Modern Trends in Electrical Power Distribution Systems

Kylan Robinson, Engineering Director

Prepared for the NSRP Electrical Technologies Panel

3 April 2024

Distribution systems are becoming more…

SOPHISTICATED

CONNECTED

SECURE

About SEL

Schweitzer Engineering Laboratories, Inc.

OUR MISSION STATEMENT

Making electric power safer, more reliable, and more economical

From 1982…

- Founded by Dr. Edmund O. Schweitzer, III in 1982
- Released world's first microprocessor relay, the SEL-21, in 1984

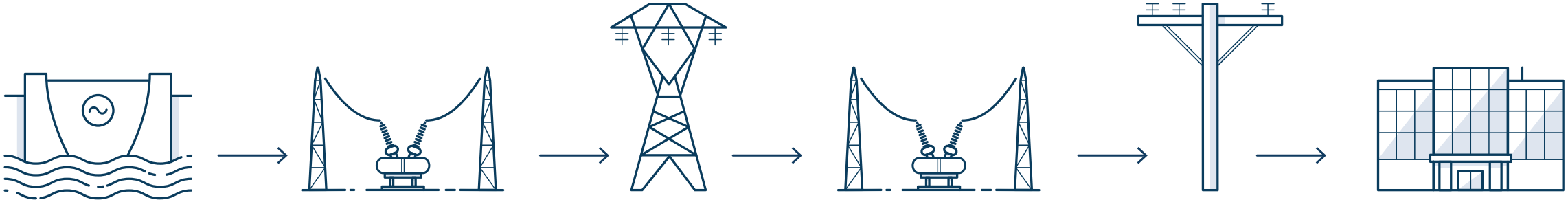
…to now

- 5 electronic device factories
- 169 countries with SEL products
- 107 sales and support offices
- 6,000+ employees around the world

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

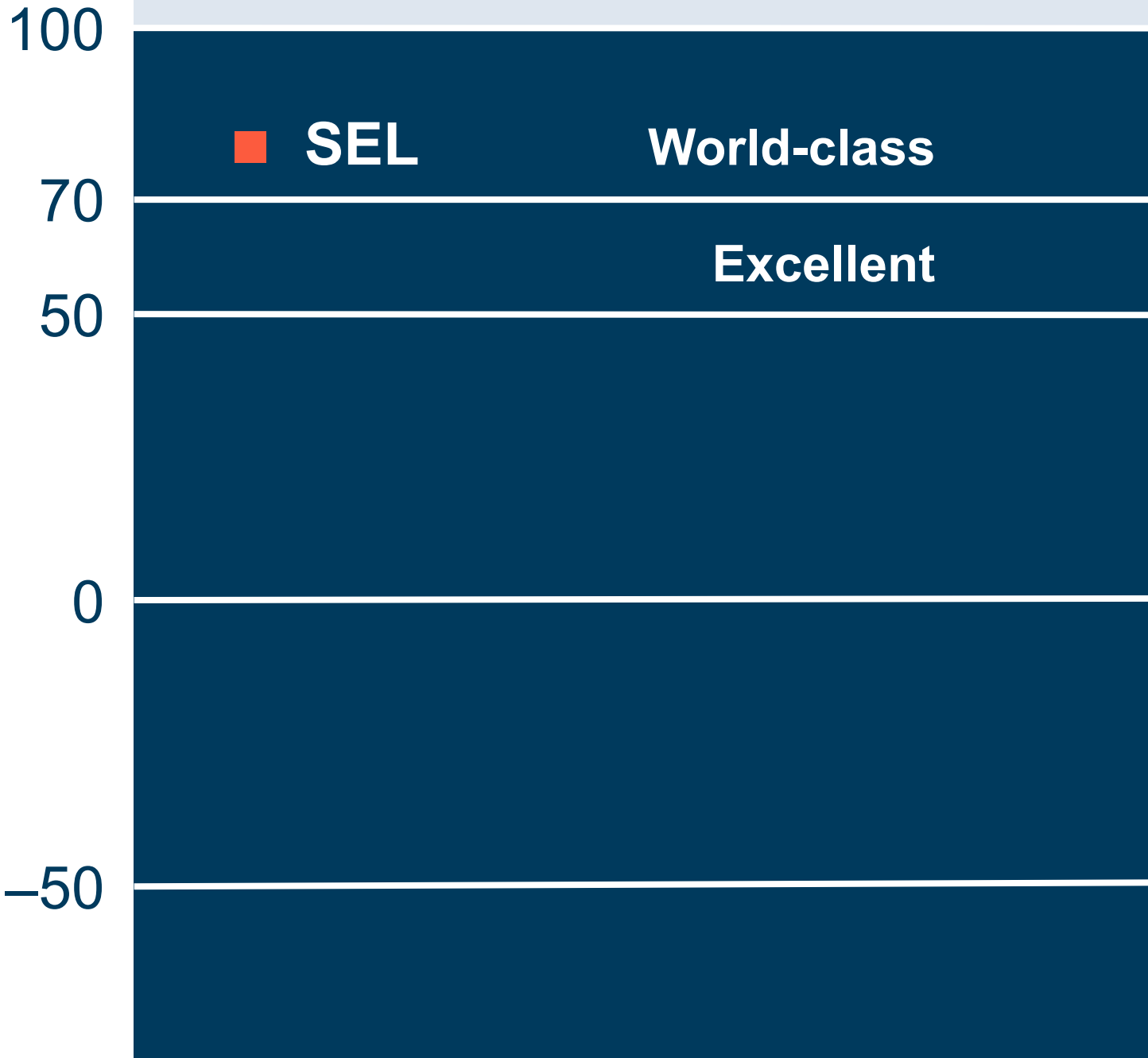
We provide end-to-end solutions

- Automation
- Communications
- Protection and control
- Metering
- Computing and software
- Security for critical infrastructure
- Engineering services
- Training



