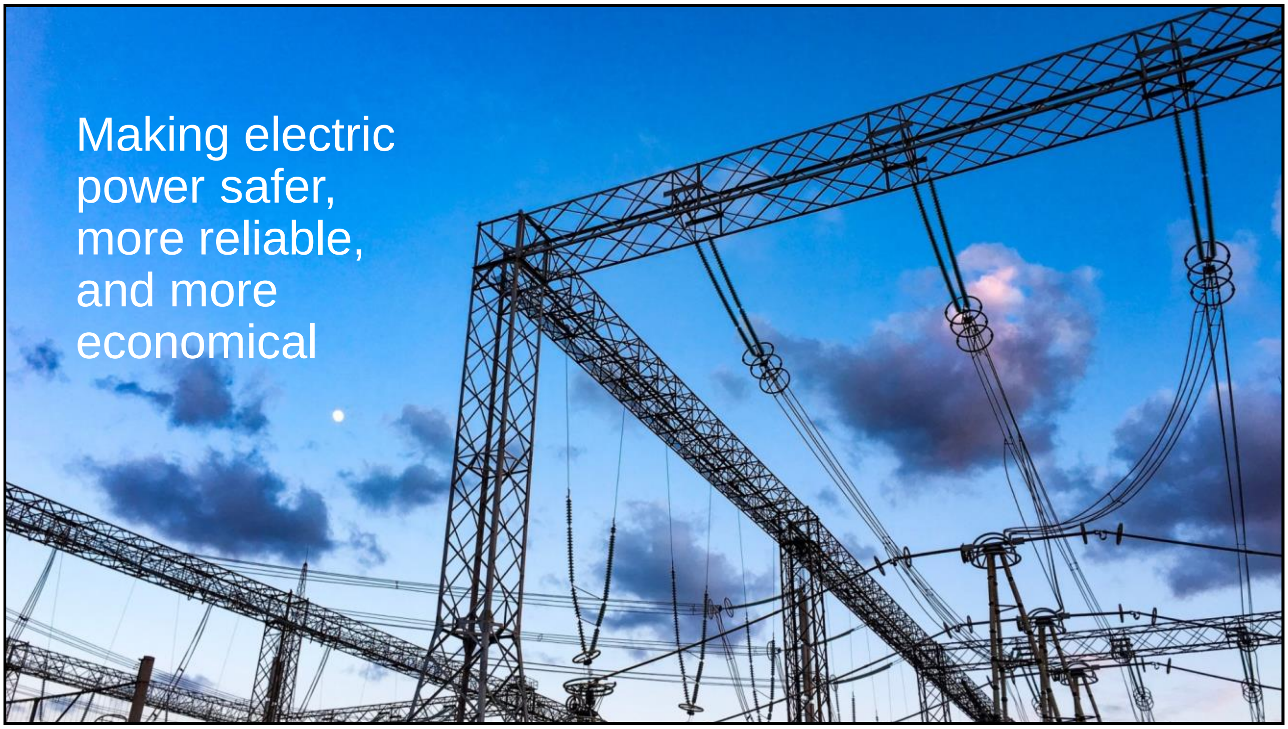
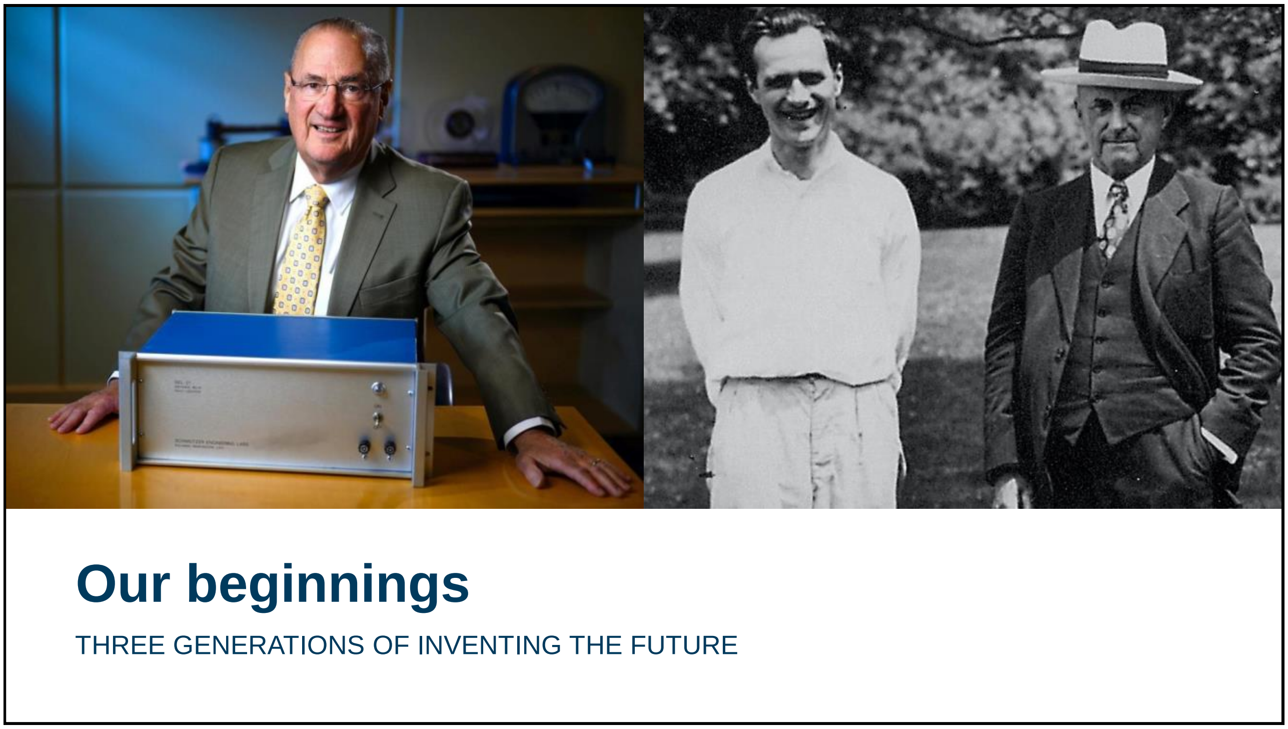
OT cybersecurity system with SEL technology and expertise

SEL

SEL corporate overview



Making electric power safer, more reliable, and more economical



Our beginnings

THREE GENERATIONS OF INVENTING THE FUTURE

From 1982…

Founded by Dr. Schweitzer,
in **1982**

Released world's first digital protective relay, the **SEL-21**,
in **1984**

…to now

4 electronic device factories

166 countries with SEL products

107 sales and support offices

5,300 employees around the world

Edmund O.
SCHWEITZER, III

Digital Protective Relay

National Inventors
Hall of Fame

We **invent**, **design**, **build**, and **support**
solutions that protect and control power systems

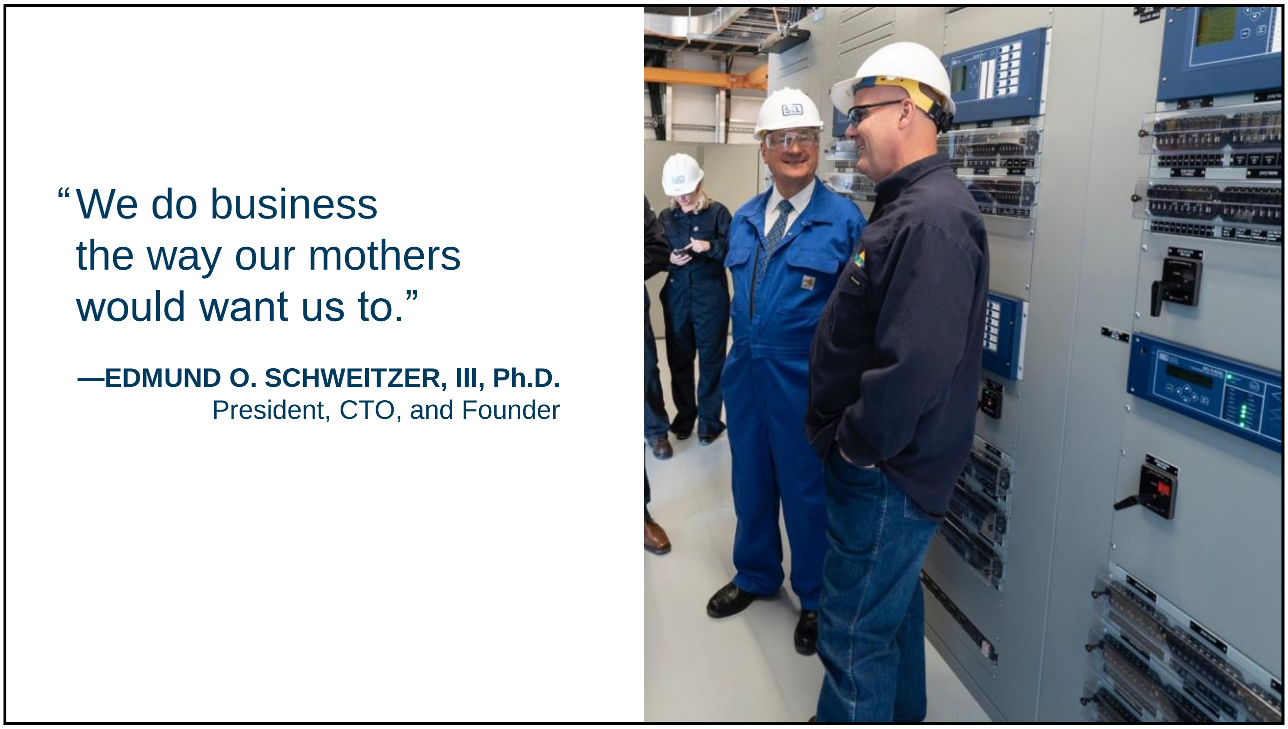
We provide **end-to-end solutions**

Computing Protection/control Software Automation Communications Training

Security for critical infrastructure Engineering services Precise time Metering

100% employee-owned

SO WE CAN PUT OUR CUSTOMERS FIRST



> "We do business the way our mothers would want us to."

—EDMUND O. SCHWEITZER, III, Ph.D.
President, CTO, and Founder

WE LIVE OUR VALUES

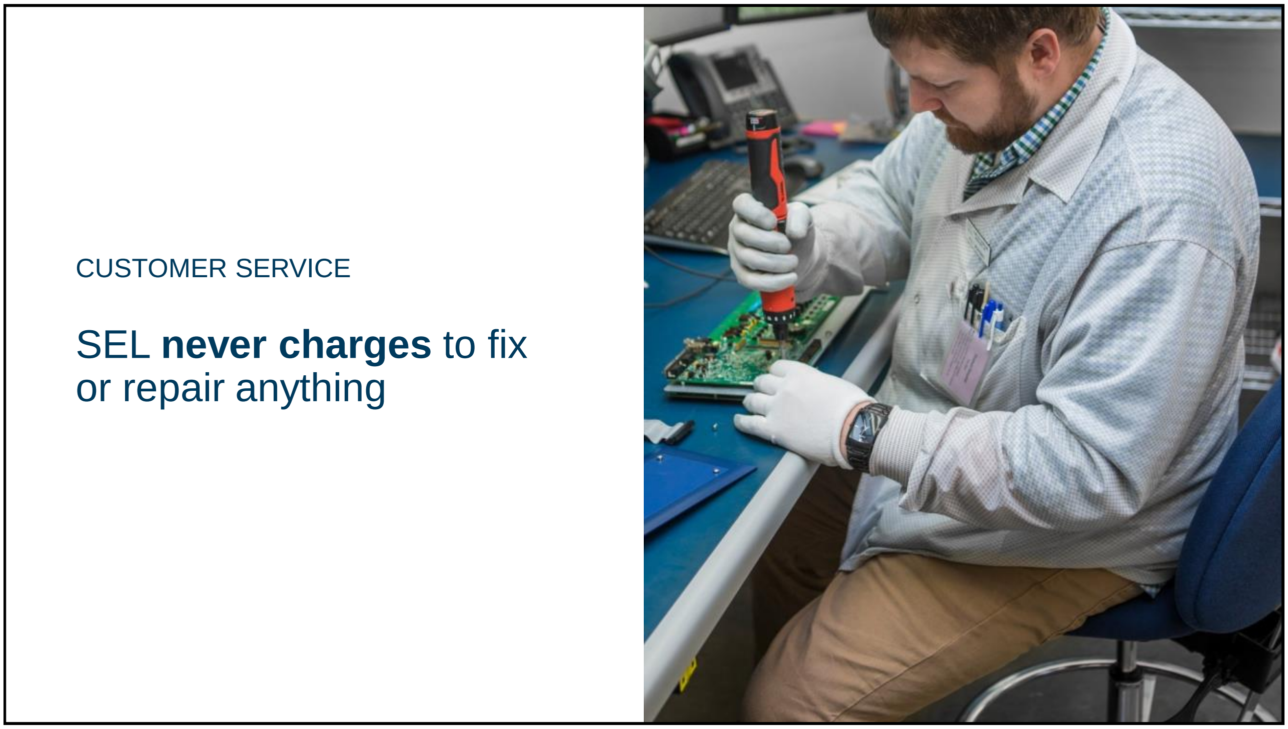
Quality
Customer focus
Discipline
Communication
Integrity
Creativity
Community
Ownership
Dignity of work

CUSTOMER SERVICE

No-questions-asked **warranty** is included for all SEL products

CUSTOMER SERVICE

SEL Product Hospital responds to **each returned product** quickly

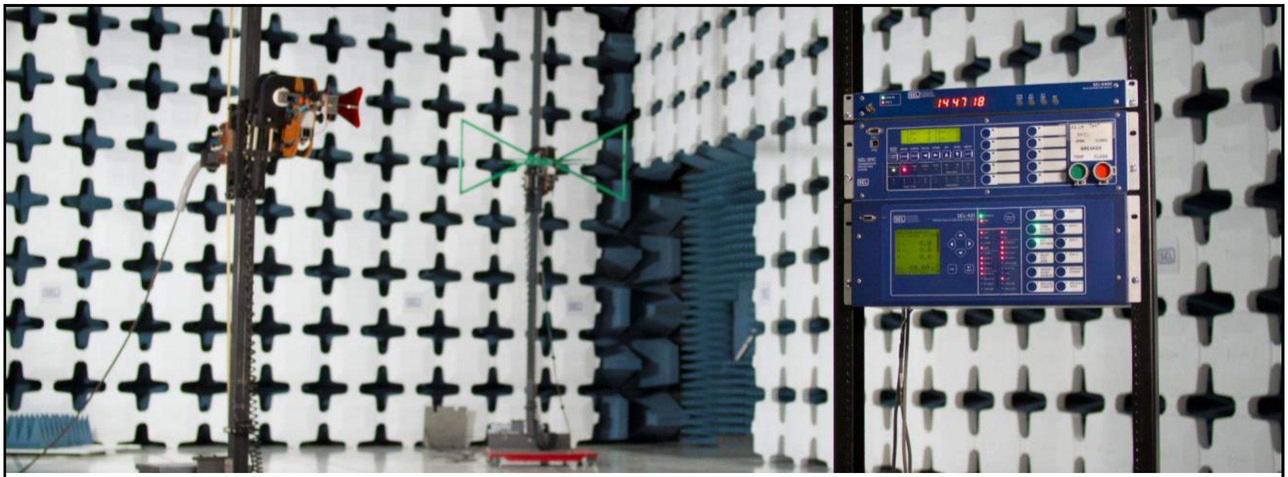


CUSTOMER SERVICE

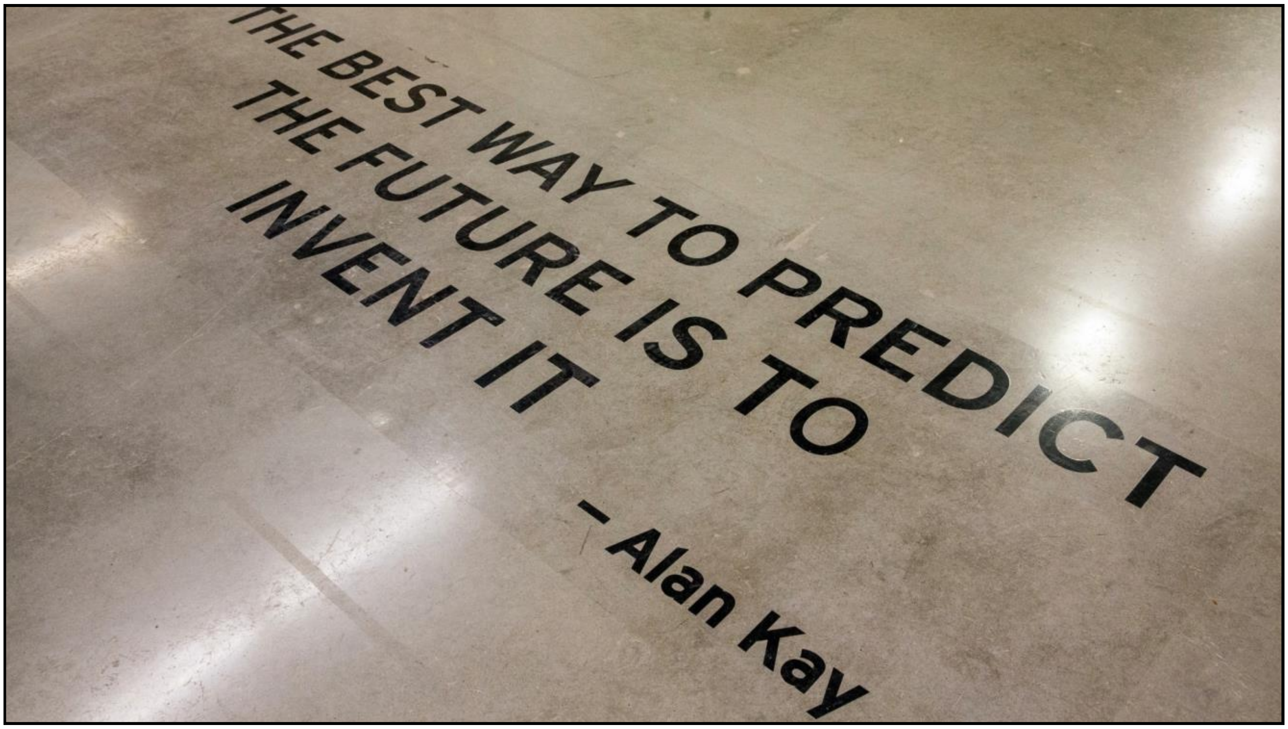
SEL **never charges** to fix or repair anything

CUSTOMER SERVICE

If we cannot fix it,
SEL replaces unit for free



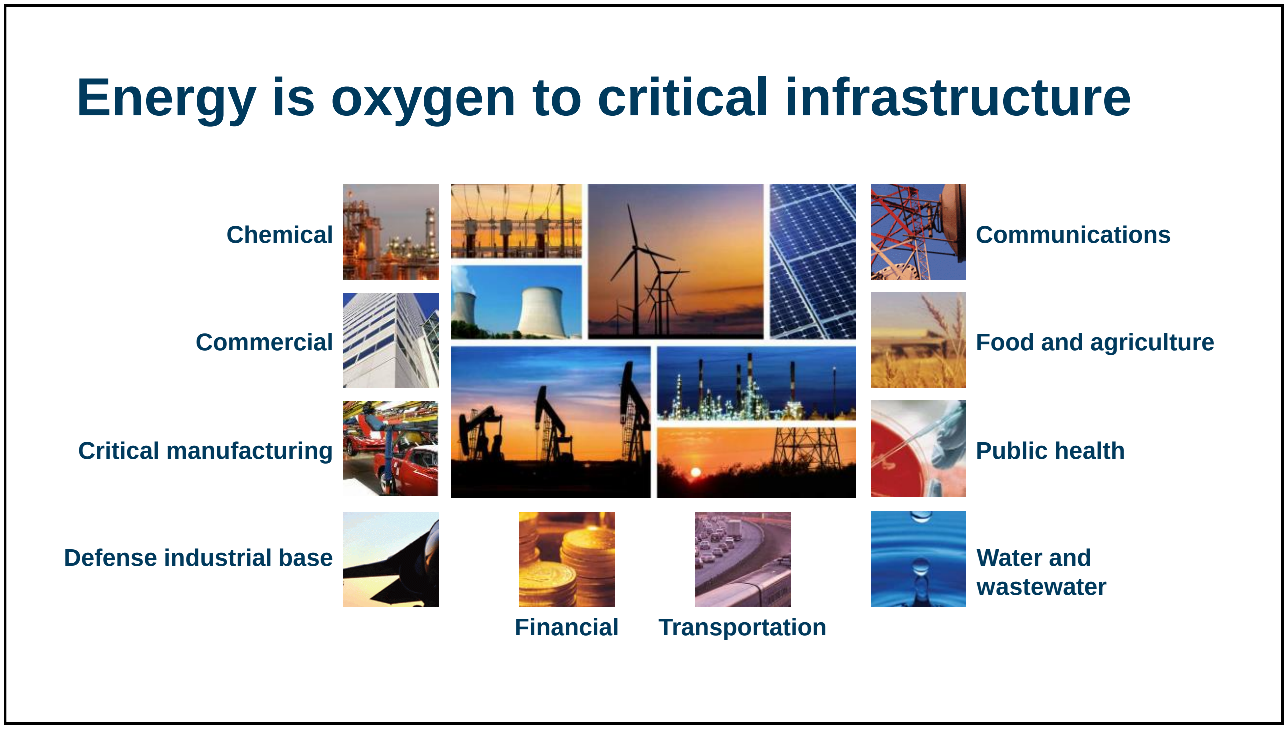
We build **quality** and **reliability** into
our products by designing for simplicity



Holistic look at competing risks

Overview – learning objectives

- Risk is always evolving and requires continuous monitoring and improvement
- Risk decisions must be made with finite amount of time, money, and people
- Risk must be looked at holistically (**never** put cyber in a silo)
- Including security in design reduces total cost of ownership and significantly reduces most risk



Energy is oxygen to critical infrastructure

Chemical

Commercial

Critical manufacturing

Defense industrial base

Financial

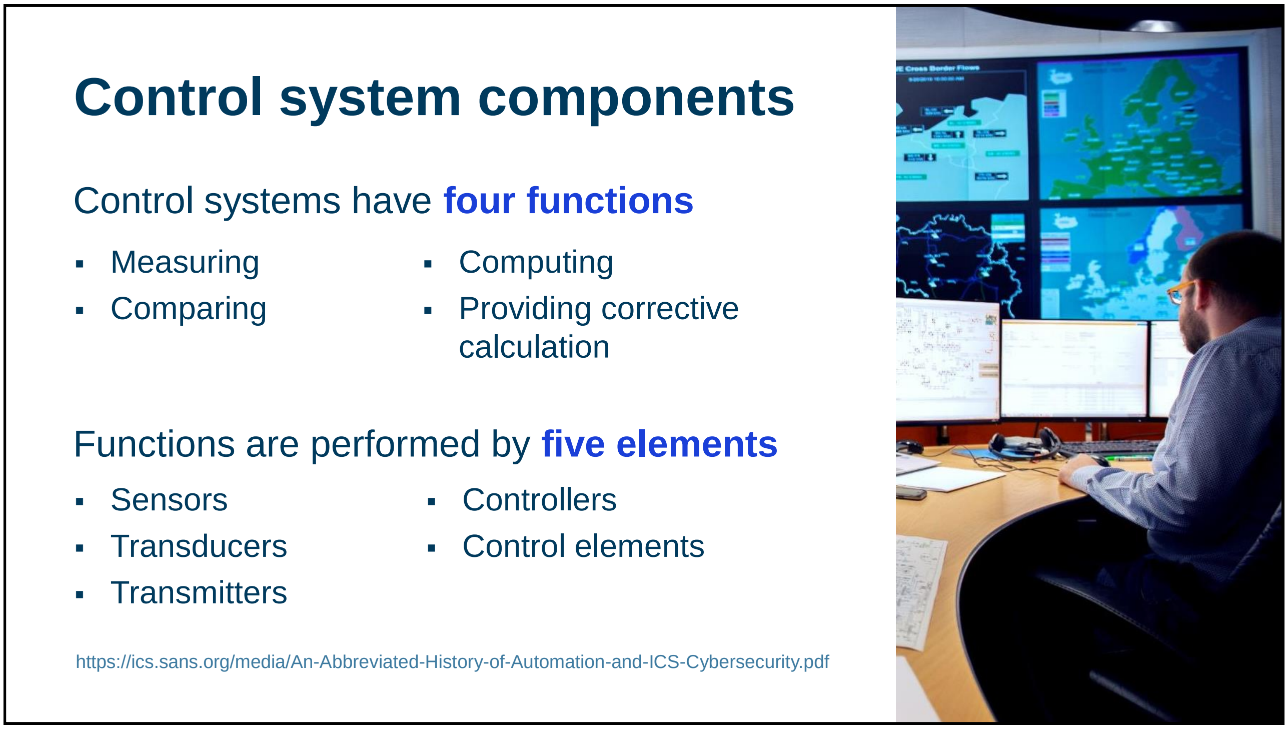
Transportation

Communications

Food and agriculture

Public health

Water and wastewater



Control system components

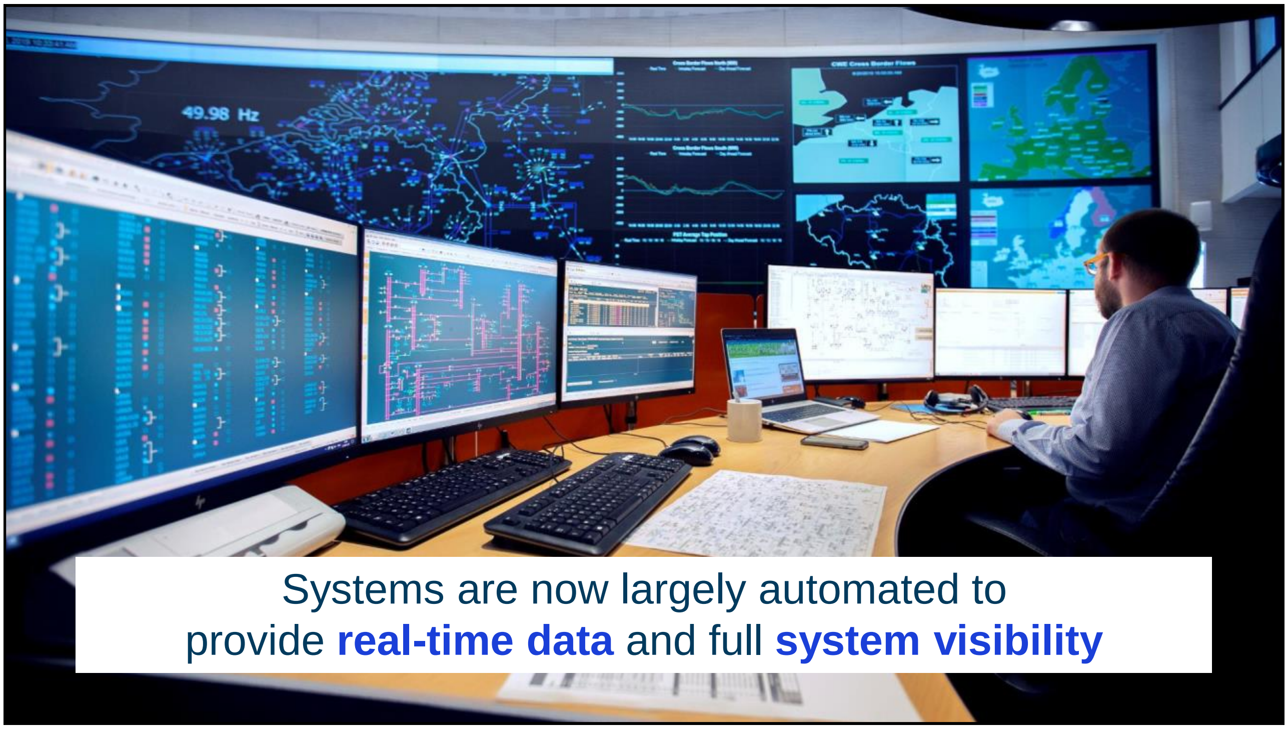
Control systems have **four functions**

- Measuring
- Comparing
- Computing
- Providing corrective calculation

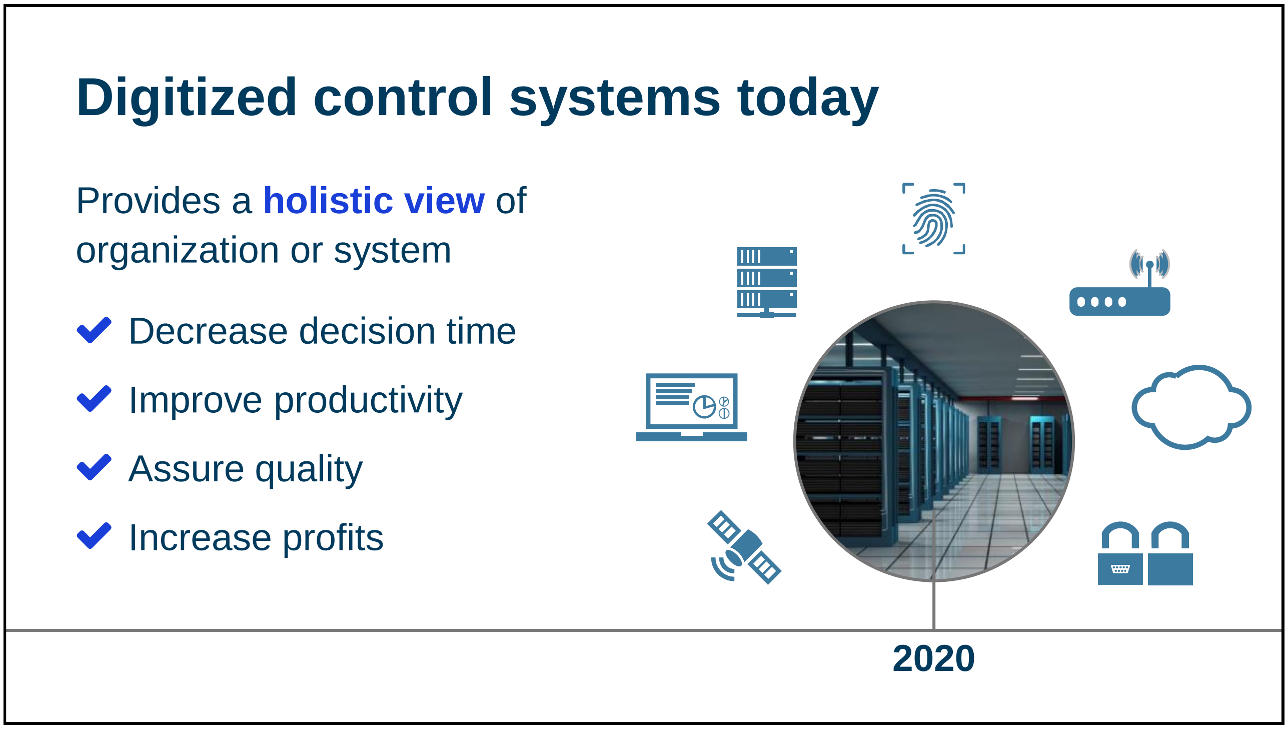
Functions are performed by **five elements**

- Sensors
- Transducers
- Transmitters
- Controllers
- Control elements

https://ics.sans.org/media/An-Abbreviated-History-of-Automation-and-ICS-Cybersecurity.pdf



Systems are now largely automated to
provide **real-time data** and full **system visibility**



Digitized control systems today

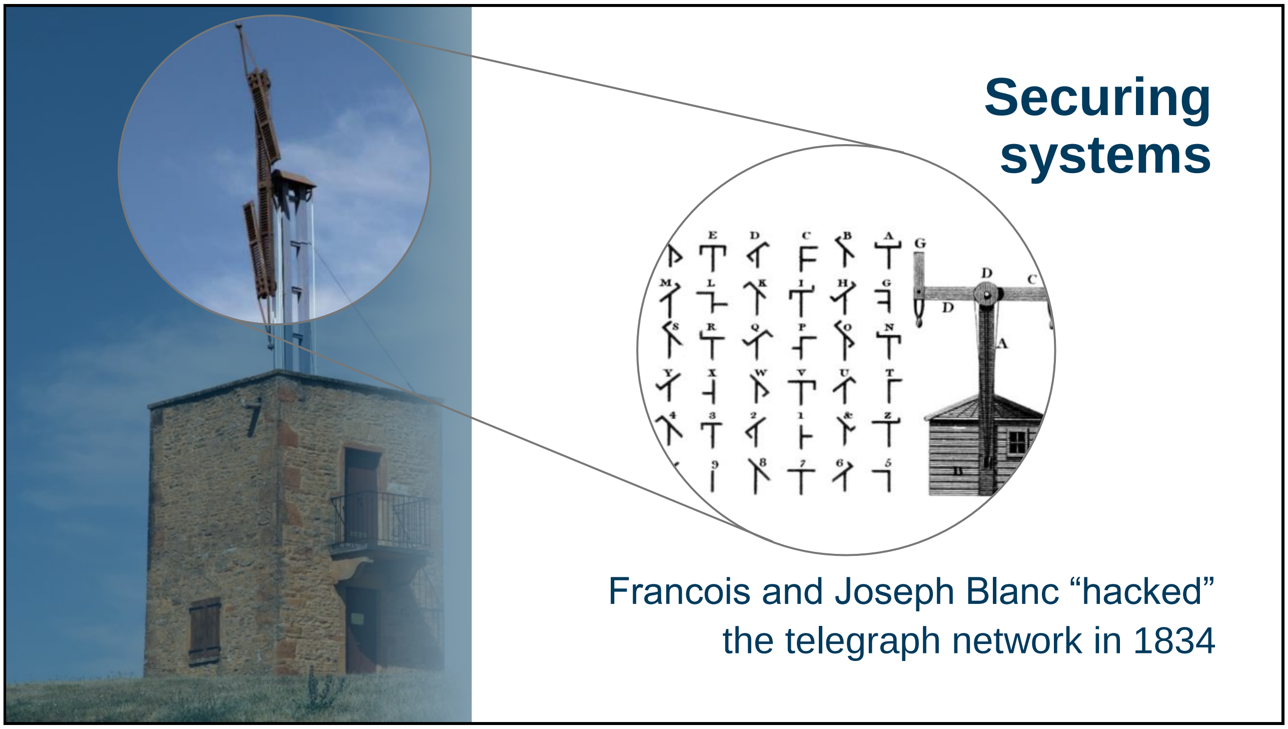
Provides a **holistic view** of organization or system

✓ Decrease decision time

✓ Improve productivity

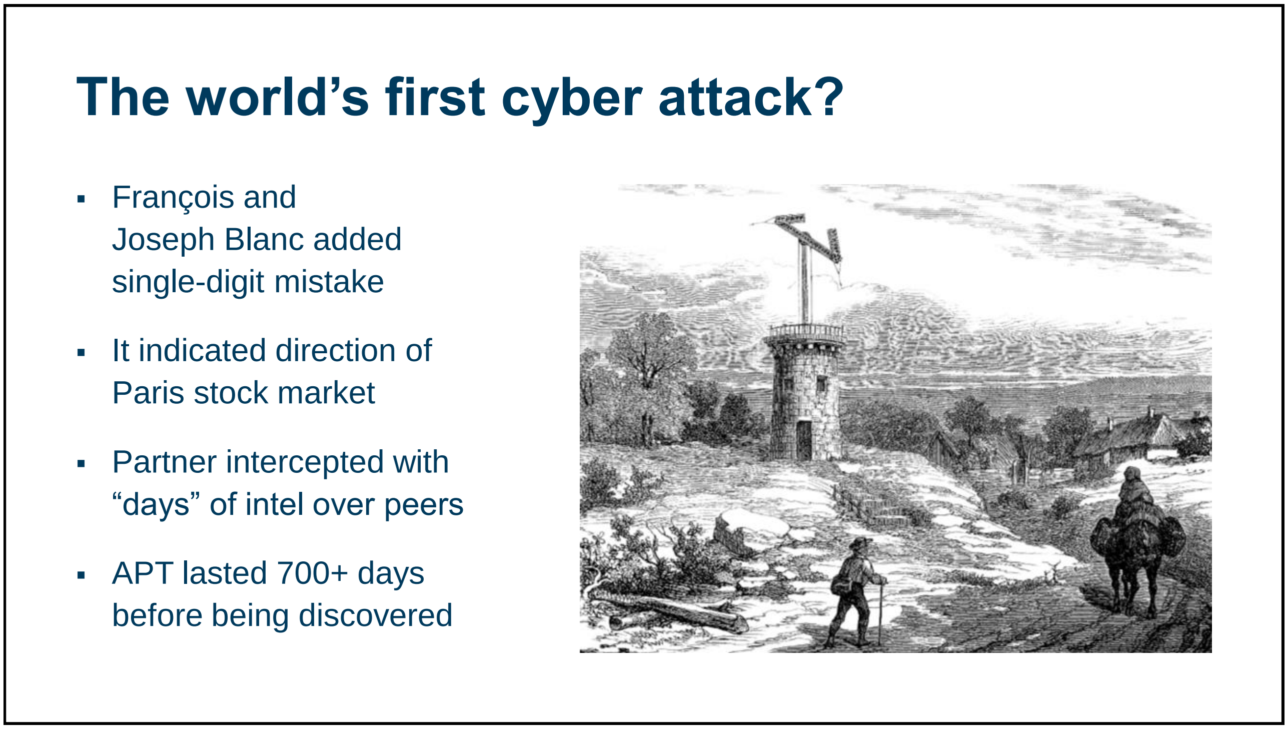
✓ Assure quality

✓ Increase profits



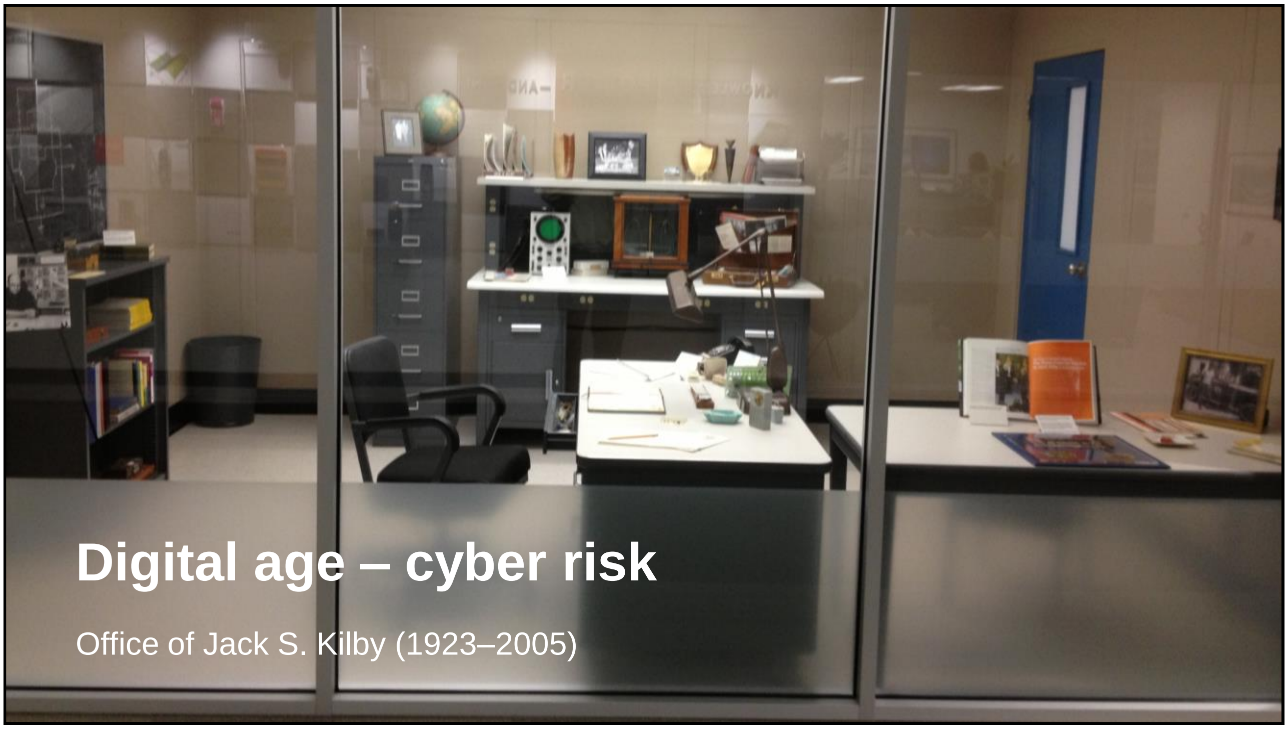
Securing systems

Francois and Joseph Blanc “hacked” the telegraph network in 1834



The world’s first cyber attack?

