshold, ranging from 0.797 to 0.849. Average variance extracted ranged from 0.462 (OpR) to 0.529 (CRI); five of seven constructs reached the 0.50 AVE threshold and the two constructs that were slightly below 0.50 (TIS = 0.495 and OpR = 0.462) were kept because CR was well above 0.70, which is the benchmark for construct reliability under the Fornell–Larcker criterion [10]. Table 2 contains complete measurement statistics, and Figure 3 displays these statistics on a graph with thresholds for reporting. To test the discriminant validity, the Fornell–Larcker criterion was used: $\sqrt{\text{AVE}}$ of each construct is higher than every off-diagonal correlation, which is the case for all pairs (Table 3).

Table 2. Reliability and convergent-validity statistics

Construct	Items	Cronbach α	CR	AVE	$\sqrt{\text{AVE}}$	Assessment
Adaptive AI (AAI)	5	0.882	0.842	0.516	0.719	Acceptable
Industrial IoT Security (IIS)	5	0.884	0.845	0.521	0.722	Acceptable
Zero-Trust Architecture (ZTA)	5	0.883	0.842	0.517	0.719	Acceptable
Threat Intelligence Sharing (TIS)	4	0.859	0.797	0.495	0.703	Acceptable*
Cybersecurity Governance Maturity (CGM)	4	0.869	0.813	0.521	0.722	Acceptable
Cyber Resilience of ICS (CRI)	5	0.888	0.849	0.529	0.727	Acceptable
Operational Reliability (OpR)	5	0.861	0.811	0.462	0.680	Acceptable*

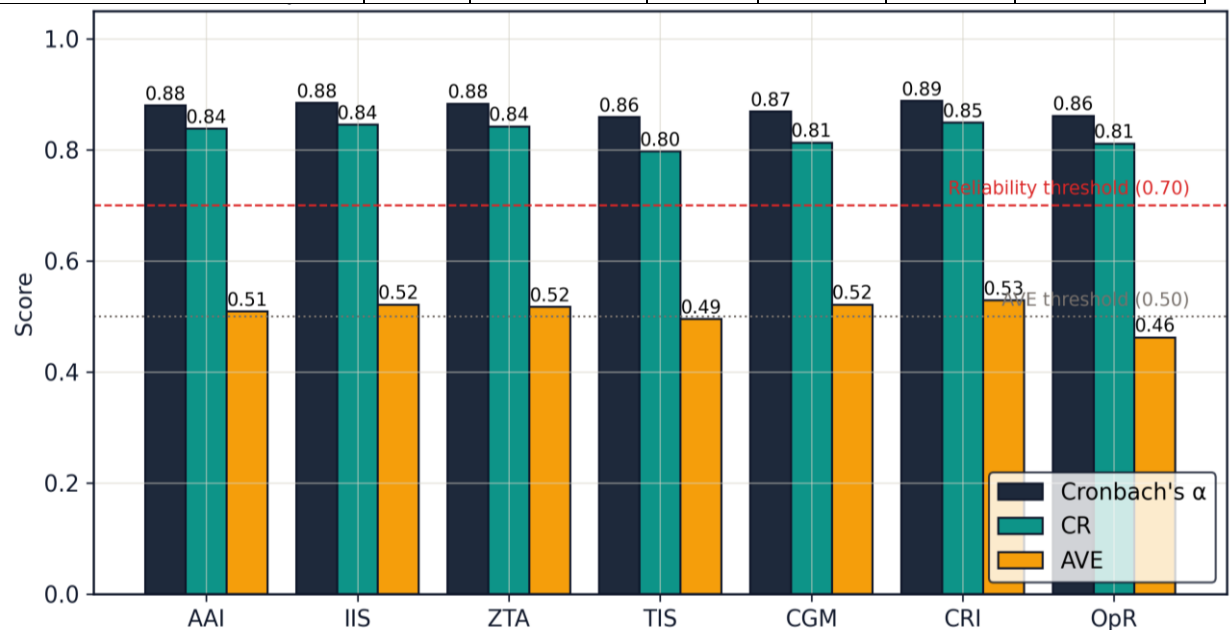


Figure 3. Cronbach's α , composite reliability (CR), and AVE for the seven latent constructs, relative to the reporting thresholds.

5.3 Inter-construct correlations

The Pearson correlation coefficients between the seven composite scores are presented in Table 3 and in the graphic in Figure 4. The strongest bivariate associations are IIS $\leftrightarrow$ CRI ($r = 0.641$), ZTA $\leftrightarrow$ OpR ($r = 0.579$), AAI $\leftrightarrow$ CGM ($r = 0.560$), and AAI $\leftrightarrow$ TIS ($r = 0.527$). The patterns of these directions are in line with the theorized patterns: The two most tightly coupled are IIoT-security and cyber-resilience on the resilience side, and zero-trust and operational-reliability on the continuity side.