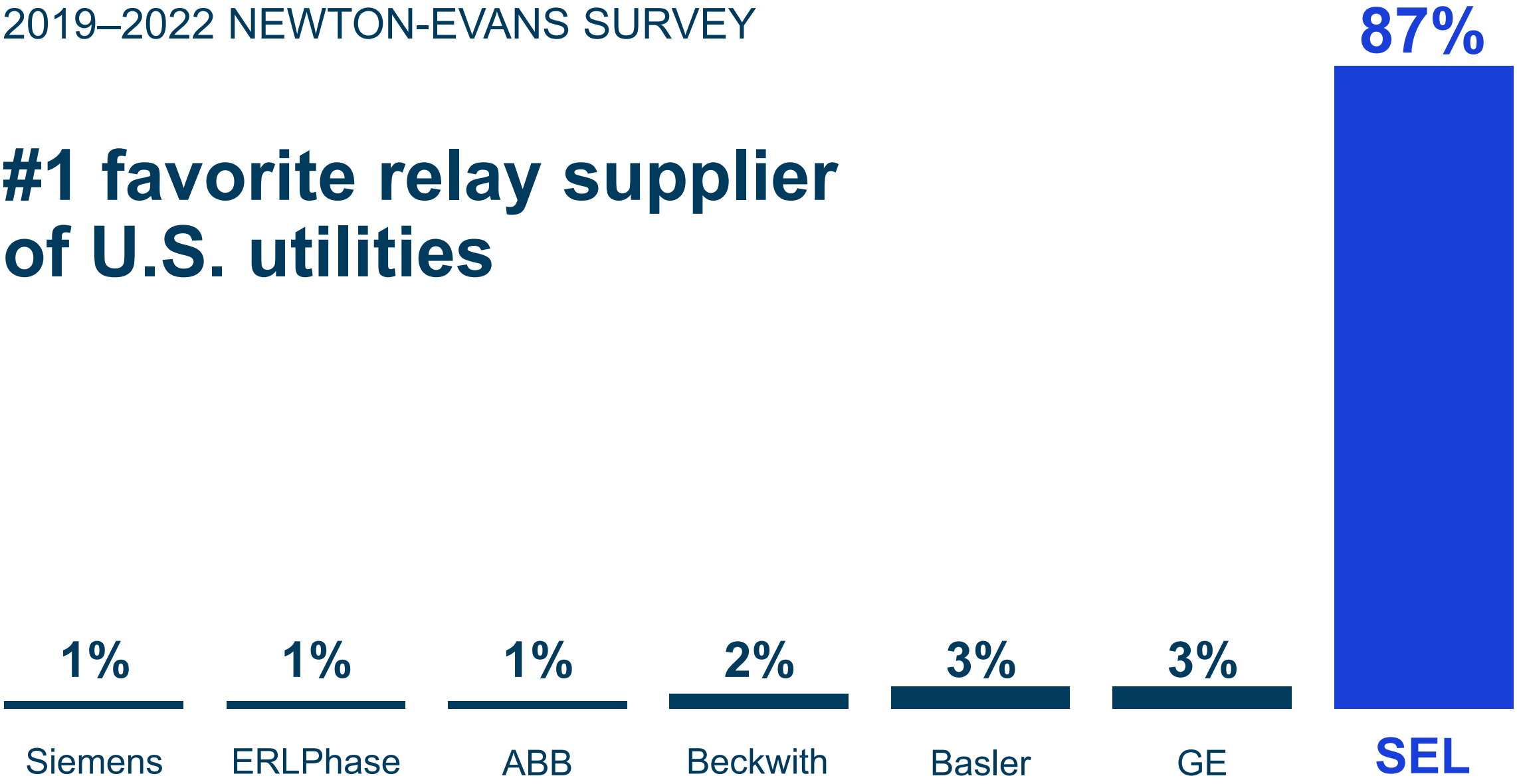
NET PROMOTER SCORE
RESULTS FOR 2022

Most global customers would recommend SEL to others



2019–2022 NEWTON-EVANS SURVEY

#1 favorite relay supplier of U.S. utilities



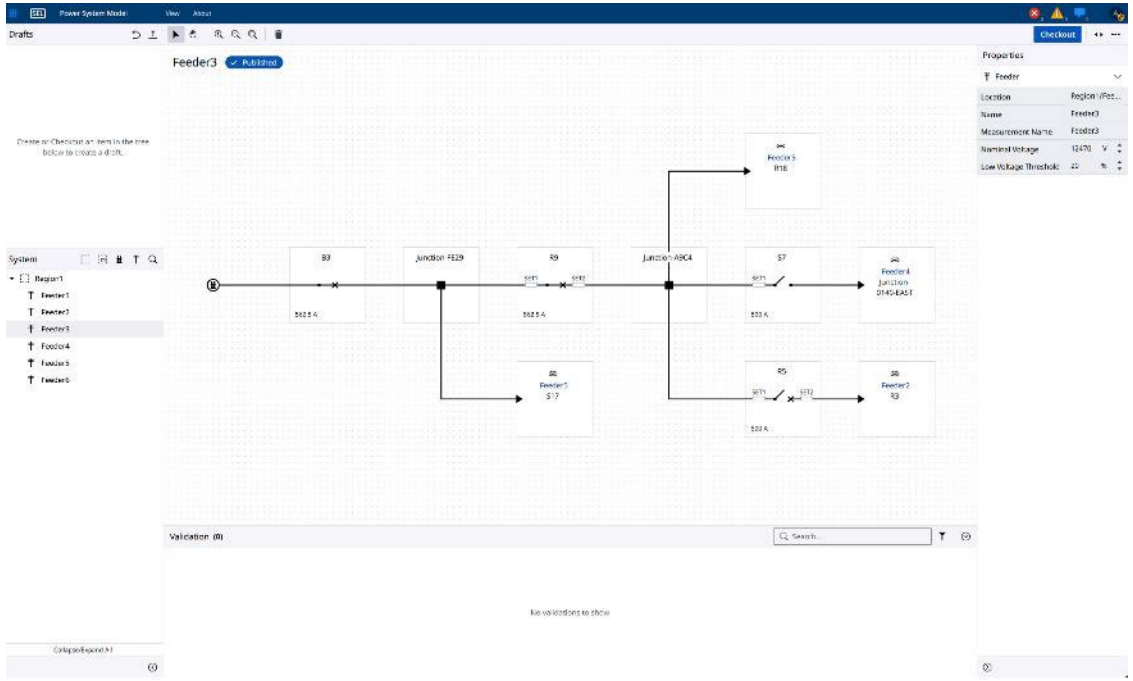
Sophistication

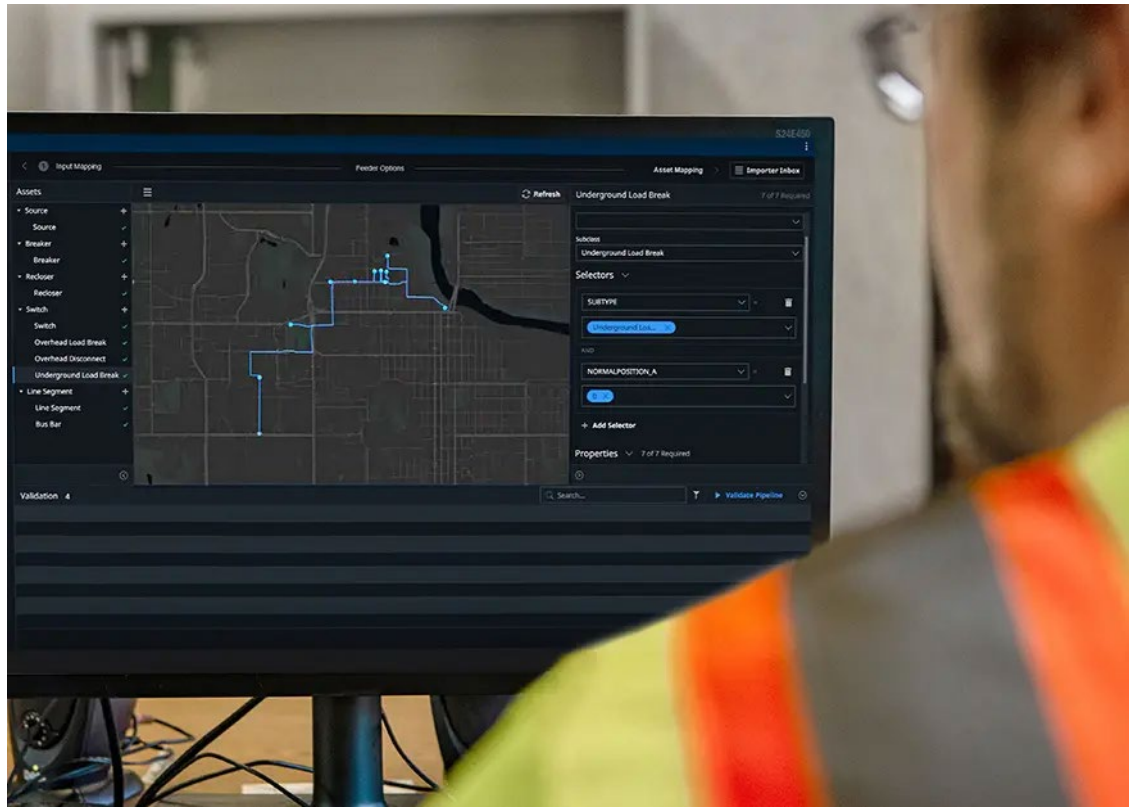
From the control house…

…to the yard

…and beyond

Fault Location, Isolation, and Service Restoration (FLISR)