- François and Joseph Blanc added single-digit mistake
- It indicated direction of Paris stock market
- Partner intercepted with “days” of intel over peers
- APT lasted 700+ days before being discovered



Digital age – cyber risk

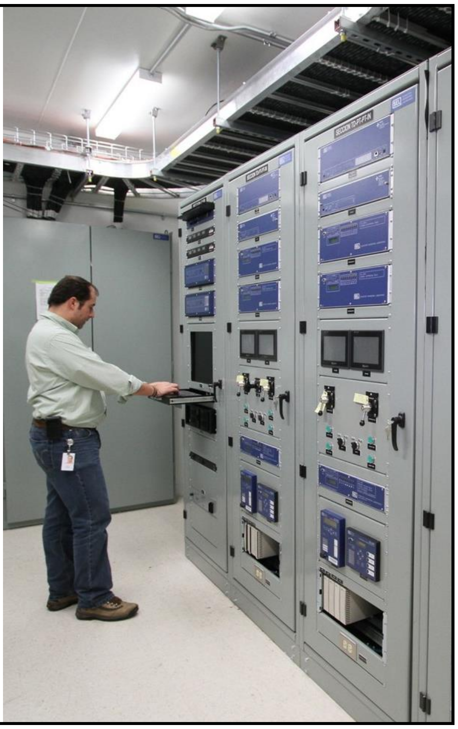
Office of Jack S. Kilby (1923–2005)

Cybersecurity challenges

- Industrial control equipment has a lifetime measured in decades
- Updates are expensive and increase operational risk
- Systems need high availability and usability
- Cultural differences exist between workers on IT and OT

Terms and definitions

- Risk
- Vulnerability
- Threat
- Exposure
- Exploit
- Mitigation (Security control)



Risk

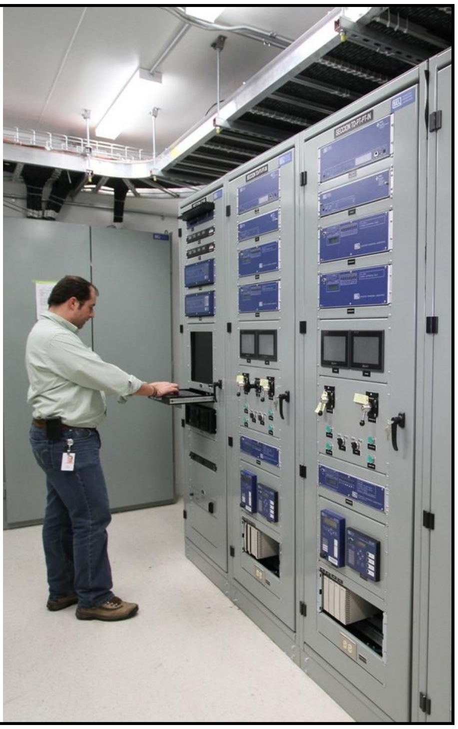
Noun

Potential of loss within situation

> ***There is risk to life when crossing the street***

Verb

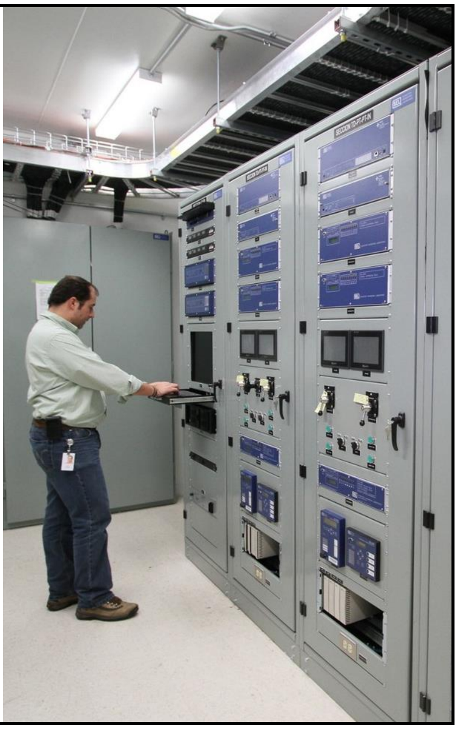
Expose to loss, hazard, or threat



Threat

Noun

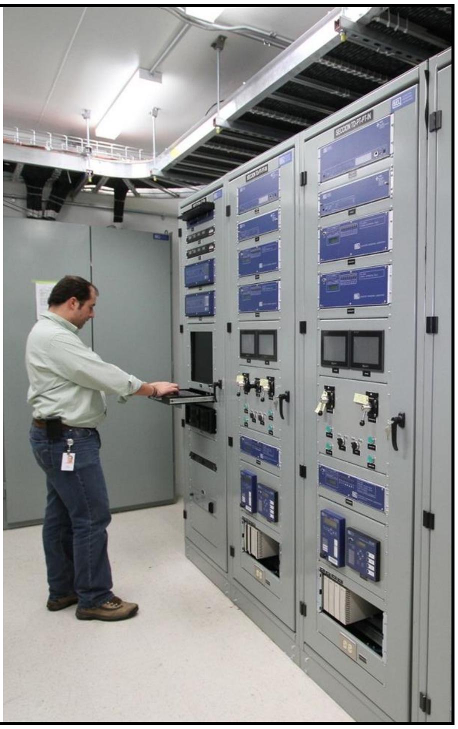
Exploits a vulnerability/weakness in a system to cause damage or loss



Vulnerability

Noun

Weakness or defect in a system making it susceptible to a threat agent, increasing risk



Exposure

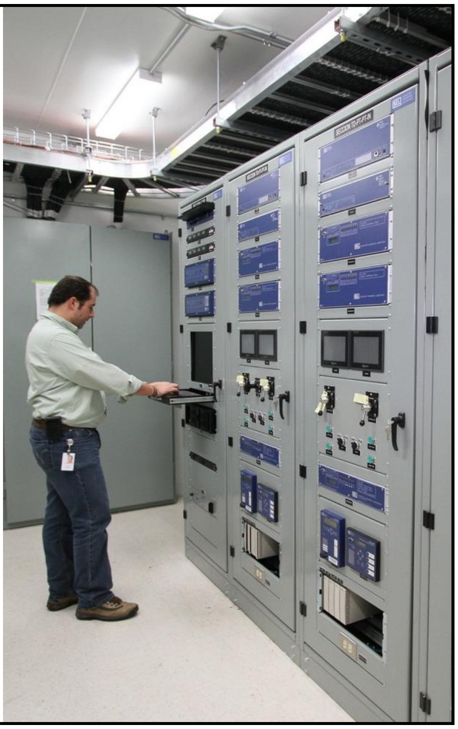
Noun

Subjected or revealed to another

Exploit

Noun

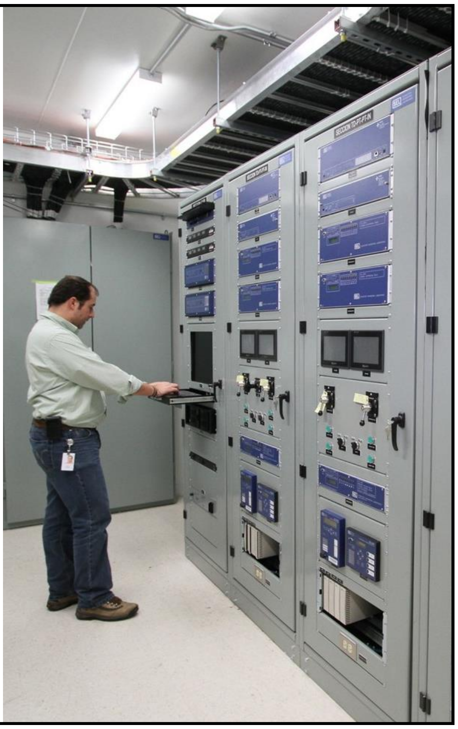
Mechanism to employ a flaw
or weakness



Mitigation

Noun

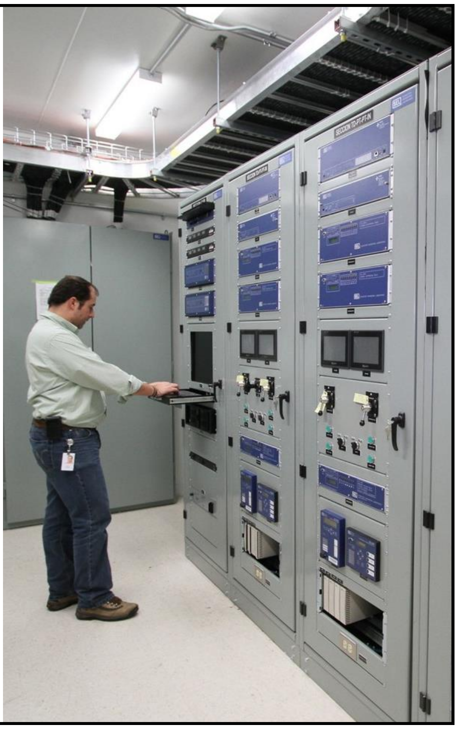
Alleviates a vulnerability or
deters a threat reducing risk



Risk – term used in

- Finance and economics
- Insurance
- Life Safety
- Organizational security

```
Risk = Loss * Likelihood
```



No silver bullet in risk or cyber

Silver bullet – something that provides an immediate and extremely effective solution to a given problem or difficulty, especially one that is normally very complex or hard to resolve

Every action to reduce risk increases the time, talent, and cost for an adversary to reach their end state

Not just a technology problem

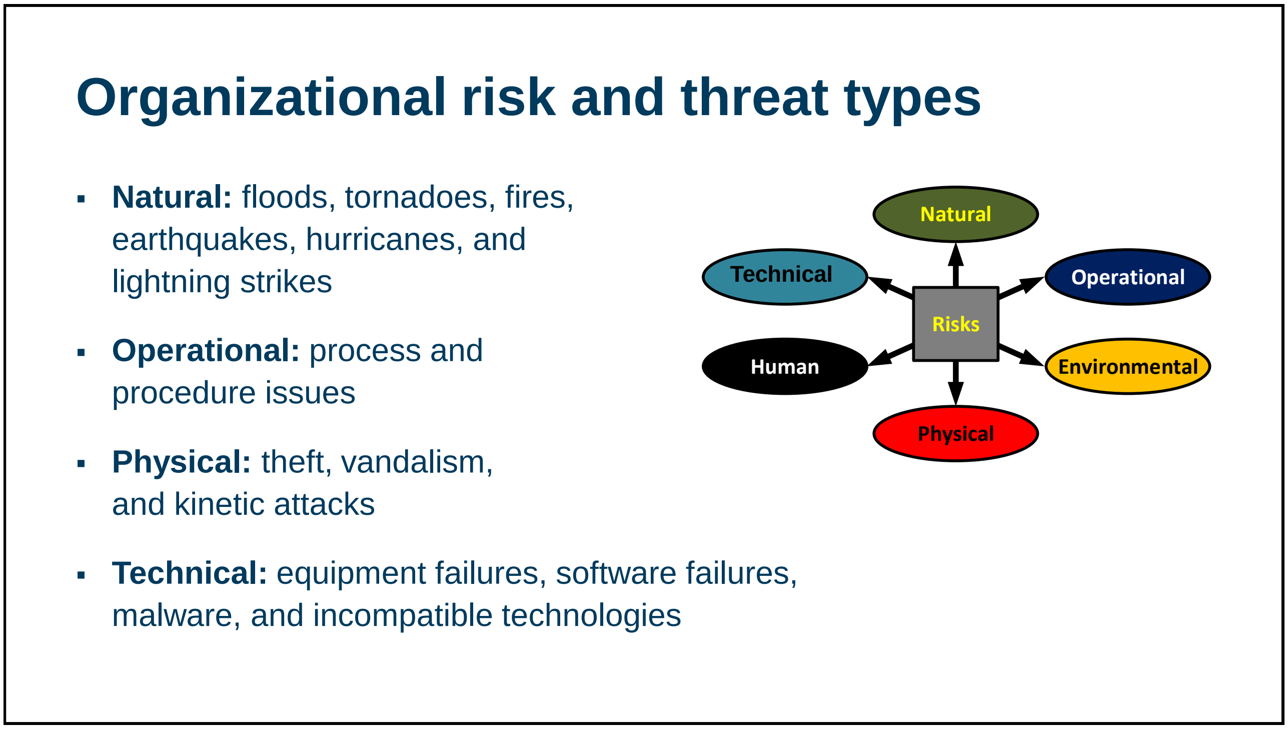
- Note that it is C-Suite driven
- Incorporate importance into plans, policies, and procedures
- Have training and awareness program
- Bypass technology – direct to human

Never put cyber dollars in a silo

- Realize organizations have competing risks – **all are important!**
- Perform business impact analysis
- Must prioritize all risks and make risk-based decisions
- Recognize competing finite resources of **time** vs. **talent** vs. **dollars**

Ultimately, this is a C-Suite decision

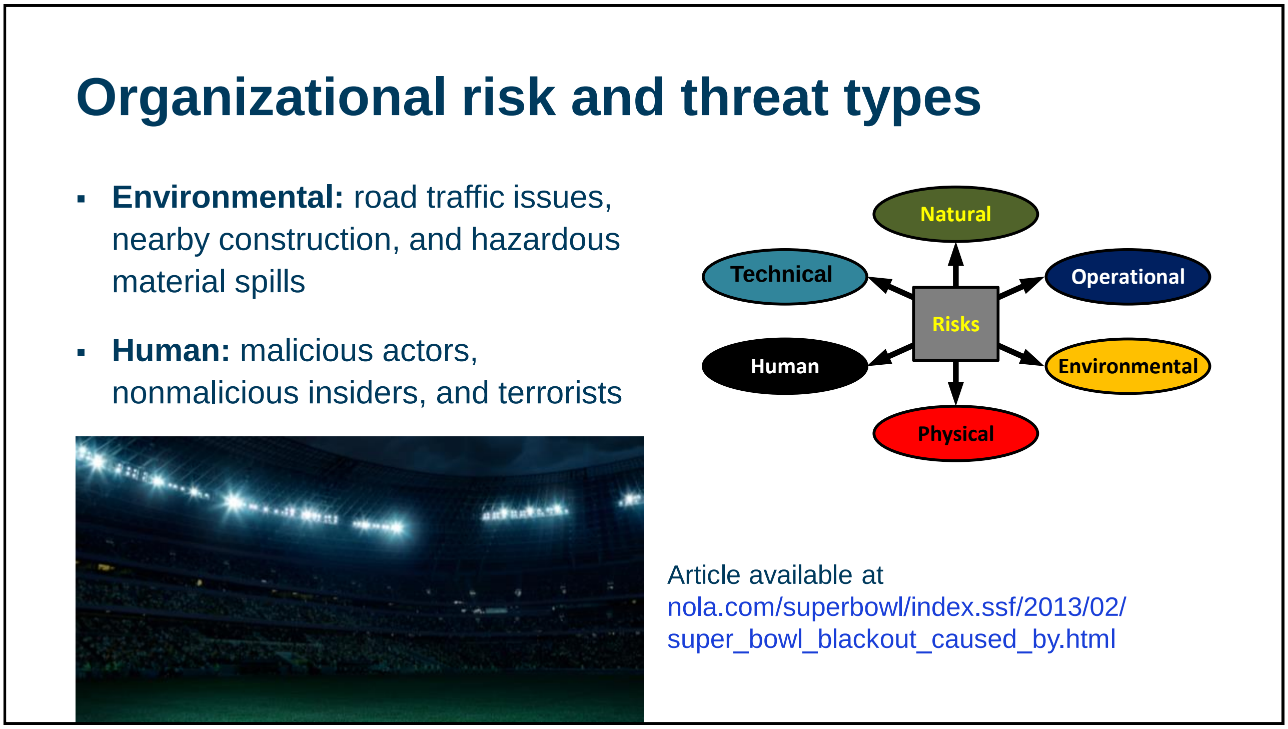
Cyber risk makes it difficult to calculate return on investment



Organizational risk and threat types

- **Natural:** floods, tornadoes, fires, earthquakes, hurricanes, and lightning strikes
- **Operational:** process and procedure issues
- **Physical:** theft, vandalism, and kinetic attacks
- **Technical:** equipment failures, software failures, malware, and incompatible technologies

Natural
Technical
Operational
Risks
Human
Environmental
Physical

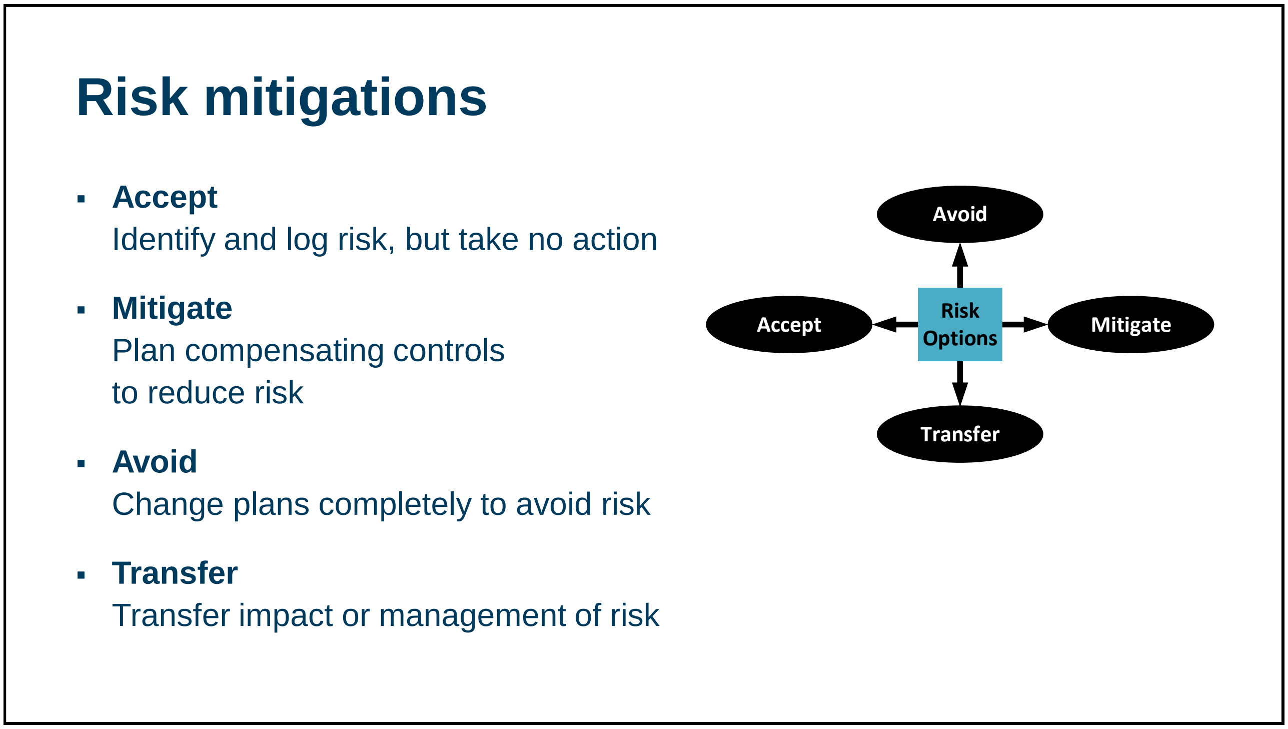


Organizational risk and threat types

- **Environmental:** road traffic issues, nearby construction, and hazardous material spills
- **Human:** malicious actors, nonmalicious insiders, and terrorists

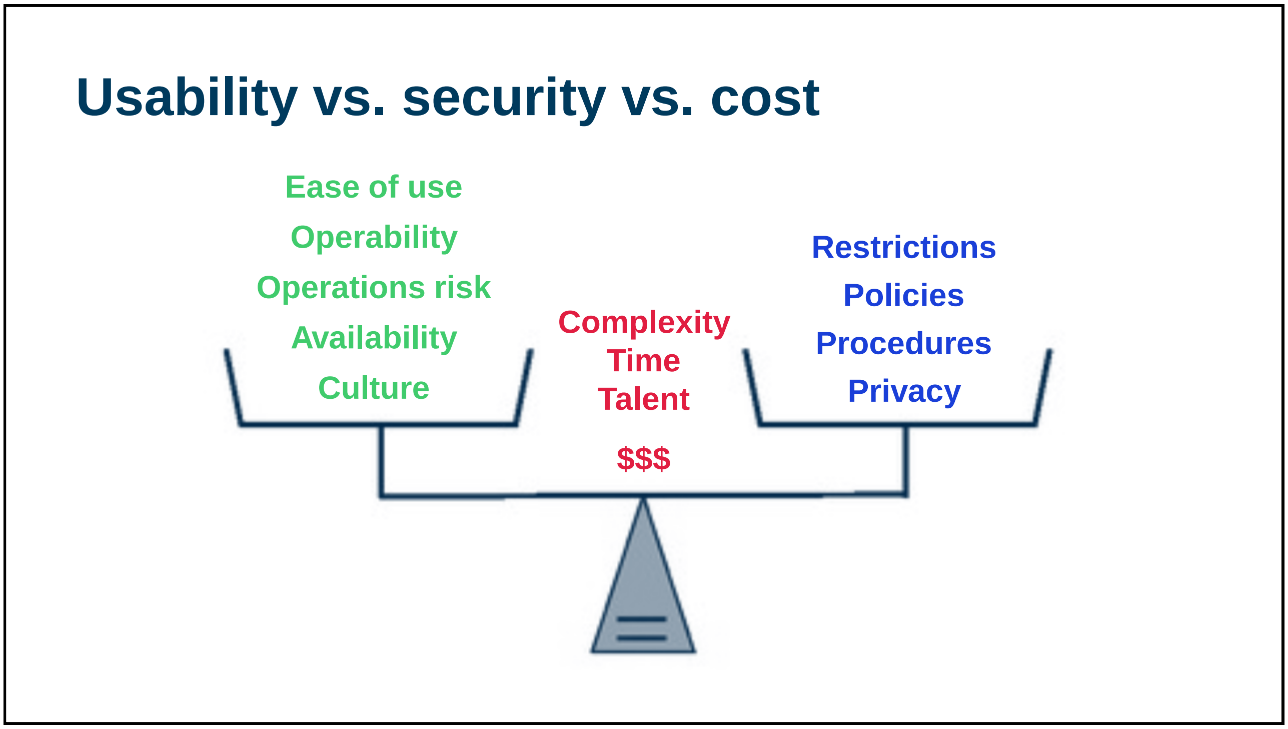
Natural
Technical
Operational
Risks
Human
Environmental
Physical

Article available at nola.com/superbowl/index.ssf/2013/02/super_bowl_blackout_caused_by.html



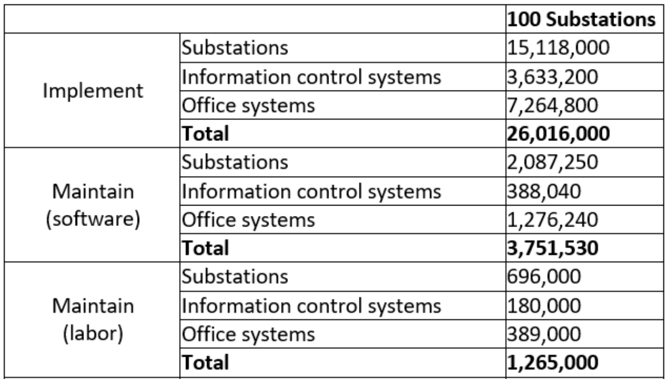
Risk mitigations

- **Accept**
  Identify and log risk, but take no action
- **Mitigate**
  Plan compensating controls
  to reduce risk
- **Avoid**
  Change plans completely to avoid risk
- **Transfer**
  Transfer impact or management of risk



Usability vs. security vs. cost

European TSO case study



		100 Substations
Implement	Substations	15,118,000
	Information control systems	3,633,200
	Office systems	7,264,800
	Total	**26,016,000**
Maintain (software)	Substations	2,087,250
	Information control systems	388,040
	Office systems	1,276,240
	Total	**3,751,530**
Maintain (labor)	Substations	696,000
	Information control systems	180,000
	Office systems	389,000
	Total	**1,265,000**

€26M Design to commission

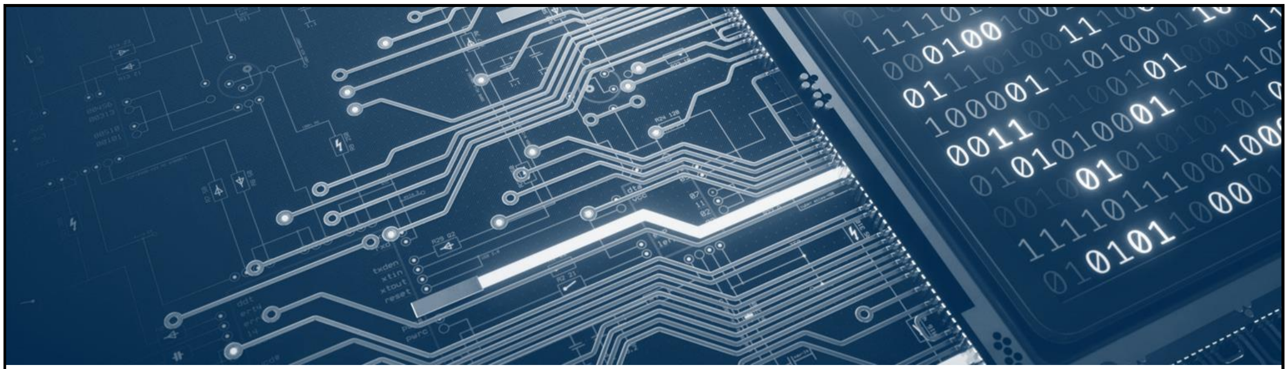
€5M Maintenance and labor

Cost of implementing cybersecurity is based on EU Emerging Security Standards (2015)

In a well-designed system, the adversary must get EVERYTHING done perfectly to not get caught and reach an impact

Final thoughts

- Risk is always evolving and requires continuous monitoring and improvement
- Risk decisions must be made with finite amount of time, money, and people
- Risk must be looked at holistically (**never** put cyber in a silo)
- Including security in design reduces total cost of ownership and significantly reduces most risk

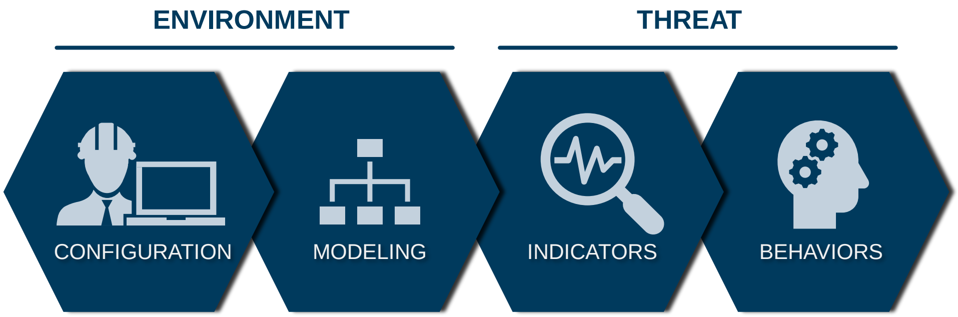


Threat landscape – continuous understanding and monitoring

Digital transformation of industrial control system has increased risk to civilization

Information technology (IT) methods jeopardize operational technology (OT) control systems

The four types of threat detection



ENVIRONMENT

THREAT

CONFIGURATION

MODELING

INDICATORS

BEHAVIORS

ICS/OT cybersecurity challenges

Asset visibility

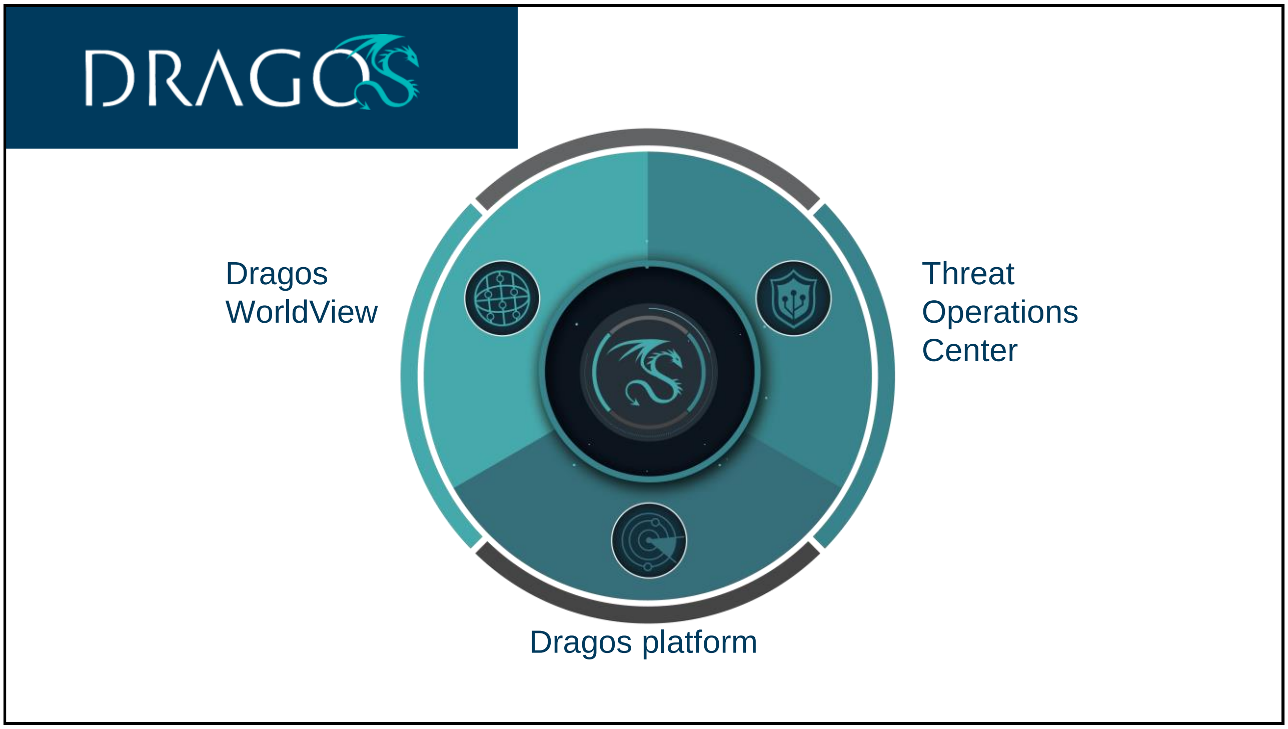
What's on my network? How has it changed over time?

Threat visibility

Am I compromised? How do I respond?

Limited personnel and skillsets

What training do we need?
How do I converge IT and OT?