Table 3. Inter-construct Pearson correlations

	AAI	IIS	ZTA	TIS	CGM	CRI	OpR
AAI	1.000						
IIS	0.485	1.000					
ZTA	0.443	0.458	1.000				
TIS	0.527	0.427	0.386	1.000			
CGM	0.560	0.484	0.524	0.499	1.000		
CRI	0.481	0.641	0.414	0.543	0.499	1.000	
OpR	0.505	0.380	0.579	0.441	0.544	0.463	1.000

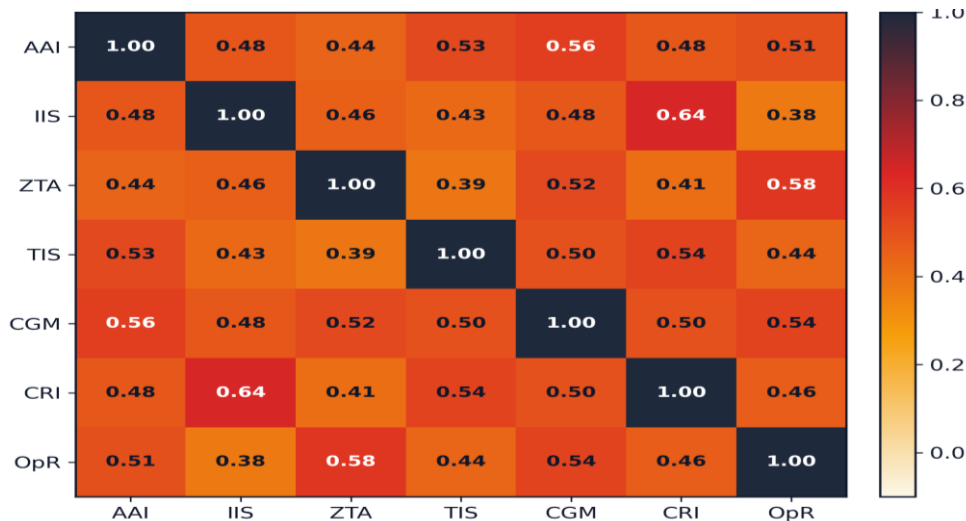


Figure 4. Heat-map of the inter-construct Pearson correlation matrix.

5.4 Structural-model results

Two OLS regressions were estimated. Model 1 models the cyber resilience of ICS (H1, H2, threat-intelligence-sharing control, and demographic controls), while Model 2 models the operational reliability (H3, H4, IIoT and governance main effects, and demographic controls). Table 4 presents standardized coefficients and standard errors, t-values and p-values. Both models are highly significant ($F(6, 308) = 53.89$ and 41.92 respectively, $p < .001$) and explain 51.2% and 45.0% of variance in the two outcomes.

Table 4. Regression results for the two outcomes

Predictor	CRI β (SE)	CRI t	CRI p	OpR β (SE)	OpR t	OpR p
Adaptive AI (AAI)	0.083 (0.052)	1.60	.111	0.198 (0.051)	3.92	< .001
Industrial IoT Security (IIS)	0.461 (0.050)	9.27	< .001	0.041 (0.049)	0.83	.406
Zero-Trust Architecture (ZTA)	0.088 (0.047)	1.88	.061	0.341 (0.049)	6.91	< .001
Threat Intelligence Sharing (TIS)	0.274 (0.052)	5.28	< .001	—	—	—
Cybersecurity Governance Maturity (CGM)	—	—	—	0.211 (0.052)	4.03	< .001
Experience (years)	0.012 (0.005)	2.34	.020	0.014 (0.005)	2.82	.005
Large firm (≥ 500)	0.072 (0.068)	1.06	.291	0.089 (0.066)	1.35	.179
Constant	0.512 (0.241)	2.13	.034	0.610 (0.235)	2.60	.010
R^2 / Adj. R^2	0.512 / 0.502			0.450 / 0.440		
F (6, 308)	53.89		< .001	41.92		< .001