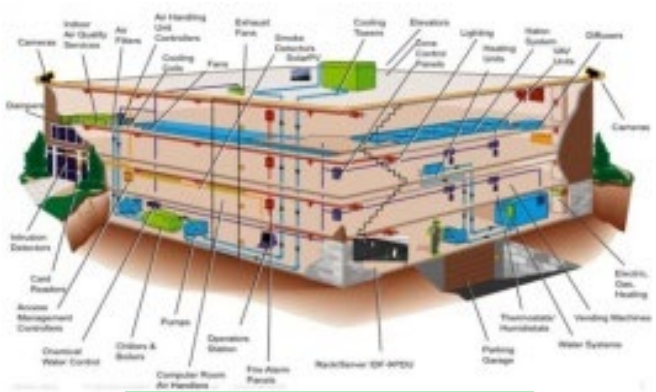




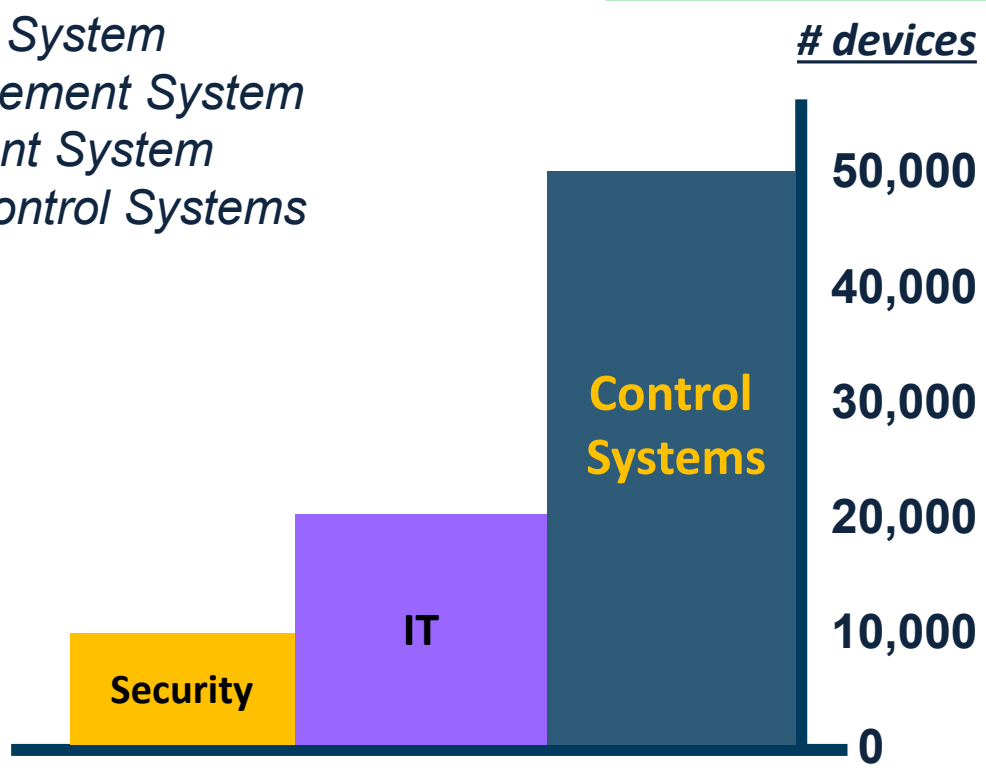
System-wide monitoring and control

What's in your building?

- *Fire Sprinkler System*
- *Interior Lighting Control*
- *Intrusion Detection*
- *Land Mobile Radios*
- *Renewable Energy Voltaic Systems*
- *Shade Control System*
- *Smoke and Purge*
- *Physical Access Control*
- *Vertical Transport System (Elevators and Escalators)*
- *Advanced Metering Infrastructure*
- *Building Automation System*
- *Building Management Control*
- *CO2 Monitoring*
- *Electronic Security System*
- *Emergency Management System*
- *Energy Management System*
- *Exterior Lighting Control Systems*
- *Fire Alarm System*