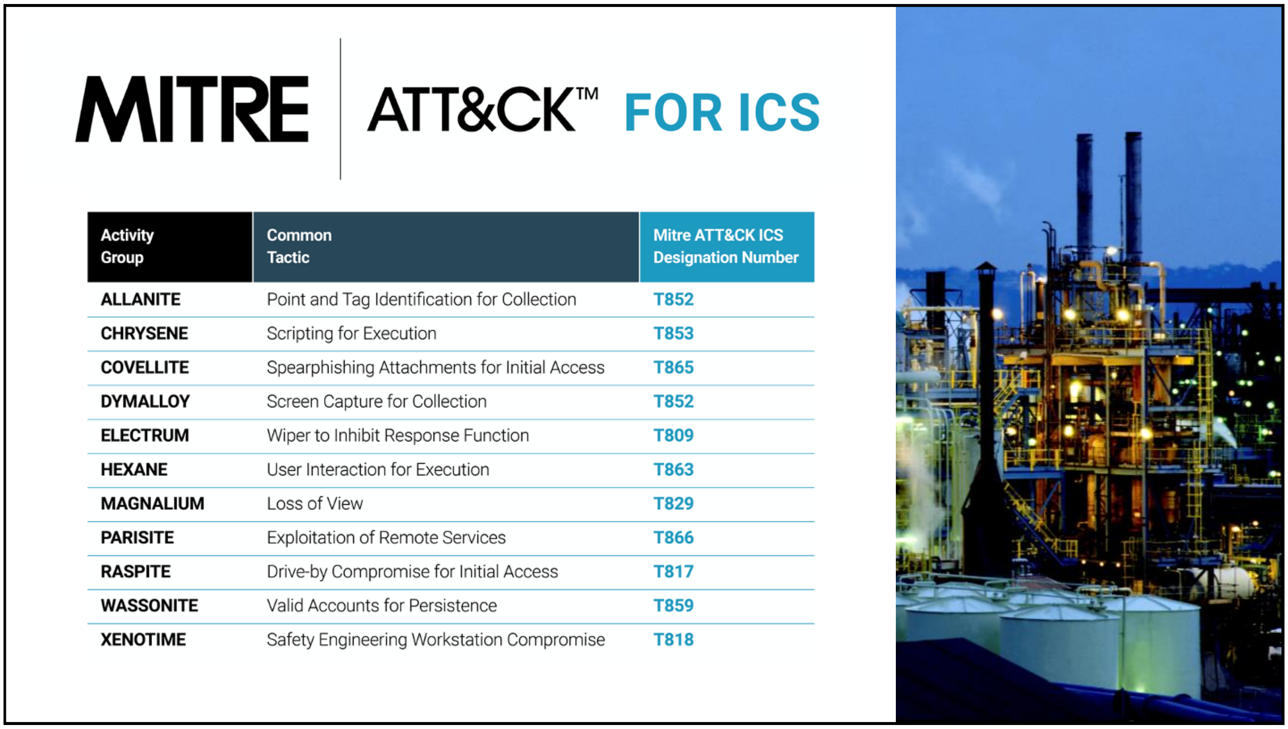
DRAGOS

Dragos WorldView

Threat Operations Center

Dragos platform

Threat Activity Groups



MITRE | ATT&CK™ FOR ICS

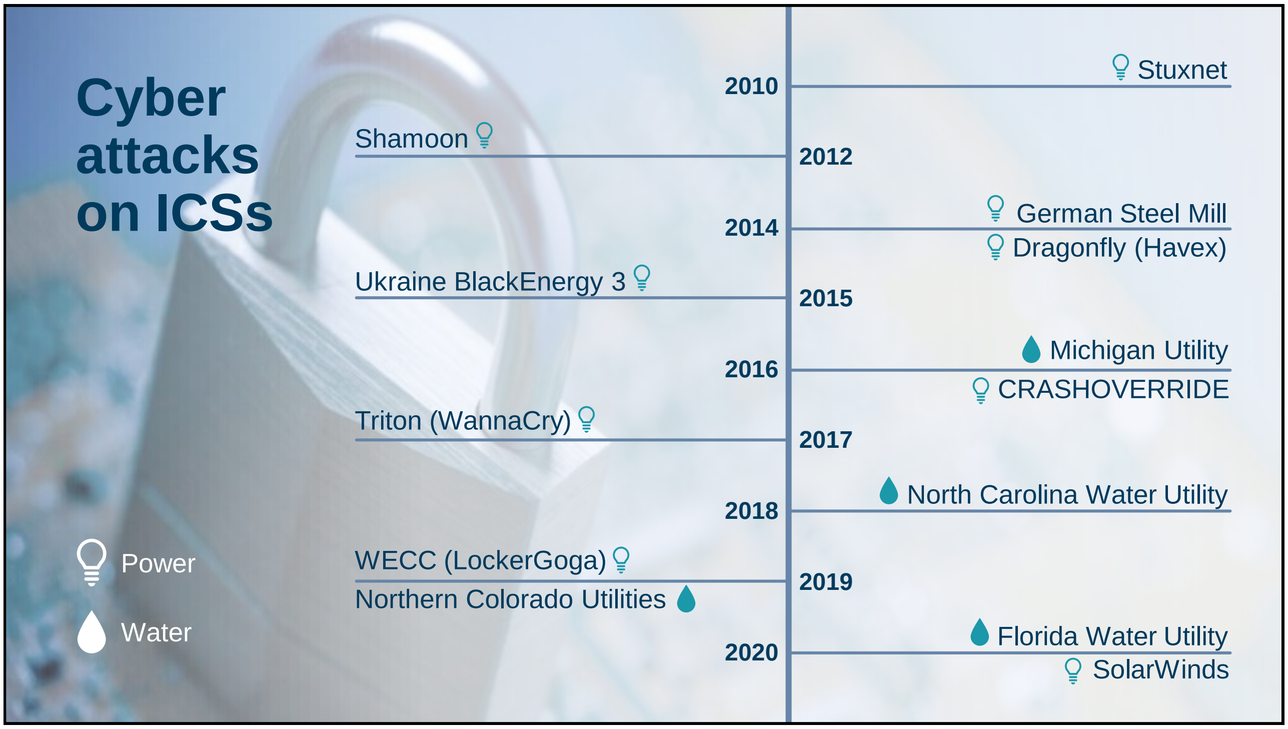
Activity Group	Common Tactic	Mitre ATT&CK ICS Designation Number
ALLANITE	Point and Tag Identification for Collection	T852
CHRYSENE	Scripting for Execution	T853
COVELLITE	Spearphishing Attachments for Initial Access	T865
DYMALLOY	Screen Capture for Collection	T852
ELECTRUM	Wiper to Inhibit Response Function	T809
HEXANE	User Interaction for Execution	T863
MAGNALIUM	Loss of View	T829
PARISITE	Exploitation of Remote Services	T866
RASPITE	Drive-by Compromise for Initial Access	T817
WASSONITE	Valid Accounts for Persistence	T859
XENOTIME	Safety Engineering Workstation Compromise	T818

MITRE ATT&CK Framework

Initial Access	Execution	Persist.	Evasion	Discovery	Lateral Movement	Collection	Command & Control	Inhibit Response	Impair Control	Impact
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
Replication Through Removable Media	Project File Infection		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download	Loss of Safety
Spearphishing Attachment	Scripting					Point & Tag Identification		Device Restart/Shutdown	Rogue Master Device	Loss of View
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop	Manipulation of Control
Wireless Compromise						Role Identification		Modify Alarm Settings	Spoof Reporting Message	Manipulation of View
						Screen Capture		Modify Control Logic	Unauthorized Command Message	Theft of Operational Information
								Program Download		
								Rootkit		
								System Firmware		
								Utilize/Change Operating Mode		

In a well-designed system, the adversary must get EVERYTHING done perfectly to not get caught and reach an impact

Cyber attacks on ICSs



💡 Power

💧 Water

2010 Stuxnet 💡

2012 Shamoon 💡

2014 💡 German Steel Mill
💡 Dragonfly (Havex)

2015 Ukraine BlackEnergy 3 💡

2016 💧 Michigan Utility
💡 CRASHOVERRIDE

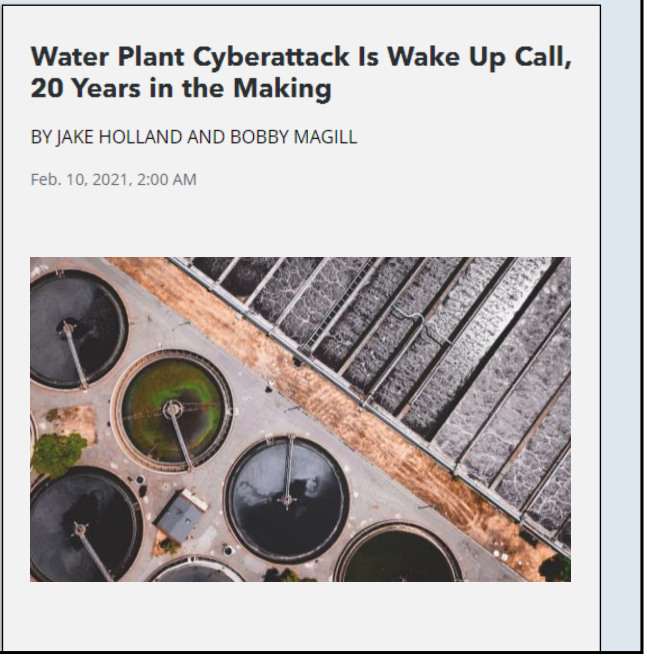
2017 Triton (WannaCry) 💡

2018 💧 North Carolina Water Utility

2019 WECC (LockerGoga) 💡
Northern Colorado Utilities 💧

2020 💧 Florida Water Utility
💡 SolarWinds

Operational threat – no plan resulted in inability to secure assets

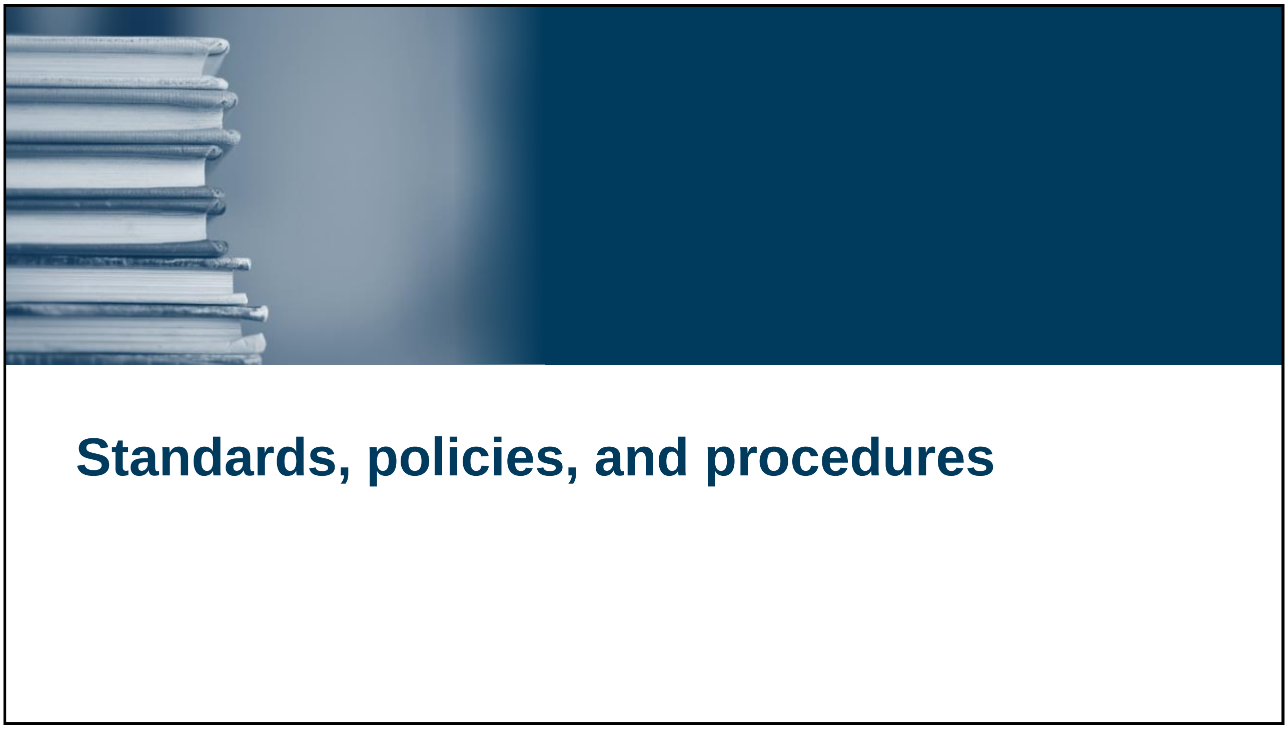


Water Plant Cyberattack Is Wake Up Call, 20 Years in the Making

BY JAKE HOLLAND AND BOBBY MAGILL

Feb. 10, 2021, 2:00 AM

Source: news.bloomberglaw.com



Standards, policies, and procedures

Policy, process, and procedures

- Note that it is C-Suite driven
- Incorporate importance into plans, policies, and procedures
- Have training and awareness program
- Bypass technology – direct to human

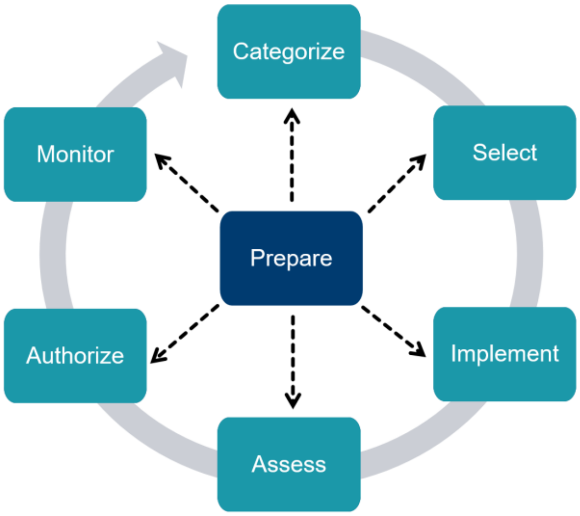
Process – series of related tasks

Processes are structured steps designed to accomplish the objective of meeting the stated policy

Process example

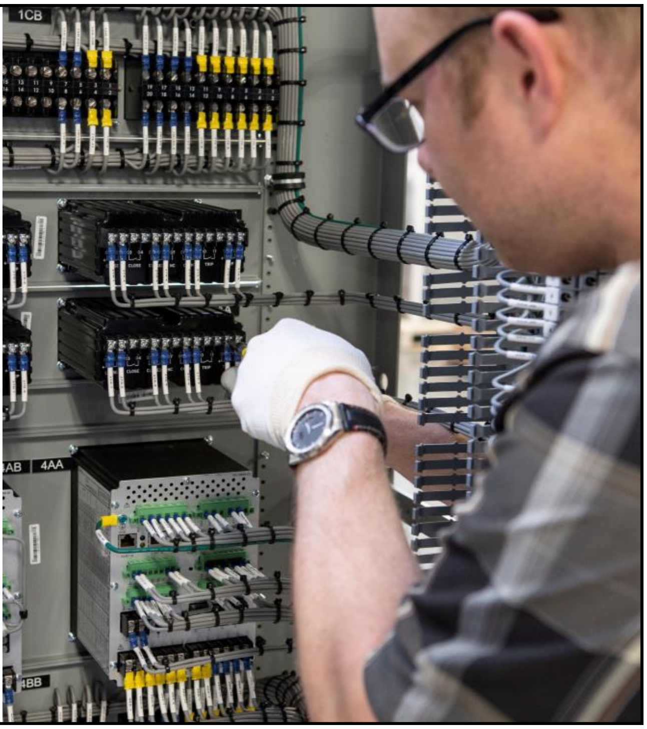
Organization risk management process

- Identify systems
- Select security controls
- Implement controls
- Assess controls
- Authorize controls
- Monitor controls



Procedure – prescriptive and repeatable

Procedures are step-by-step work instructions of the process



Before regulation, you need standards and frameworks

Before standards and frameworks, you need innovation

ISO 27002-2013

Canadian CSE Top 10

NIST CSF 1.2

IEC 62443

CIS

NERC CIPv7

HIPAA

NIST RMF and 800-53r5

PCI DSS 3.2

Australian Top 35

Victorian PDSF v1.0

COBIT 5

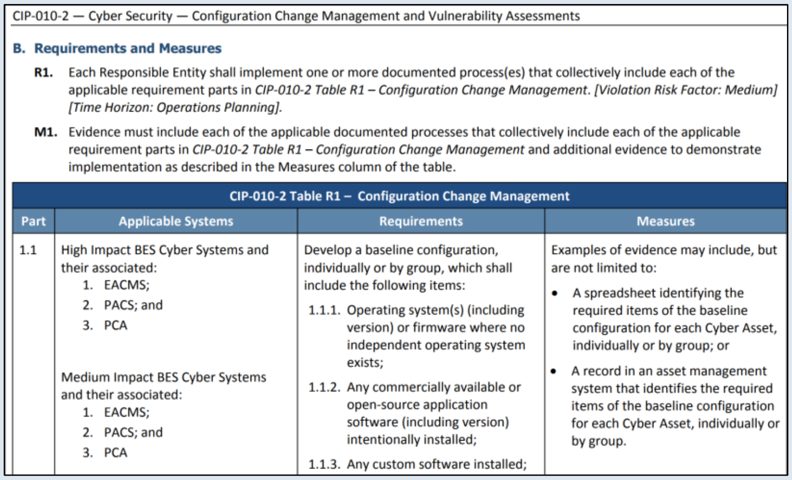
NSA MNT

GCHQ 10 Steps

DHS CDM Program

Standards – specific requirements

Standards define security requirements and serve as guide for how to comply with requirements



CIP-010-2 — Cyber Security — Configuration Change Management and Vulnerability Assessments

B. Requirements and Measures

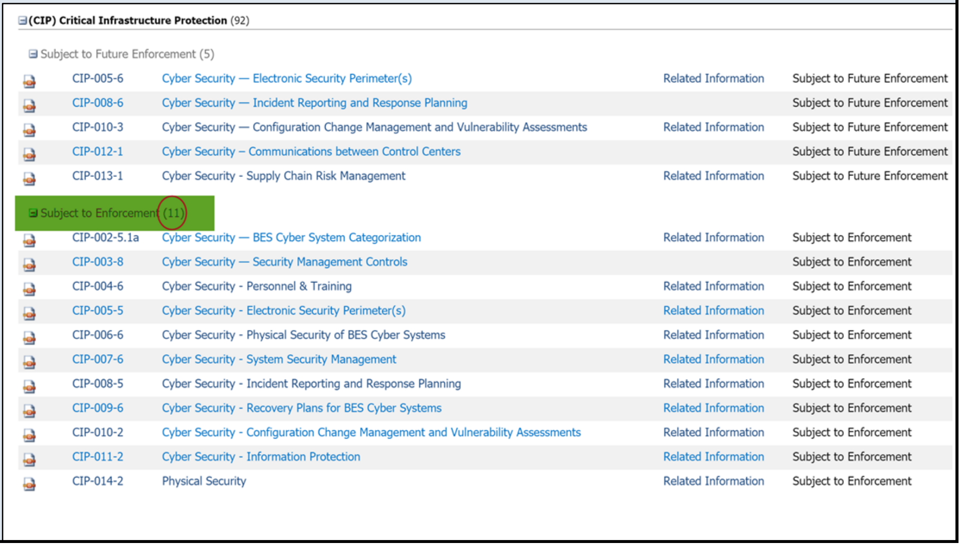
R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-2 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*.

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-2 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-2 Table R1 – Configuration Change Management			
Part	Applicable Systems	Requirements	Measures
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed;	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.

NERC CIP standards

Available at
nerc.com



(CIP) Critical Infrastructure Protection (92)

Subject to Future Enforcement (5)

CIP-005-6	Cyber Security — Electronic Security Perimeter(s)	Related Information	Subject to Future Enforcement
CIP-008-6	Cyber Security — Incident Reporting and Response Planning		Subject to Future Enforcement
CIP-010-3	Cyber Security — Configuration Change Management and Vulnerability Assessments	Related Information	Subject to Future Enforcement
CIP-012-1	Cyber Security – Communications between Control Centers		Subject to Future Enforcement
CIP-013-1	Cyber Security - Supply Chain Risk Management	Related Information	Subject to Future Enforcement

Subject to Enforcement (11)

CIP-002-5.1a	Cyber Security — BES Cyber System Categorization	Related Information	Subject to Enforcement
CIP-003-8	Cyber Security — Security Management Controls		Subject to Enforcement
CIP-004-6	Cyber Security - Personnel & Training	Related Information	Subject to Enforcement
CIP-005-5	Cyber Security - Electronic Security Perimeter(s)	Related Information	Subject to Enforcement
CIP-006-6	Cyber Security - Physical Security of BES Cyber Systems	Related Information	Subject to Enforcement
CIP-007-6	Cyber Security - System Security Management	Related Information	Subject to Enforcement
CIP-008-5	Cyber Security - Incident Reporting and Response Planning	Related Information	Subject to Enforcement
CIP-009-6	Cyber Security - Recovery Plans for BES Cyber Systems	Related Information	Subject to Enforcement
CIP-010-2	Cyber Security - Configuration Change Management and Vulnerability Assessments	Related Information	Subject to Enforcement
CIP-011-2	Cyber Security - Information Protection	Related Information	Subject to Enforcement
CIP-014-2	Physical Security	Related Information	Subject to Enforcement

Regulations – mandatory government requirements

Regulations define cybersecurity requirements mandated by a government body and required compliance by law, for the system to operate

To ensure systems are complying to these requirements, there are periodic compliance audits

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION
ISA
ISA-62443
NIST
Cybersecurity Framework
SP800-53, SP800-82
IEC
ISO
ISO/IEC 2700x
IEC 62443
Center for Internet Security
20 Critical Security Controls

Guidelines – recommendations

Guidelines provide other suggestions and recommendations but are not prescriptive

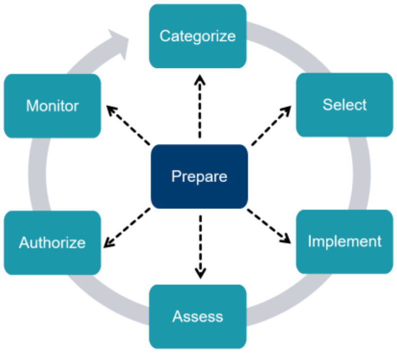
Using guidelines, you can add additional stringent controls

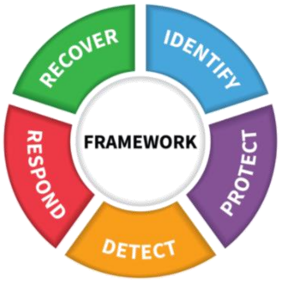
Frameworks – overall security program guide

Cybersecurity frameworks are sets of standards and best practices put together to help mission-critical infrastructures achieve cybersecurity and resiliency goals

Example
NIST Cybersecurity Framework
nist.gov/topics/cybersecurity
nist.gov/cyberframework

NIST risk management framework

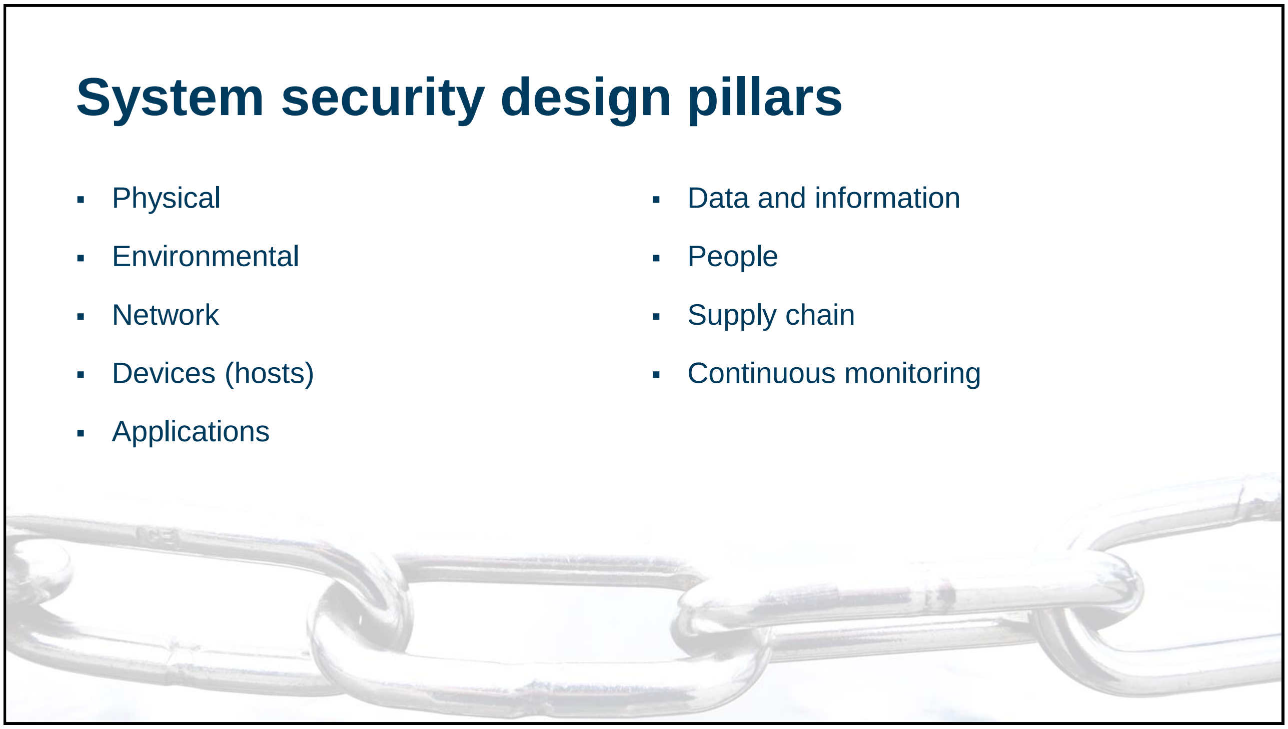




NIST cybersecurity framework

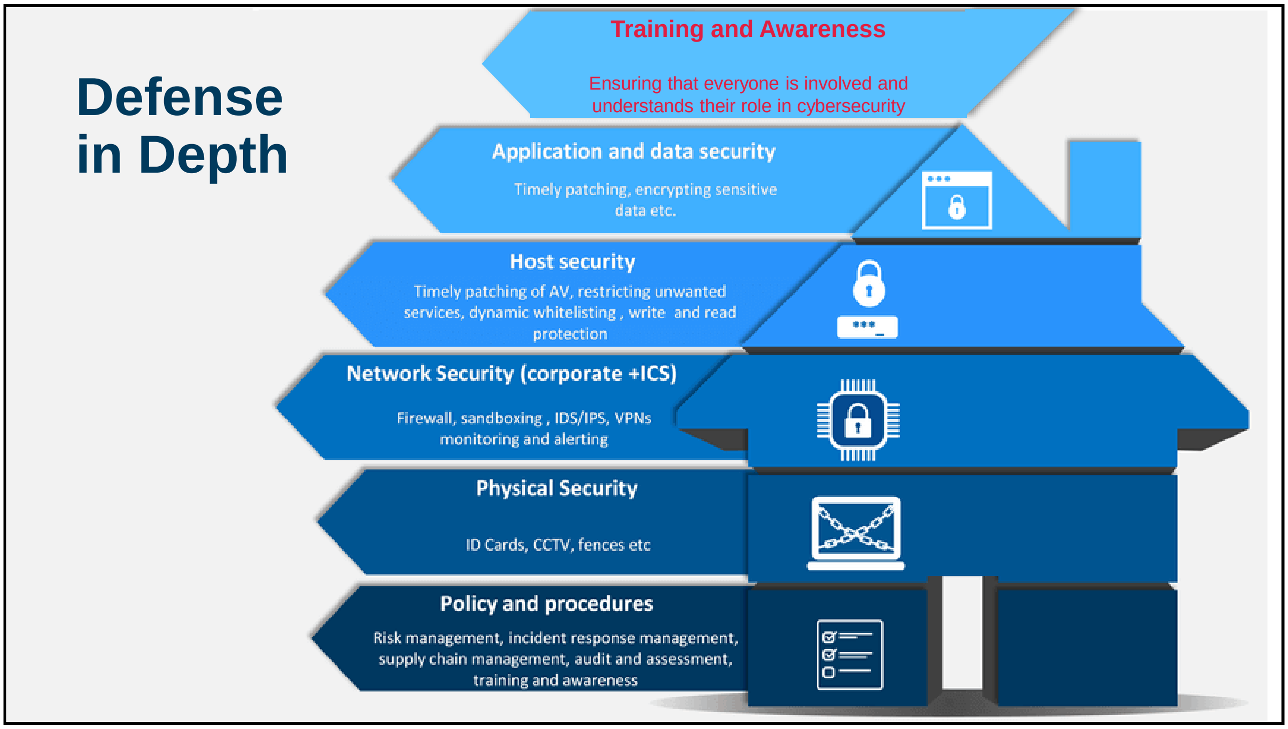
Security framework	Identify	Identify baseline system and prioritize risk to implement selected security controls	Risk management
	Protect	Assess implementation and authorize system risks	
	Detect	Monitor continuous monitoring tools	
	Respond	Execute plans, policies, and procedures to analyze and contain situation	Contingency and incident response
	Recover	Eradicate and recover system to previous state	
	Learn	Review event to improve plans, policies, and procedures	

Security by design



System security design pillars

- Physical
- Environmental
- Network
- Devices (hosts)
- Applications
- Data and information
- People
- Supply chain
- Continuous monitoring



Defense in Depth

Training and Awareness

Ensuring that everyone is involved and understands their role in cybersecurity

Application and data security

Timely patching, encrypting sensitive data etc.

Host security

Timely patching of AV, restricting unwanted services, dynamic whitelisting , write and read protection

Network Security (corporate +ICS)

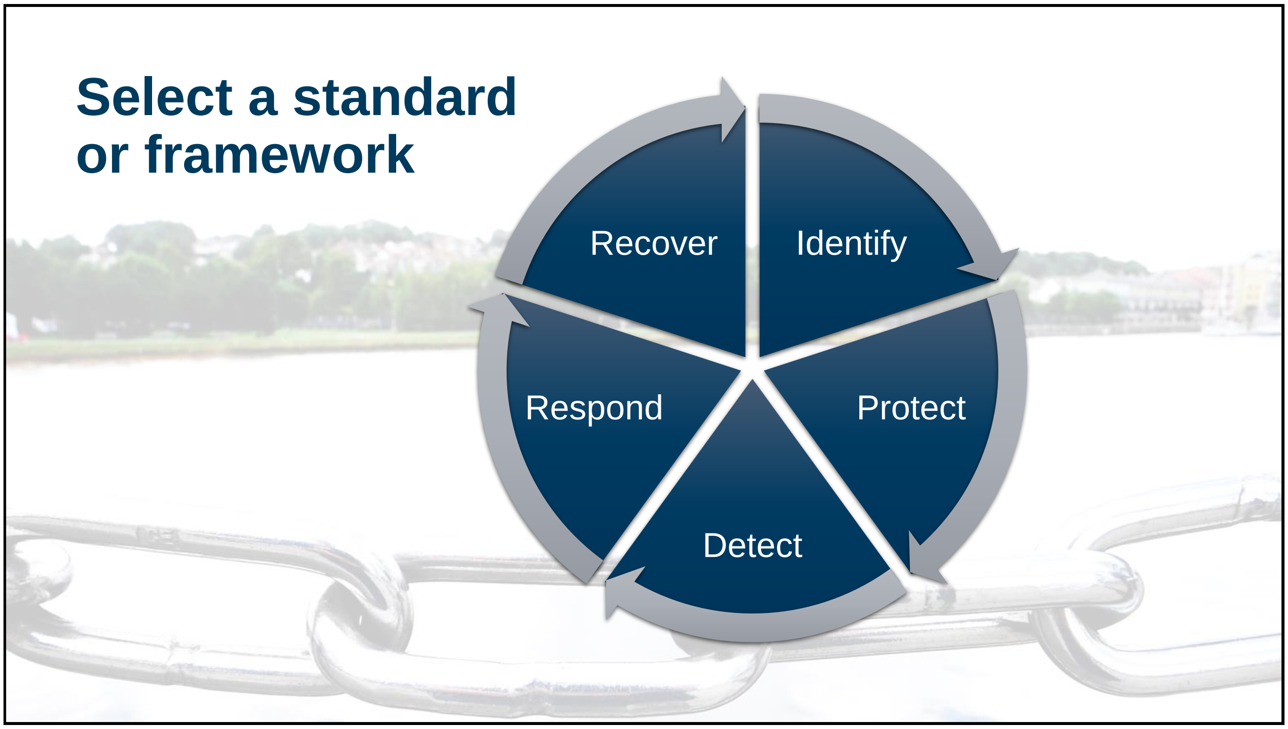
Firewall, sandboxing , IDS/IPS, VPNs monitoring and alerting

Physical Security

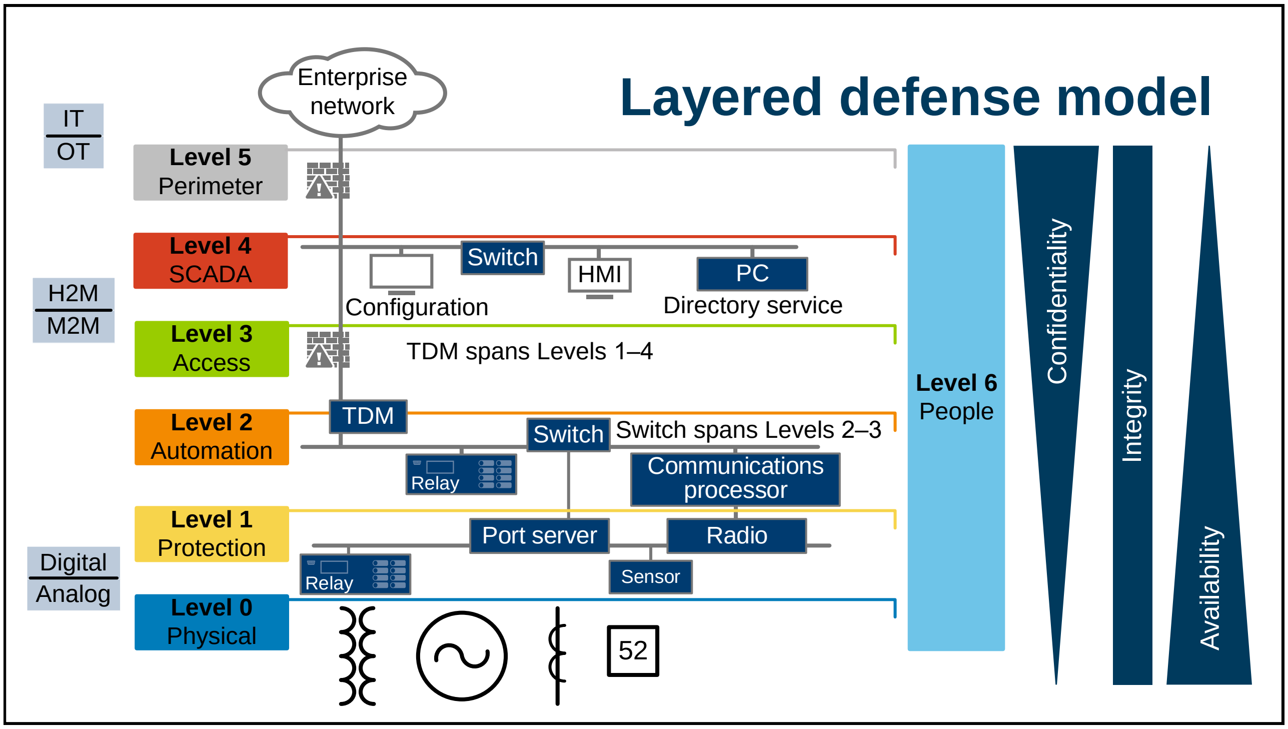
ID Cards, CCTV, fences etc

Policy and procedures

Risk management, incident response management, supply chain management, audit and assessment, training and awareness



Select a standard or framework



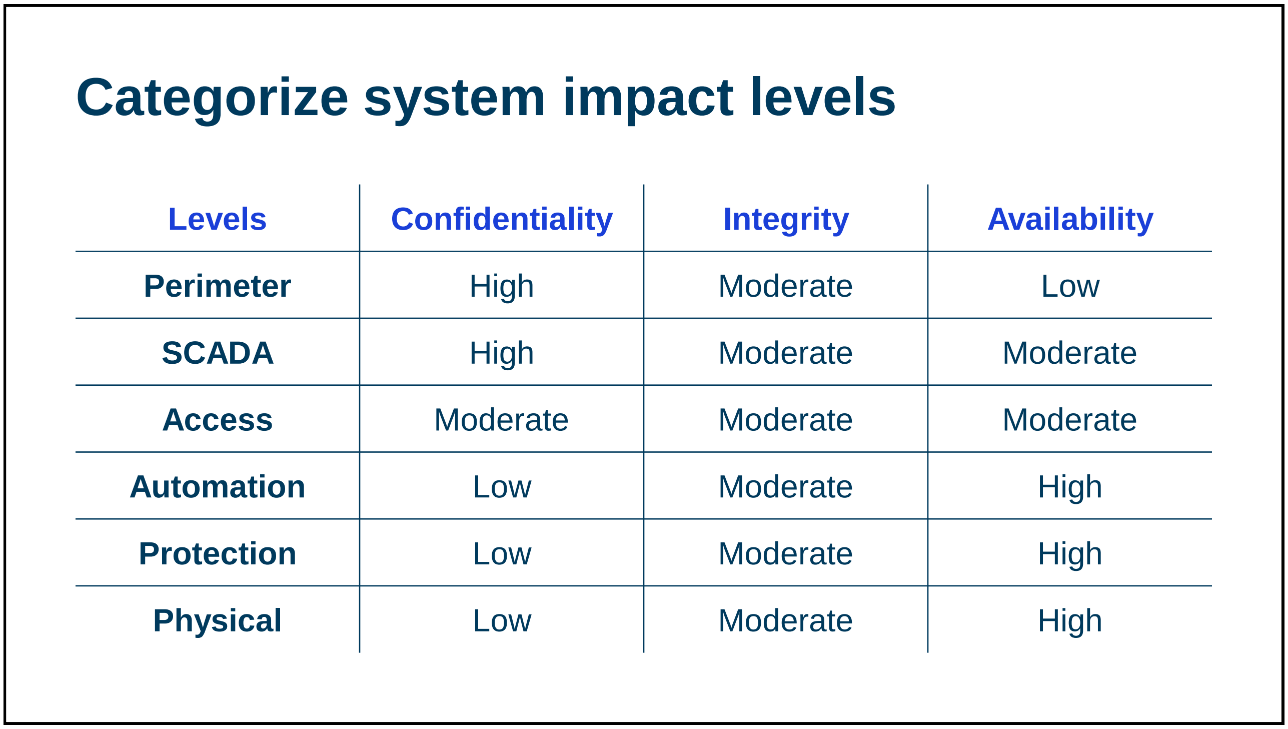
Layered defense model

Go to example system

Categorize system

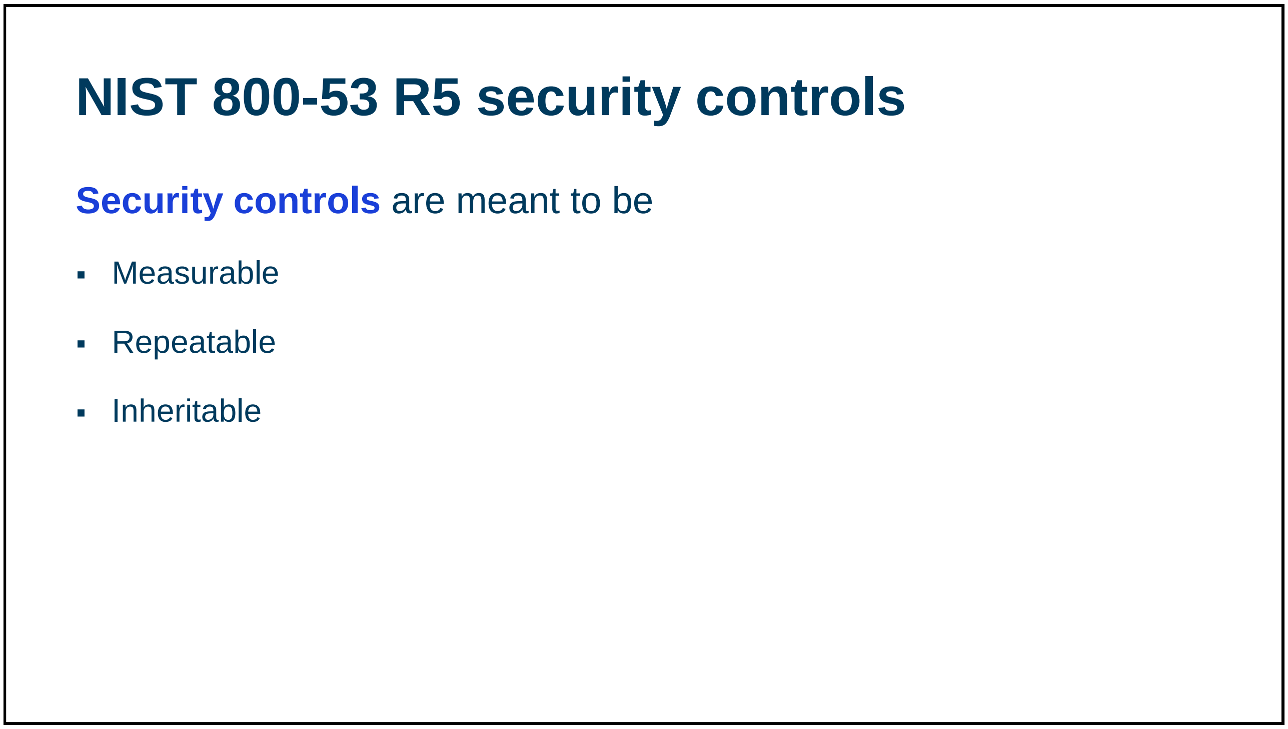
System failure impact

- High – catastrophic
- Moderate – serious adverse effect
- Low – limited adverse effect