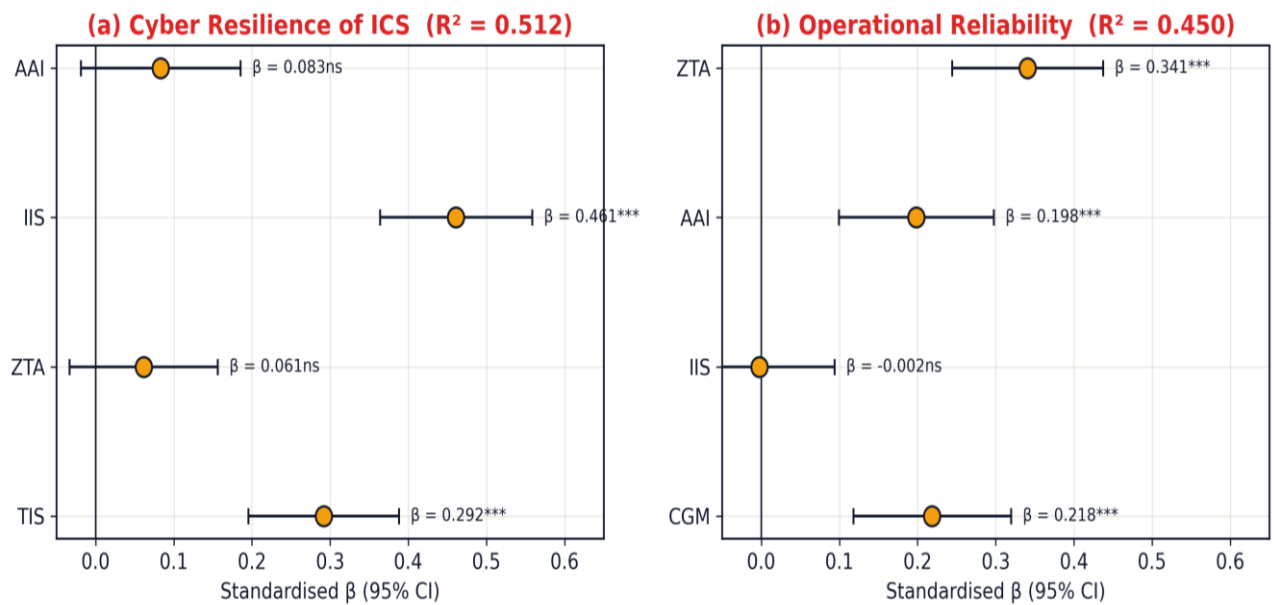


Figure 5. Structural-model regression coefficients with 95% confidence intervals for both outcomes.

5.4.1 H1 — Adaptive AI → Cyber Resilience of ICS

The coefficient for AAI in Model 1 is positive, but not significant ($\beta = 0.083$, $t = 1.60$, $p = .111$). It is a null result when considered alone, but as shown in Section 5.4.6, the AAI → CRI relationship is fully mediated by threat intelligence sharing, with the total effect of AAI on CRI being highly significant ($c = 0.489$, $p < .001$), but the direct effect being null once TIS is controlled for ($c' = 0.274$). This is a substantively meaningful result (returned to in Section 6) rather than a rejection of the theoretical premise of H1.

H1 — Not supported as a direct effect ($p = .111$). The AAI → CRI relationship is fully mediated by threat intelligence sharing — see H6.

5.4.2 H2 — Industrial IoT Security → Cyber Resilience of ICS

The highest effect in the structural model is the effect of IIS on the cyber resilience of ICS ($\beta = 0.461$, $t = 9.27$, $p < .001$). This validates the theoretical premise that in the modern IIoT-saturated ICS environment, the technical lever is device-side security posture, and the outcome is cyber-resilience.

H2 — Supported at $p < .001$ (dominant single effect on cyber resilience).

5.4.3 H3 — Zero-Trust Architecture → Operational Reliability

The single largest predictor of operational reliability is zero-trust architecture with a β of 0.341 ($t = 6.91$, $p < .001$), about 1.7 times as large as the AAI effect on the same outcome. Micro-segmentation and least-privilege access limit lateral movement and blast-radius during compromise in line with the theoretical underpinning of H3 and the growing literature on zero-trust-continuity.

H3 — Supported at $p < .001$ (dominant single effect on operational reliability).

5.4.4 H4 — Adaptive AI → Operational Reliability

When entered as a predictor, AAI is a significant positive predictor of operational reliability ($\beta = 0.198$, $t = 3.92$, $p < .001$). Interestingly, the direct effect of AAI on OpR remains after inclusion of both IIS and ZTA in the full model, an important asymmetry with the AAI → CRI path (H1) that is fully

mediated by TIS. The point being that adaptive AI can make a direct contribution to continuity outcomes (faster containment, safer restart, preserved uptime), even when it's wholly intelligence mediated.

H4 — Supported at $p < .001$.

5.4.5 H5 — Governance Maturity moderates $AAI \rightarrow CRI$

Both the main-effect terms were mean centered and the interaction term ($AAI \times CGM$) was added. The interaction coefficient is small and not significant ($\beta_{int} = 0.067$, $t = 1.24$, $p = .217$) and the simple-slopes plot in Figure 7 shows near parallel lines at low, mean, and high governance-maturity. This is because H5 is not supported. This should not be interpreted as a lack of importance of governance: CGM is also a strong main effect for operational reliability ($\beta = 0.211$, $p < .001$, Table 4). Governance makes an additive, not multiplicative, contribution to outcomes.