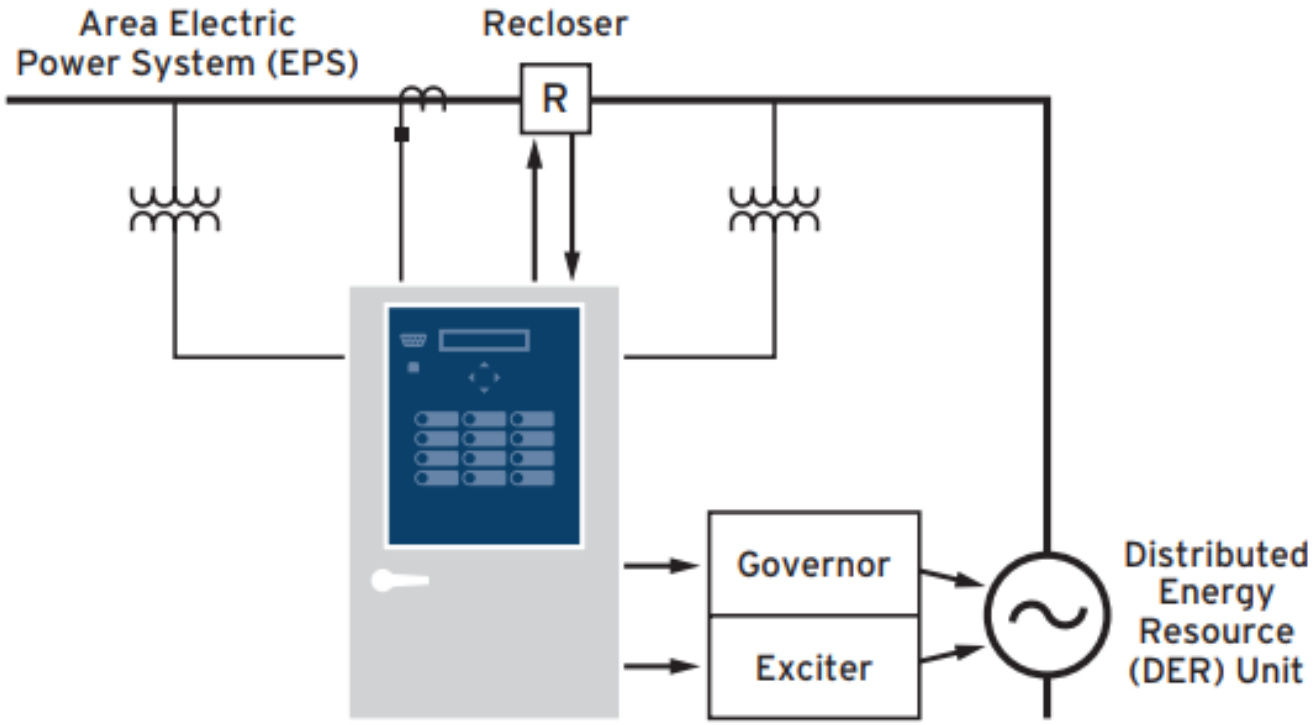
2M ft^2, 6k workers



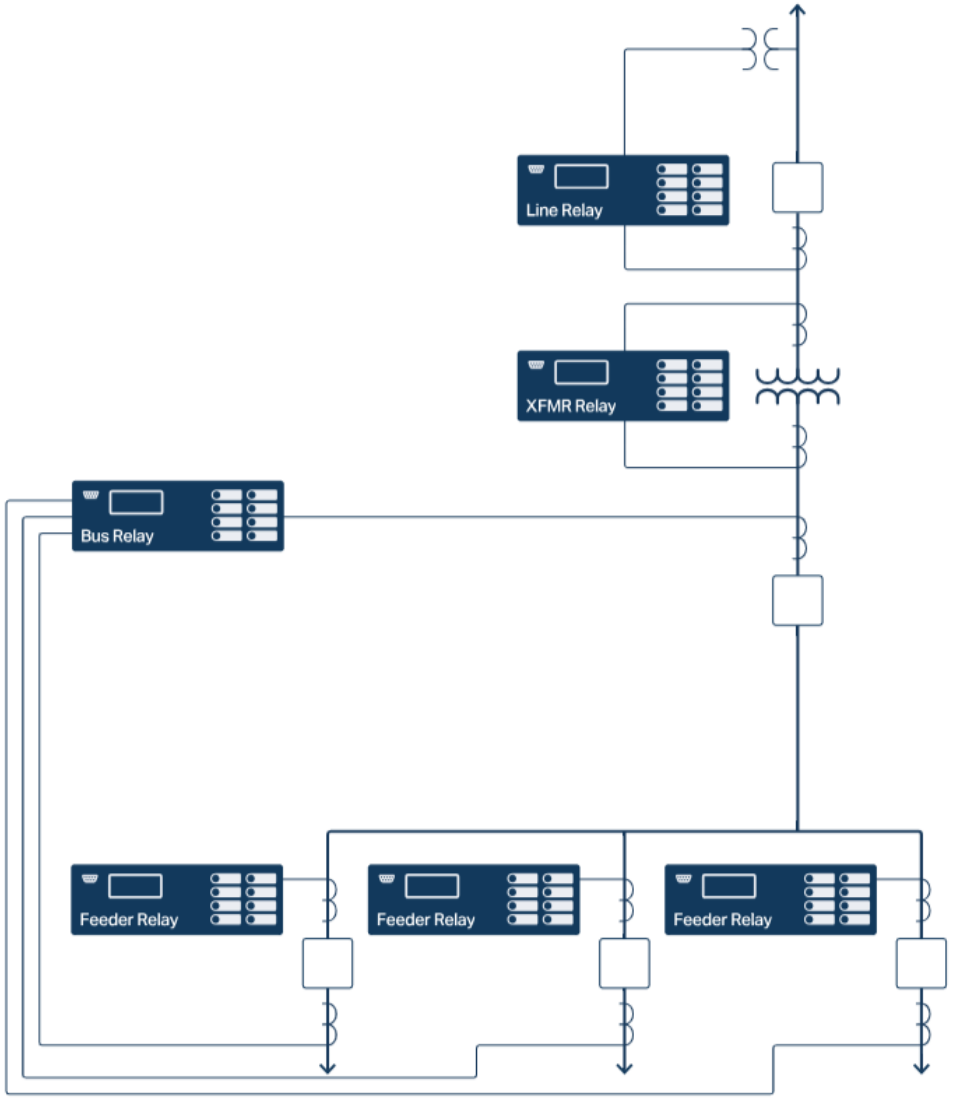
Distributed energy resources

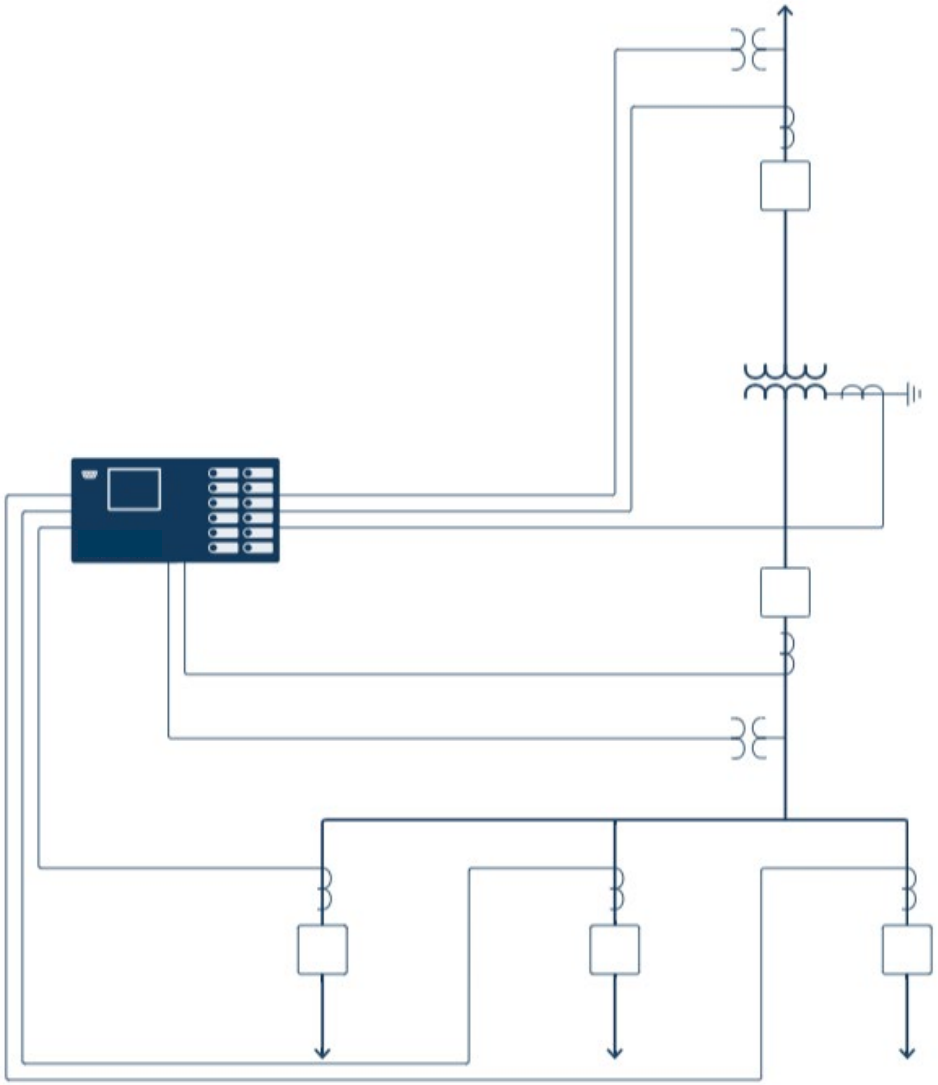
IEEE 1547-2018

Protection and fast islanding detection



Centralized protection

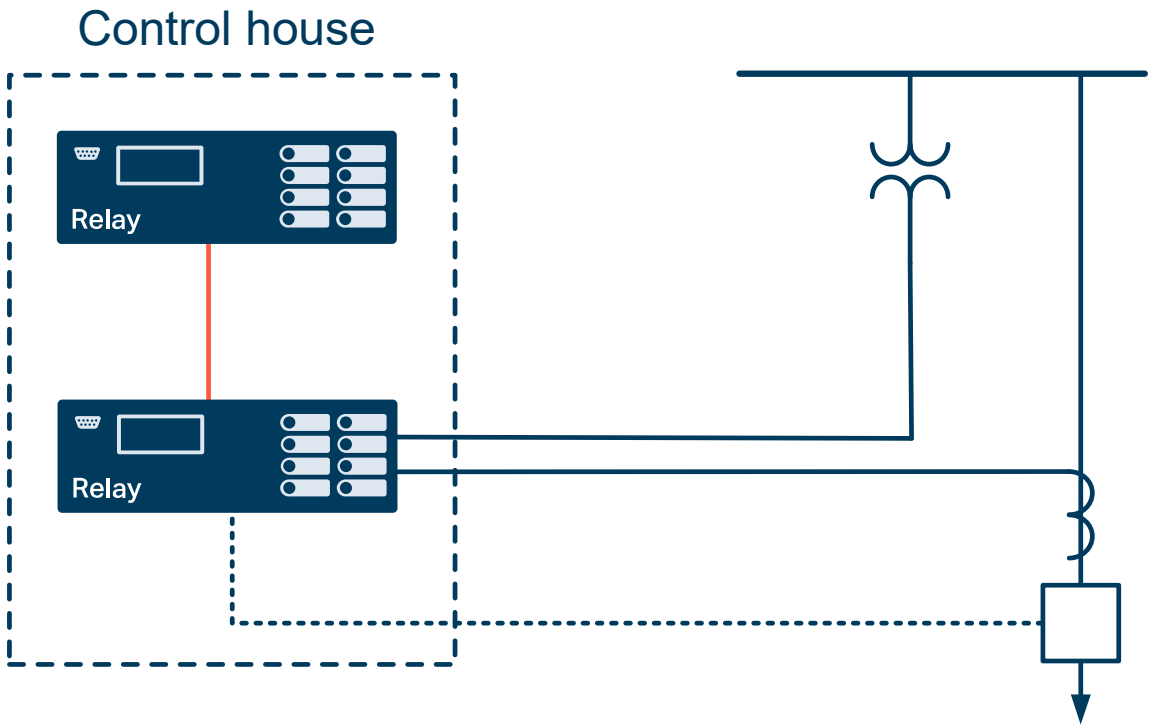