Categorize system impact levels

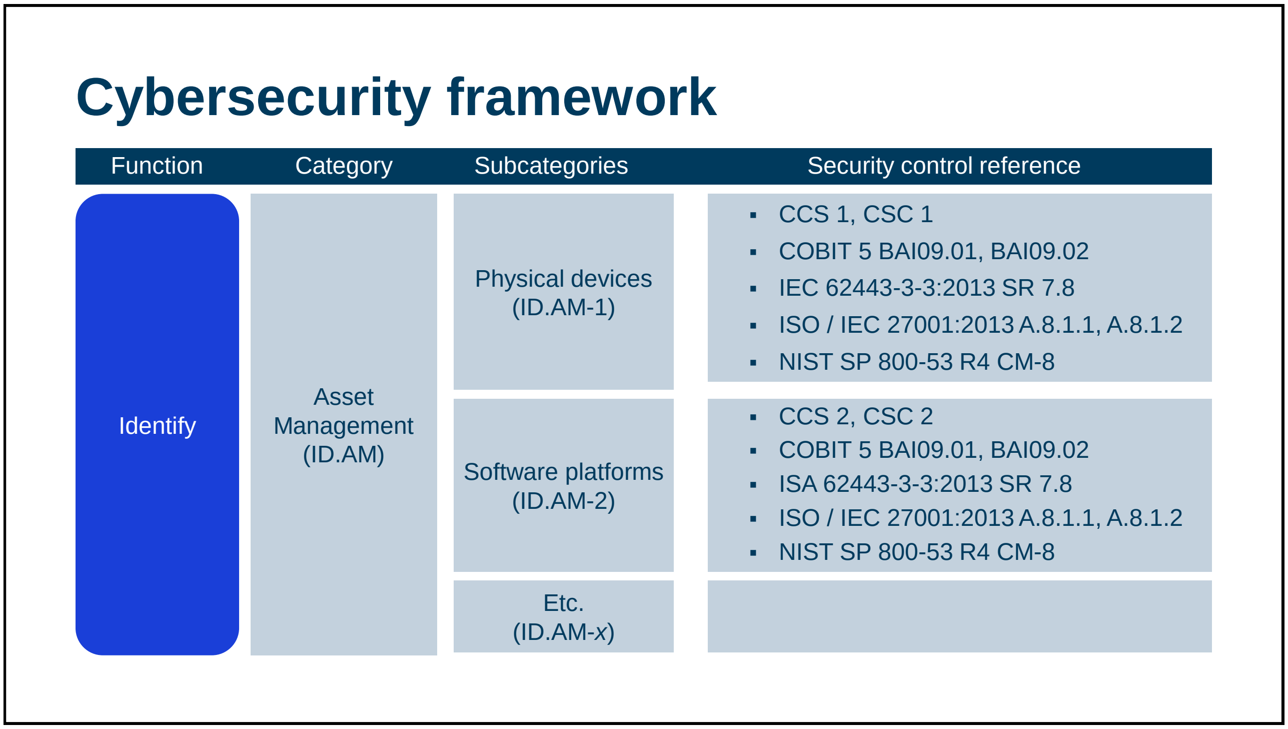
Levels	Confidentiality	Integrity	Availability
Perimeter	High	Moderate	Low
SCADA	High	Moderate	Moderate
Access	Moderate	Moderate	Moderate
Automation	Low	Moderate	High
Protection	Low	Moderate	High
Physical	Low	Moderate	High



NIST 800-53 R5 security controls

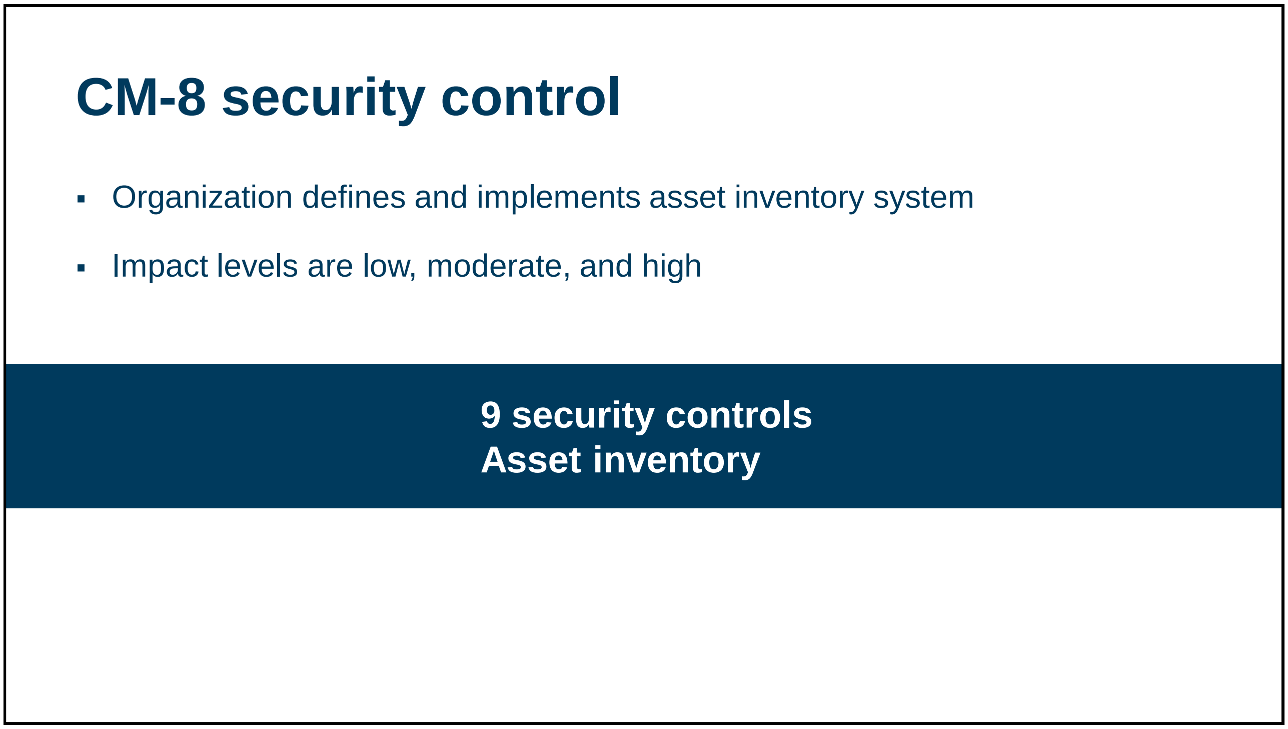
Security controls are meant to be

- Measurable
- Repeatable
- Inheritable



Cybersecurity framework

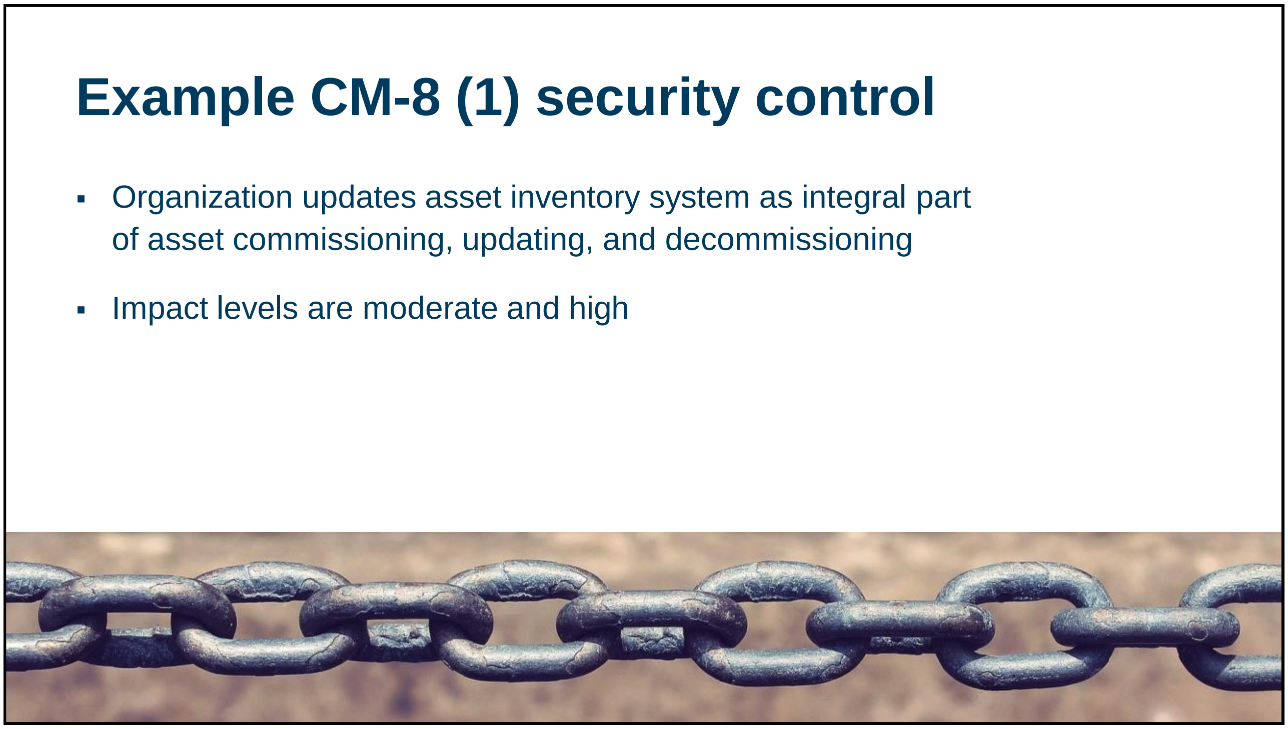
Function	Category	Subcategories	Security control reference
Identify	Asset Management (ID.AM)	Physical devices (ID.AM-1)	▪ CCS 1, CSC 1 ▪ COBIT 5 BAI09.01, BAI09.02 ▪ IEC 62443-3-3:2013 SR 7.8 ▪ ISO / IEC 27001:2013 A.8.1.1, A.8.1.2 ▪ NIST SP 800-53 R4 CM-8
		Software platforms (ID.AM-2)	▪ CCS 2, CSC 2 ▪ COBIT 5 BAI09.01, BAI09.02 ▪ ISA 62443-3-3:2013 SR 7.8 ▪ ISO / IEC 27001:2013 A.8.1.1, A.8.1.2 ▪ NIST SP 800-53 R4 CM-8
		Etc. (ID.AM-*x*)	



CM-8 security control

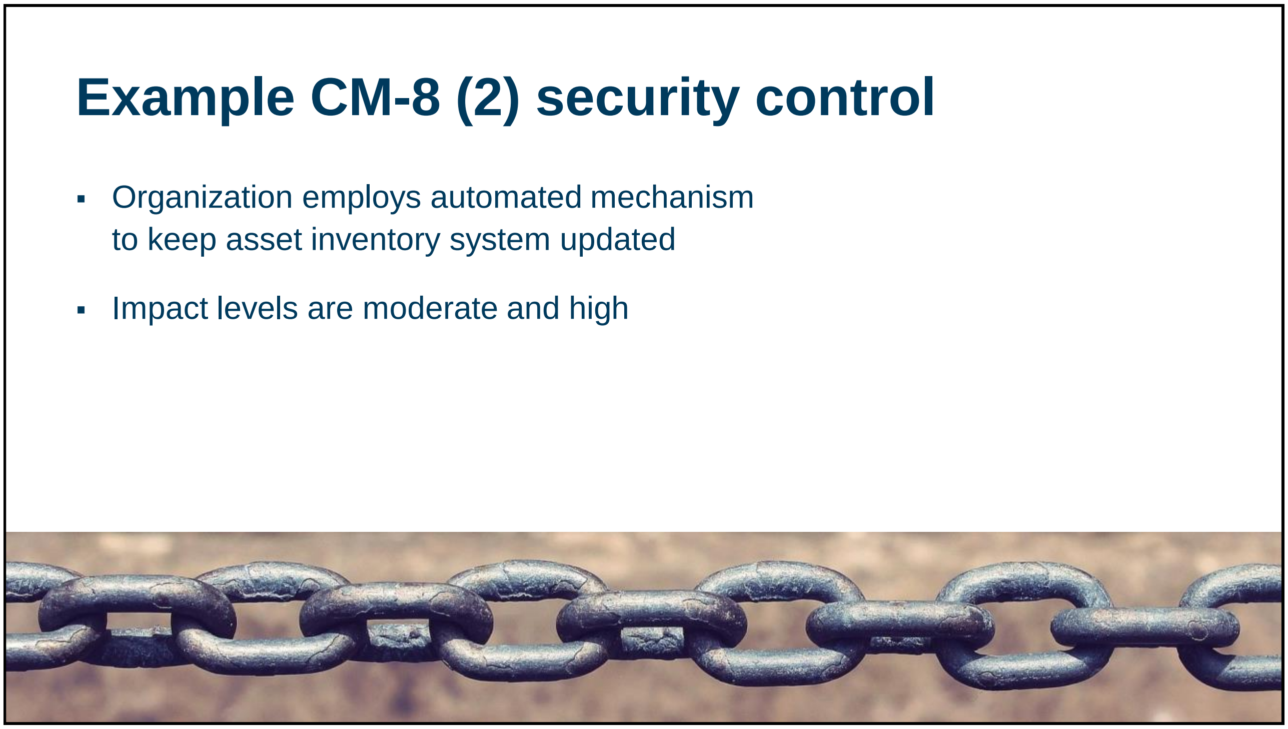
- Organization defines and implements asset inventory system
- Impact levels are low, moderate, and high

9 security controls
Asset inventory



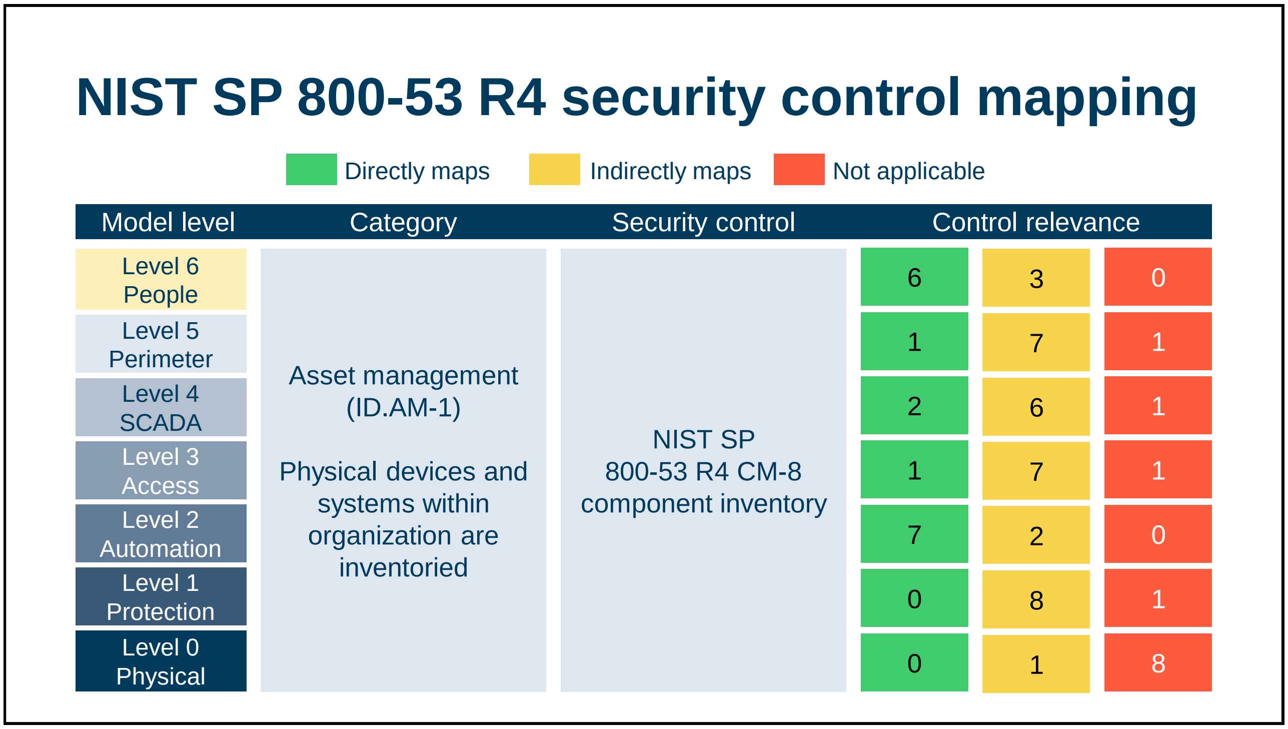
Example CM-8 (1) security control

- Organization updates asset inventory system as integral part of asset commissioning, updating, and decommissioning
- Impact levels are moderate and high



Example CM-8 (2) security control

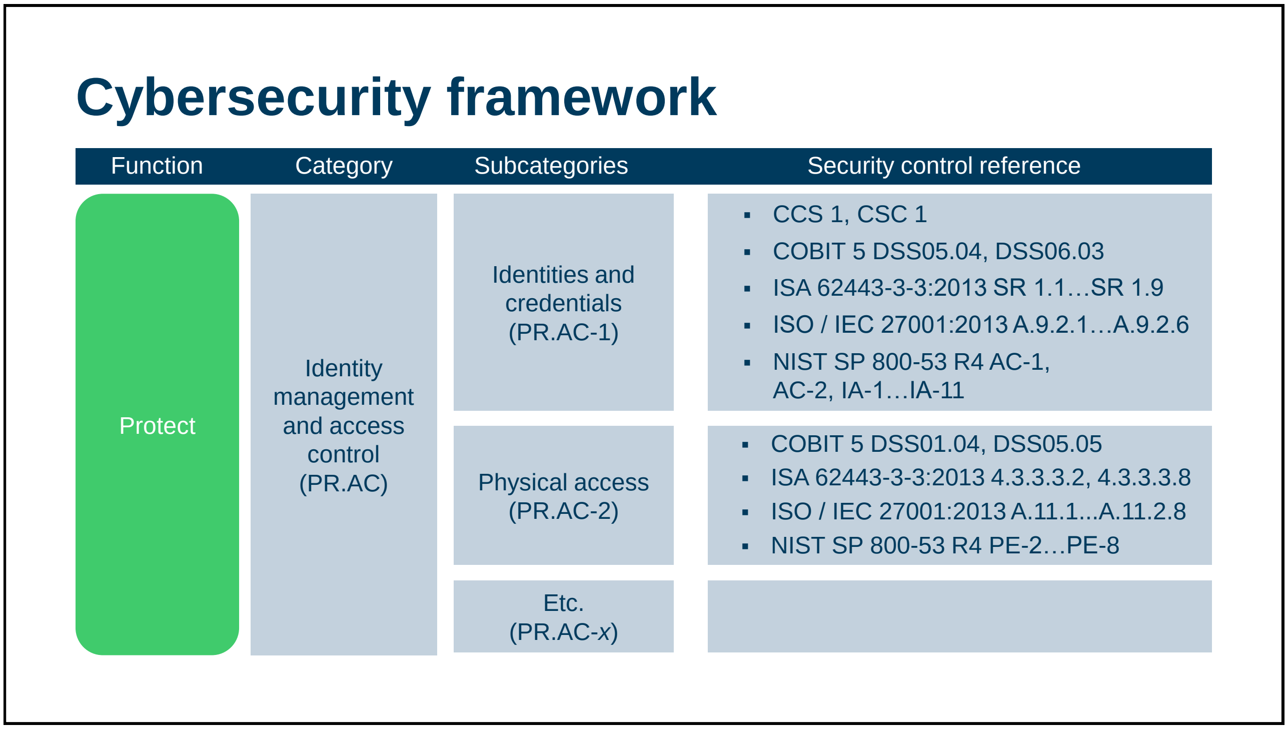
- Organization employs automated mechanism to keep asset inventory system updated
- Impact levels are moderate and high



NIST SP 800-53 R4 security control mapping

🟩 Directly maps 🟨 Indirectly maps 🟥 Not applicable

Model level	Category	Security control	Control relevance		
			🟩	🟨	🟥
Level 6 People	Asset management (ID.AM-1) Physical devices and systems within organization are inventoried	NIST SP 800-53 R4 CM-8 component inventory	6	3	0
Level 5 Perimeter			1	7	1
Level 4 SCADA			2	6	1
Level 3 Access			1	7	1
Level 2 Automation			7	2	0
Level 1 Protection			0	8	1
Level 0 Physical			0	1	8



Cybersecurity framework

Function	Category	Subcategories	Security control reference
Protect	Identity management and access control (PR.AC)	Identities and credentials (PR.AC-1)	▪ CCS 1, CSC 1 ▪ COBIT 5 DSS05.04, DSS06.03 ▪ ISA 62443-3-3:2013 SR 1.1…SR 1.9 ▪ ISO / IEC 27001:2013 A.9.2.1…A.9.2.6 ▪ NIST SP 800-53 R4 AC-1, AC-2, IA-1…IA-11
		Physical access (PR.AC-2)	▪ COBIT 5 DSS01.04, DSS05.05 ▪ ISA 62443-3-3:2013 4.3.3.3.2, 4.3.3.3.8 ▪ ISO / IEC 27001:2013 A.11.1...A.11.2.8 ▪ NIST SP 800-53 R4 PE-2…PE-8
		Etc. (PR.AC-*x*)	

IA-5 security control

- Organization manages system credentials for authentication
- Impact levels are low, moderate, and high

14 security controls
Identification and authorization

IA-5 (1) security control

- Organization enforces minimum password complexity
- Impact levels are low, moderate, and high

IA-5 (5) security control

- Organization requires integrators to create unique credentials in place of asset defaults before or at time of commissioning
- Impact levels are moderate and high

NIST SP 800-53 R4 security control mapping

🟩 Directly maps 🟨 Indirectly maps 🟥 Not applicable

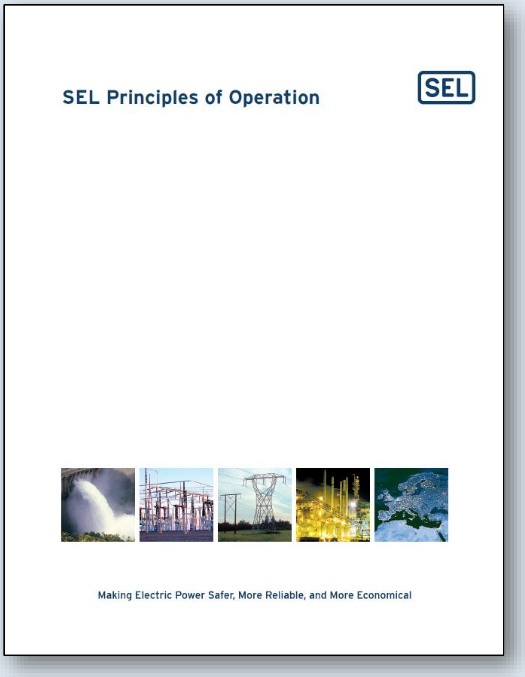
Model level	Category	Security control	Control relevance		
Level 6 People	Identity management and access control (PR.AC-6) Identities are proofed and bound credentials	NIST SP 800-53 R4 IA-5 authenticator management	7	3	4
Level 5 Perimeter			3	6	5
Level 4 SCADA			6	3	5
Level 3 Access			3	4	7
Level 2 Automation			5	5	3
Level 1 Protection			2	4	8
Level 0 Physical			0	0	14

Security framework	Identify	Identify baseline system and prioritize risk to implement selected security controls	Risk management
	Protect	Assess implementation and authorize system risks	
	Detect	Monitor continuous monitoring tools	
	Respond	Execute plans, policies, and procedures to analyze and contain situation	Contingency and incident response
	Recover	Eradicate and recover system to previous state	
	Learn	Review event to improve plans, policies, and procedures	

Supply chain security

Security

Must be foundation of organization's DNA



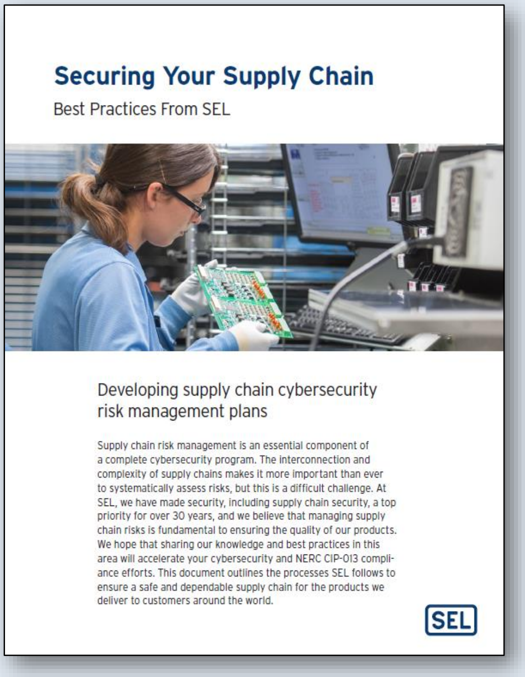
SEL Principles of Operation

SEL

Making Electric Power Safer, More Reliable, and More Economical

Securing your supply chain

Essential component of complete cybersecurity program



Securing Your Supply Chain

Best Practices From SEL

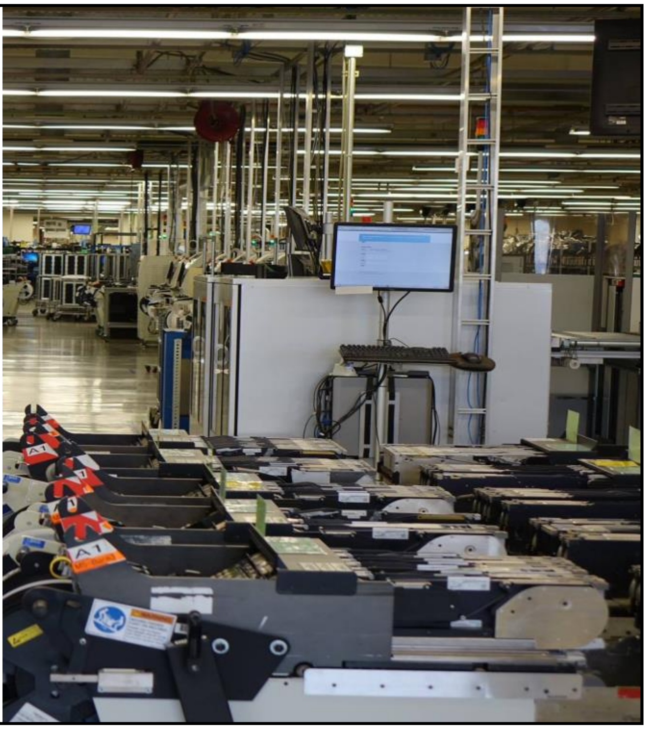
Developing supply chain cybersecurity risk management plans

Supply chain risk management is an essential component of a complete cybersecurity program. The interconnection and complexity of supply chains makes it more important than ever to systematically assess risks, but this is a difficult challenge. At SEL, we have made security, including supply chain security, a top priority for over 30 years, and we believe that managing supply chain risks is fundamental to ensuring the quality of our products. We hope that sharing our knowledge and best practices in this area will accelerate your cybersecurity and NERC CIP-013 compliance efforts. This document outlines the processes SEL follows to ensure a safe and dependable supply chain for the products we deliver to customers around the world.

SEL

Quality = security

- Industry presence
- Customer trust
- Warranty
- Reliability indicators
- Return and repairs
- Technical support
- Quality assurance
  selinc.com/support/warranty/



Nurture trusted supplier partnerships

- Use holistic approach to supplier evaluation
- Trust but verify
- Pursue redundancy whenever possible
- Cultivate lasting supplier relationships

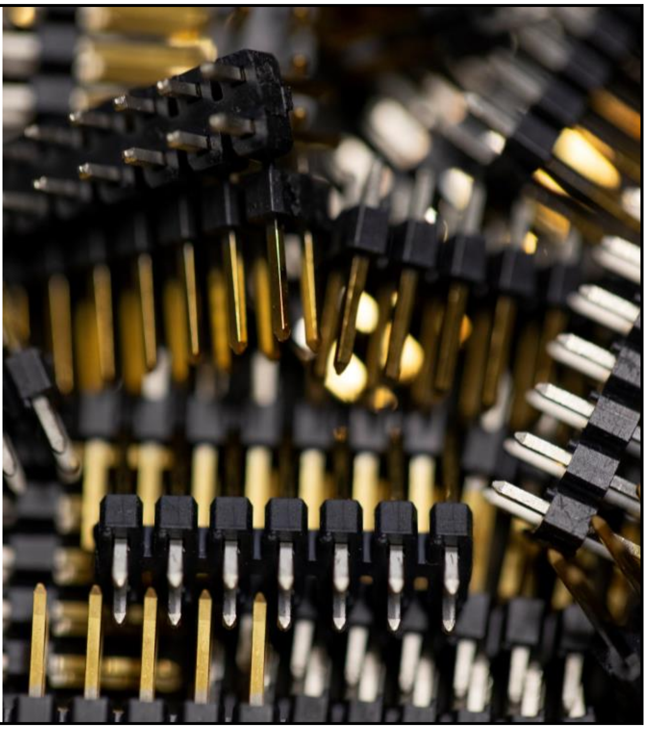
92

Continuous supply chain assessment

- Analyze business and threat intelligence
- Assess suppliers based on risk
- Scrutinize shipping services
- Use multiple vertices

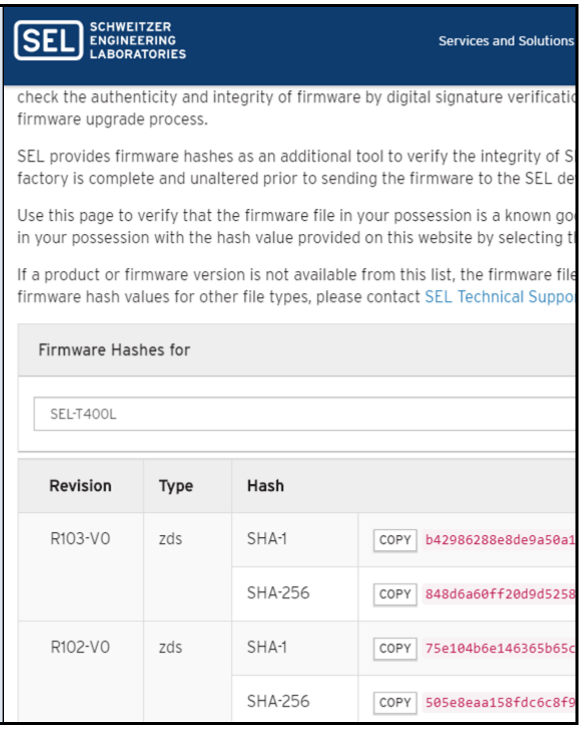
Component integrity assurance

- Verify vendor security practices and processes
- Qualify and continuously test each component
- Procure directly from manufacturer if possible
- Examine to verify authenticity



Verification of software integrity and authenticity

- Protection products continuously verify software integrity and disable themselves if corruption is detected
- Control products whitelist applications at the kernel level
- FW/SW is digitally signed
- FW/SW can be authenticated by reference hash values published on SEL website



check the authenticity and integrity of firmware by digital signature verificatio
firmware upgrade process.

SEL provides firmware hashes as an additional tool to verify the integrity of S
factory is complete and unaltered prior to sending the firmware to the SEL de

Use this page to verify that the firmware file in your possession is a known go
in your possession with the hash value provided on this website by selecting t

If a product or firmware version is not available from this list, the firmware file
firmware hash values for other file types, please contact SEL Technical Suppo

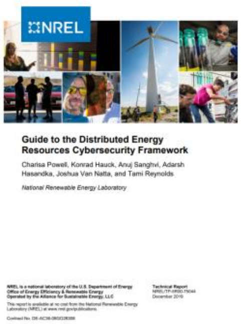
Firmware Hashes for

SEL-T400L

Revision	Type	Hash	
R103-V0	zds	SHA-1	COPY b42986288e8de9a50a1
		SHA-256	COPY 848d6a60ff20d9d5258
R102-V0	zds	SHA-1	COPY 75e104b6e146365b65c
		SHA-256	COPY 505e8eaa158fdc6c8f9

Contracting language

- Typical language seen
  - "sibre" in Appendix Z
  - Multiple frameworks
  - No security control overlay
- Security controls selected by end user during design process
- Balance between cost vs. usability vs. security
- Secure by design but with options to "dial" cyber



Guide to the Distributed Energy Resources Cybersecurity Framework

Charisa Powell, Konrad Hauck, Anuj Sanghvi, Adarsh Hasandka, Joshua Van Natta, and Tami Reynolds

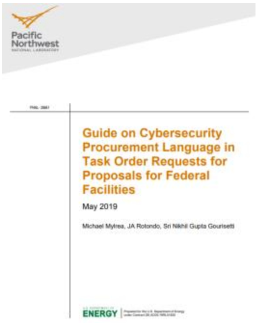
National Renewable Energy Laboratory

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Contract No. DE-AC36-08GO28308

Technical Report
NREL/TP-5R00-75044
December 2019



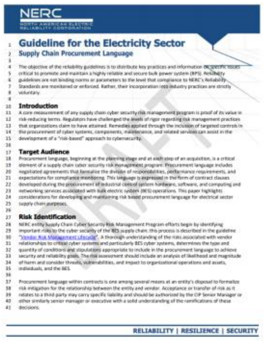
PNNL-28861

Guide on Cybersecurity Procurement Language in Task Order Requests for Proposals for Federal Facilities

May 2019

Michael Mylrea, JA Rotondo, Sri Nikhil Gupta Gourisetti

ENERGY



Guideline for the Electricity Sector
Supply Chain Procurement Language

The objective of the reliability guidelines is to distribute key practices and information on specific issues critical to promote and maintain a highly reliable and secure bulk power system (BPS). Reliability guidelines are not binding norms or parameters to the level that compliance to NERC's Reliability Standards are monitored or enforced. Rather, their incorporation into industry practices are strictly voluntary.

Introduction

A core measurement of any supply chain cyber security risk management program is proof of its value in risk-reducing terms. Regulators have challenged the levels of rigor regarding risk management practices that organizations claim to have attained. Remedies applied through the inclusion of targeted controls in the procurement of cyber systems, components, maintenance, and related services can assist in the development of a "risk-based" approach to cybersecurity.

Target Audience

Procurement language, beginning at the planning stage and at each step of an acquisition, is a critical element of a supply chain cyber security risk management program. Procurement language includes negotiated agreements that formalize the division of responsibilities, performance requirements, and expectations for compliance monitoring. This language is expressed in the form of contract clauses developed during the procurement of industrial control system hardware, software, and computing and networking services associated with bulk electric system (BES) operations. This paper highlights considerations for developing and maintaining risk based procurement language for electrical sector supply chain purposes.

