CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA

CYBER PHYSICAL SYSTEMS

CONTROL ENVIRONMENT LABORATORY RESOURCE (CELR)

An environment to experience the effects of kinetic cyber physical attacks

MAY 2020

Overview

The Control Environment Laboratory Resource (CELR) is an environment for government and private industry partners to experience the possible effects of kinetic cyber physical attacks. CELR allows users to perform security research on industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems.

CELR is a test range that uses multiple platforms capable of hosting simulated risk scenarios against real critical infrastructure (CI) processes. CELR enables the study of complete cyber warfare against our Nation's CI targets, which society relies on to maintain our way of life. CELR is highly adaptable, simulates numerous corporate network configurations, and provides control system hardware and kinetic outputs of various CI sectors. With the ability to host multiple concurrent simulations, analysts across the Nation can interact with the environment while being both on and offsite through extended range connections.

CELR is unique because it:

- Combines functional ICS/SCADA systems with threat actor tactics, techniques, and procedures (TTPs)
- Hosts simulations for both red and blue teams to experience specific threat actor TTPs
- Shows disruptive and destructive consequences of cyber attacks against ICS and how to defend against them

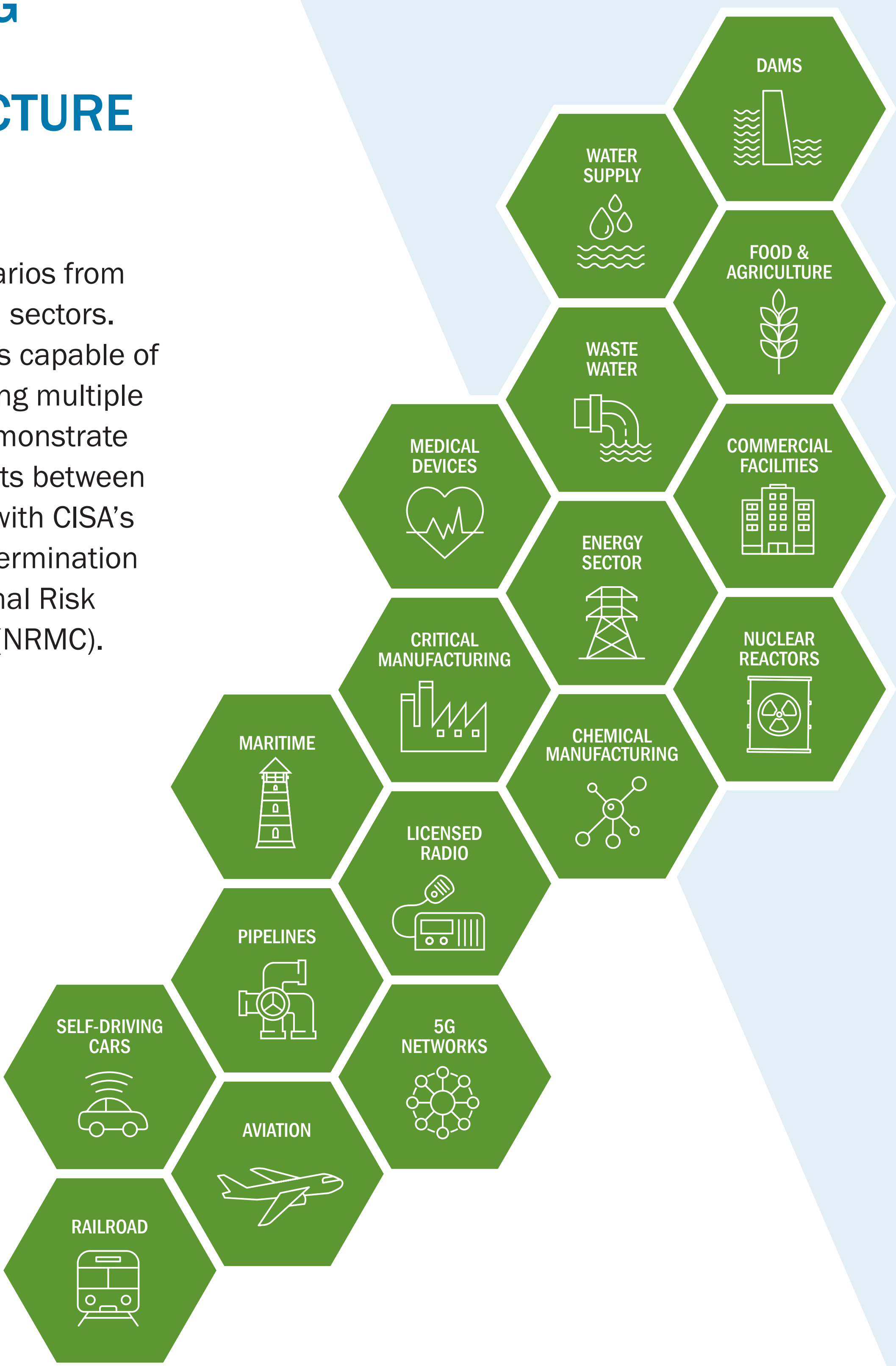
CELR supports:

- Concurrent simulations supporting diverse user groups
- Custom corporate environments ranging from small business to international conglomerates
- 16 sector-specific scenarios for ICS skids
- Remote access to simulations

SUPPORTING CRITICAL INFRASTRUCTURE SECTORS

CELR simulates scenarios from each of the 16 critical sectors. The CELR test range is capable of concurrently supporting multiple exercises and can demonstrate potential kinetic effects between sectors. CELR aligns with CISA's priorities and risk determination set by the CISA National Risk Management Center (NRMC).

CELR SCENARIO TOPICS



CELR USERS

CELR provides a research zone, permitting its users to simulate speculative risk scenarios that would otherwise introduce unacceptable risk to production environments. This laboratory environment provides opportunities for enhancing the way government and industry partners defend ICS networks. Potential users include, but are not limited to:

- Federal civilian agencies (e.g., Department of Energy [DOE], Department of Justice [DOJ], Department of the Interior [DOI])
- U.S. asset owner operators
- Vendors/integrators
- Department of Defense (DOD) Cyber Protection Teams (CPTs)
- National Security Agency (NSA)
- Academia researchers
- Third-party cyber firms and researchers
- International partners

CISA designed CELR with Critical Infrastructure partners in mind and to serve as many industry groups as possible. The range is a common environment where a variety of partners can research, learn, and share TTPs.

CELR CAPABILITIES

CELR enables hands-on research of sensitive systems. The core capabilities of the range include:

Study red team capabilities, techniques, artifacts, and impacts within specific network configurations

Enabling blue teams to hone defensive skills and develop new processes for detecting malicious cyber activity

Validate and understand the impact of vulnerabilities within ICS hardware and configurations

CELR notably differs from traditional Operational Technology (OT) ranges in its focus on ICS technologies and the ability to simulate cyberattacks carried out to the point of physical disruption and destruction. Unlike attack scenarios of traditional ranges, CELR-generated attack scenarios integrate kinetic motion to successfully account for infrastructural interdependencies across unique test scenarios. The capability to accurately respond in real time enables CELR to go beyond static simulation and support teams engaging across the entire cyberattack life cycle—from internet entry points to external demilitarized zone (DMZ), corporate Local Area Network (LAN), and ICS networks, and physical components.

CELR facilitates the user’s ability to study the interdependencies between processes as well as sectors, critical to strengthening the Nation’s collective defense against complex attacks—such as those seen during the HatMan, CrashOverride, and BlackEnergy campaigns—in an ever-evolving threat landscape. CELR allows users to encounter elements involving physical limitations of equipment, the magnitude of unrelated datasets, and to understand the associated second-order effects. This visibility provides responders key insights to better inform detection mechanisms and defensive strategies.

FOCUS AREA #1

INCIDENT RESPONSE

- Government
- Private Sector

USE CASE

Gaining visibility into threat activity, vulnerabilities, management risks, capacity deficiencies, and other risks

An incident response team is preparing to respond to reported threat actor behavior. The victim network configuration details are preloaded into a CELR test environment. A red team simulates the attack methodology known to be used by the suspected threat actor. Using CELR, the incident response team rehearses the deployment of their tools, refining the processes they will use, and identifying more effective methods for identifying the activity in the contested environment. As a result, once onsite, the team avoids pitfalls and isolates the threat actor more quickly, shortening the engagement and mitigating the impacts of the attacker.