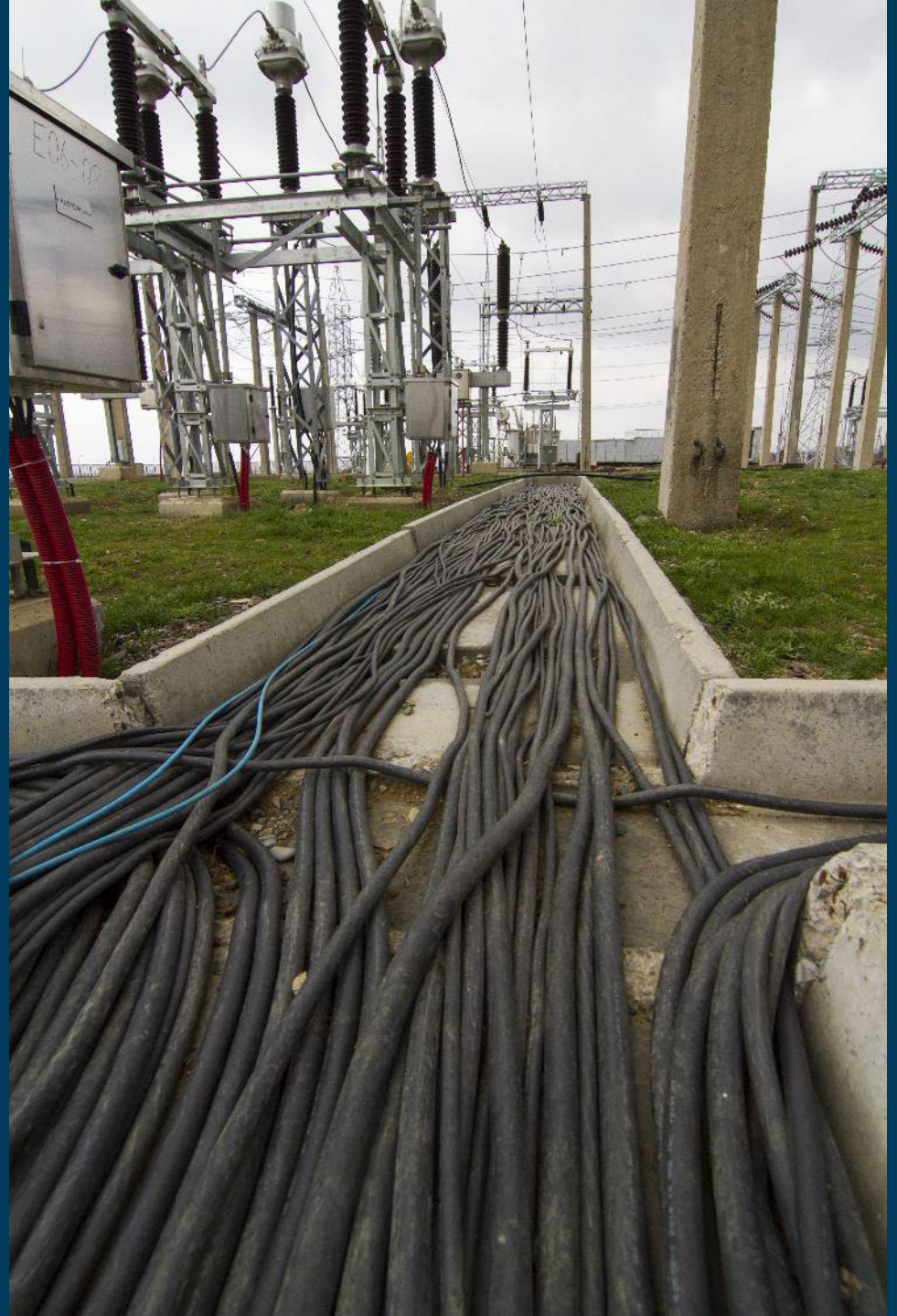
Shipboard power system priorities

- Cost
- Schedule
- Size
- Weight
- Commonality

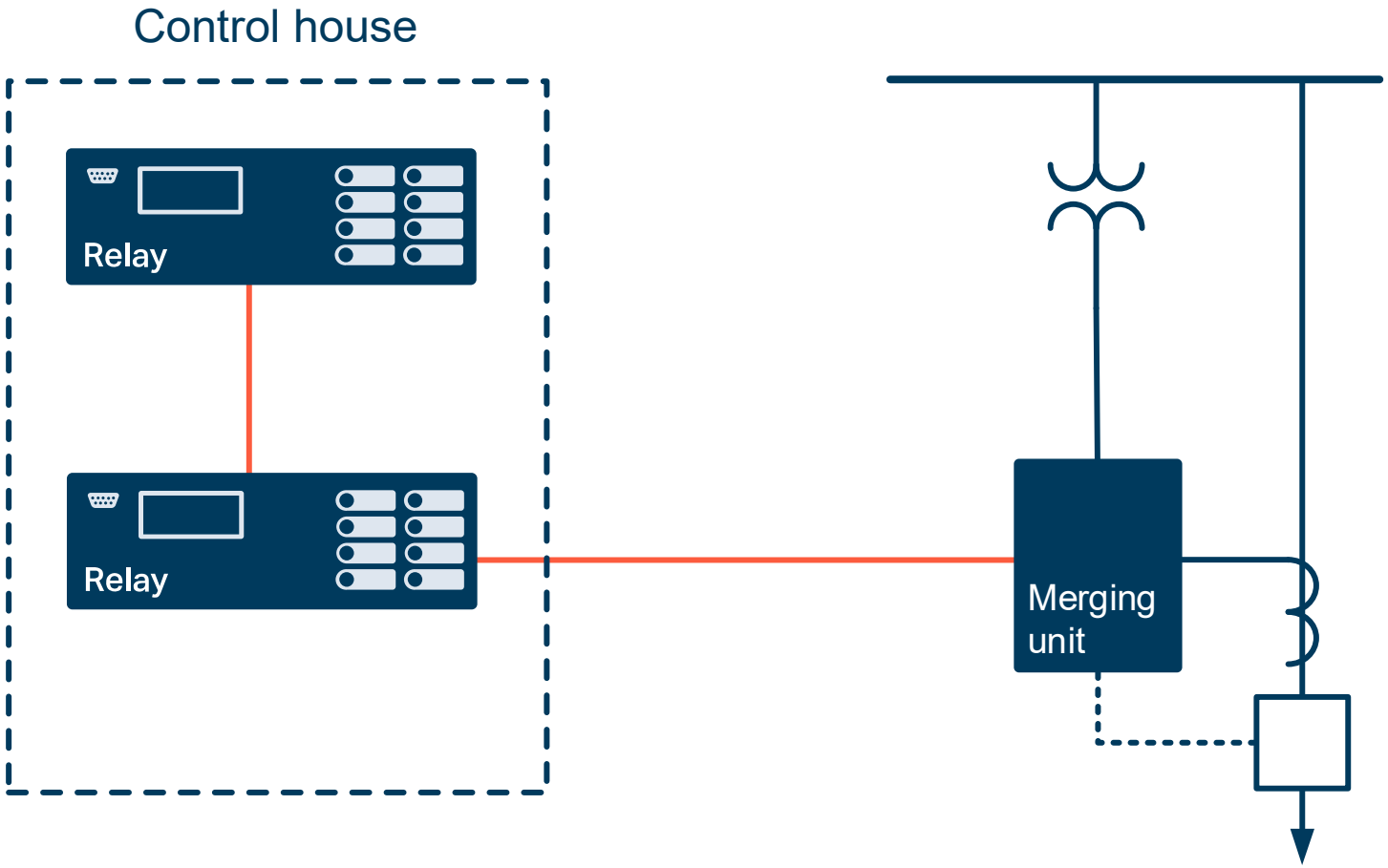
Interconnection



Hardwired connections have been standard



Digital secondary systems use communications