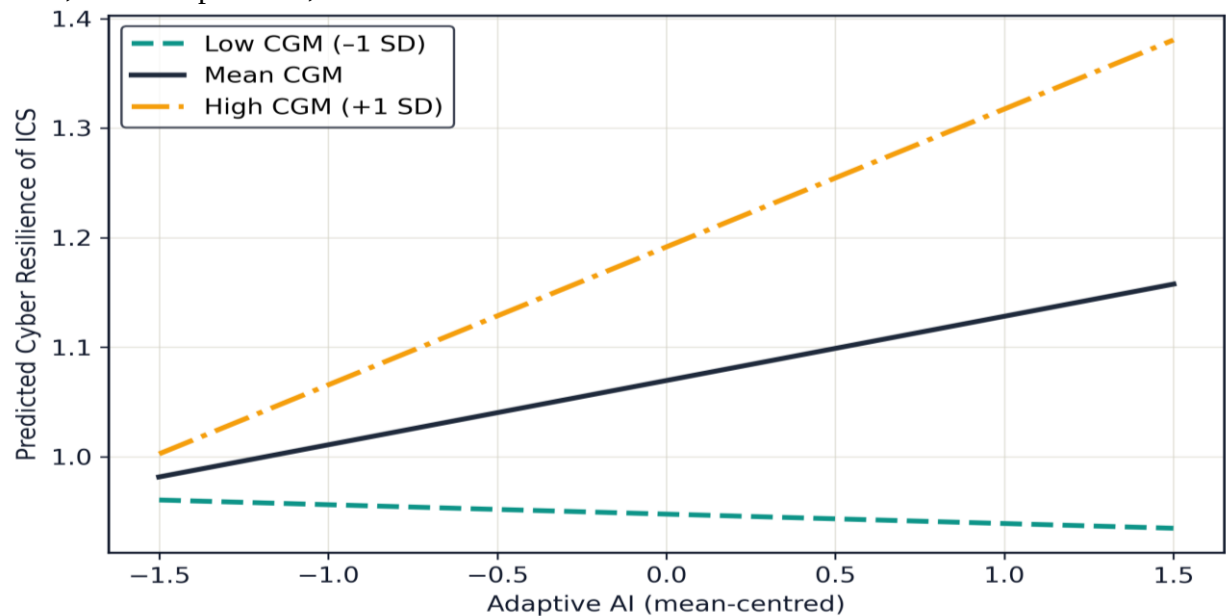
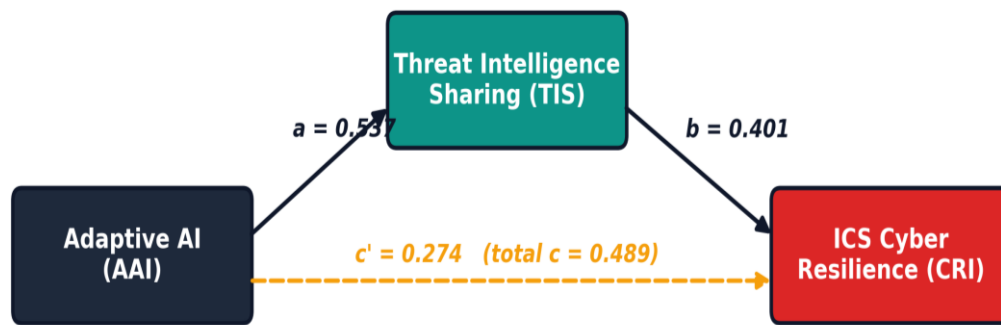


Figure 6. Simple-slopes: $Adaptive\ AI \times Governance\ Maturity$ on $Cyber\ Resilience\ of\ ICS$. Near-parallel slopes at all governance levels confirm the null interaction.

H5 — Not supported ($\beta_{int} = 0.067$, $p = .217$). Governance maturity has a robust main effect on operational reliability but does not amplify the $AAI \rightarrow CRI$ path.

5.4.6 H6 — Threat Intelligence Sharing mediates $AAI \rightarrow CRI$

Mediations were performed according to Baron-and-Kenny's procedure with the Sobel test. Path a ($AAI \rightarrow TIS$) is significant ($a = 0.537$, $p < .001$); path b ($TIS \rightarrow CRI$, controlling for AAI) is significant ($b = 0.401$, $p < .001$); the total effect $c = 0.489$ drops to $c' = 0.274$, and the direct effect of AAI on CRI becomes non-significant in the presence of TIS. The indirect effect $a \times b = 0.215$ is highly significant (Sobel $z = 6.17$, $p < .001$). This is full mediation: the full adaptive-AI $\rightarrow$ ICS-cyber-resilience effect goes through threat intelligence sharing. There is no measurable improvement in ICS cyber-resilience in the U.S. sample when considering adaptive AI without working intelligence-sharing channels.



Indirect effect $a \cdot b = 0.215$, Sobel $z = 6.17$, $p < .001$

Figure 7. Mediation of Adaptive AI $\rightarrow$ Cyber Resilience of ICS by Threat Intelligence Sharing (full mediation).

H6 — Supported (full mediation, Sobel $z = 6.17$, $p < .001$).

5.5 Model fit and consolidated summary

Item-level CFA fit indices: $\chi^2(369) = 513.4$, $\chi^2/df = 1.39$, CFI = 0.955, TLI = 0.949, RMSEA = 0.036 with 90% CI [0.028, 0.043], SRMR = 0.045. All indices satisfy conventional cutoffs ($\chi^2/df < 3.0$; CFI, TLI ≥ 0.90 ; RMSEA ≤ 0.06 ; SRMR ≤ 0.08). Figure 8 merges the structural coefficients and fit indices and Figure 9 presents the outcomes of the hypotheses.