Risk Identification

NERC entity Supply Chain Cyber Security Risk Management Program efforts begin by identifying important risks to the cyber security of the BES supply chain; this process is described in the guideline "Vendor Risk Management Lifecycle". A thorough understanding of the risks associated with vendor relationships to critical cyber systems and particularly BES cyber systems, determines the type and quantity of conditions and stipulations appropriate to include in the procurement language to achieve security and reliability goals. The risk assessment should include an analysis of likelihood and magnitude of harm and consider threats, vulnerabilities, and impact to organizational operations and assets, individuals, and the BES.

Procurement language within contracts is one among several means at an entity's disposal to formalize risk mitigation for the relationship between the entity and vendor. Acceptance or transfer of risk as it relates to a third party may carry specific liability and should be authorized by the CIP Senior Manager or other similarly senior manager or executive with a solid understanding of the ramifications of these decisions.

RELIABILITY | RESILIENCE | SECURITY

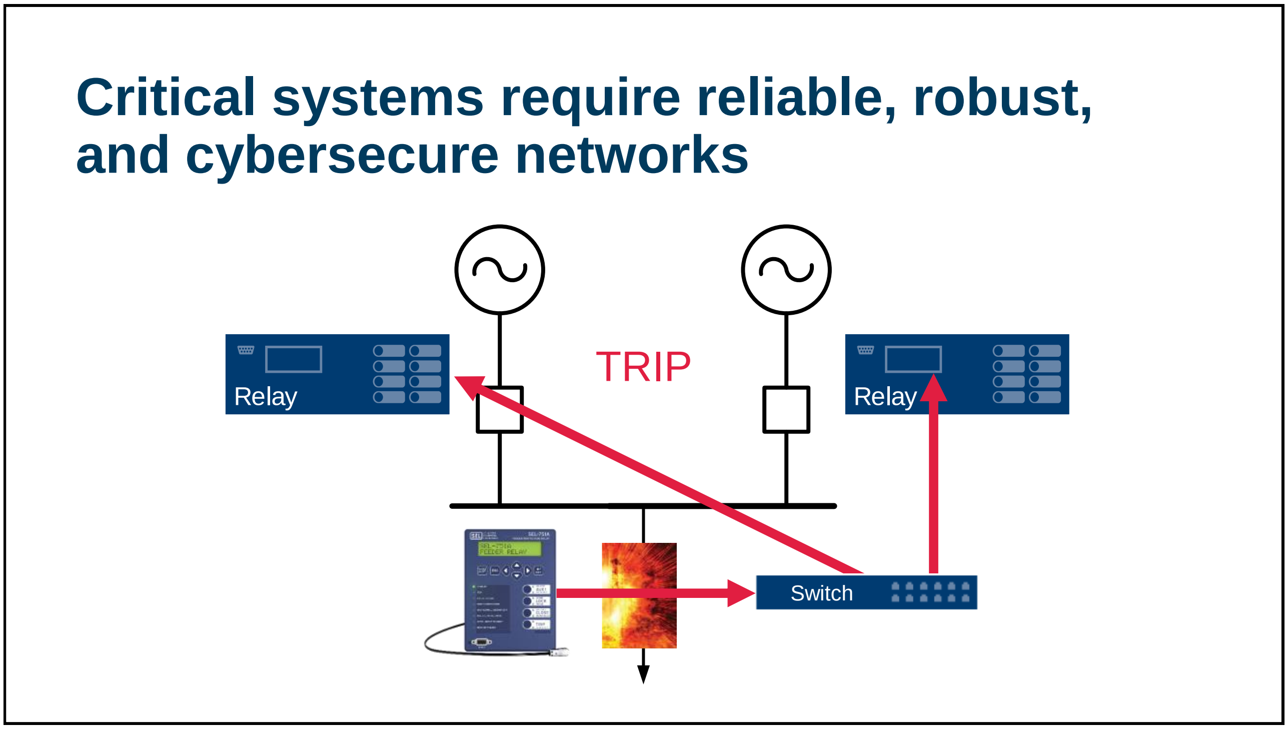
EEI
Edison Electric INSTITUTE

Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk

Version 2.0

May 2020

SEL OT SDN discussion



Critical systems require reliable, robust, and cybersecure networks

Relay

TRIP

Relay

Switch

SEL SDN

Software-Defined
Networking for OT

Improve cybersecurity by allowlisting network flows

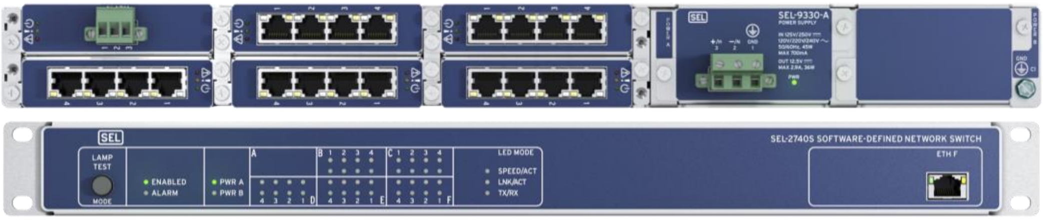
Achieve failover times 100x faster than traditional networking

More precisely control network traffic in substations and FRCS

Automate data collection for security auditing

SEL-2740S SDN Switch

- Flexible 4-port Ethernet module options
- IEEE 1613 compliance
- KEMA certification
- –40° to +85°C operating range
- Dual power supplies



SEL-2742S SDN Switch

- 12 ports, including 2 PoE+ ports
- DIN-rail or surface mounting capability
- IEEE 1613 compliance
- –40° to +85°C operating range
- Dual power sources

Getting to know SDN terminology

Flow
Single communications session that matches ingress rule and has set of forwarding instructions

OpenFlow
Open-source standard defining protocol for interoperable way that switches and flow controller communicate for configuration and monitoring purposes

Flow controller
Central controller that programs switch flow tables

How SDN works

Match fields

Match rule based on portion of Ethernet packet

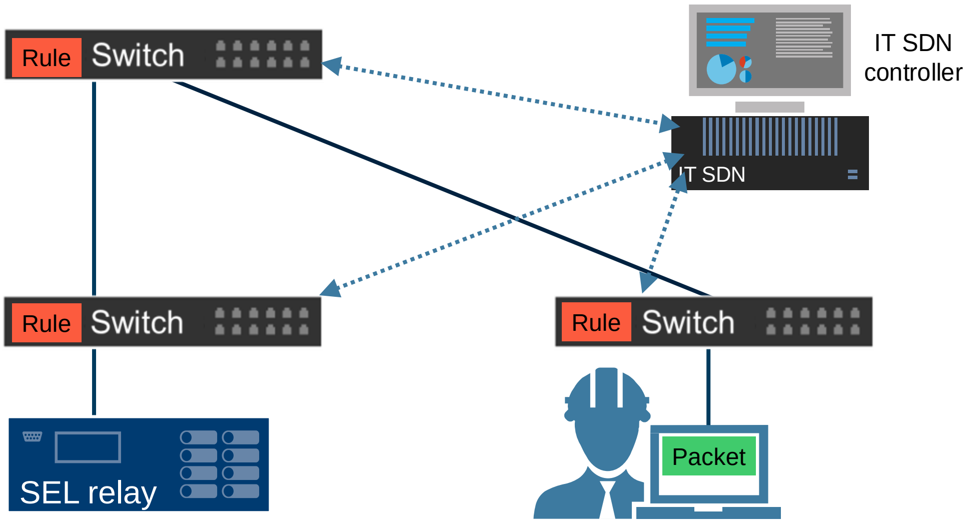
Instructions

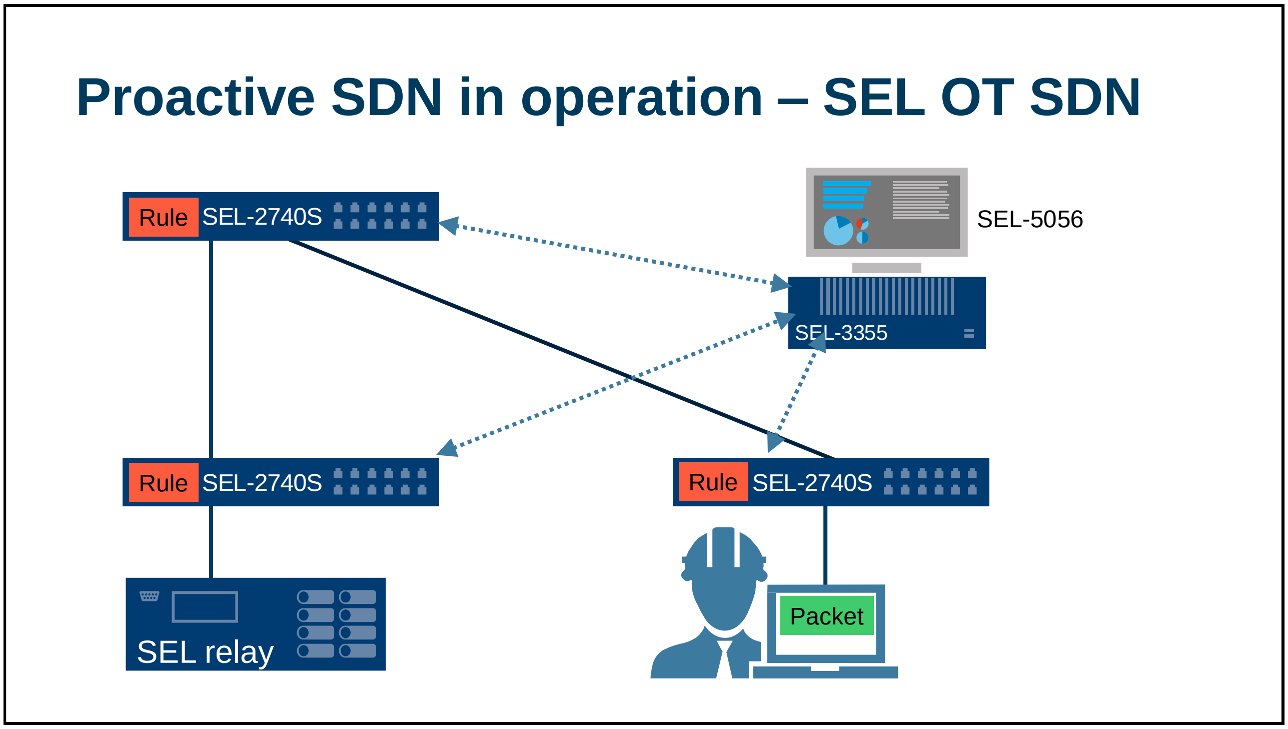
Perform one or more (groups) programmed actions

Counters

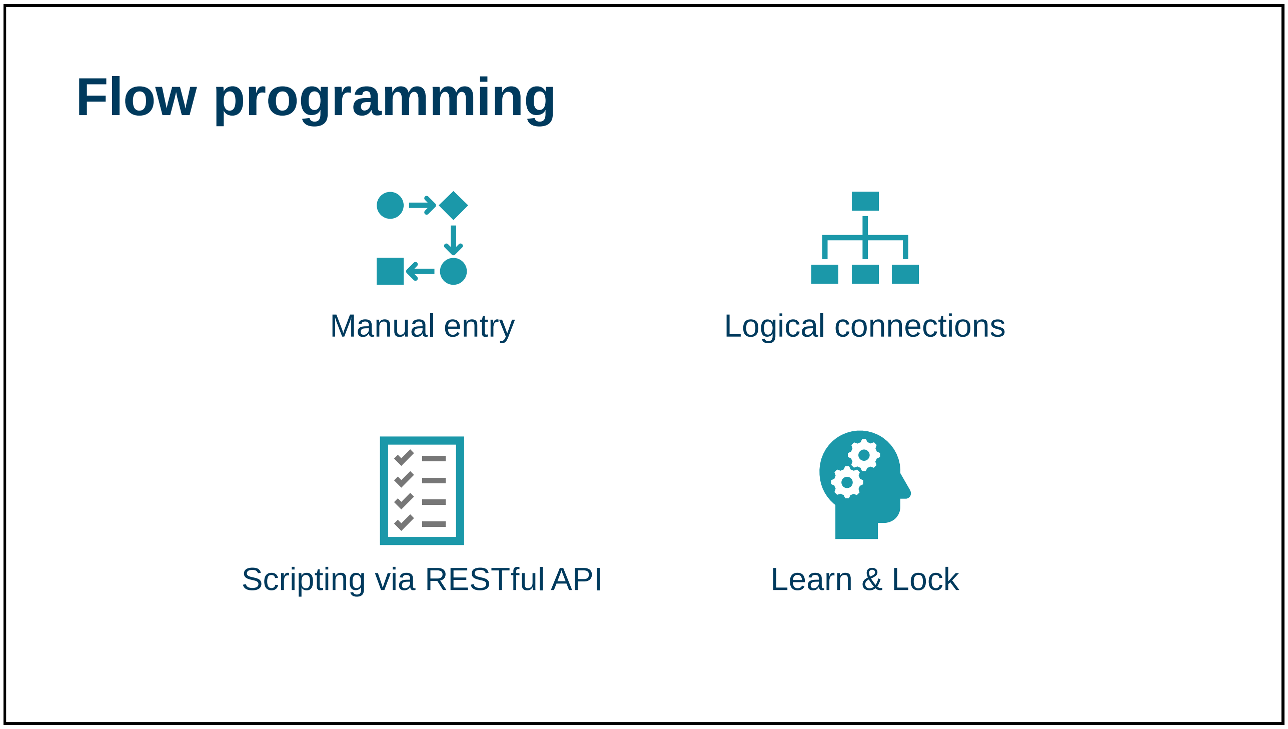
Increment counters and send counter data to centralized point

Reactive SDN in operation – typical IT SDN





Proactive SDN in operation – SEL OT SDN



Flow programming

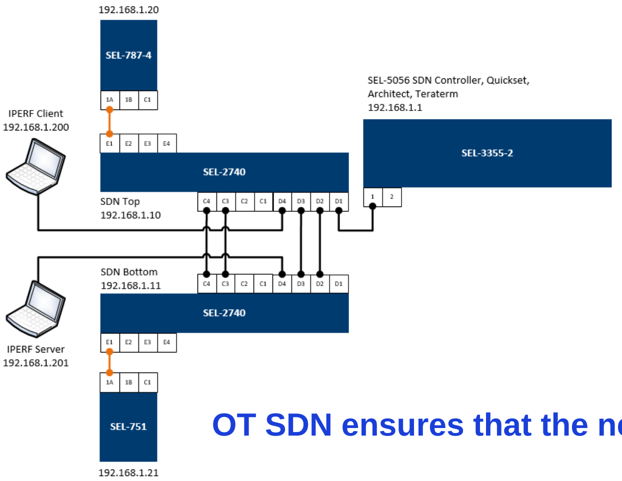
Manual entry

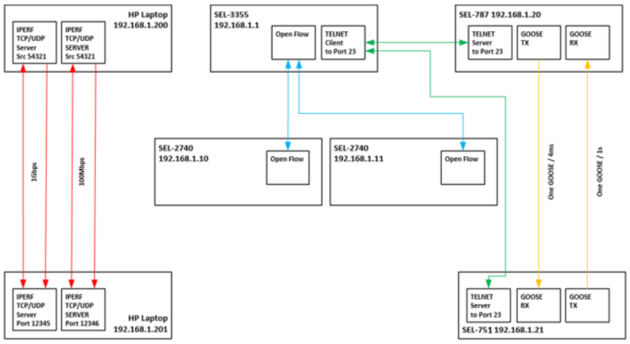
Logical connections

Scripting via RESTful API

Learn & Lock

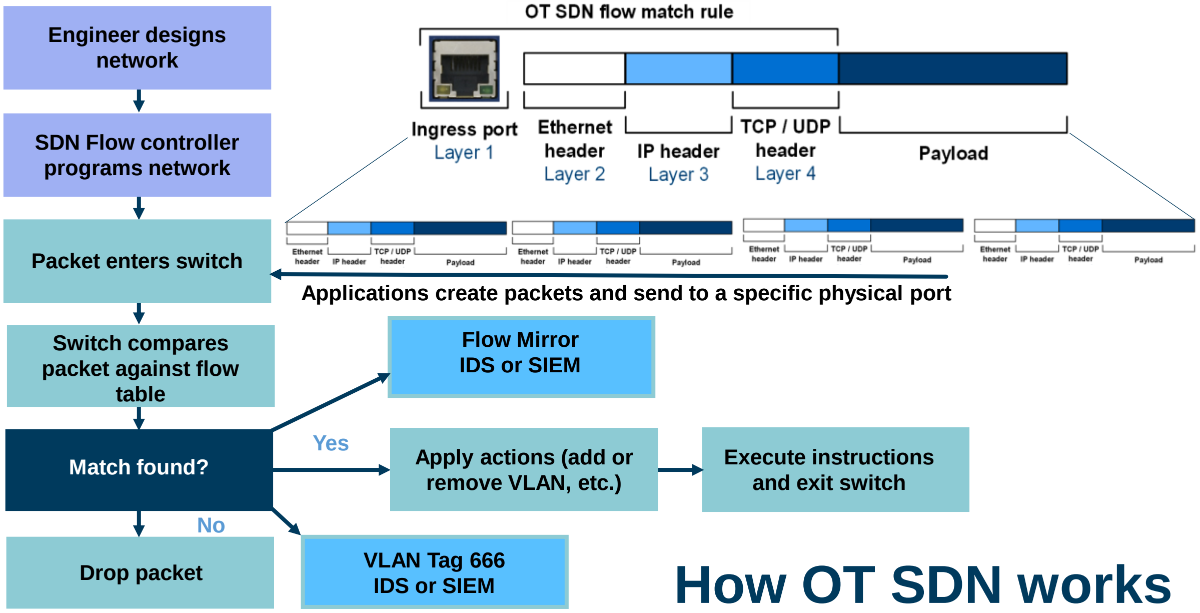
Network diagram + dataflow diagram = baseline and asset management





OT SDN ensures that the network enforces plans and policy!

How OT SDN works


Engineer designs network

SDN Flow controller programs network

Packet enters switch

Switch compares packet against flow table

Match found?

Yes

No

Flow Mirror IDS or SIEM

Apply actions (add or remove VLAN, etc.)

Execute instructions and exit switch

Drop packet

VLAN Tag 666 IDS or SIEM

OT SDN flow match rule

Ingress port Layer 1

Ethernet header Layer 2

IP header Layer 3

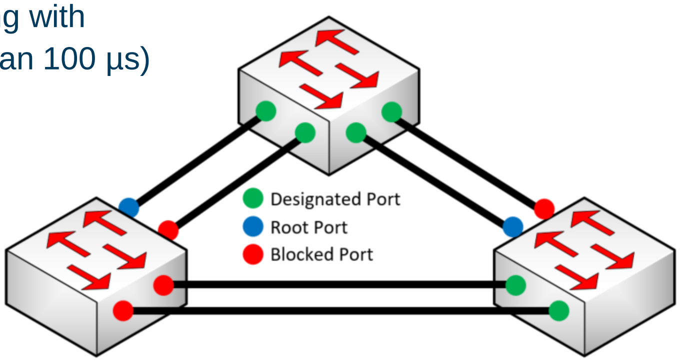
TCP / UDP header Layer 4

Payload

Applications create packets and send to a specific physical port

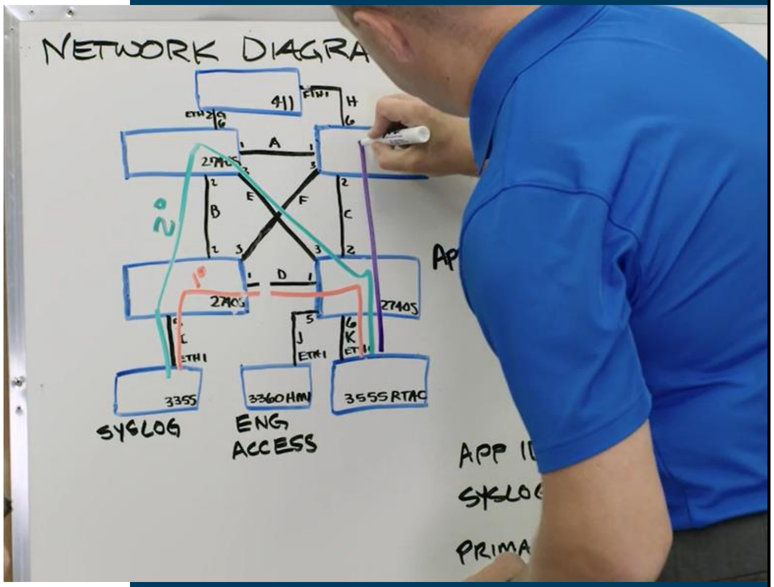
SDN is two orders of magnitude faster!

- Traditional RSTP does not meet the needs of protection traffic (~20 to 100 ms)
- Preplanned traffic engineering with OT SDN fast failover (less than 100 µs)



SDN simplifies how networks are engineered

- Removal of network restrictions
- Removal of plug-and-play
- Freedom to traffic-engineer for your application



SEL SDN performance

Failover times under 100 µs vs. 10–30+ ms for traditional networks (for GOOSE, process bus, and arc flash)

Greater ability to manage substation networks

Unlike RSTP switches, no blocked ports to limit bandwidth

LAN security prevents plug-and-play services

Performance

Cybersecurity

Securing networks with OT SDN – only allow data you want onto your network

- Ethernet assumes trust
- OT SDN requires preapproval
- Security is part of every switch
- Fewer security network devices are required

SEL SDN benefits – cybersecurity and network management

Improved cybersecurity

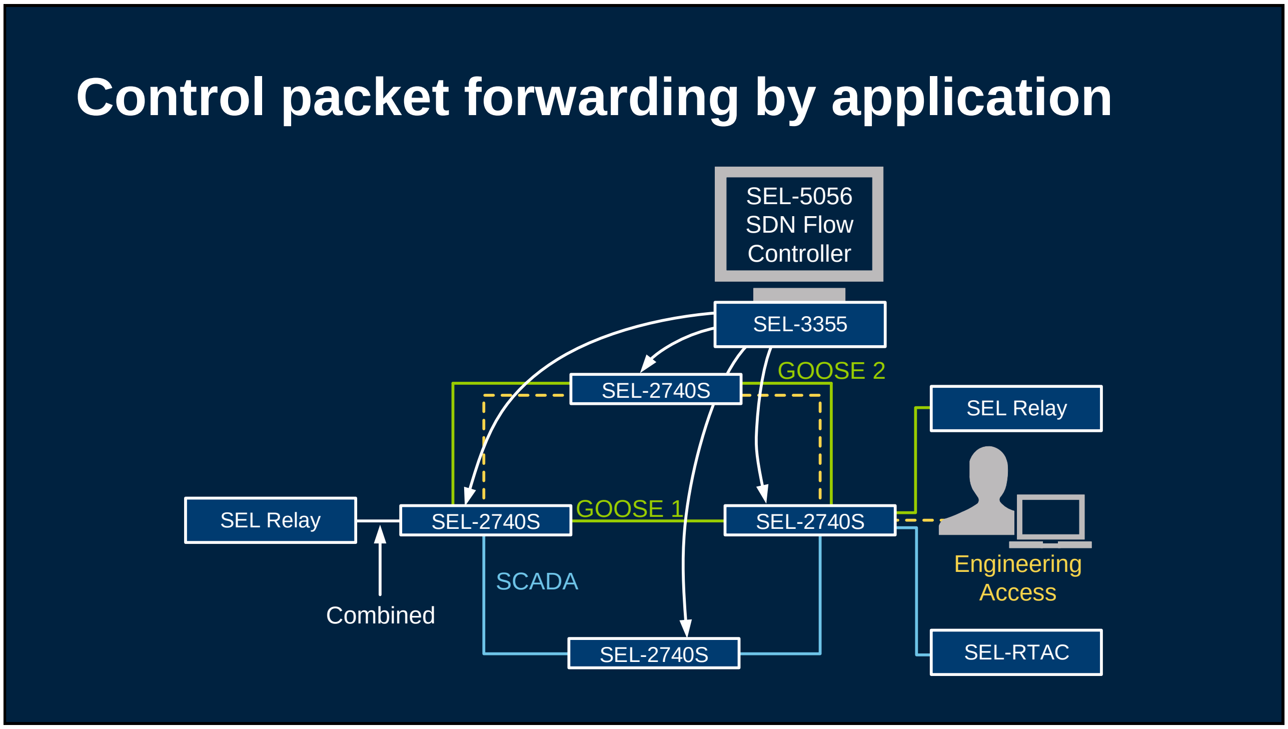
Employs deny-by-default approach

Eliminates attack-prone elements of traditional networking (MAC tables, RSTP, and broadcast / multicast)

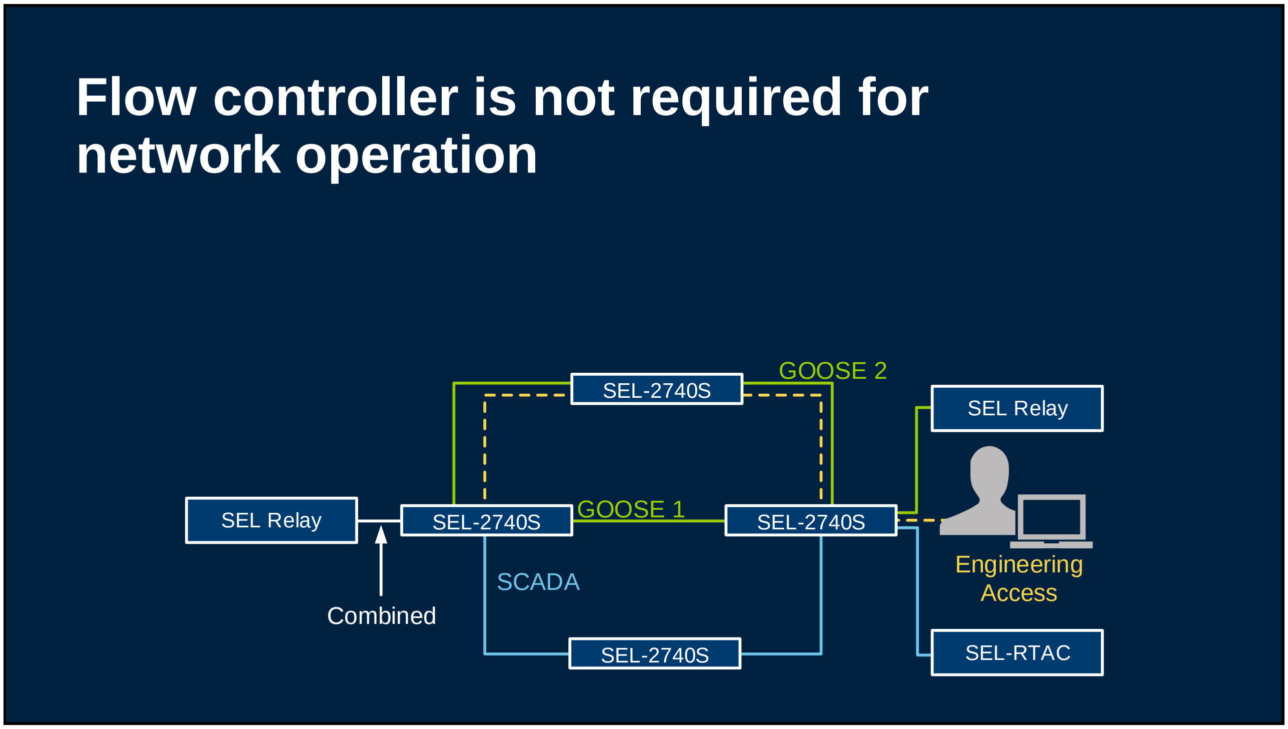
Uses Syslog event logging through controller or switches

Automated data collection for security auditing

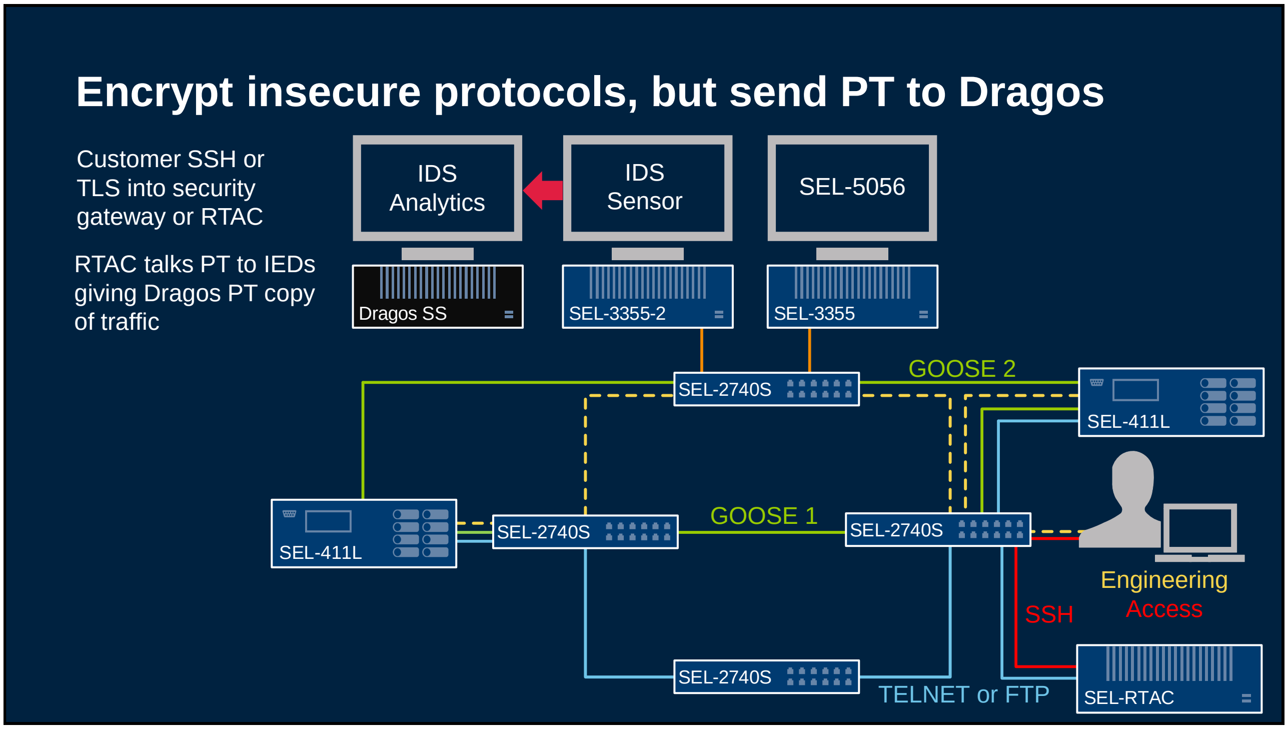
Centralized management of switches



Control packet forwarding by application



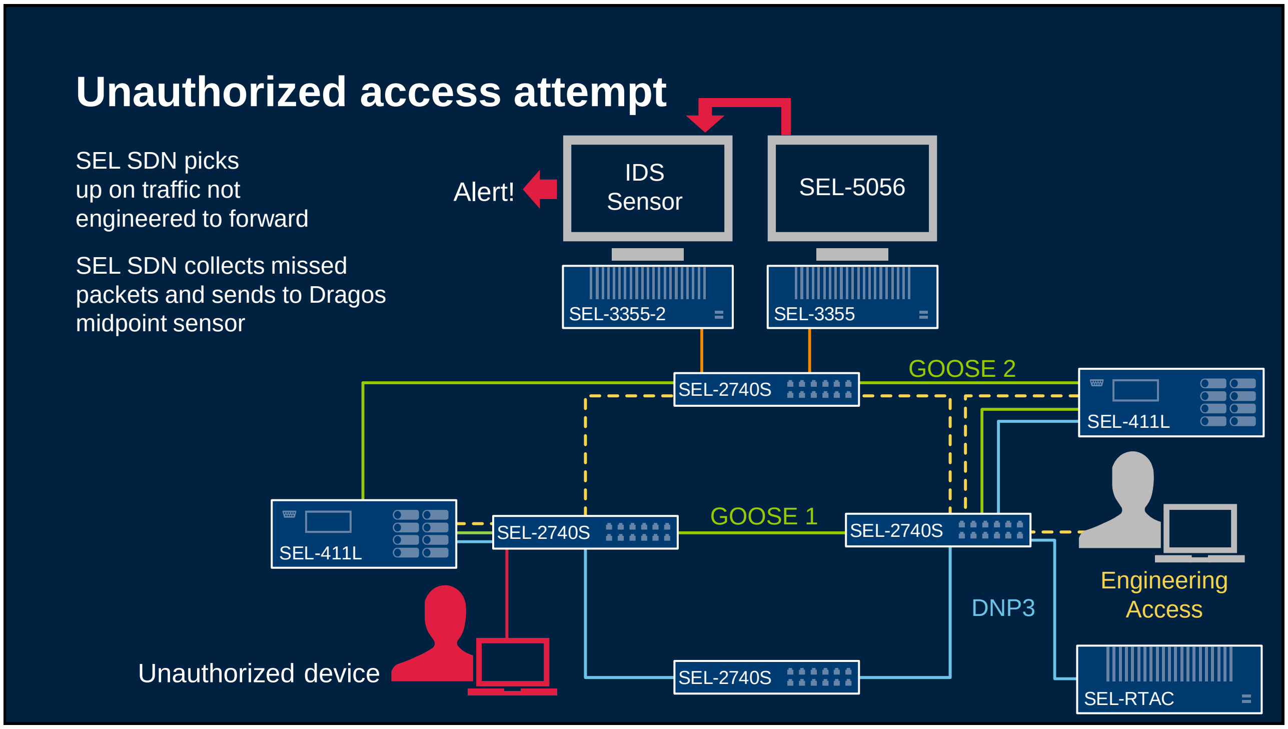
Flow controller is not required for network operation



Encrypt insecure protocols, but send PT to Dragos

Customer SSH or TLS into security gateway or RTAC

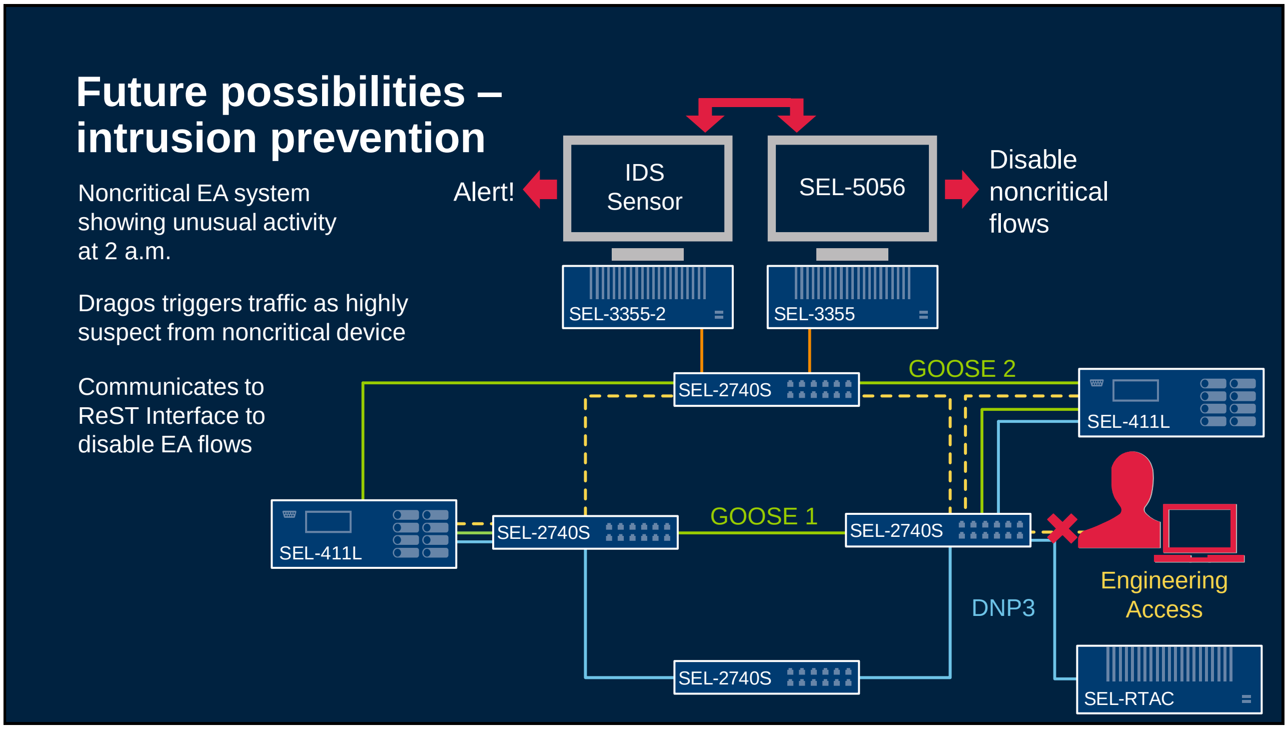
RTAC talks PT to IEDs giving Dragos PT copy of traffic



Unauthorized access attempt

SEL SDN picks up on traffic not engineered to forward

SEL SDN collects missed packets and sends to Dragos midpoint sensor

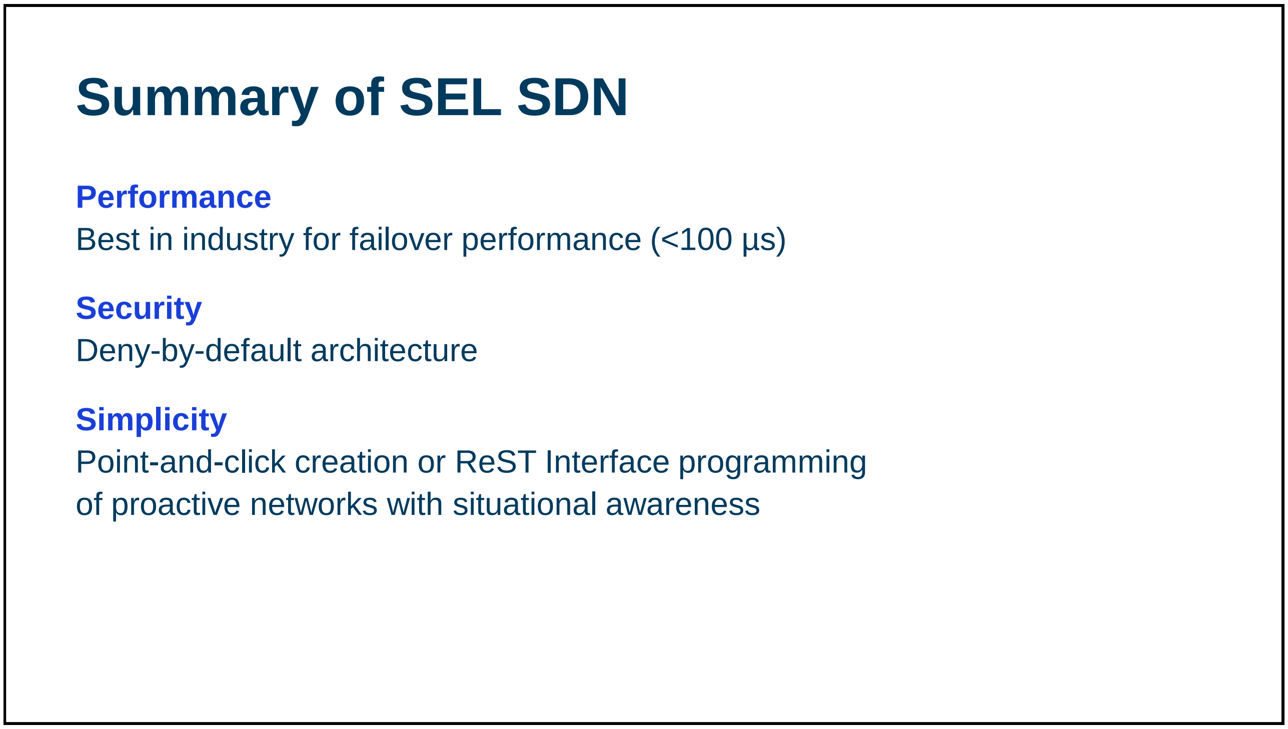


Future possibilities – intrusion prevention

Noncritical EA system showing unusual activity at 2 a.m.