Benefits

- PREPARE FOR AN ENGAGEMENT
- REPLAY AN ENGAGEMENT
- DEVELOP SKILLS
- ATTAIN GROUND TRUTH
- DEVELOP PROCESSES

FOCUS AREA #2

VULNERABILITY DISCOVERY

Government

Cyber Firms & Researchers

USE CASE

Recreating conditions, testing mitigations, and generating detection mechanisms

In response to a suspected vulnerability in a specific product line, a vulnerability researcher requests a CELR configuration reflective of industry and incorporating a specific product. The researcher verifies the suspected vulnerability but determines a number of environmental conditions that must be present for harm to occur. The same CELR environment is later used to validate the effectiveness of the patch provided by the vendor. As a result of using CELR in this vulnerability disclosure process, the public alert more accurately reflects the actual risk of the vulnerability and avoids assigning an over-inflated vulnerability score that causes undue alarm.

Benefits

- VULNERABILITIES
- VALIDATE VULNERABILITIES
- EVALUATE CAUSE AND EFFECT

FOCUS AREA #3

MITIGATION & PREVENTION

Asset Owners & Operators

Cyber Firms & Researchers

USE CASE

Taking actions to address the risks: prevention, response, mitigation, governance, and capacity building

A major U.S. utility company responsible for electric generation and distribution, as well as natural gas pipelines, works with CELR to configure a replica of their ICS network. The simulated network has a cyber monitoring and response configuration like their real-world environment. Using CELR, the utility company releases the latest ICS malware into the contained environment, monitoring the activity and impacts of the malicious code. They confirm their current tooling and analyst capabilities are effective at detecting the malware on their transmission network but identify concerns on their generation systems where the malware is able to propagate. In the simulation, two of the turbines within the primary generation plant exceed maximum rotational speed and are destroyed. The results of this test environment scenario give the utility the necessary documentation and understanding to gain stakeholder support to acquire and implement the necessary mitigation controls to protect against a real-world attack.

Benefits

- CYBER THREAT INFORMATION SHARING
- GOVERNANCE, CAPACITY BUILDING, AND ARCHITECTURE
- SIMULATE HIGH-IMPACT SCENARIOS
- CYBER TEAM SKILLS DEVELOPMENT

FOCUS AREA #4

IMPACT AND CONSEQUENCE ANALYSIS

Government

Private Sector

USE CASE

Calculating the costs of cyber physical attacks and measuring the performance of mitigations

An industry consortium is struggling to understand the level of disruption and/or destruction that could occur as a result of cyberattack. A CELR environment is developed, baselined against a configuration validated by asset owner operators. Using this network as a target, red teams infiltrate, transverse, and compromise critical components of the physical processes. Shown both in real-time as well as captured in recorded format, CELR is used to demonstrate both significant process disruption and destruction to asset owners, industry oversight, regulators, legislators, and financial investors of both the seriousness of cyber attack as well as the viability of various mitigations to reduce the overall risks.

Benefits

- ANALYZE SECTOR DEPENDENCIES
- CALCULATE IMPACT AND RISK
- DEMONSTRATE KINETIC CONSEQUENCES

CELR Timeline

		PHASE 1 Current Capabilities	PHASE 2 Next 12 Months	PHASE 3 3-5 Years
# of Simultaneous Simulations		2	4	7
Simulations per Year		20	50	200+
PARTICIPANTS	CISA - Glebe	X	X	X
	CISA - Idaho	X	X	X
	CISA - Pensacola		X	X
	Federal Civilian Agencies		X	X
	DOD CPT Teams		X	X
	U.S. Asset Owner Operators		X	X
	Vendors/Integrators			X
	Academia			X
	Third-party Cyber Firms and Researchers			X
	International Partners			X
LOCATIONS	CISA - Glebe	X	X	X
	CISA - Idaho	X	X	X
	CISA - Pensacola			X
	Other FFRDC Locations		X	X
	Academia Collaborations			X
	Private Entities			X
	Remote Participant Access		X	X
	Remote Skid (Persistent)			X
CORPORATE ENIVIRONMENT	Small Corporation	X	X	X
	Utility Cooperative		X	X
	Typical Federal Agency	X	X	X
	Typical SLTT		X	X
	Typical Academia		X	X
	Replicate Actual Network (Low Fidelity)		X	X
	Replicate Actual Network (High Fidelity)			X