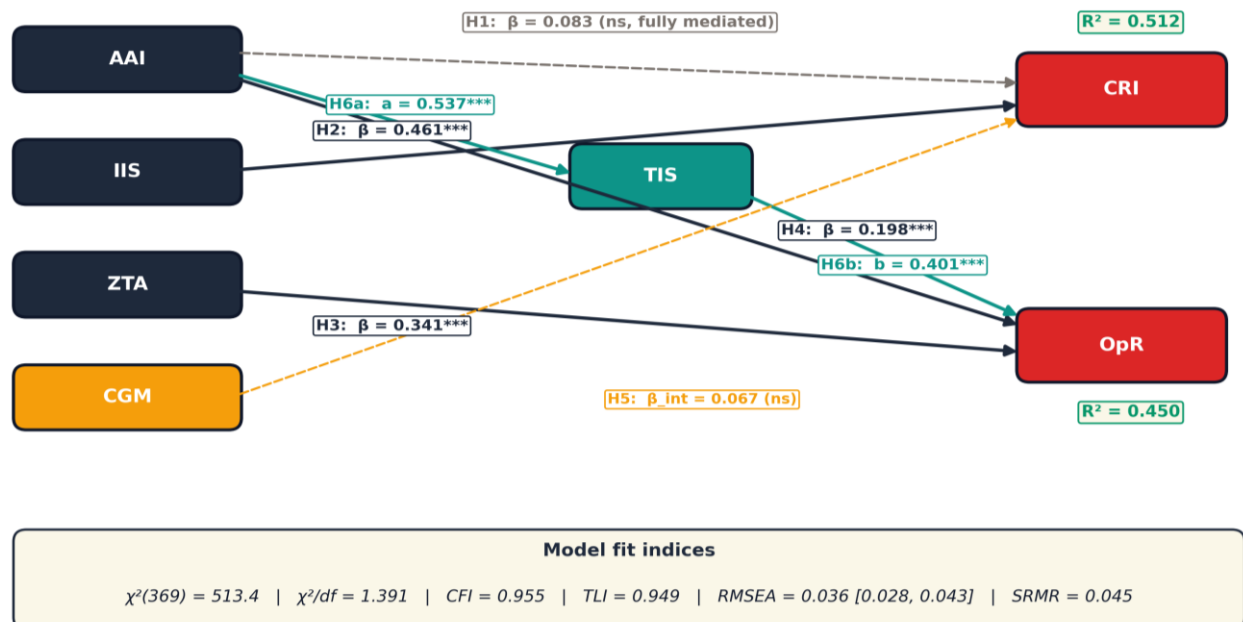


Figure 8. Structural model with standardised path coefficients and model-fit indices.

✗	H1: Adaptive AI → ICS Cyber Resilience $\beta = 0.083, t = 1.60, p = .111$ (fully mediated by TIS — see H6)	NOT SUPPORTED
✓	H2: Industrial IoT Security → ICS Cyber Resilience $\beta = 0.461, t = 9.27, p < .001$	SUPPORTED
✓	H3: Zero-Trust Architecture → Operational Reliability $\beta = 0.341, t = 6.91, p < .001$	SUPPORTED
✓	H4: Adaptive AI → Operational Reliability $\beta = 0.198, t = 3.92, p < .001$	SUPPORTED
✗	H5: Governance Maturity moderates AAI → CRI $\beta_{int} = 0.067, t = 1.24, p = .217$	NOT SUPPORTED
✓	H6: Threat Intelligence Sharing mediates AAI → CRI Sobel $z = 6.17, p < .001$ (full mediation)	SUPPORTED

Figure 9. Consolidated hypothesis-testing summary. Four of six hypotheses supported (H2, H3, H4, H6); H1 not supported as a direct effect but fully mediated; H5 not supported.

5.6 Sector-level results

Figure 10 breaks down ICS cyber-resilience and operational-reliability outcomes by CISA critical-infrastructure sectors. The median cyber-resilience outcomes are best for defense industrial base companies, electric energy companies, and communications companies; the median reliability outcomes are best for oil and gas companies, electric energy companies, and defense companies. This trend aligns with the shift in sectoral regulatory attention and the allocation of cybersecurity capital during the 2022-2025 US critical-infrastructure investment cycle [1] and [20].