Dragos triggers traffic as highly suspect from noncritical device

Communicates to ReST Interface to disable EA flows



Summary of SEL SDN

Performance
Best in industry for failover performance (<100 µs)

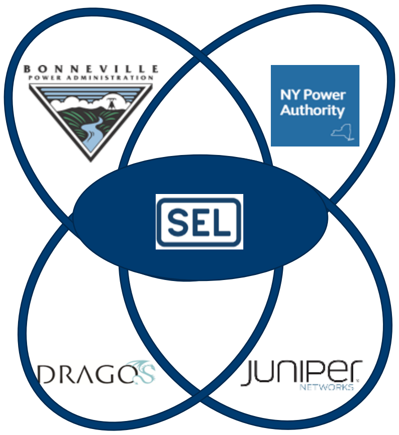
Security
Deny-by-default architecture

Simplicity
Point-and-click creation or ReST Interface programming of proactive networks with situational awareness

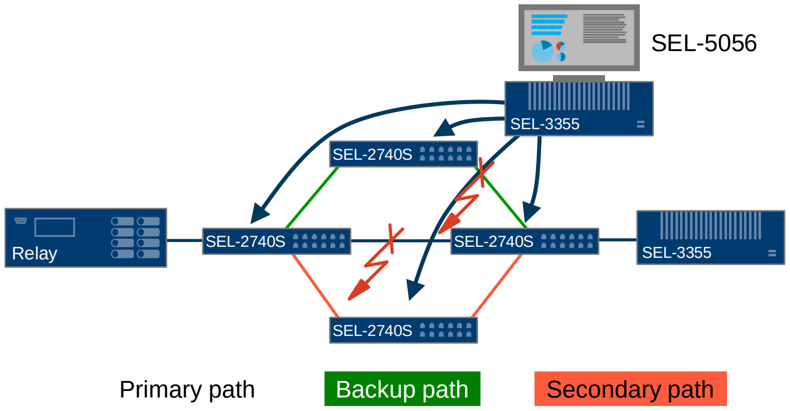
SEL Blueframe™ platform and applications

Ambassador project overview – objectives

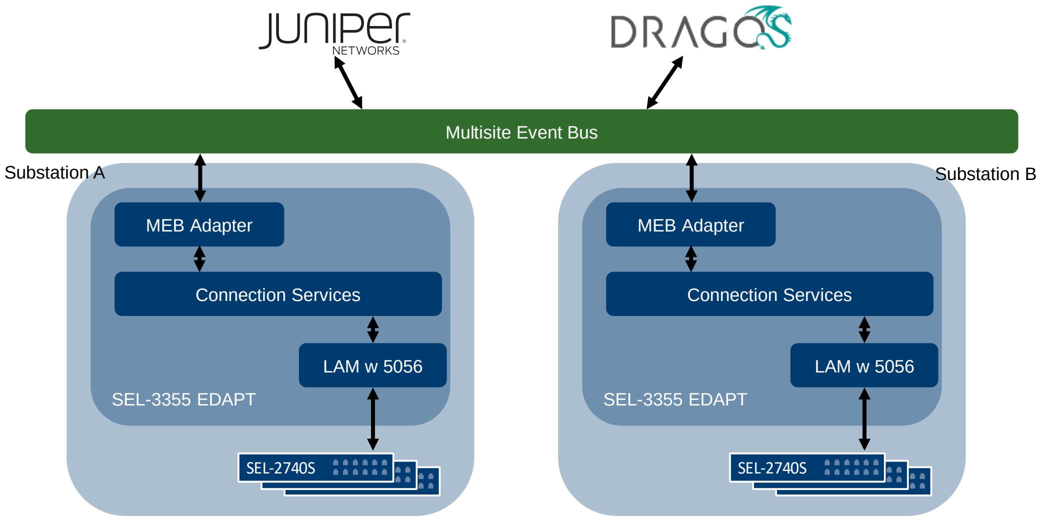
- To strengthen cybersecurity for energy delivery systems using proven DOE OT SDN technology, the ambassador project shall research, develop, demonstrate, and productize a joint manufacturer solution capable of managed trust and data sharing between multiple software applications for improving awareness and visualization of utilities' enterprise and OT systems
- Ambassador intends to address CEDS Topic Area 4: Cybersecure Cloud-based Technologies in the Operational Technology (OT) Environment



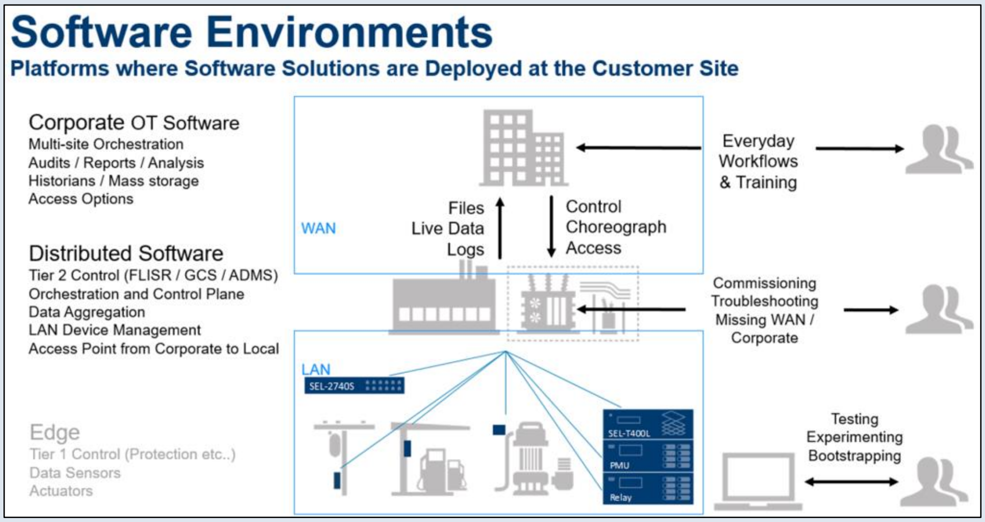
Today’s present SOA – DoE OT SDN



Advancing the SOA



Today’s utility application state



Software Environments

Platforms where Software Solutions are Deployed at the Customer Site

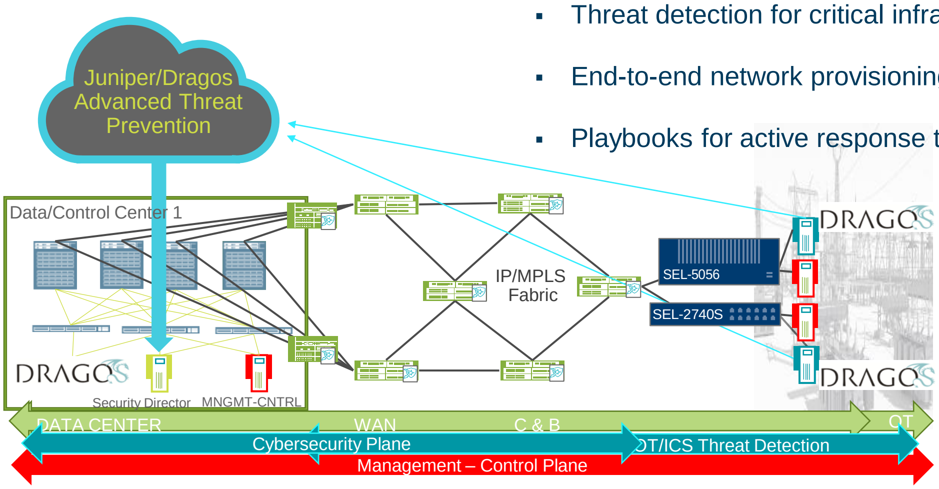
Corporate OT Software
Multi-site Orchestration
Audits / Reports / Analysis
Historians / Mass storage
Access Options

Distributed Software
Tier 2 Control (FLISR / GCS / ADMS)
Orchestration and Control Plane
Data Aggregation
LAN Device Management
Access Point from Corporate to Local

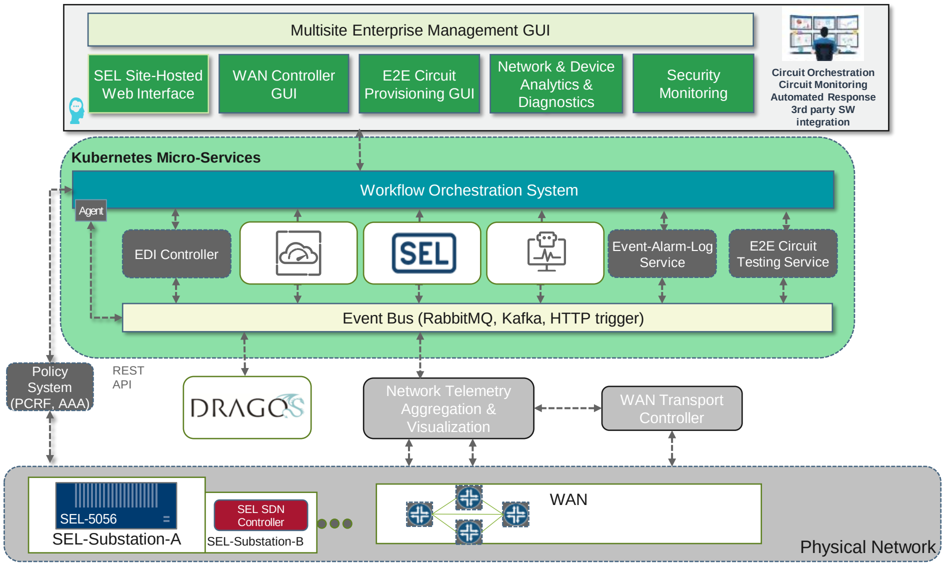
Edge
Tier 1 Control (Protection etc..)
Data Sensors
Actuators

Full-stack enterprise + OT solution

- Threat detection for critical infrastructure
- End-to-end network provisioning
- Playbooks for active response to ICS/OT attacks



IT/OT convergence solutions



Multisite Enterprise Management GUI

SEL Site-Hosted Web Interface

WAN Controller GUI

E2E Circuit Provisioning GUI

Network & Device Analytics & Diagnostics

Security Monitoring

Circuit Orchestration
Circuit Monitoring
Automated Response
3rd party SW integration

Kubernetes Micro-Services

Workflow Orchestration System

Agent

EDI Controller

SEL

Event-Alarm-Log Service

E2E Circuit Testing Service

Event Bus (RabbitMQ, Kafka, HTTP trigger)

Policy System (PCRF, AAA)

REST API

DRAGOS

Network Telemetry Aggregation & Visualization

WAN Transport Controller

SEL-5056

SEL-Substation-A

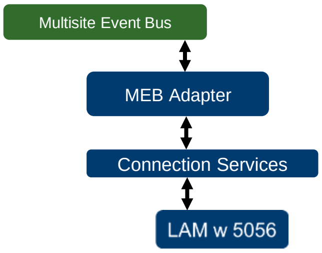
SEL SDN Controller

SEL-Substation-B

WAN

Physical Network

Multisite event bus adapter



Multisite Event Bus

MEB Adapter

Connection Services

LAM w 5056

Authenticate

to MEB broker

Translate

provisioning and teardown requests from MEB

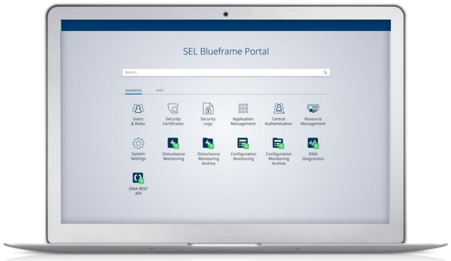
to Connection Services model

Publish

configuration and diagnostic information to MEB

for enterprise monitoring and threat hunting context

Blueframe application platform



Secure – provides safe methods to share information between applications

Flexible – allows selection of needed applications and hardware

Simple – centralizes access to IED data, permissions, and security parameters

Scalable – supports systems of any size

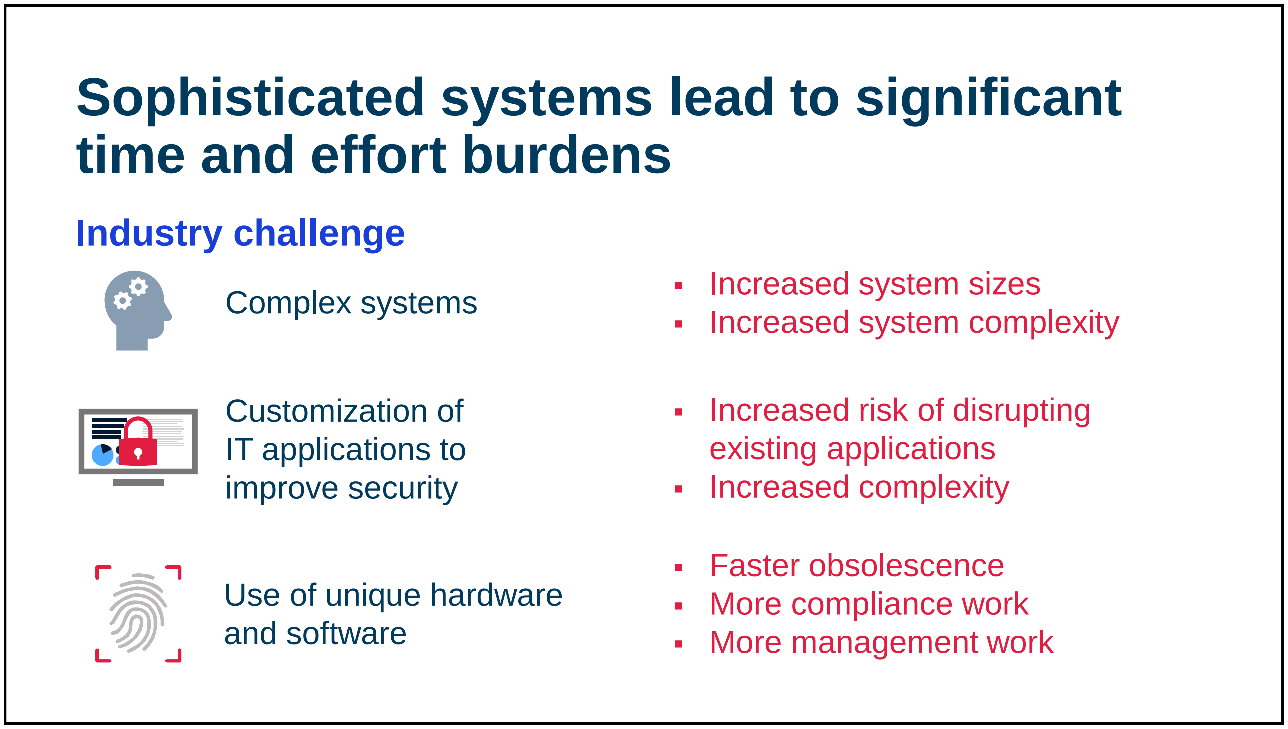
Data Management and Automation (DMA) applications

Simplify IED data collection with full automation and simple configuration

Secure data collection with single-point controlled access to device data and passwords

Improve data longevity with DMA short-term archiving using publication and API support

Improve data utilization through automated data normalization and single interface for analysis tool access



Sophisticated systems lead to significant time and effort burdens

Industry challenge

Complex systems

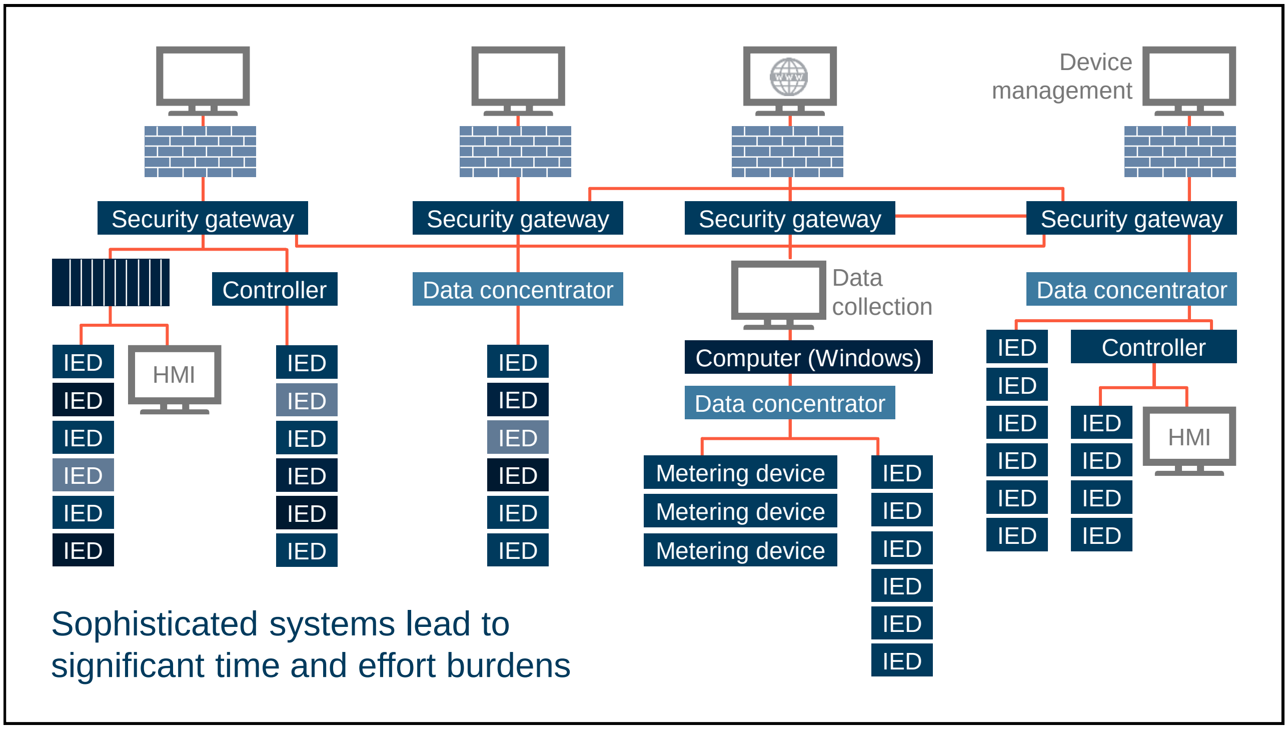
- Increased system sizes
- Increased system complexity

Customization of IT applications to improve security

- Increased risk of disrupting existing applications
- Increased complexity

Use of unique hardware and software

- Faster obsolescence
- More compliance work
- More management work



Device management

Security gateway

Security gateway

Security gateway

Security gateway

Controller

IED
IED
IED
IED
IED
IED

HMI

IED
IED
IED
IED
IED
IED

Data concentrator

IED
IED
IED
IED
IED
IED

Data collection

Computer (Windows)

Data concentrator

Metering device
Metering device
Metering device

IED
IED
IED
IED
IED
IED

Data concentrator

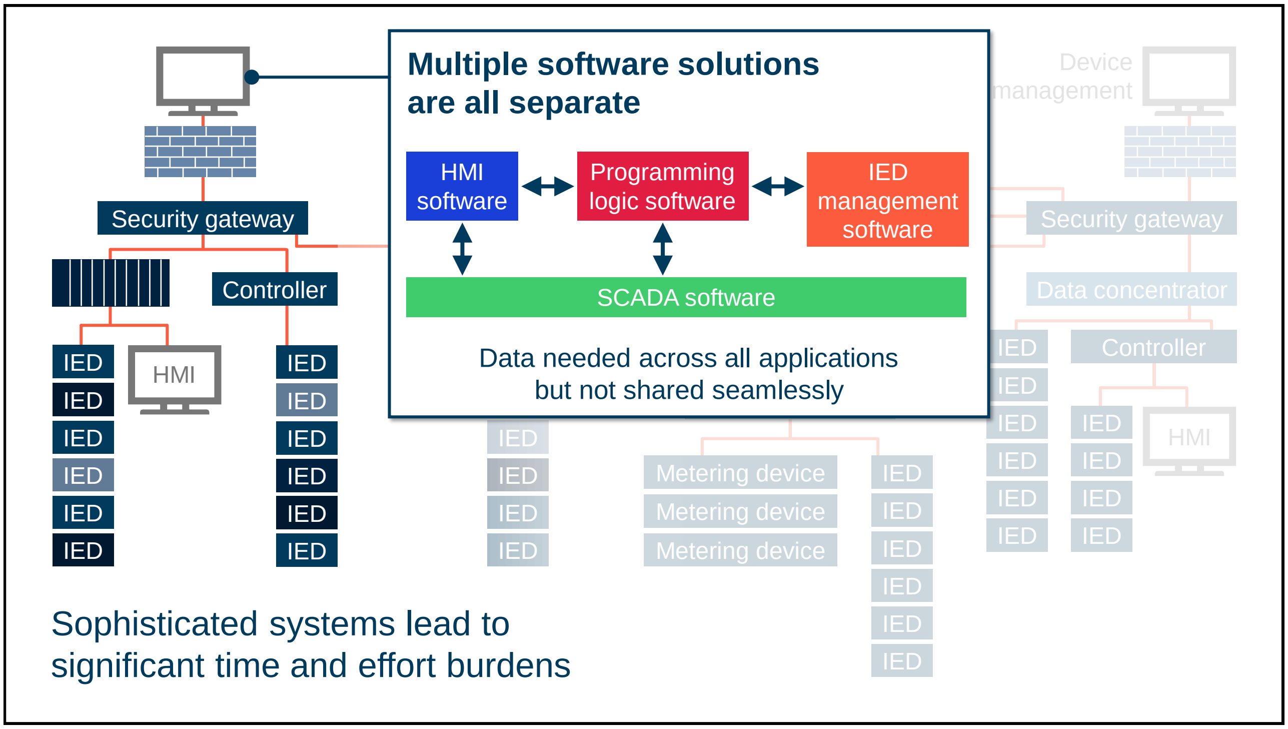
Controller

IED
IED
IED
IED
IED
IED

IED
IED
IED
IED

HMI

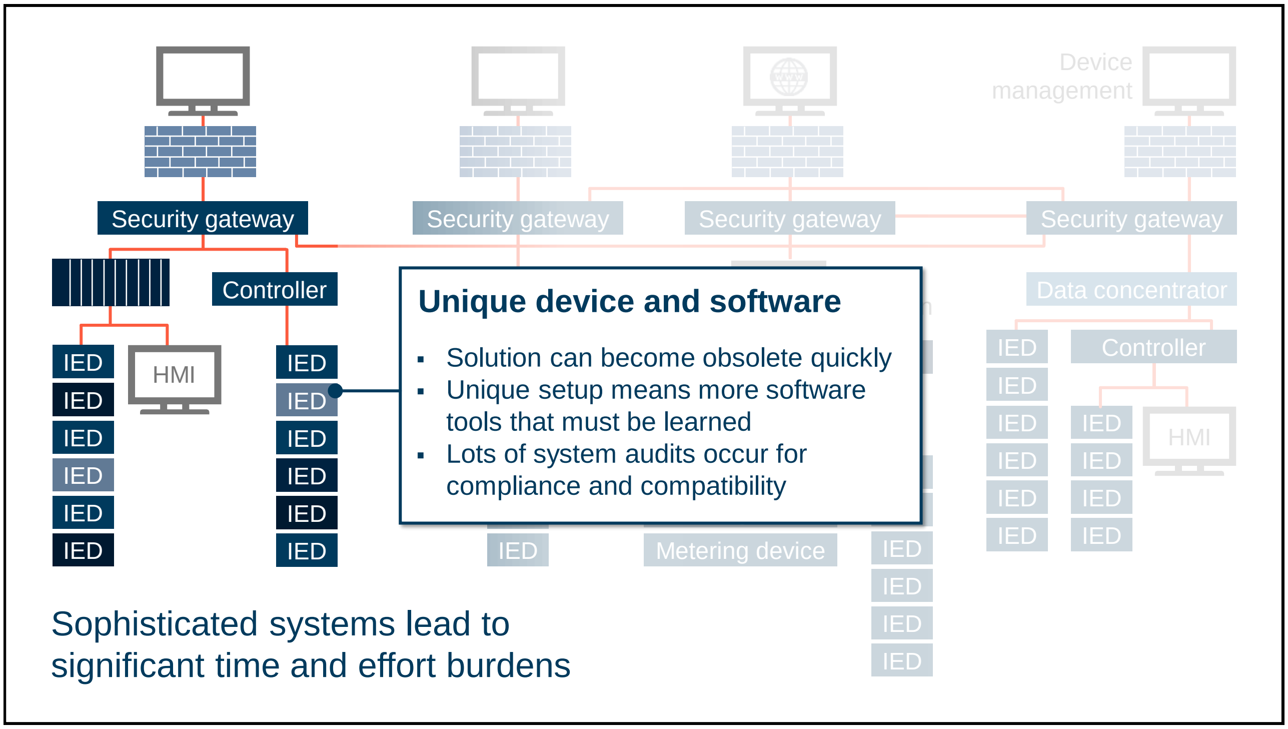
Sophisticated systems lead to significant time and effort burdens



Multiple software solutions are all separate

Data needed across all applications but not shared seamlessly

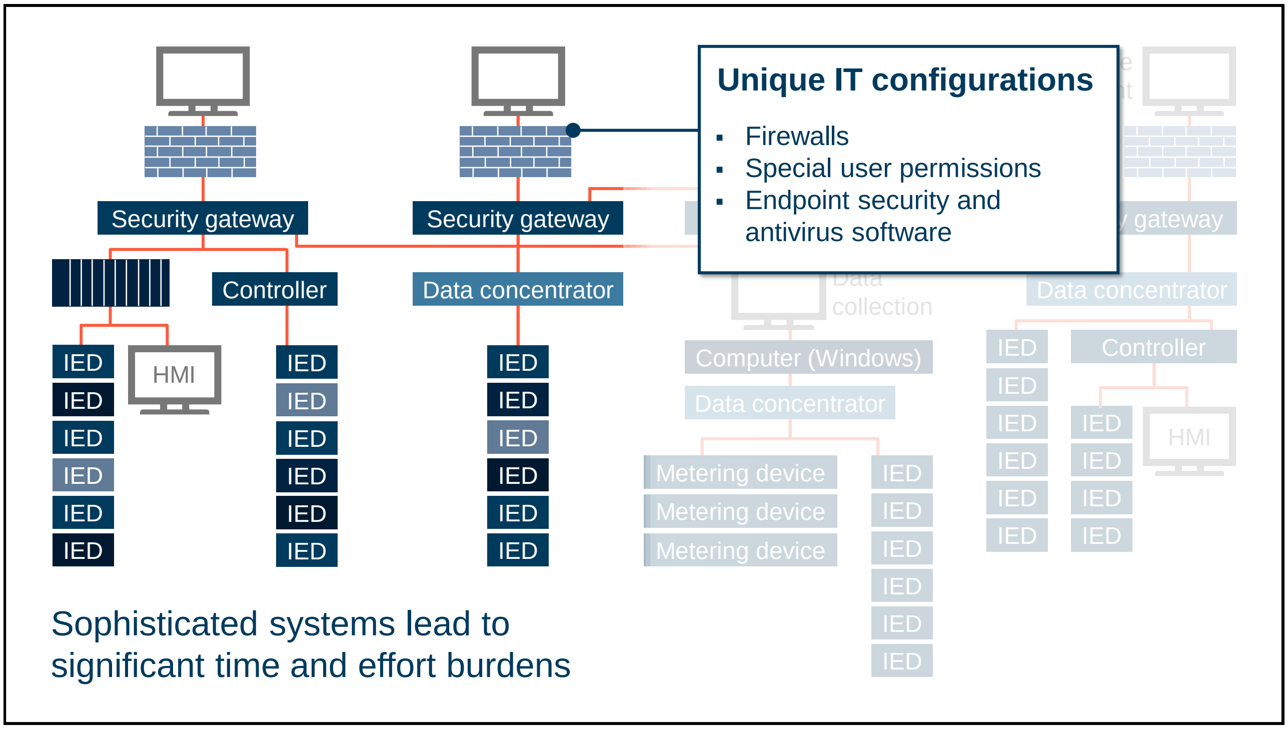
Sophisticated systems lead to significant time and effort burdens



Unique device and software

- Solution can become obsolete quickly
- Unique setup means more software tools that must be learned
- Lots of system audits occur for compliance and compatibility

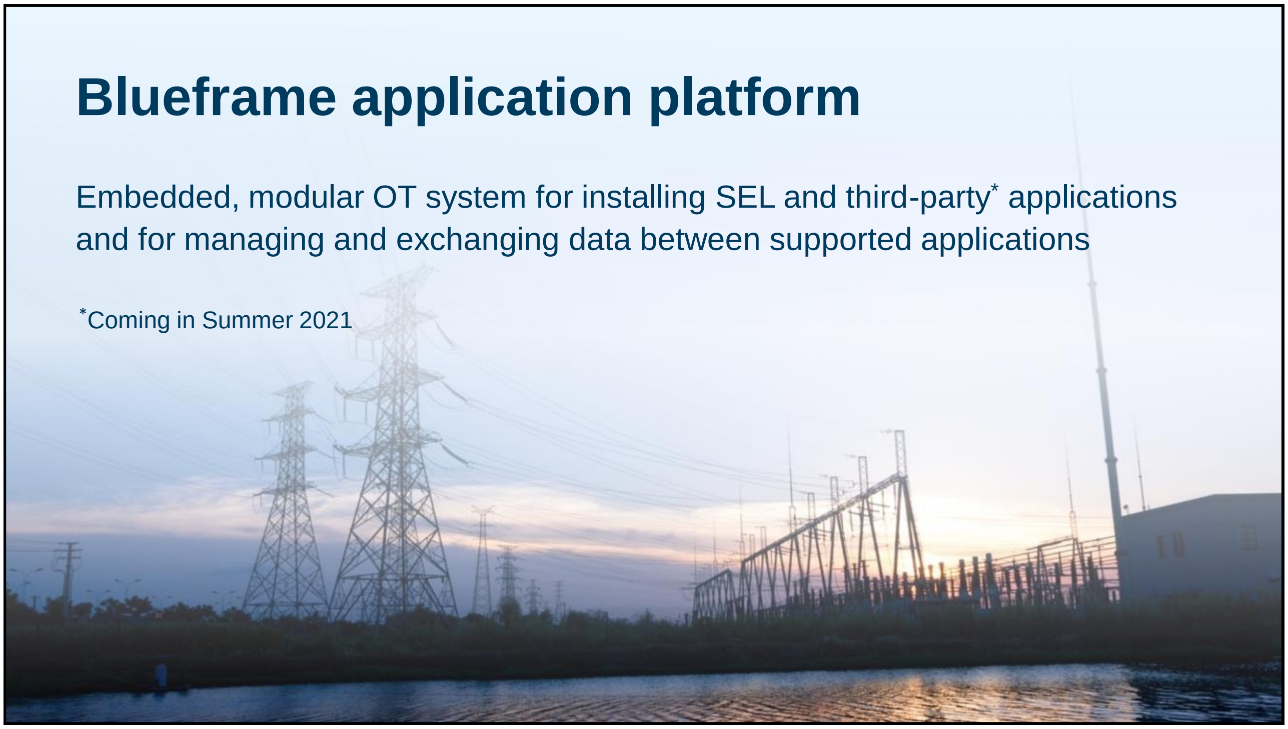
Sophisticated systems lead to significant time and effort burdens



Unique IT configurations

- Firewalls
- Special user permissions
- Endpoint security and antivirus software

Sophisticated systems lead to significant time and effort burdens



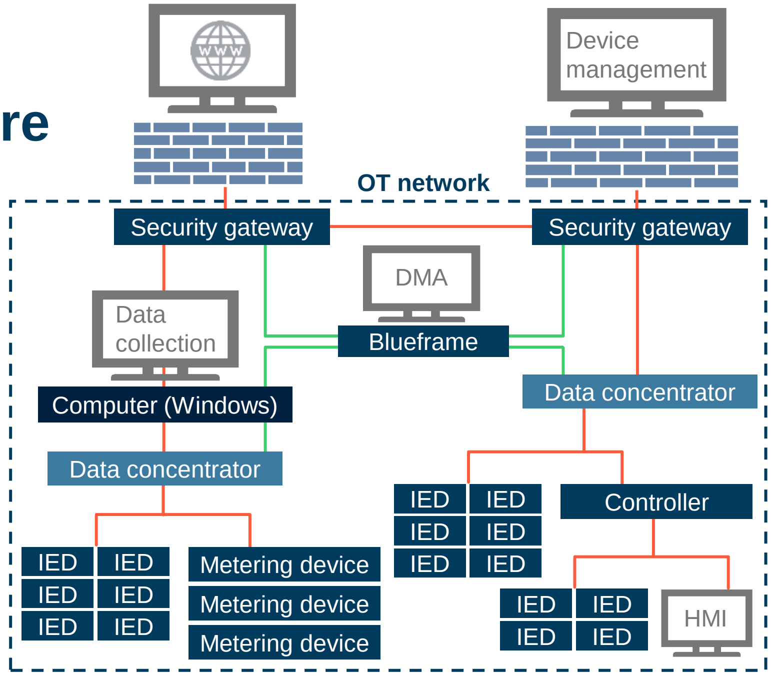
Blueframe application platform

Embedded, modular OT system for installing SEL and third-party* applications and for managing and exchanging data between supported applications

*Coming in Summer 2021

Consolidate multiple hardware capabilities into single platform

- Improve security by reducing system access points
- Reduce system design complexity
- Reduce maintenance touchpoints



OT network

Device management

Security gateway

Security gateway

DMA

Data collection

Blueframe

Computer (Windows)

Data concentrator

Data concentrator

IED IED IED IED IED IED

Metering device

Metering device

Metering device

IED IED IED IED IED IED

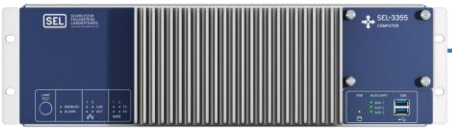
Controller

IED IED IED IED

HMI

New application ecosystem from SEL

Hardware



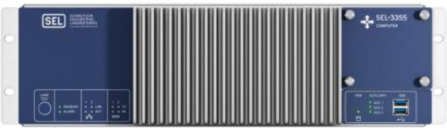
Runs embedded on
SEL automation controllers

