Federal Register Notice: 89 FR 78915, Federal Register :: Networking and Information Technology Research and Development Request for Information on Cyber-Physical Systems Resilience Research, September 26, 2024.

Request for Information on the National Cyber-Physical Systems Resilience Plan

Luis Garcia

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government. We bear no responsibility for the accuracy, legality, or content of the responses and external links included in this document.

Response to NSF Request for Information on Resilience of Cyber-Physical Systems

Federal Register Notice: 89 FR 78915

Submitted by:
Luis Garcia
Assistant Professor
University of Utah

Date: October 26, 2024

Response to RFI on Cyber-Physical System Resilience

As CPS security researchers, we recognize the pressing need for standardized frameworks to guide resilience efforts across diverse cyber-physical systems (CPS), particularly given the range of resilience needs. Beyond traditional threats posed by malicious actors, CPS resilience encompasses naturally occurring events that stress systems, from extreme weather to unprecedented surges in demand during large-scale events like the Olympics. While these scenarios vary, they underscore the need for resilient CPS to withstand deliberate attacks and naturally occurring system-stressing events. Yet, the industry's approach to resilience modeling remains inconsistent, with a lack of unified standards or widely accessible frameworks to guide this resilience across all infrastructure scales.

Digital Twinning in Industry and the Need for Standardization

Digital twinning has emerged as a promising resilience approach, enabling high-fidelity simulations to project system behavior and address vulnerabilities in real-time. For instance, stadiums have adopted digital twin technology to leverage continuous data insights to anticipate and mitigate operational challenges, from the complexity of event logistics to potential system strain during the Olympics. However, access to digital twin technology is limited for smaller, resource-constrained sectors, where resilience measures are critical yet often unaffordable. This lack of standardization leaves essential systems without the guidance to implement cost-effective digital twins for projecting resilience, exacerbating risks for communities that cannot afford redundancy or specialized technology.

Current industry strategies heavily promote redundancy, as seen in Rockwell Automation's guidelines for Distributed Control Systems (DCS) and the IEC 62443 framework. However, for under-resourced municipalities, redundancy at all levels is not feasible–especially when organizations may not understand the need for resiliency. Instead, resilience models should emphasize sustainable, scalable solutions prioritizing resilience-by-design, ensuring critical systems can withstand high-impact events like natural disasters. Standardizing digital twin technology with adaptable models would help bridge this gap, creating affordable pathways for resilience across various industries.

Labor Shortages and the Future of AI in Safety-Critical Infrastructure

A less visible yet critical resilience challenge is the ongoing labor shortage in safety-critical industries, from utilities to manufacturing. High turnover rates, complex training demands, and difficulty retaining skilled operators—especially with expertise in cybersecurity practices—are compounding vulnerabilities within critical infrastructure. The trend towards using AI solutions as stand-ins for human operators appears inevitable, particularly for maintaining 24/7 operations in environments where retention is difficult. However, AI-driven automation in these settings must be met with robust guardrails, including cybersecurity and operational integrity safeguards, to protect against potential exploitation or failure. In this context, standardized frameworks for integrating AI solutions within CPS resilience models will be key, ensuring that such systems are both adaptive and secure over time.

Cross-Domain Resilience and the Need for Semantic Standards

While frameworks like MITRE ATT&CK for ICS categorize Tactics, Techniques, and Procedures (TTPs), they lack comprehensive support for resilience across domains. Many prior attacks demonstrate that attackers exploit common abstractions and shared physics across critical infrastructure, targeting similar sensors and actuator mechanisms—such as valves, pumps, and dosing processes—used in sectors like water treatment, oil processing, and gas infrastructure. By formalizing these common targets regarding their impact on physical operations across sectors, we can proactively model OT attack semantics, enabling a more fine-grained approach to threat modeling. This approach would equip defenders to anticipate cross-domain vulnerabilities as attackers increasingly focus on operational disruptions that apply universally across CPS domains.