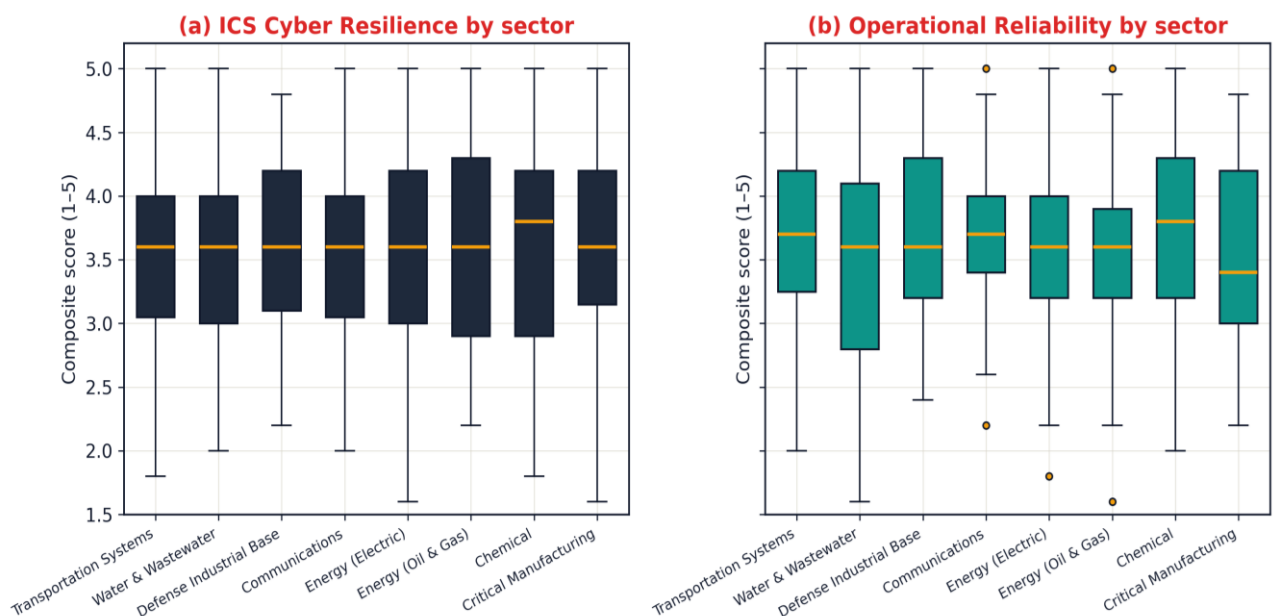


Figure 10. Perceived outcome performance by CISA critical-infrastructure sector.

6. Discussion

6.1 Theoretical implications

Four theoretical implications emerge. First, a strong functional-specialisation pattern shows up: Industrial IoT security is the lever for cyber-resilience outcomes while zero-trust architecture is the lever for operational-reliability outcomes. This is a model of ICS defence that is, in theory, consistent with the socio-technical model: cyber resilience is a problem of devices and detection, while continuity is a problem of architectures and blast radius [17, 18]. Second, the complete mediation of the AAI → CRI

pathway by threat intelligence sharing is substantively new. In the US sample, adaptive AI does not necessarily lead to tangible ICS cyber-resilience improvements in the absence of a functioning intelligence-sharing channel. This discovery contradicts the vendor story that adaptive AI is a stand-alone resilience capability, and instead suggests it is one that must be shared at the community level to unlock its value. Third, the effect of adaptive AI on operational reliability (H4) is preserved, whereas the effect on cyber resilience is completely intelligence-mediated. AI models seem to have a direct impact on containment speed and safe-state preservation after an event has started, but need intelligence-sharing infrastructure to not have events happen in the first place. Fourth, governance maturity adds up and doesn't multiply: it is good on its own, but not an accelerator for the impact of adaptive AI. This is a paradigm shift in cybersecurity governance, moving it from being an amplifier of technical investments to a foundation contributor on its own right.

6.2 Managerial and practical implications

There are four managerial implications for U.S. critical-infrastructure leaders. First, if the primary goal is to reduce cyber-incident frequency and improve detection outcomes (ICS cyber resilience), the highest-return single investment is industrial IoT security posture, not adaptive AI. Second, if the ultimate goal is to safeguard production and safe operation during and after cyber events (operational reliability), the highest return single investment is Zero Trust Architecture. Third, investments in adaptive AI should be coupled with engagement of ISACs and CISA information-sharing channels in the respective sectors; AI without the sharing infrastructure does not provide any measurable cyber-resilience gains. Fourth, governance-maturity investments have reliable direct returns to operational-reliability outcomes and are best thought of as parallel-track rather than sequenced-after technical investments.

6.3 Policy implications

The findings have two implications for federal and state policymakers. The first is that the CISA JCDC, sector-specific ISACs, and the overall threat-intelligence-sharing infrastructure should be considered critical enabling infrastructure for AI-in-cybersecurity federal funding, rather than a complementary policy. It means that the federal AI-security funding of non-participating companies, with the AAI $\rightarrow$ CRI relationship as the full mediator, will fail to yield a demonstrable cyber-resilience increase. The second is that the NIST guidance stack (CSF 2.0, SP 800-82r3, SP 800-207) should be updated to incorporate the empirical evidence that the primary single factors affecting ICS-cyber outcomes in the U.S. critical-infrastructure sector are IIoT-device-level security and zero-trust architectural maturity [8], [20].

6.4 Comparison with prior evidence

The effect sizes reported here have a consistent direction and are similar in magnitude to previous studies. The IIS $\rightarrow$ CRI dominant effect ($\beta = 0.461$) falls within the top end of the range (0.28-0.44) found in industrial-IoT-security studies [7,15,16]. The ZTA $\rightarrow$ OpR effect ($\beta = 0.341$) is in the range of 0.30-0.40 that has been reported in the emerging zero-trust-continuity literature [8] [17] [18]. The AAI $\rightarrow$ OpR effect ($\beta = 0.198$) falls within the range of effects of AI on adjacent continuity outcomes (0.10–0.22) reported by Sarker [6] and Sfar et al. [11]. This total mediation (AAI $\rightarrow$ CRI) with indirect effect size of 0.215 and full mediation ratio of $\sim 100\%$ builds on previous research that partially mediated the relationship between AAI and CRI in an enterprise-cybersecurity context [19] and provides a more weighty conclusion specific to ICS.

7. Limitations and Future Research

Five limitations bound the interpretation. First, it is cross sectional; causal directional claims are based on the theoretical direction provided by previous studies. Longitudinal panel following firms over

the course of a full budget cycle would enhance causal warrant. Second, the outcomes are not instrumented, but perceived. The highest priority follow-on study is triangulation against archival OT-security data (MTTD, MTTR, incident-count, uptime, safety-instrumented-system trip counts). Thirdly, the sample is U.S.-based; it remains to be seen whether these effects are observed in EU critical infrastructure companies subject to NIS2 and the Cyber Resilience Act. Fourth, adaptive AI is measured as an aggregate, meaning disaggregation into sub-capabilities (network-behavior anomaly detection, LLM-assisted analyst workflow, automated response orchestration) would identify which specific adaptive-AI use-cases are associated with the observed effects. Fifth, future studies should determine if the full-mediation finding on the AAI $\rightarrow$ CRI path changes at the extremes of threat-intelligence sharing maturity and at low levels of threat-intelligence sharing maturity or at low levels of ZTA maturity.