- SEL-3350 New
- SEL-3355
- SEL-3360

New application ecosystem from SEL

Hardware → Platform

Blueframe application platform

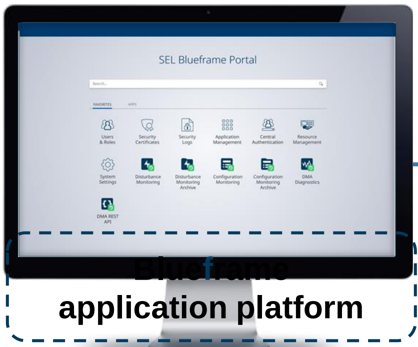


Secure platform

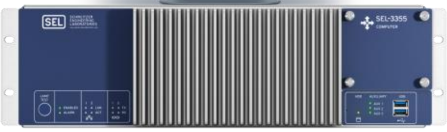
- Intuitive, simple interface
- Enables modular application environment
- Deploys several security methods

New application ecosystem from SEL

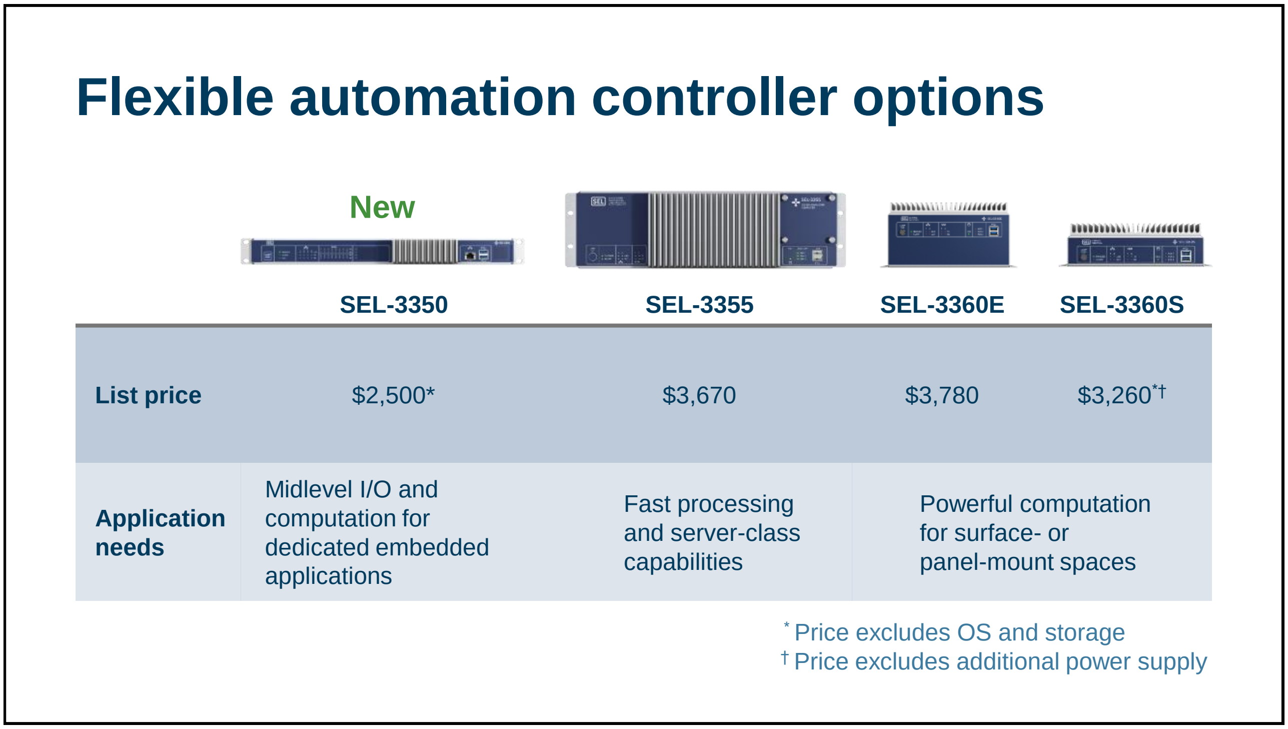
Hardware → Platform → Application and tools


SEL Blueframe Portal

Blueframe application platform



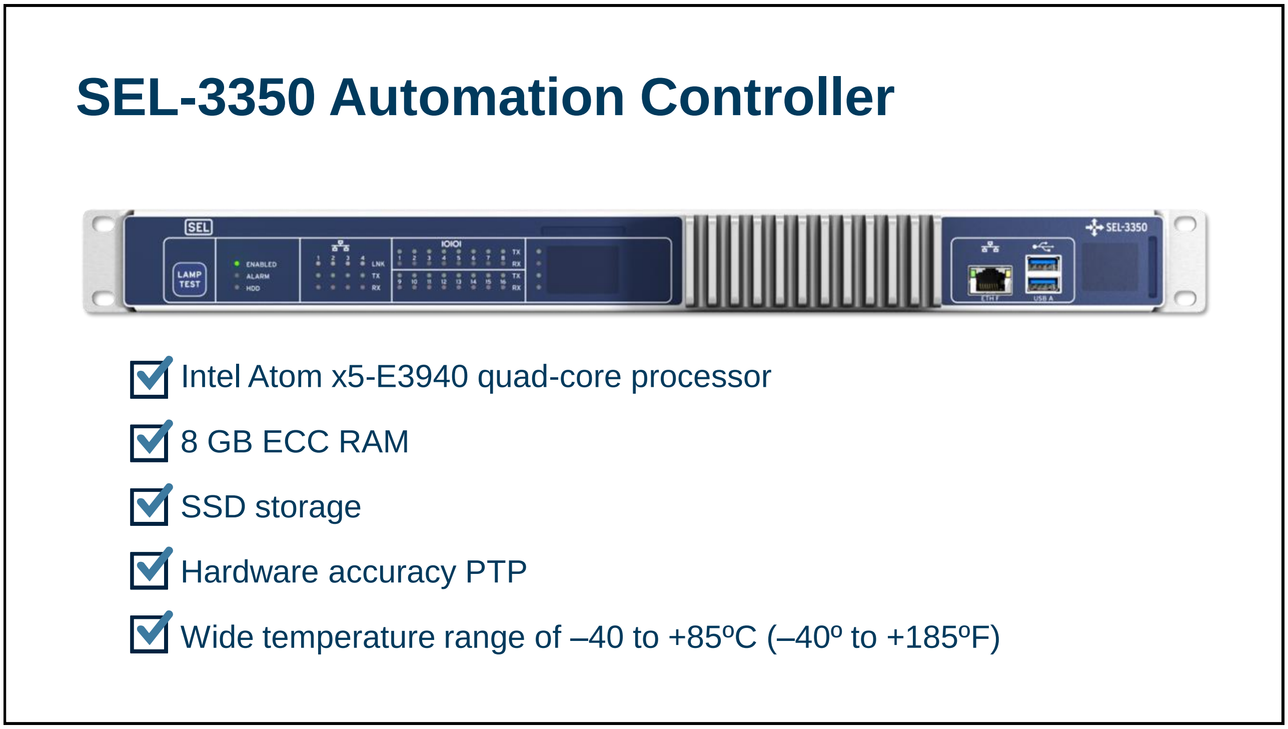
- Management tools
  - User management
  - Resource management
  - Security tools
- Applications
  - Are designed to be modular and independent
  - Share same data subscriptions through platform for security and efficiency



Flexible automation controller options

	SEL-3350	SEL-3355	SEL-3360E	SEL-3360S
List price	$2,500*	$3,670	$3,780	$3,260*†
Application needs	Midlevel I/O and computation for dedicated embedded applications	Fast processing and server-class capabilities	Powerful computation for surface- or panel-mount spaces	

* Price excludes OS and storage
† Price excludes additional power supply



SEL-3350 Automation Controller

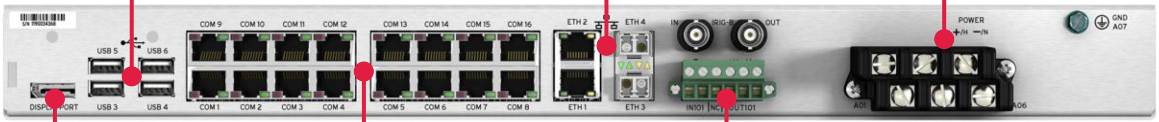
- ☑ Intel Atom x5-E3940 quad-core processor
- ☑ 8 GB ECC RAM
- ☑ SSD storage
- ☑ Hardware accuracy PTP
- ☑ Wide temperature range of –40 to +85ºC (–40º to +185ºF)

SEL-3350 features

Four USB 2.0 ports

Four high-speed configurable copper or fiber Gigabit Ethernet ports

Built-in power supplies



DisplayPort monitor

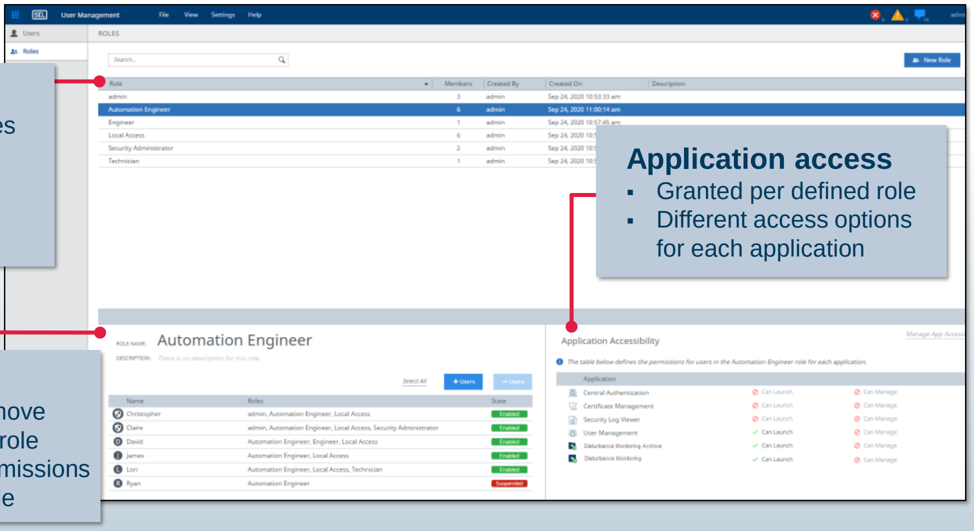
16 built-in RJ45 EIA-232 / EIA-485 ports

Configurable digital / analog input

Increase security with a need-to-know system

- Whitelisting
- Configurable roles
- User access to system, applications, and data
- Security logs

Simplify system security



Role	Members	Created By	Created On	Description
admin	3	admin	Sep 24, 2020 10:53:33 am	
Automation Engineer	6	admin	Sep 24, 2020 11:00:14 am	
Engineer	1	admin	Sep 24, 2020 10:57:45 am	
Local Access	6	admin	Sep 24, 2020 10:5	
Security Administrator	2	admin	Sep 24, 2020 10:5	
Technician	1	admin	Sep 24, 2020 10:5	

ROLE NAME: Automation Engineer

DESCRIPTION: *There is no description for this role.*

Name	Roles	State
Christopher	admin, Automation Engineer, Local Access	Enabled
Claire	admin, Automation Engineer, Local Access, Security Administrator	Enabled
David	Automation Engineer, Engineer, Local Access	Enabled
James	Automation Engineer, Local Access	Enabled
Lori	Automation Engineer, Local Access, Technician	Enabled
Ryan	Automation Engineer	Suspended

Application Accessibility

The table below defines the permissions for users in the Automation Engineer role for each application.

Application		
Central Authentication	⊘ Can Launch	⊘ Can Manage
Certificate Management	⊘ Can Launch	⊘ Can Manage
Security Log Viewer	⊘ Can Launch	⊘ Can Manage
User Management	✓ Can Launch	⊘ Can Manage
Disturbance Monitoring Archive	✓ Can Launch	⊘ Can Manage
Disturbance Monitoring	✓ Can Launch	⊘ Can Manage

User roles

- User-defined roles for permissions management
- Customizable role permissions

Application access

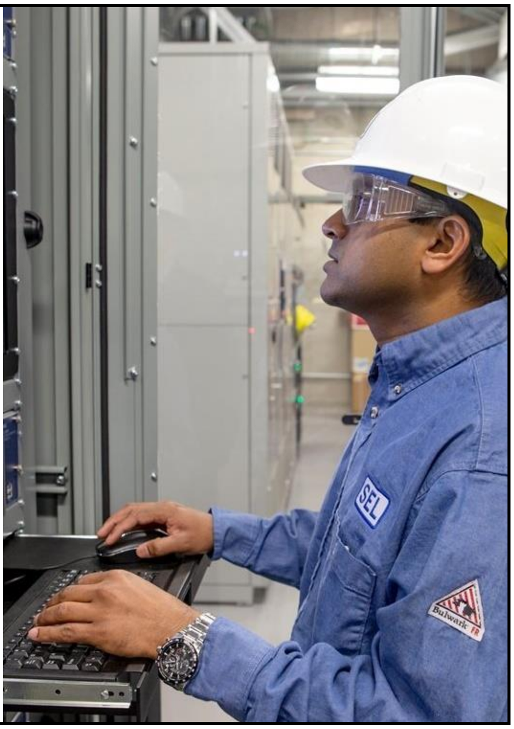
- Granted per defined role
- Different access options for each application

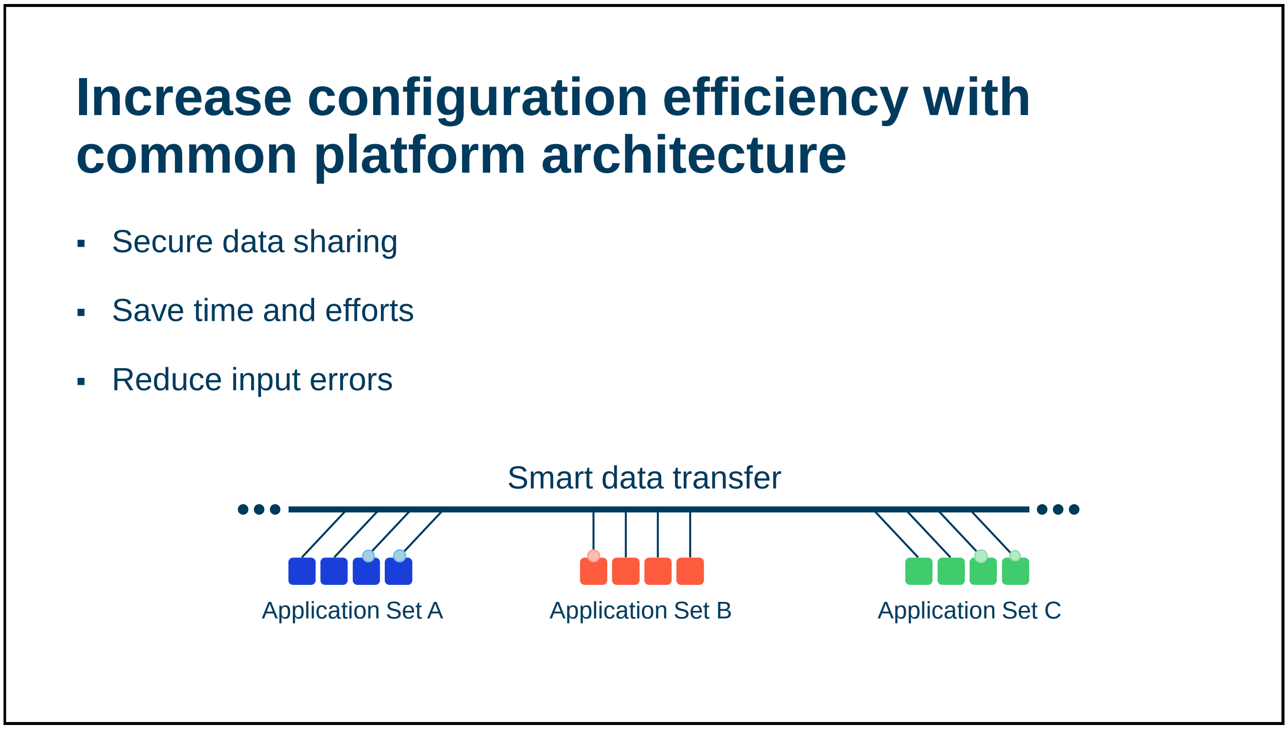
Role members

- Easily add or remove users from each role
- Users inherit permissions and access of role

Centralize different task operations from a single interface

- Manage user access permissions, security parameters, and IED data management
- Customize system functionality with modular applications without adding complexity





Increase configuration efficiency with common platform architecture

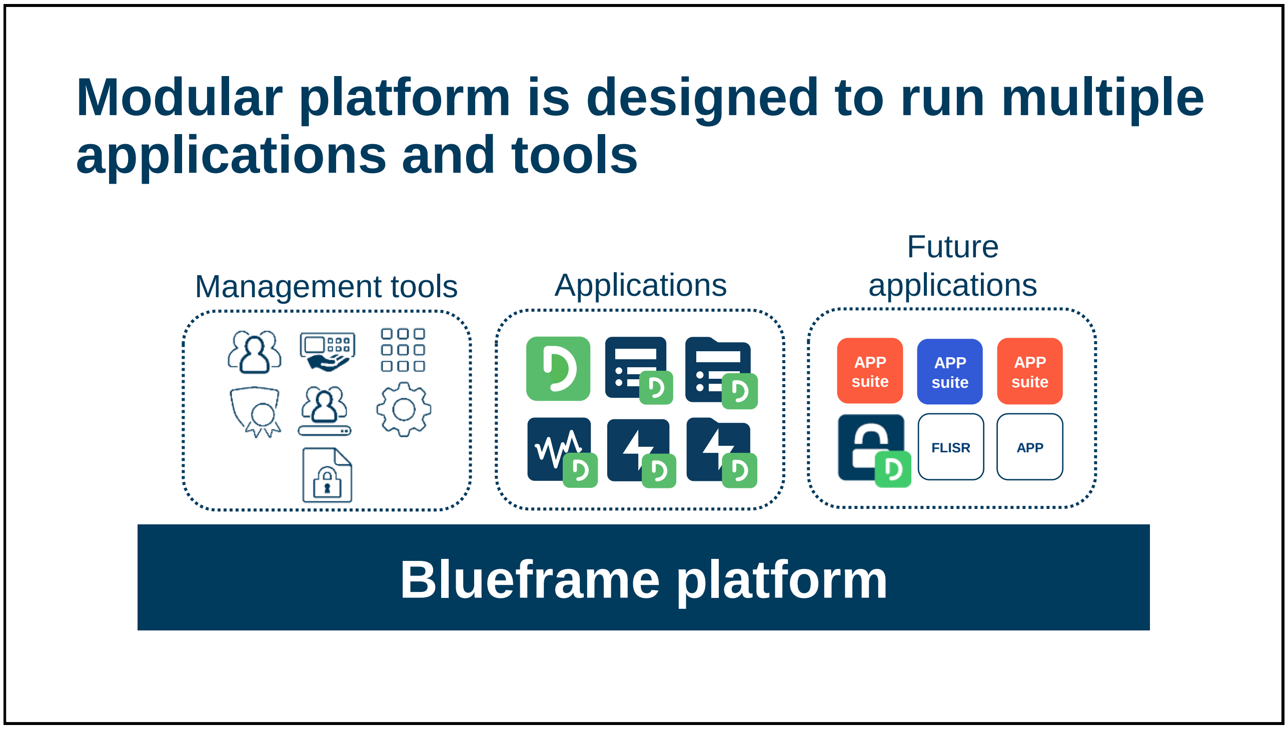
- Secure data sharing
- Save time and efforts
- Reduce input errors

Smart data transfer

Application Set A

Application Set B

Application Set C



Modular platform is designed to run multiple applications and tools

Management tools

Applications

Future applications

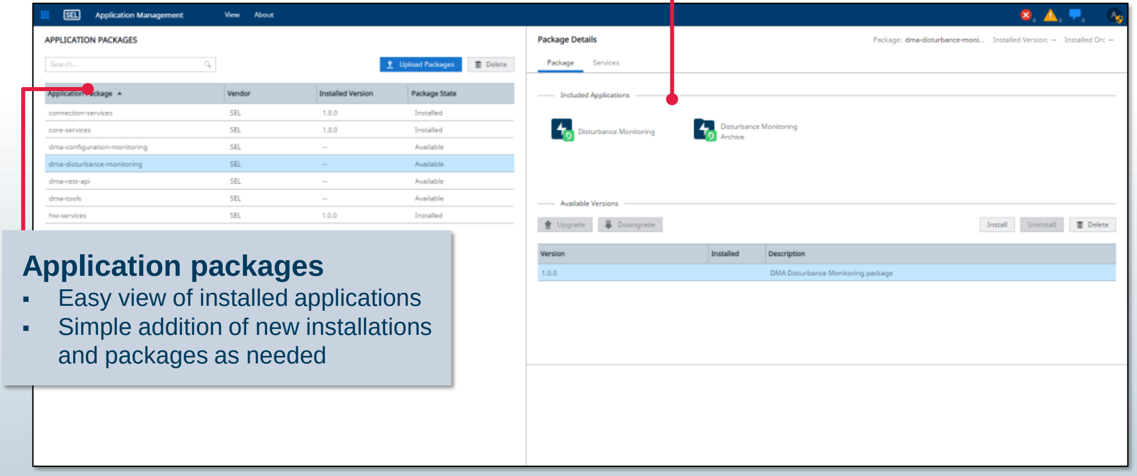
APP suite
APP suite
APP suite
FLISR
APP

Blueframe platform

Centralized system application management

Application details

- Control your versions
- Verify services
- Review system diagnostics



APPLICATION PACKAGES

Application Package ▲	Vendor	Installed Version	Package State
connection-services	SEL	1.0.0	Installed
core-services	SEL	1.0.0	Installed
dma-configuration-monitoring	SEL	--	Available
dma-disturbance-monitoring	SEL	--	Available
dma-rest-api	SEL	--	Available
dma-tools	SEL	--	Available
hw-services	SEL	1.0.0	Installed

Package Details

Package: dma-disturbance-moni... Installed Version: -- Installed On: --

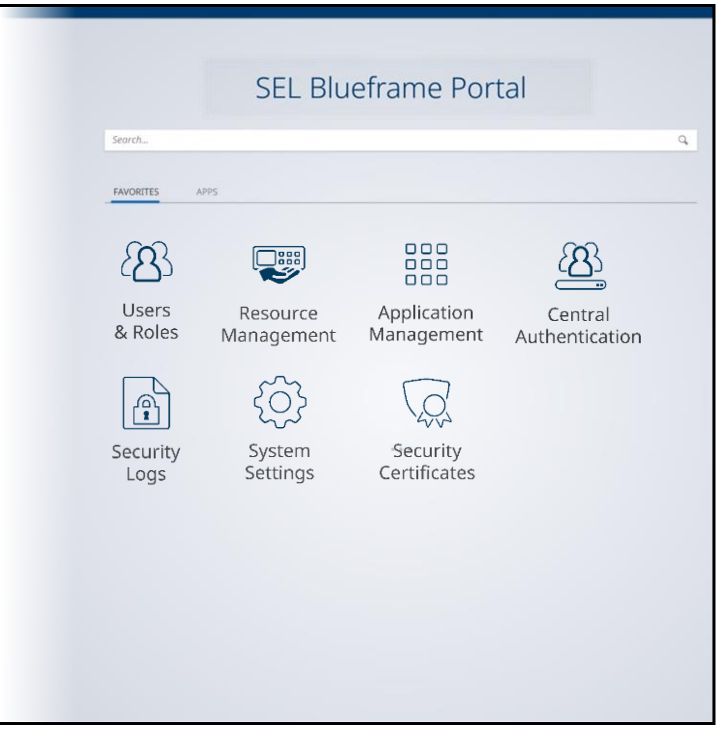
Version	Installed	Description
1.0.0		DMA Disturbance Monitoring package

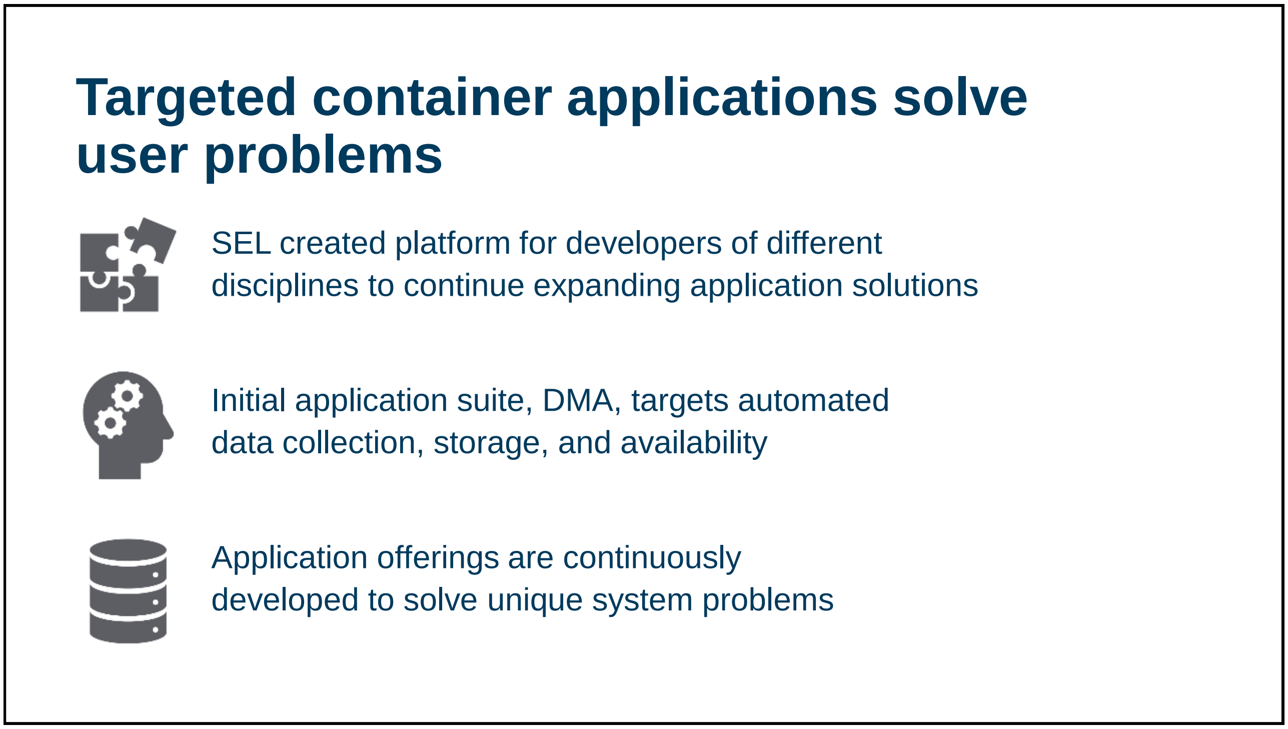
Application packages

- Easy view of installed applications
- Simple addition of new installations and packages as needed

Standard management tools

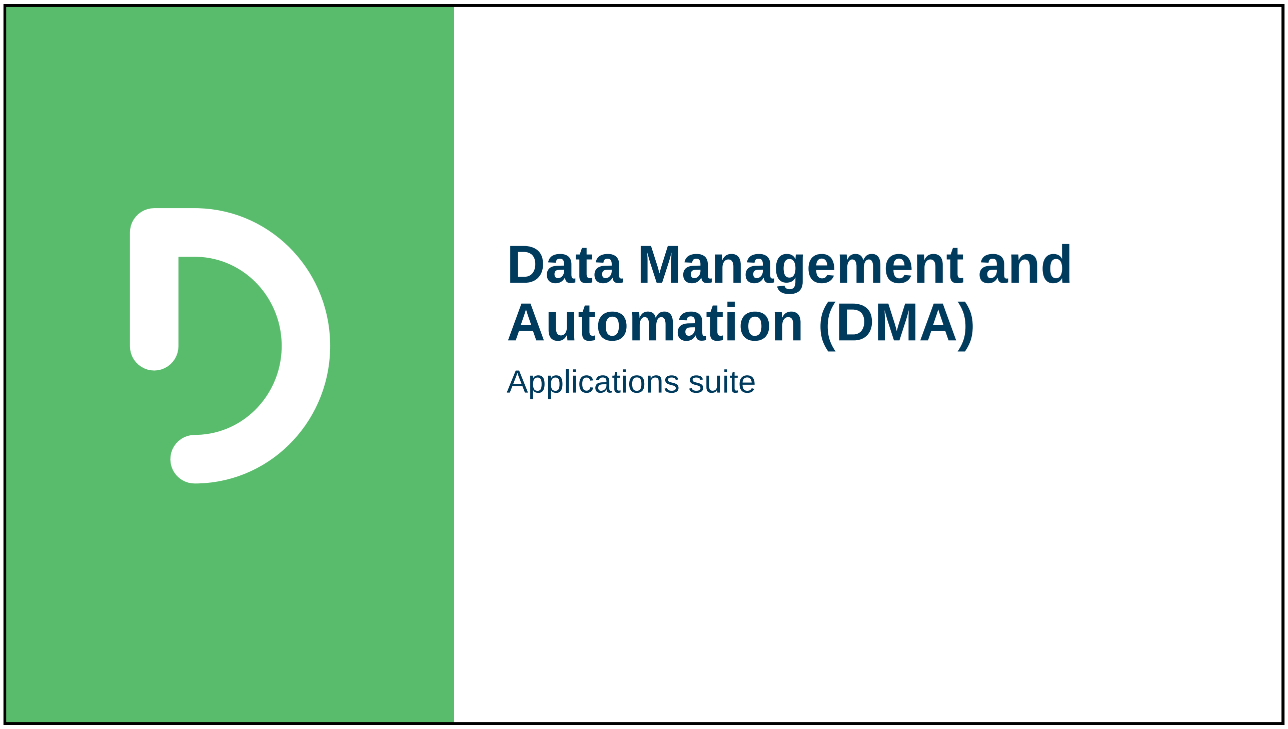
- User management
- Resource management
- Security log viewer
- Central authentication
- Certification management
- Application management
- System settings





Targeted container applications solve user problems

- SEL created platform for developers of different disciplines to continue expanding application solutions
- Initial application suite, DMA, targets automated data collection, storage, and availability
- Application offerings are continuously developed to solve unique system problems

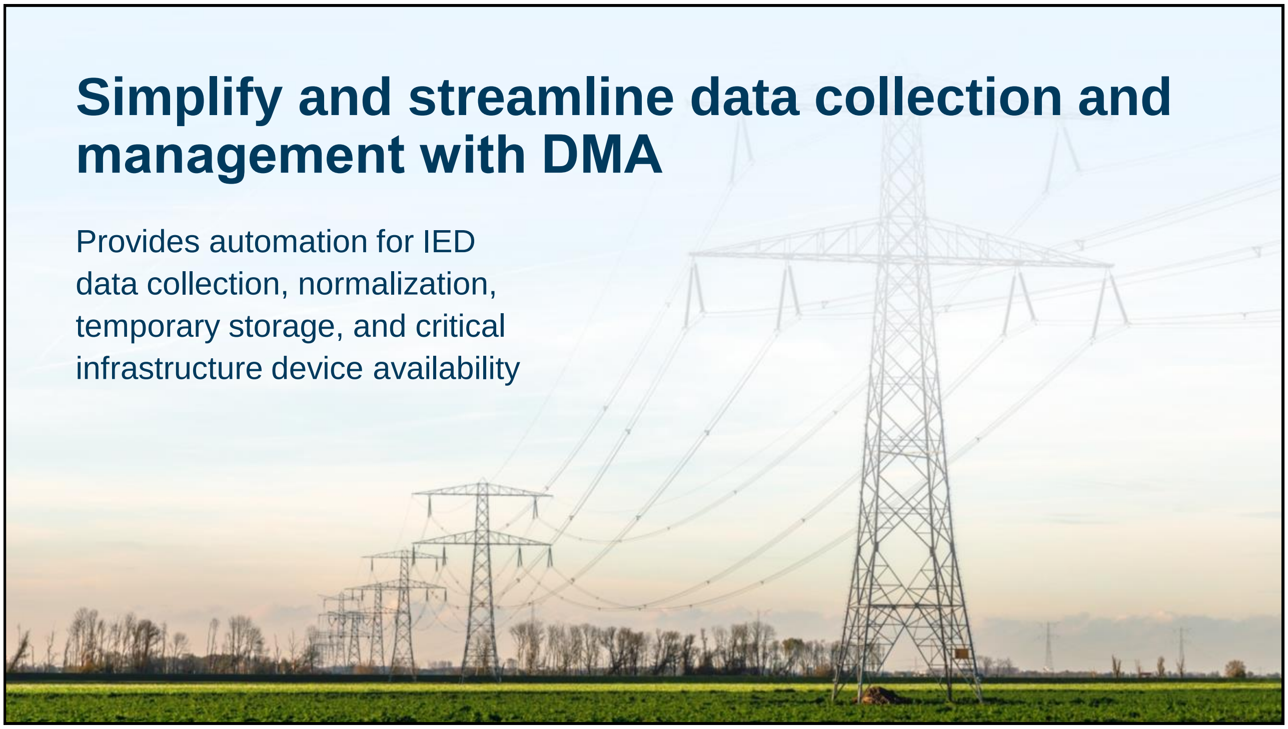


Data Management and Automation (DMA)

Applications suite

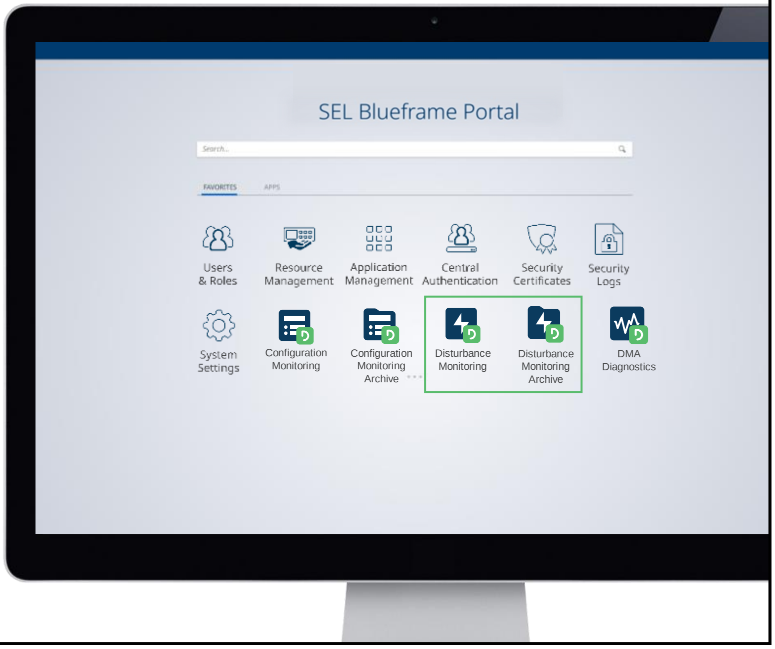
Simplify and streamline data collection and management with DMA

Provides automation for IED data collection, normalization, temporary storage, and critical infrastructure device availability



Disturbance Monitoring

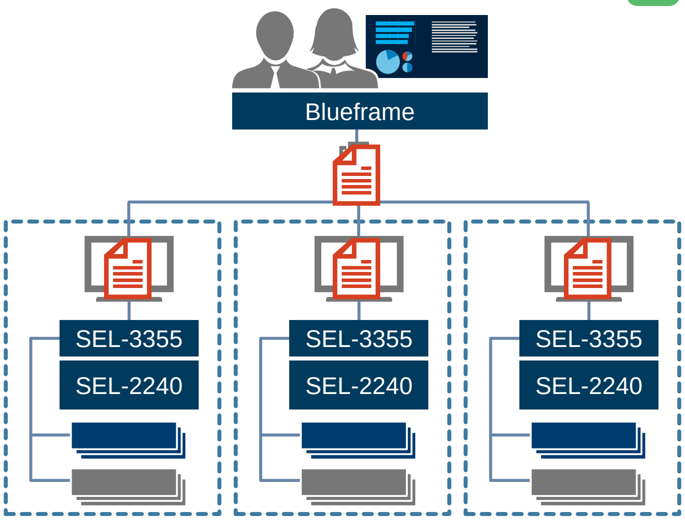
- Automated collection of event reports and SOE information
- RTAC listening support
- Short-term repository with API access
- Custom views of collected data