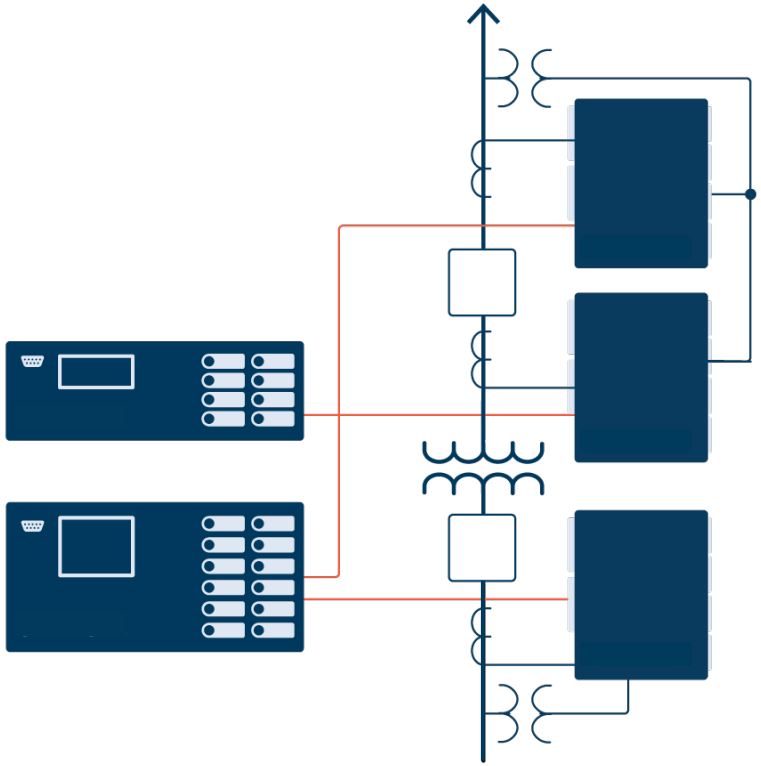


Digitization of secondary systems solves industry challenges

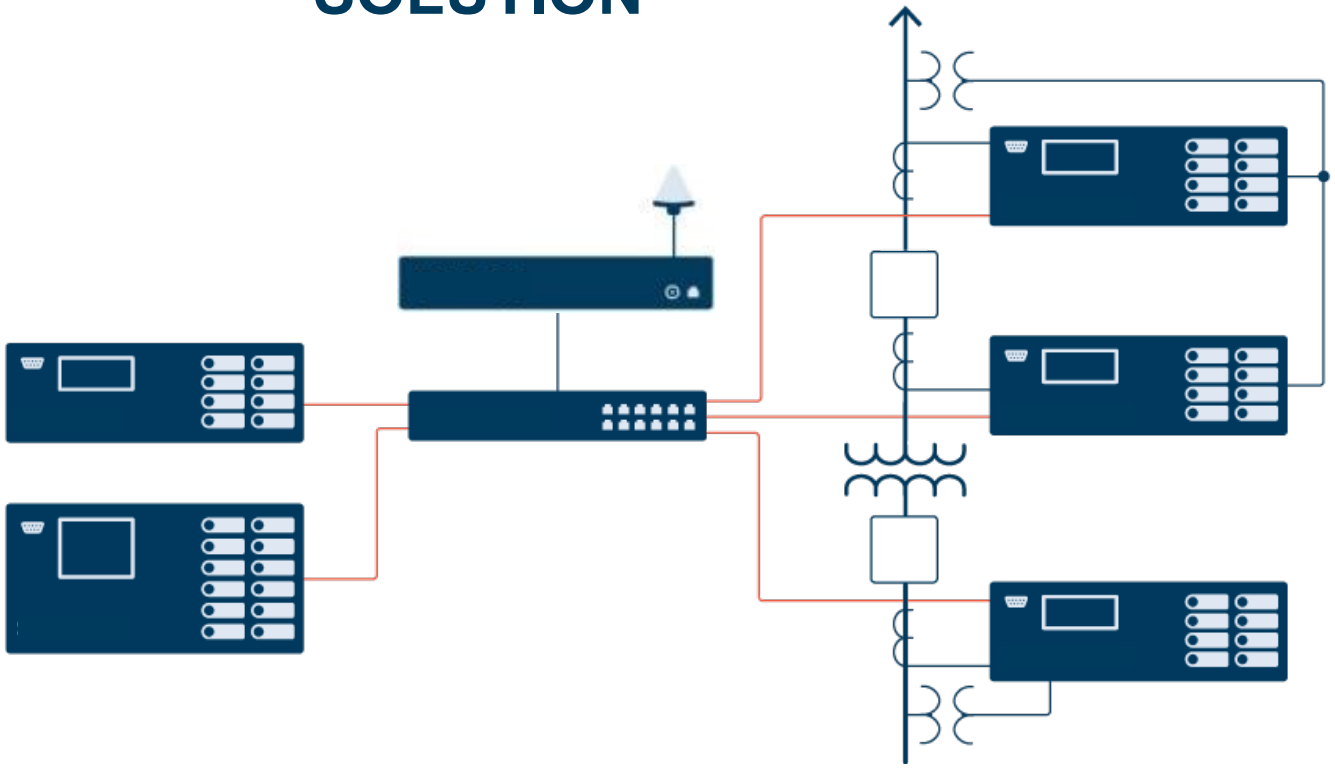
- Reduce substation construction and expansion costs
- Improve personnel safety
- Increase flexibility by replacing copper with fiber