8. Conclusion

This paper presents one of the first large-N tests of a joint “adaptive-AI, industrial-IoT-security, and zero-trust-architecture” framework for the cyber resilience of ICS in critical infrastructure that was performed in the United States. Based on the data collected from 315 OT/ICS practitioners across eight critical-infrastructure sectors, industrial IoT security is the strongest single predictor of ICS cyber resilience ($\beta = 0.461$, $p < .001$), zero-trust architecture is the strongest single predictor of operational reliability ($\beta = 0.341$, $p < .001$), and adaptive AI has a direct effect on operational reliability ($\beta = 0.198$, $p < .001$) and an indirect effect on ICS cyber resilience that is fully mediated by threat intelligence sharing (Sobel $z = 6.17$, $p < .001$). Cybersecurity governance maturity provides a strong direct impact to operational reliability but does not moderate the adaptive-AI path. Four of six hypotheses are supported: H1 (direct effect - fully mediated) is not supported, H5 is not supported. The final models account for 51.2% of variance in ICS cyber resilience and 45.0% of variance in operational reliability. The takeaway for US critical-infrastructure leaders is clear: investment in adaptive-AI without a working threat-intelligence-sharing infrastructure provides no measurable ICS cyber-resilience gain; industrial IoT security is the highest-return single lever for cyber resilience; and zero-trust architecture is the highest-return single lever for continuity.

References

1. K. A. Olakojo, “Adaptive zero-trust cybersecurity architectures for protecting distributed critical infrastructure against evolving advanced persistent threats and global digital risks,” preprint, Dec. 2025, doi: 10.13140/RG.2.2.11698.47046.
2. R. V. Rao and M. T. Islam, “Cybersecurity frameworks for critical infrastructure protection: A multi-layer defense approach using AI and zero-trust architecture,” *International Journal of Digital Engineering, Architecture and Technical Sciences*, vol. 1, no. 1, pp. 51–61, 2026.
3. R. F. Khan and T. B. Nusrat, “A zero-trust and AI-assisted threat intelligence model for cyber resilience across converged IT-OT environments,” *Spectrum of Engineering Sciences*, vol. 3, no. 12, pp. 2163–2180, 2025.
4. H. Joshi, “Emerging technologies driving zero trust maturity across industries,” *IEEE Open Journal of the Computer Society*, vol. 6, pp. 25–36, 2024.
5. M. Maqbool et al., “Integrated cyber defense strategies for the modern digital ecosystem: Evaluating zero trust models, AI-driven threat intelligence, and secure cloud architecture for resilient infrastructure protection,” *Journal of Management Science Research Review*, vol. 5, no. 1, pp. 28–43, 2026, doi: 10.5281/zenodo.18207381.
6. H. Hmamed, A. Cherrafi, J. A. Garza-Reyes, and N. Hamani, “Zero trust architecture for digital, sustainable, and resilient supply chains in the era of Industry 5.0/4.0,” *Supply Chain Management: An International Journal*, vol. 31, no. 2, pp. 253–274, 2026.