Aggregate system incidents

- Oscillography
- SOE
- Direct IED support
- MMS file transfer

Coming soon



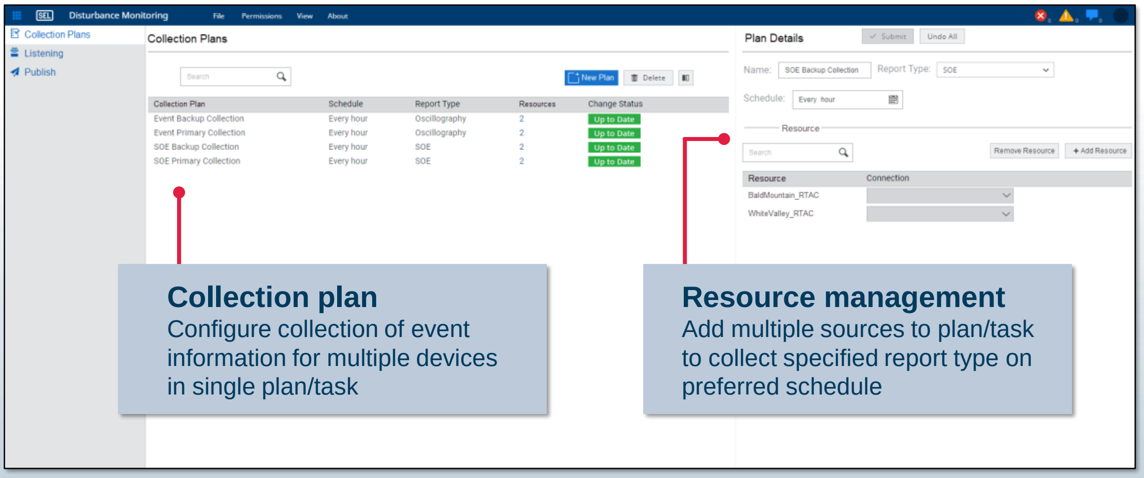
Expedite system restoration after a fault

- Gather oscillography and SOE information from supported devices
- Utilize RTACs to aggregate and expedite data collection

- View SOE information interspersed with oscillography for global system view

- Aggregate normalized data format
- Securely distribute it for analysis or to historian tools over public APIs

Configure systems of all magnitudes efficiently



Collection Plans

Collection Plan	Schedule	Report Type	Resources	Change Status
Event Backup Collection	Every hour	Oscillography	2	Up to Date
Event Primary Collection	Every hour	Oscillography	2	Up to Date
SOE Backup Collection	Every hour	SOE	2	Up to Date
SOE Primary Collection	Every hour	SOE	2	Up to Date

Plan Details

Name: SOE Backup Collection Report Type: SOE

Schedule: Every hour

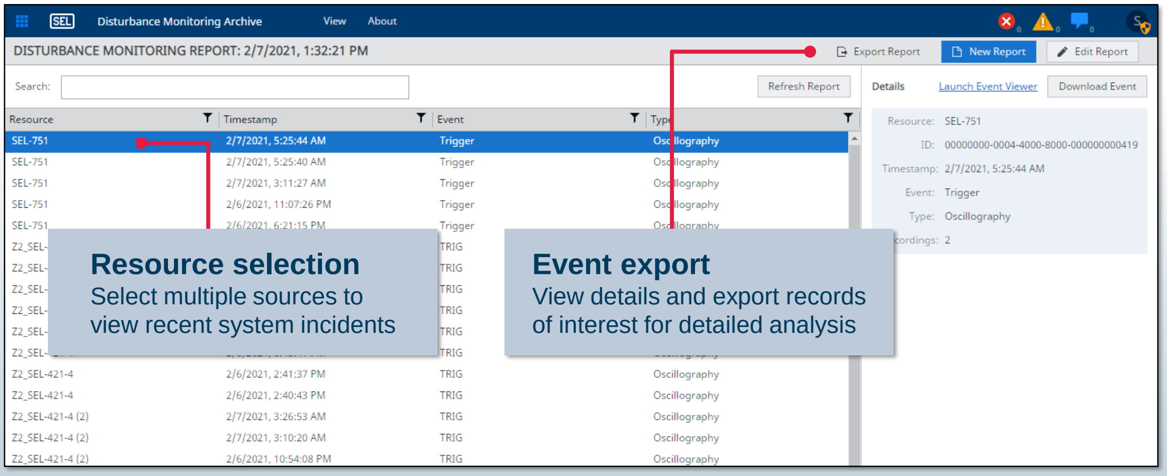
Resource

Resource	Connection
BaldMountain_RTAC	
WhiteValley_RTAC	

Collection plan
Configure collection of event information for multiple devices in single plan/task

Resource management
Add multiple sources to plan/task to collect specified report type on preferred schedule

Conveniently view event data for any device from single location



DISTURBANCE MONITORING REPORT: 2/7/2021, 1:32:21 PM

Search:

Resource	Timestamp	Event	Type
SEL-751	2/7/2021, 5:25:44 AM	Trigger	Oscillography
SEL-751	2/7/2021, 5:25:40 AM	Trigger	Oscillography
SEL-751	2/7/2021, 3:11:27 AM	Trigger	Oscillography
SEL-751	2/6/2021, 11:07:26 PM	Trigger	Oscillography
SEL-751	2/6/2021, 6:21:15 PM	Trigger	Oscillography
Z2_SEL-	[illegible]	TRIG	[illegible]
Z2_SEL-	[illegible]	TRIG	[illegible]
Z2_SEL-	[illegible]	TRIG	[illegible]
Z2_SEL-	[illegible]	TRIG	[illegible]
Z2_SEL-	[illegible]	TRIG	[illegible]
Z2_SEL-	[illegible]	TRIG	Oscillography
Z2_SEL-421-4	2/6/2021, 2:41:37 PM	TRIG	Oscillography
Z2_SEL-421-4	2/6/2021, 2:40:43 PM	TRIG	Oscillography
Z2_SEL-421-4 (2)	2/7/2021, 3:26:53 AM	TRIG	Oscillography
Z2_SEL-421-4 (2)	2/7/2021, 3:10:20 AM	TRIG	Oscillography
Z2_SEL-421-4 (2)	2/6/2021, 10:54:08 PM	TRIG	Oscillography

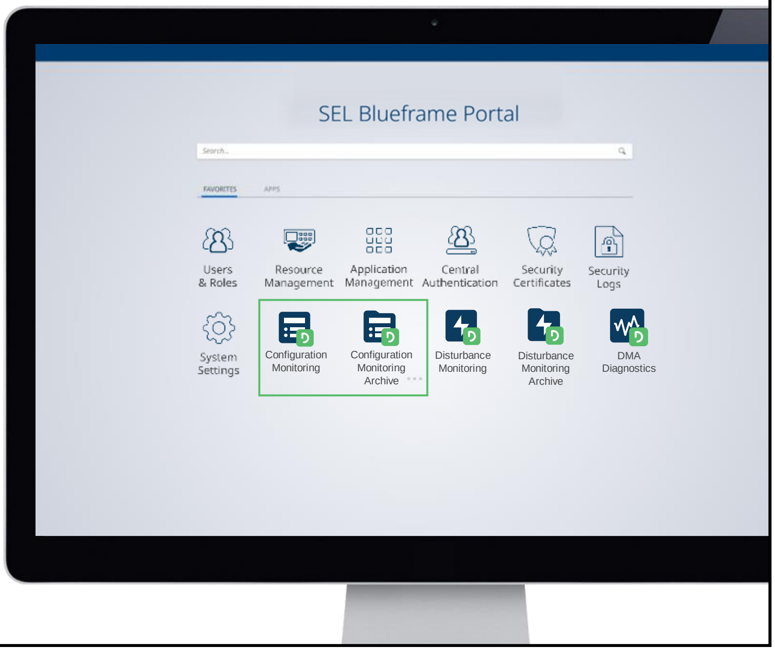
Resource: SEL-751
ID: 00000000-0004-4000-8000-000000000419
Timestamp: 2/7/2021, 5:25:44 AM
Event: Trigger
Type: Oscillography
cordings: 2

Resource selection
Select multiple sources to view recent system incidents

Event export
View details and export records of interest for detailed analysis

Configuration Monitoring

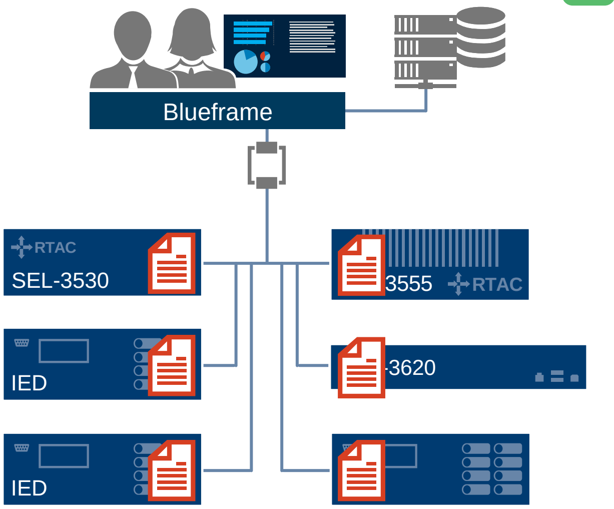
- Automated collection of settings data
- Firmware ID version and device identity version collection and viewing



Easily verify settings and software state

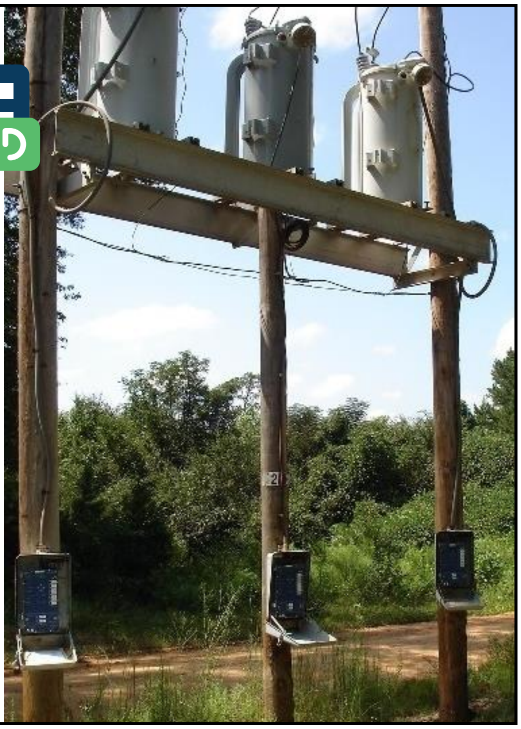
- RTAC properties
- SEL-651R settings and properties
- Firmware audits
- Settings audits
- Security gateway settings
- Automated notifications

Coming soon

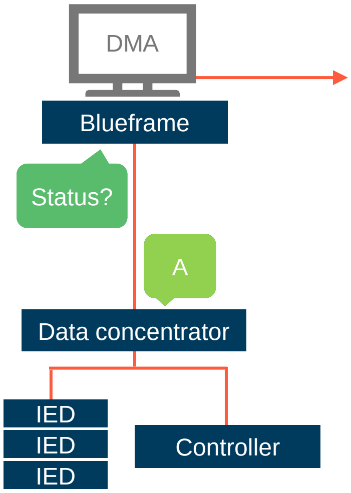


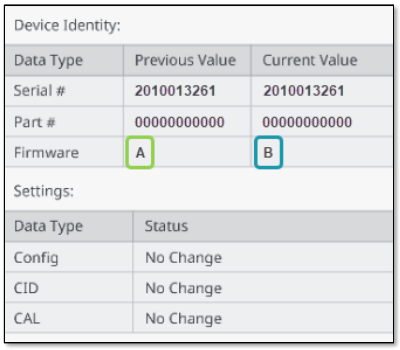
Simplify, expedite, and increase reliability of device integrity checks

- Automate device identity checks to maintain understanding of system devices
- Maximize efficiency by only collecting detected changes
- Securely move settings to settings management repository for comparison



Rapidly assess device identity status





Device Identity:

Data Type	Previous Value	Current Value
Serial #	2010013261	2010013261
Part #	00000000000	00000000000
Firmware	A	B

Settings:

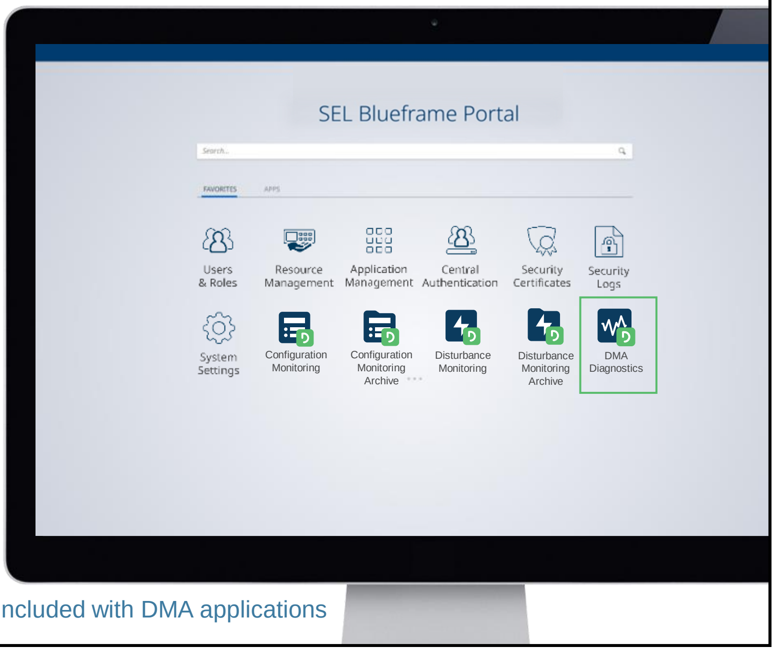
Data Type	Status
Config	No Change
CID	No Change
CAL	No Change

- Generate summary for multiple devices
- Export to settings management software

DMA Diagnostics

Support tool for system status, diagnostics, and troubleshooting

- Status information
- Detailed logging
- Device communication status
- Automation process failure/success indication



Included with DMA applications

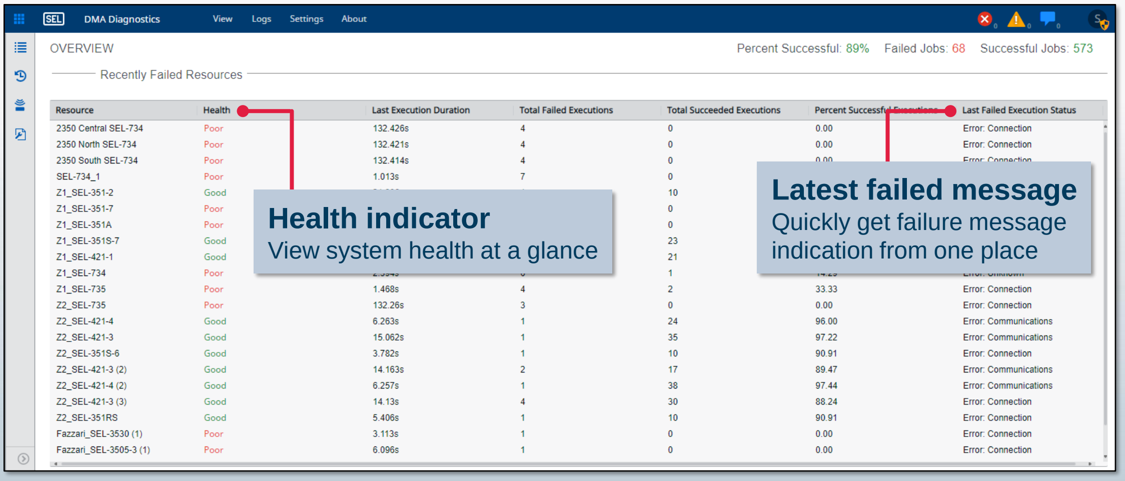
Automation state and troubleshooting at your fingertips

Quickly assess health of recently queried devices to ensure successful collection

Troubleshoot devices where data collection is failing with easy-to-understand status messages and execution logs

Quickly assess effect of automated collection plans on system to determine optimal configuration

Gain insight into automated system operations



OVERVIEW

Percent Successful: 89% Failed Jobs: 68 Successful Jobs: 573

Recently Failed Resources

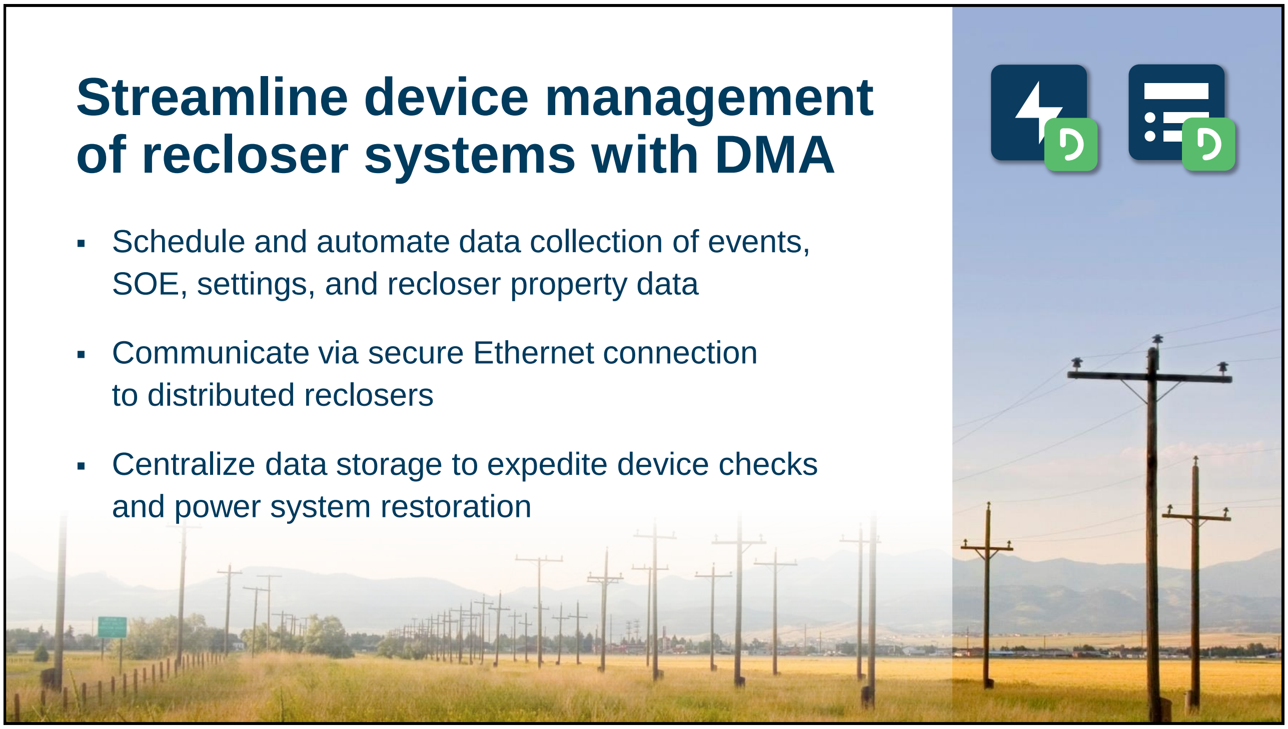
Resource	Health	Last Execution Duration	Total Failed Executions	Total Succeeded Executions	Percent Successful Executions	Last Failed Execution Status
2350 Central SEL-734	Poor	132.426s	4	0	0.00	Error: Connection
2350 North SEL-734	Poor	132.421s	4	0	0.00	Error: Connection
2350 South SEL-734	Poor	132.414s	4	0	0.00	Error: Connection
SEL-734_1	Poor	1.013s	7	0		
Z1_SEL-351-2	Good			10		
Z1_SEL-351-7	Poor			0		
Z1_SEL-351A	Poor			0		
Z1_SEL-351S-7	Good			23		
Z1_SEL-421-1	Good			21		
Z1_SEL-734	Poor	2.394s	6	1	14.29	Error: Unknown
Z1_SEL-735	Poor	1.468s	4	2	33.33	Error: Connection
Z2_SEL-735	Poor	132.26s	3	0	0.00	Error: Connection
Z2_SEL-421-4	Good	6.263s	1	24	96.00	Error: Communications
Z2_SEL-421-3	Good	15.062s	1	35	97.22	Error: Communications
Z2_SEL-351S-6	Good	3.782s	1	10	90.91	Error: Connection
Z2_SEL-421-3 (2)	Good	14.163s	2	17	89.47	Error: Communications
Z2_SEL-421-4 (2)	Good	6.257s	1	38	97.44	Error: Communications
Z2_SEL-421-3 (3)	Good	14.13s	4	30	88.24	Error: Connection
Z2_SEL-351RS	Good	5.406s	1	10	90.91	Error: Connection
Fazzari_SEL-3530 (1)	Poor	3.113s	1	0	0.00	Error: Connection
Fazzari_SEL-3505-3 (1)	Poor	6.096s	1	0	0.00	Error: Connection

Health indicator
View system health at a glance

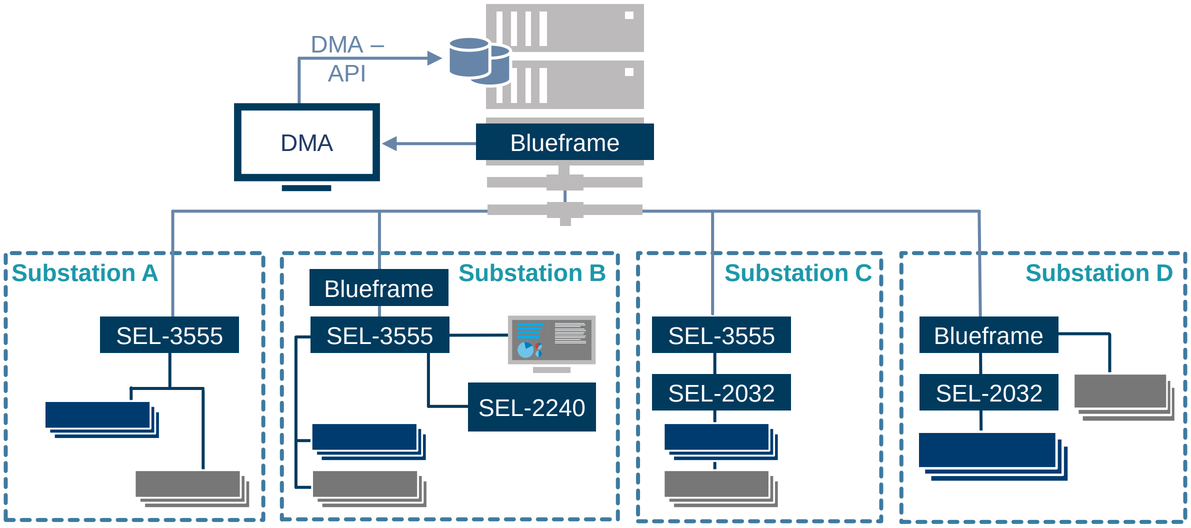
Latest failed message
Quickly get failure message indication from one place

Streamline device management of recloser systems with DMA

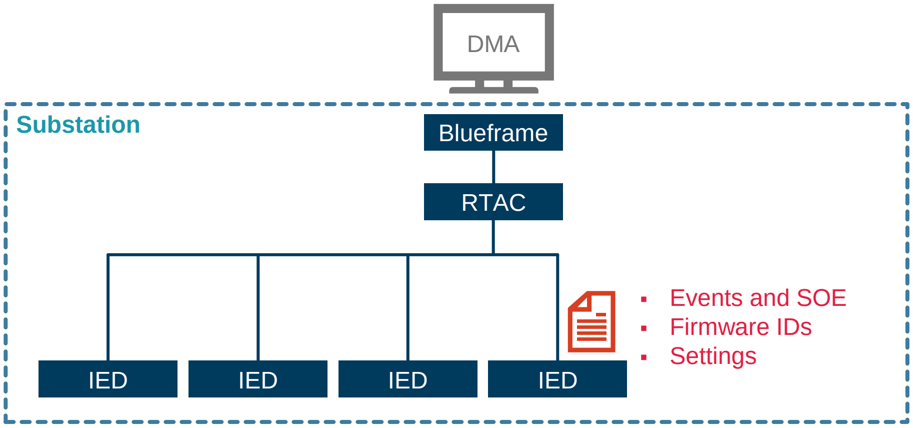
- Schedule and automate data collection of events, SOE, settings, and recloser property data
- Communicate via secure Ethernet connection to distributed reclosers
- Centralize data storage to expedite device checks and power system restoration



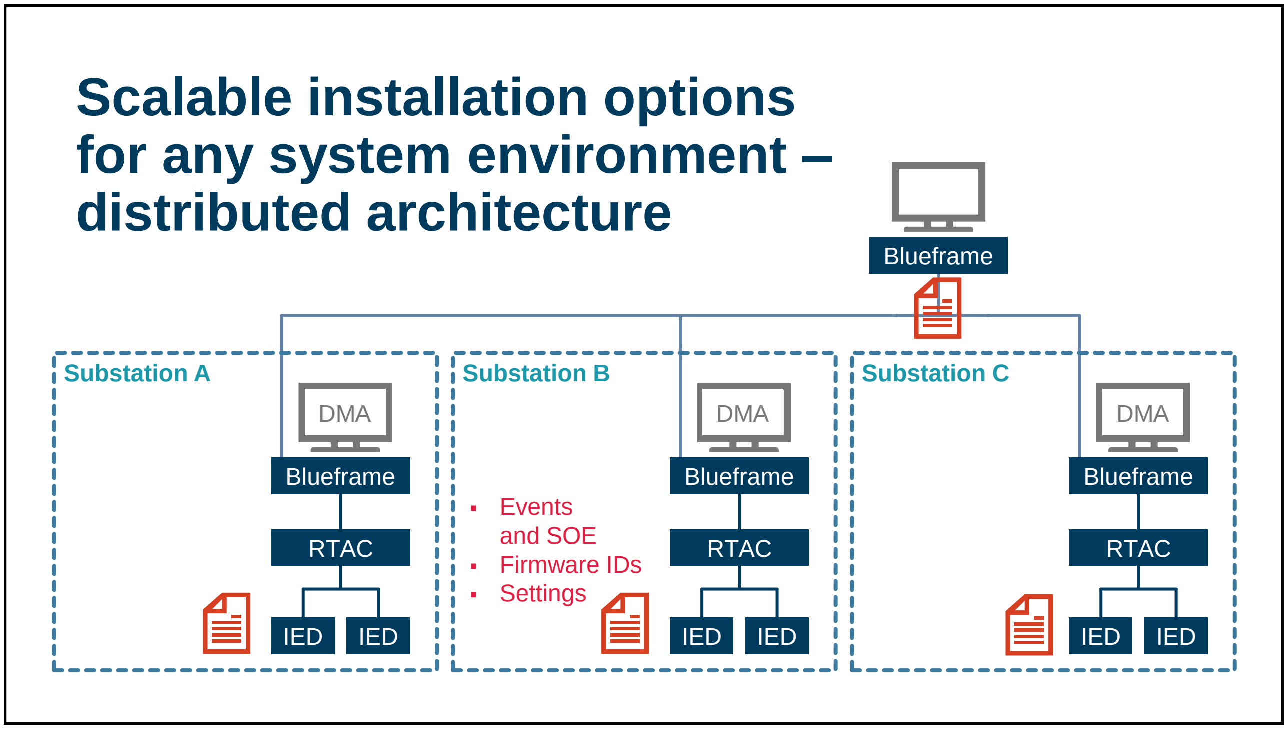
Adaptable solution for new or retrofit systems



Scalable installation options for any system environment – substation architecture

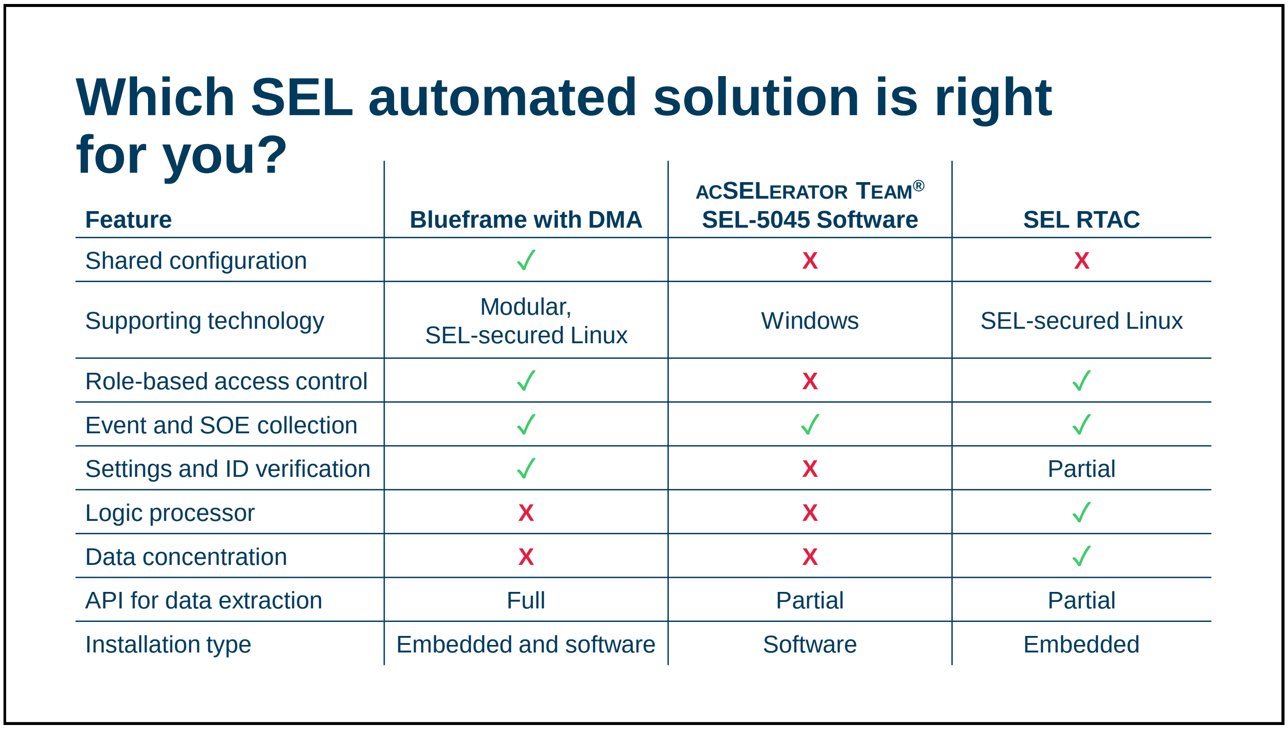


- Events and SOE
- Firmware IDs
- Settings



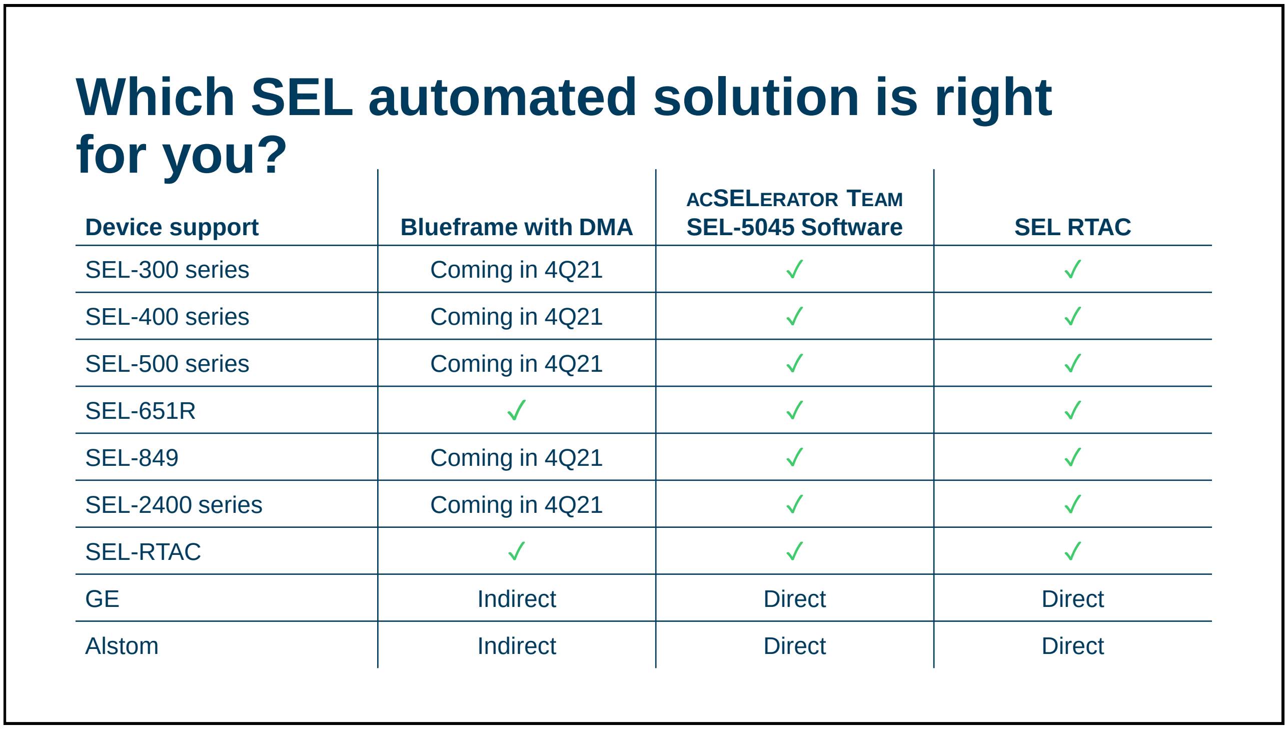
Scalable installation options for any system environment – distributed architecture

- Events and SOE
- Firmware IDs
- Settings



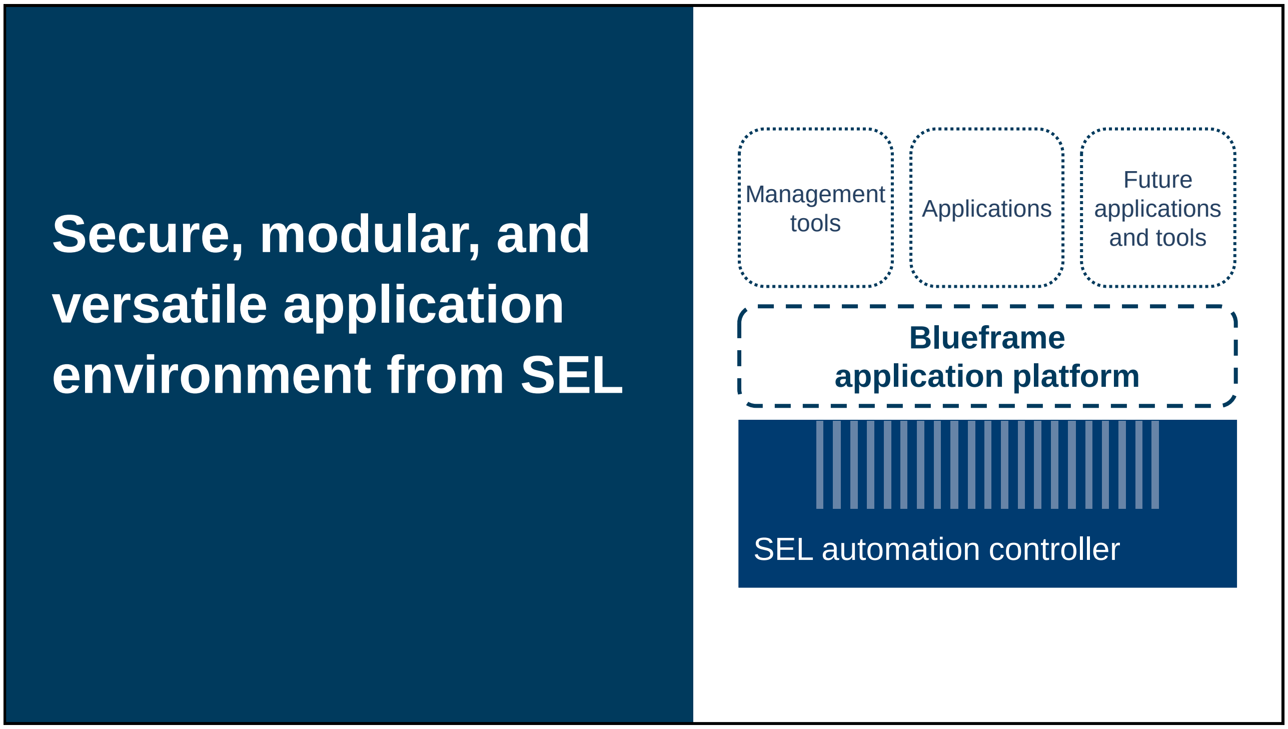
Which SEL automated solution is right for you?

Feature	Blueframe with DMA	ACSELERATOR TEAM® SEL-5045 Software	SEL RTAC
Shared configuration	✓	X	X
Supporting technology	Modular, SEL-secured Linux	Windows	SEL-secured Linux
Role-based access control	✓	X	✓
Event and SOE collection	✓	✓	✓
Settings and ID verification	✓	X	Partial
Logic processor	X	X	✓
Data concentration	X	X	✓
API for data extraction	Full	Partial	Partial
Installation type	Embedded and software	Software	Embedded



Which SEL automated solution is right for you?

Device support	Blueframe with DMA	ACSELERATOR TEAM SEL-5045 Software	SEL RTAC
SEL-300 series	Coming in 4Q21	✓	✓
SEL-400 series	Coming in 4Q21	✓	✓
SEL-500 series	Coming in 4Q21	✓	✓
SEL-651R	✓	✓	✓
SEL-849	Coming in 4Q21	✓	✓
SEL-2400 series	Coming in 4Q21	✓	✓
SEL-RTAC	✓	✓	✓
GE	Indirect	Direct	Direct
Alstom	Indirect	Direct	Direct



Secure, modular, and versatile application environment from SEL

Management tools
Applications
Future applications and tools
Blueframe application platform
SEL automation controller

Thank you

SEL SCHWEITZER ENGINEERING LABORATORIES