Choose the DSS solution that fits best

POINT-TO-POINT SOLUTION



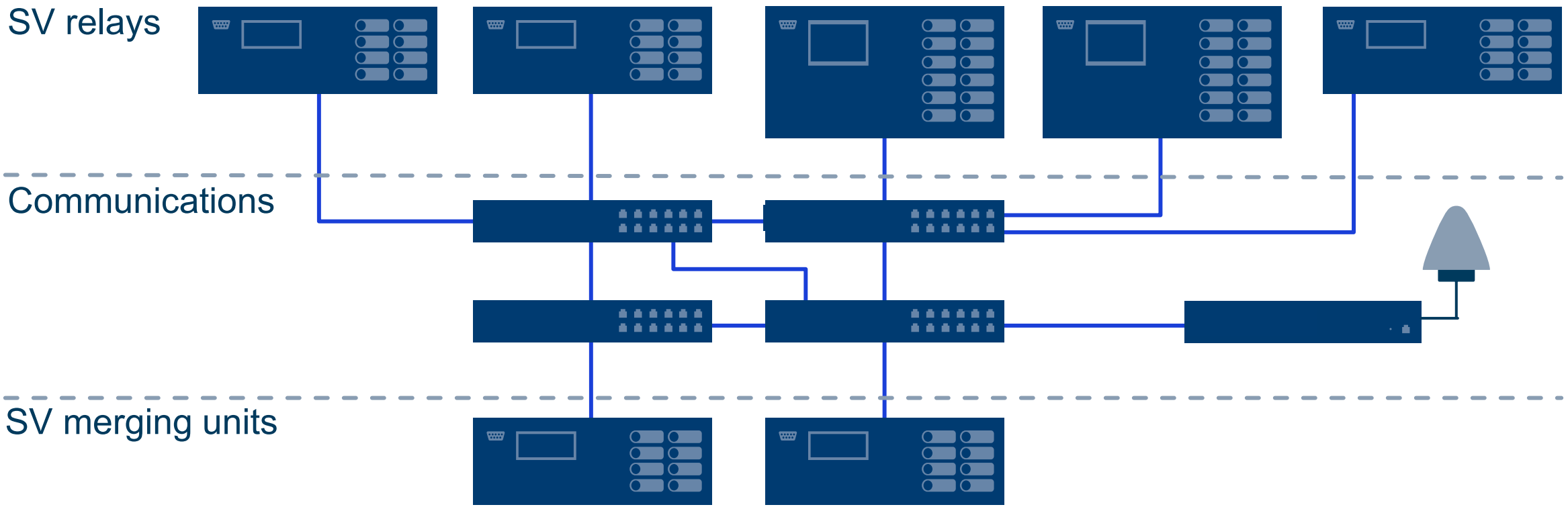
IEC 61850 SAMPLED VALUES SOLUTION



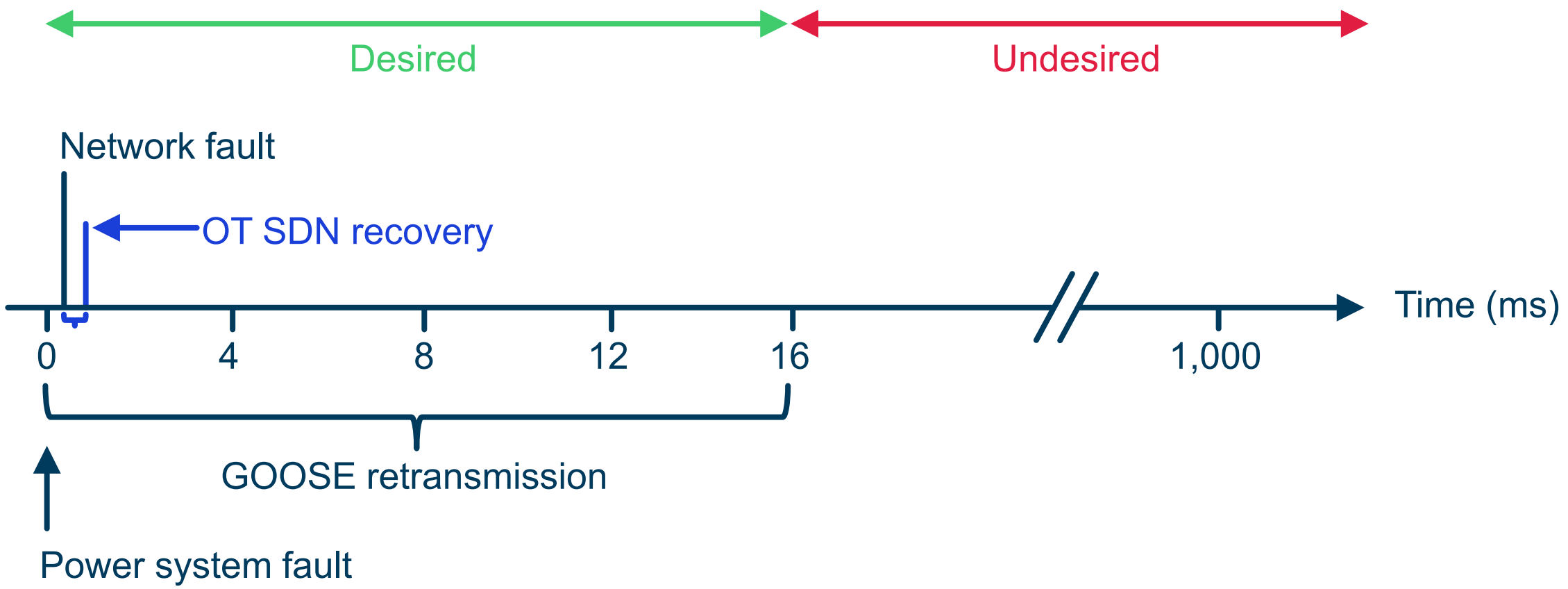
IEC 61850

1. Introduction and overview
2. Glossary
3. General requirements
4. System and project management
5. Communication requirements for functions and device models
6. Configuration language
7. Basic communication structure, GOOSE
8. Mappings to MMS
9. Mappings to SV
10. Conformance testing