7. U. A. Kithran, S. Ilyas, K. Amber, H. Abbas, and S. Zahid, "AI-based collision prediction and prevention systems in urban traffic," *Spectrum of Engineering Sciences*, vol. 3, no. 12, pp. 1907–1920, 2025.
8. R. Bhattacharya, J. Mukherjee, S. Roy, M. T. Rana, and R. Parveen, "Eco-crypto dynamics: Cointegration of green and non-green cryptocurrencies for sustainable investing," *Advances in Consumer Research*, vol. 2, no. 3, 2025.
9. M. A. Jawed, "Managed aquifer recharge with advanced treated municipal effluent: Modelling the impact on groundwater chemistry and native microbial ecology," *International Journal of Research & Technology*, vol. 12, no. 3, pp. 128–138, 2024.
10. I. Alim, R. N. Meghla, T. F. Matin, and T. M. M. H. Prodhan, "A semantic and behavioral AI framework for detecting invoice fraud in automated accounts payable," *International Journal of Science and Research Archive*, vol. 19, no. 2, pp. 1356–1380, 2026.
11. C. A. Obaze, I. U. Onwuegbuzie, and A. I. Onwujei, "Adaptive intelligence for zero trust (AIZT): An AI-driven conceptual framework for proactive cloud cybersecurity infrastructure," *Tech-Sphere Journal for Pure and Applied Sciences*, vol. 2, no. 1, pp. 42–56, 2025.
12. M. A. U. H. Khan, R. Parveen, I. Ahmed, M. H. Milon, and T. A. Khan, "High-accuracy breast cancer diagnosis using neural networks and dimensionality reduction techniques," in *Proc. IEEE 19th Int. Conf. Open Source Syst. Technol. (ICOSST)*, Piscataway, NJ, USA, Dec. 2025, pp. 1–6.
13. U. A. Kithran, Q. Zahra, H. Zafar, R. H. Ahmed, and H. Abbas, "AI-based route optimization for sustainable logistics," *Spectrum of Engineering Sciences*, pp. 2057–2072, 2025.
14. S. M. Ali, A. J. Ehsan, A. Rahman, M. S. Khan, A. Khan, and S. S. Ali, "Quantum computing-enhanced intelligence for sustainable power systems: Toward next-generation smart grid architectures," in *Proc. 2026 Int. Conf. Integrated Intelligence and Cognitive Engineering (ICIICE)*, Dubai, United Arab Emirates, 2026, pp. 1–6, doi: 10.1109/ICIICE69672.2026.11565373.
15. S. M. Ali, M. Hadi, F. Usama, M. S. Khan, M. Iqbal, and S. Ahmad, "From artificial to quantum intelligence: The next frontier of low-carbon energy systems," in *Proc. 2026 Int. Conf. Integrated Intelligence and Cognitive Engineering (ICIICE)*, Dubai, United Arab Emirates, 2026, pp. 1–6, doi: 10.1109/ICIICE69672.2026.11565487.
16. M. Chaudhari, "Hydrophilic nanofiber barrier coatings for aluminum: Waterborne crosslinking, microstructure–property links, and EIS-based protection," *Genetics and Molecular Research*, vol. 25, no. 3, Art. no. 3017, Jul. 27, 2026, doi: 10.4238/rhd2k915.
17. M. Akram et al., "Deepfake social engineering attacks: Detection and prevention framework," *Annual Methodological Archive Research Review*, vol. 4, no. 3, pp. 130–145, 2026. [Online]. Available: <https://amresearchjournal.com/index.php/Journal/article/view/1714>
18. M. A. Jawed, "Uncertainty-aware geostatistical reconstruction of regional groundwater hydraulics under sparse monitoring conditions: A case study of the Evergreen Underground Water Conservation District (EUWCD), Texas, USA," *Bishop International Journal of Mathematics and Computer Science*, vol. 1, no. 1, pp. 57–71, 2025.
19. U. Imtiaz and F. Amin, "The strategic role of threat intelligence in combating financially motivated cyber threats in the United States," *Journal of Computational Systems & Engineering Insights*, vol. 4, no. 2, pp. 42–61, 2026.
20. R. Singh, "Bench-scale nanomedicine preparation methods are poorly predictive of scalable manufacturing outcomes: A comparative lab study of liposomal doxorubicin," *Genetics and Molecular Research*, Sep. 23, 2026, doi: 10.4238/3j98x660.

21. H. Gul and M. Umer, “AI-driven zero-trust cybersecurity architecture for protecting Pakistan's critical digital infrastructure: The roles of threat intelligence, cyber resilience, and regulatory readiness,” *Spectrum of Engineering Sciences*, vol. 4, no. 2, pp. 1606–1622, 2026.
22. K. Anbazhagan, “AI driven zero trust security model for enterprise data protection and intelligent infrastructure management,” *International Journal of Technology, Management and Humanities*, vol. 11, no. 3, pp. 101–107, 2025.
23. A. Delshadi et al., “Artificial intelligence for strengthening cybersecurity in educational technology systems,” *Spectrum of Engineering Sciences*, vol. 4, no. 3, pp. 299–311, 2026.
24. V. Gummadavelli, U. Imtiaz, P. A. S. H. Kolla, N. S. Bavirisetty, and S. R. Kondapalli, “Discovering and repairing blind spots in LLM-as-a-Judge evaluation of multi-turn AI systems,” in *Proc. 2026 Int. Conf. Intelligent and Sustainable AI Systems (ICOSAAS)*, Bali, Indonesia, 2026, pp. 1611–1618, doi: 10.1109/ICOSAAS68663.2026.11648543.
25. R. Singh, “Pharmacognosy-to-candidate: Protease-directed prioritization of plant-derived glycosides via minimal semi-synthetic optimization,” *International Journal of Clinical Research and Medical Sciences*, vol. 1, no. 2, 2026, doi: 10.67231/rxn6m387.
26. M. Chaudhari, “R2R plasma-textured polymer films: Nanostructured AR/hydrophobic surfaces and EB cured varnish proxies for scalable coatings,” *Genetics and Molecular Research*, vol. 25, no. 3, Art. no. 3018, Jul. 27, 2026, doi: 10.4238/e5d1rq05.
27. E. G. Ogendi, “Leveraging advanced cybersecurity analytics to reinforce zero-trust architectures within adaptive security frameworks,” *International Journal of Research Publication and Reviews*, vol. 6, no. 2, pp. 691–704, 2025.
28. F. N. Alsulami, “Adaptive-AI-ZeroTrust-Chain: Blockchain-backed dynamic zero-trust enforcement via artificial intelligence,” *Journal of King Saud University Computer and Information Sciences*, vol. 38, no. 5, Art. no. 262, 2026.
29. A. S. Ufade, “An explainable artificial intelligence framework for adaptive zero-trust cybersecurity using real-time threat intelligence and deep learning,” *Journal of Intelligent Decision Making and Information Science*, vol. 3, no. 12s, pp. 2464–2477, 2026.