CELR Timeline

		PHASE 1 Current Capabilities	PHASE 2 Next 12 Months	PHASE 3 3-5 Years
PARTICIPANTS	Internal LAN	X	X	X
	Simulated Internet		X	X
	Wi-Fi	X	X	X
	4G		X	X
	5G		X	X
	Unlicensed Radio		X	X
	Licensed Radio		X	X
	Microwave			X
	Satellite			X
	Cloud (simulated)		X	X
	Cloud (3rd Party)		X	X
	Actual Internet			X
SECTORS WITH KINETIC SKIDS	Chemical	X	X	X
	Commercial Facilities	X	X	X
	Communications			X
	Critical Manufacturing			X
	Dams		X	X
	Defense Industrial Base			X
	Emergency Services			X
	Electric Generation			X
	Electric Transmission	X	X	X
	Electric Distribution	X	X	X
	Oil and Natural Gas			X
	Financial Services			X
	Food and Agriculture			X
	Government Facilities			X
	Healthcare			X
	Information Technology			X
	Nuclear			X
	Aviation			X
	Automotive			X
	Pipeline	X	X	X
	Rail		X	X
	Maritime			X
	Water and Wastewater		X	X

Frequently Asked Questions

1 Is CELR a Capture the Flag experience?

No, although there are similarities. CELR replicates a realistic configuration (specifically filled with significant benign processes and traffic) and places network defenders in a scenario very similar to what they would experience in the real world. The focus of CELR simulations is focused on blue teams where defenders are asked to find their own way in triaging, containing, and restoring services across the entire network. No specific flags are planted, and teams should expect a very realistic (i.e. frustrating) experience.

2 Can CELR be customized with specific configurations?

Yes. Requests for specific configurations, equipment, and TTPs can be accommodated. However, the time required to integrate these requests as well as funds to procure equipment may delay the time to execute the activity.

3 Can 3rd parties bring their own tools and equipment?

Yes, within reason. We encourage parties to bring new tools, infrastructure, and other elements to increase the learning of your team as well as ours. This process takes time, so engage with us early to get the process started. If this integration is something of high value for others, consider becoming a CELR partner and integrating the infrastructure permanently within our facilities or yours.

4 Who gets priority for CELR resources?

The front-line defenders mostly likely to be targeted by our enemies get the highest priority. This determination is made given considerations for sector, threats, configuration, and the value of the 3rd party to the national defense effort.

5 Who paid for CELR?

The initial funding for CELR was paid for by U.S. taxpayer dollars. Federal funding continues to be used to maintain the CELR capability. We are currently working to develop necessary processes to establish partnerships by which others can contribute infrastructure to the CELR environment as they gain access to the overall effort.

6 Is CELR successful?

We believe the answer is yes. Already we have seen a marked improvement in incident response team capabilities and effectiveness within the federal government. We have tested tools and processes in a contained environment that reduced risk when used on live infrastructure. We have replicated tactics seen during the Russian Government's targeting of US Critical Infrastructure, and refined detections and mitigations to be more effective. We believe this is just the beginning with lots more to come.

3 Things You Need to Know

GETTING **INVOLVED**

CELR is managed by CISA Threat Hunting. Email **HIRT_ICSG@cisa.dhs.gov** to get started.

REMOTE **ACCESS**

Some CELR capabilities can be accessed remotely, eliminating the need for travel. Ask for details.

HIGH **FIDELITY**

CELR is designed to present real-world environments. Defenders must sort through mountains of benign data. Red teams must navigate through configurations and defensive tools taken straight from the field. Kinetic consequences occur when breakers pop, motors spin the wrong direction, chemicals get pumped into the wrong tanks, and PLCs get bricked.

CYBER PHYSICAL SYSTEMS

CONTROL ENVIRONMENT
LABORATORY RESOURCE (CELR)