# Increasing Cyber-Resilience of Large-Scale and Long-Lived Energy Delivery Infrastructure (EDI)

**Website:** http://cred-c.org/researchactivity/resilientscale

**Researchers (Dartmouth/Illinois):** Sean Smith, Sergey Bratus, Jason Reeves, J. Pete Brady, I. Ray Jenkins, Michael Millian, Prashant Anantharaman, Arun Anand, Rafael Brantley, Galen Brown, David Nicol (Illinois), Kartik Palani (Illinois), Elizabeth Reed (Illinois), Rakesh Kumar (Illinois)

**Industry Collaboration:**

- Automatak
- Dover Energy Automation
- General Electric
- Schweitzer Engineering Laboratories
- Waterfall Security
- Currently seeking collaborators. If interested, contact Sean W. Smith.

**Description of research activity:** In the current state of the art and practice, embedded systems are rife with security holes, with 0-days and forever-days. At larger scales in space, pushing patches to these boxes will be complicated; at larger scales in time, the cryptography and the enterprise management of these boxes (that is: the boxes may outlive their vendors) may break.

To help fix this problem, we are doing three things:

- *Prevention:* Building tools to help prevent 0-days and forever-days in the first place (e.g., hardened parsers)
- *Mitigation:* Building tools to help mitigate 0-days and forever-days discovered later (e.g., verifiable protocol filters and interface snap-ins)
- *Evaluation:* Building simulation tools to evaluate how effective such tools will be when scaled up to long-lived EDI. (E.g., what approach makes the biggest improvement? For security, can N firewalls do almost as well as 100N verifiable devices?)

**How does this research activity address the Roadmap to Achieve Energy Delivery Systems Cybersecurity?**
The activity addresses several of the Roadmap strategies.

- **Build a Culture of Security.** We seek to carefully analyze current coding practices and protocol standards in order to identify fundamental sources of vulnerabilities—and promulgate new methods to reduce or eliminate them.
- **Assess and Monitor Risk.** Evaluating the effectiveness of mitigation strategies requires modeling the attack risk (and potential damage) in current infrastructure.
- **Develop and Implement New Protective Measures to Reduce Risk.** Our research squarely addresses these concerns: how to reduce the prevalence of 0-days in EDS, and how to manage and mitigate the ones that show up anyway.
- **Manage Incidents.** We seek to understand how the deployed interfaces, protocols, and coding practices enable attack incidents to happen—in order to engineer future systems to be resilient.

**Summary of EDS gap analysis:** In EDI (e.g., smart grid) and elsewhere, we're seeing computational infrastructure transform to networks of devices distributed massively in almost any axis imaginable. The "penetrate and patch" paradigm that has managed to keep traditional computers somewhat secure will no longer work when devices become too long-lived, too cheap, too invisible, and too many. As the energy sector deploys number of low-powered embedded devices at the very edges of their networks, the attack surface increases—as does the consequences of an attack.

Will all these new interfaces be free of 0-days? If so, how will this new world be different from the old? If not, how can the industry manage and mitigate the risks posed by these increased numbers and increased exposure of computational devices?

Our research addresses prevention and mitigation of 0-day and forever-day vulnerabilities through tools such as hardened parsers and verifiable protocol filters, and provides tools to evaluate the effectiveness of the approach.

**Full EDS gap analysis:** Vulnerabilities in interfaces and protocols are endemic.

Our published research in this space documents how the state of the art in research and deployment leaves this gap unaddressed. Our 2013 paper laid out our scientific foundation for input validation vulnerabilities [LangSec 2013.] Our 2016 SecDev paper [Babel 216] catalogs a wide variety of vulnerabilities stemming from these causes and suggests some solution approaches. Our recent paper on DNP3 hardening [BCP 2016] catalogs many such problems and solutions in DNP3 specifically. Our initial modeling work [PHS 2016] explores how to model the prevalence of future zero-day blooms in order to evaluate their impact—and the effectiveness of mitigation strategies.

EDS-specific documents also call out this gap. The *DHS Procurement Language for ICS* [DHSCPL] raises items relevant to this work, such as concerns about protocol vulnerabilities (Section 10), network security architecture (Section 12), and system hardening (Section 2). *NISTR 7628* repeatedly expresses concerns about vulnerabilities: impact, prevention, and mitigation. This activity also addresses many concerns the *ES-C2M2* expresses about the need to manage risk in IT and OT, to manage threat and vulnerabilities, and assets and configurations.

**Bibliography:**

[Babel 2016] F. Momot, S. Bratus, S. Hallberg, M. Patterson. "The Seven Turrets of Babel: A Taxonomy of LangSec Errors and How to Expunge Them." *IEEE SecDec 2016.* November.

[DHS CSPL, 2009] *Department of Homeland Security: Cyber Security Procurement Language for Control Systems*, September 2009.

[DNP3 2016] S. Bratus, A. Crain, S. Hallberg, D. Hirsch, M. Patterson, M. Koo, and S. Smith. "Implementing a Vertically Hardened DNP3 Control Stack for Power Applicatons." *Second Annual Industrial Control Systems Security Workshop*. ACSAC 2016.

[ES-C2M2] *Electricity Subsector Cybersecurity Capability Maturity Model.* Version 1.1. February 2014.

[NISTIR] *Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security*. September 2010.

[LangSec 2013] L. Sasseman, M. Patterson, S. Bratus, M. Locasto, A. Shubina. "Security Applications of Formal Language Theory." *IEEE Systems Journal.* 7 (3). September 2013.

[PHS 2016] K. Palani, E. Holt, S.W. Smith. "Invisible and Forgotten: Zero-Day Blooms in the IoT." *1st IEEE PerCom Workshop on Security, Privacy, and Trust in the IoT*. March 2016.