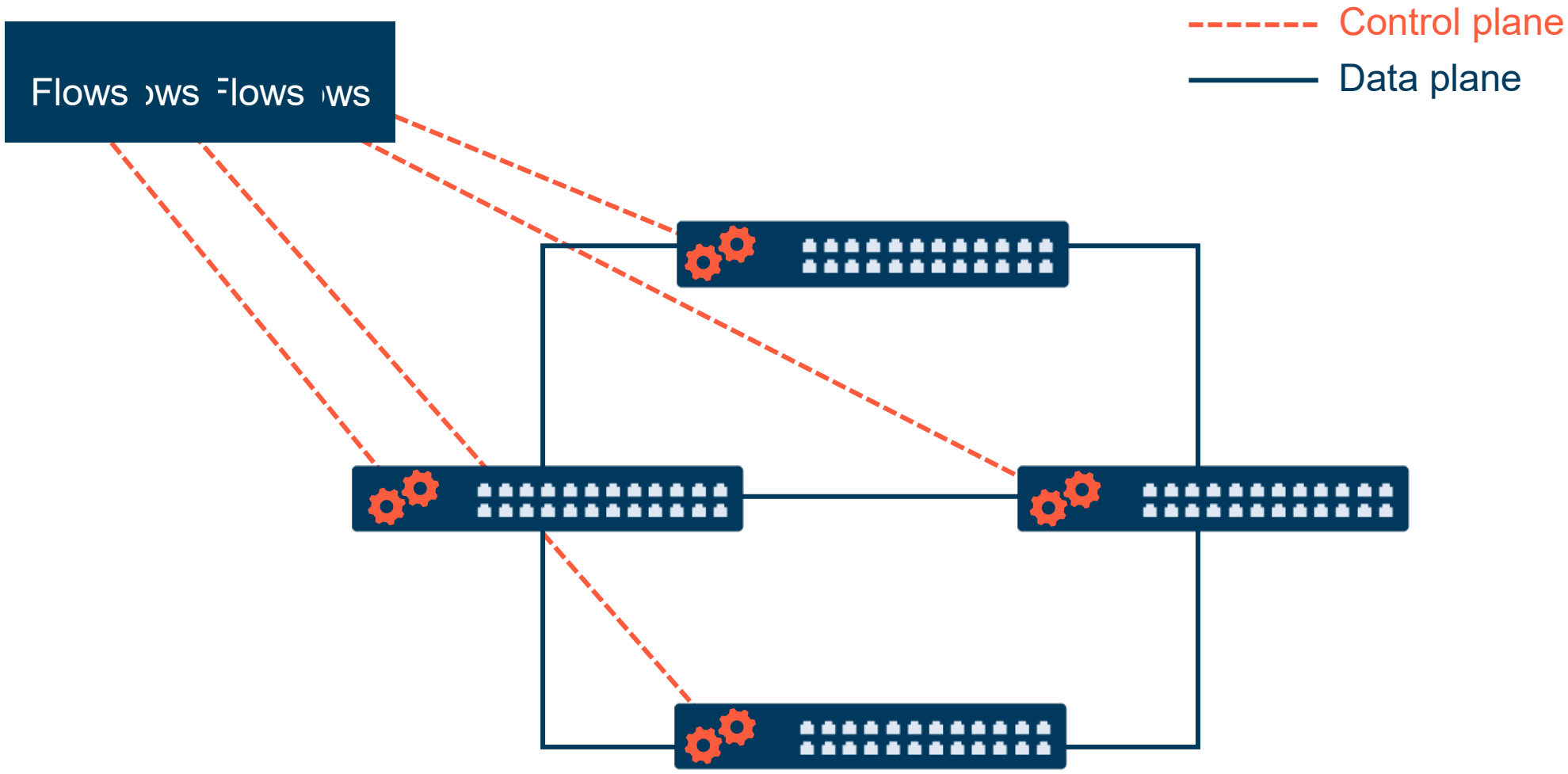
Sampled Values Architecture



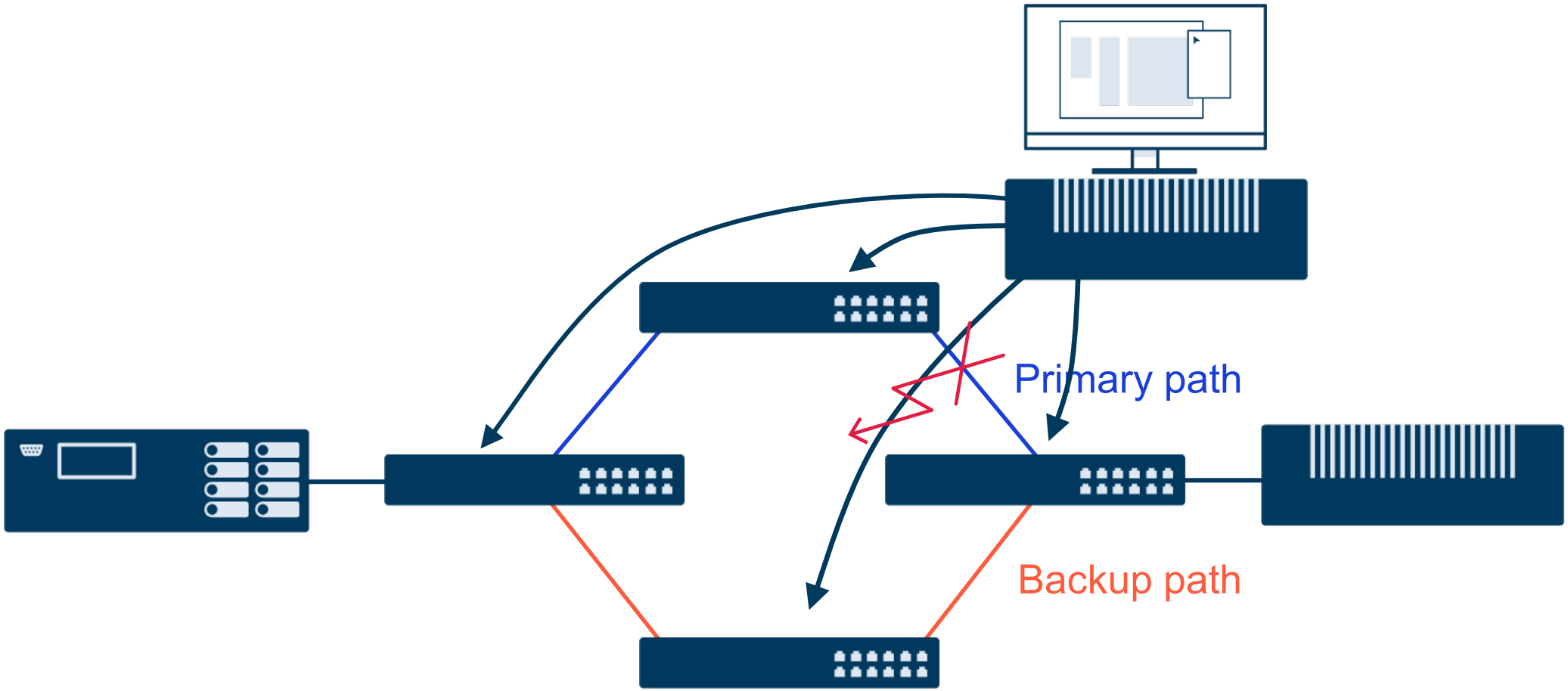
Protection-class Ethernet speeds



Separating planes



OT SDN predetermined failover paths



Cybersecurity

NERC CIP

- CIP-002 BES Cyber System Categorization
- CIP-003 Security Management Controls
- CIP-004 Personnel & Training
- CIP-005 Electronic Security Perimeter(s)
- CIP-006 Physical Security of BES Cyber Systems
- CIP-007 System Security Management
- CIP-008 Incident Reporting and Response Planning
- CIP-009 Recovery Plans for BES Cyber Systems
- CIP-010 Configuration Change Mgmt and Vuln Assessments
- CIP-011 Information Protection
- CIP-012 Communications between Control Centers
- CIP-013 Supply Chain Risk Management

NERC CIP

- Denial → Anger → Bargaining → Depression → Acceptance
- Patch management

IEC 62443

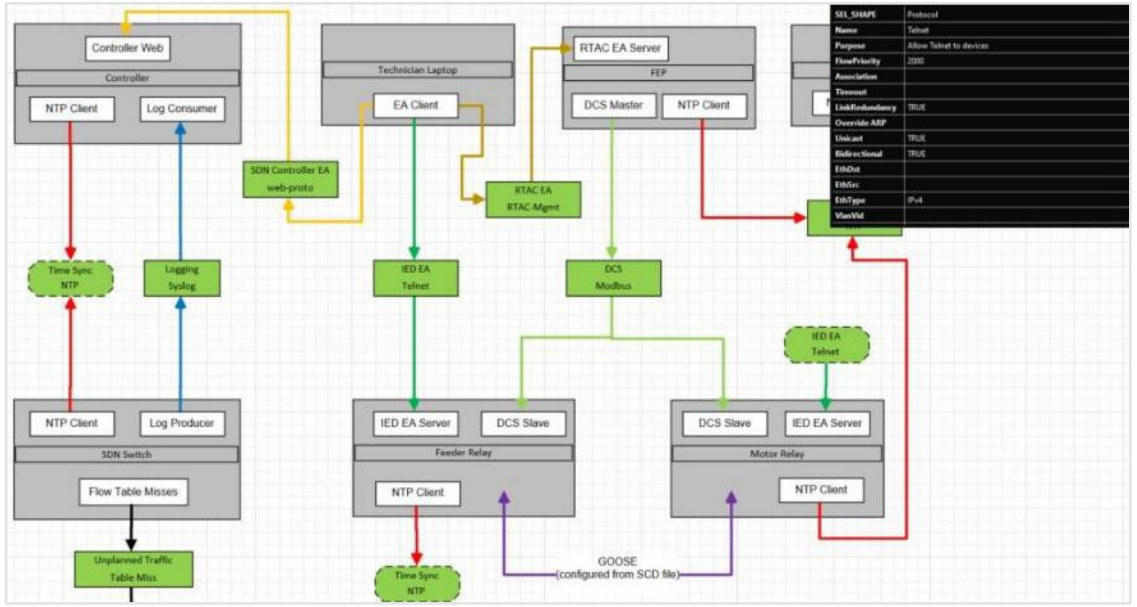
General	Policies and Procedures	System	Components and Requirements
1-1 Concepts and models	2-1 Security program requirements for IACS asset owners	3-1 Security technologies for IACS	4-1 Secure product development lifecycle requirements
1-5 Scheme for security profiles	2-3 Patch management in the IACS environment	3-2 Security risk assessment and system design	4-2 Technical security requirements for IACS components
	2-4 Requirements for IACS service providers	3-3 System security requirements and security levels	

Executive Order 14028

- Improving the Nation's Cybersecurity
  - Security and integrity of the software supply chain
  - Identify, deter, protect against, detect, and respond to malicious cyber campaigns and their actors
- Software Bill of Materials (SBOM)

Deny-by-default communications

- Only engineered ‘conversations’ are allowed
- Match criteria (Layer 1-4) checked at every hop
- Engineering drawing import



Distribution systems are becoming more…

Sophisticated

Visibility, management, and control

Connected

Protection-class communications

Secure

Standards and fundamentals

Questions?

Kylan Robinson
kylan_robinson@selinc.com