Cybersecurity in Industrial Control Systems

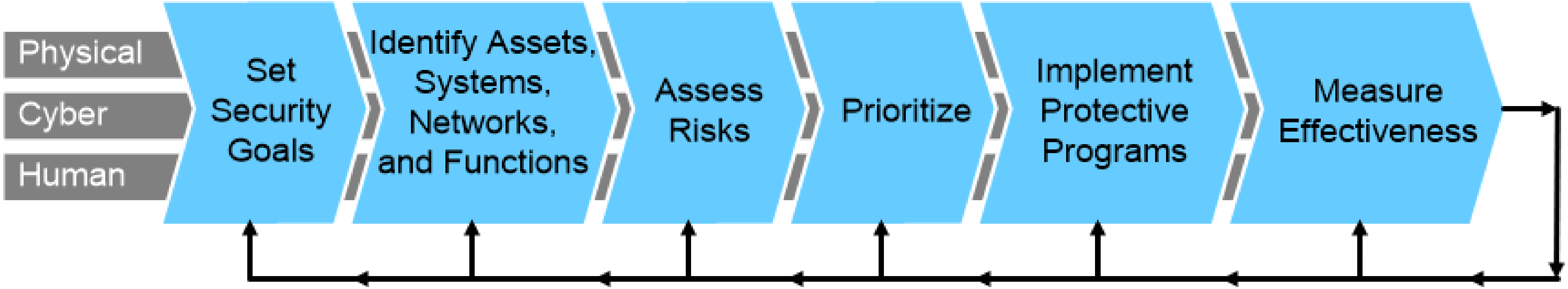
Nathan Kipp
Engineering Manager
Infrastructure Defense Product Development

© 2022 SEL

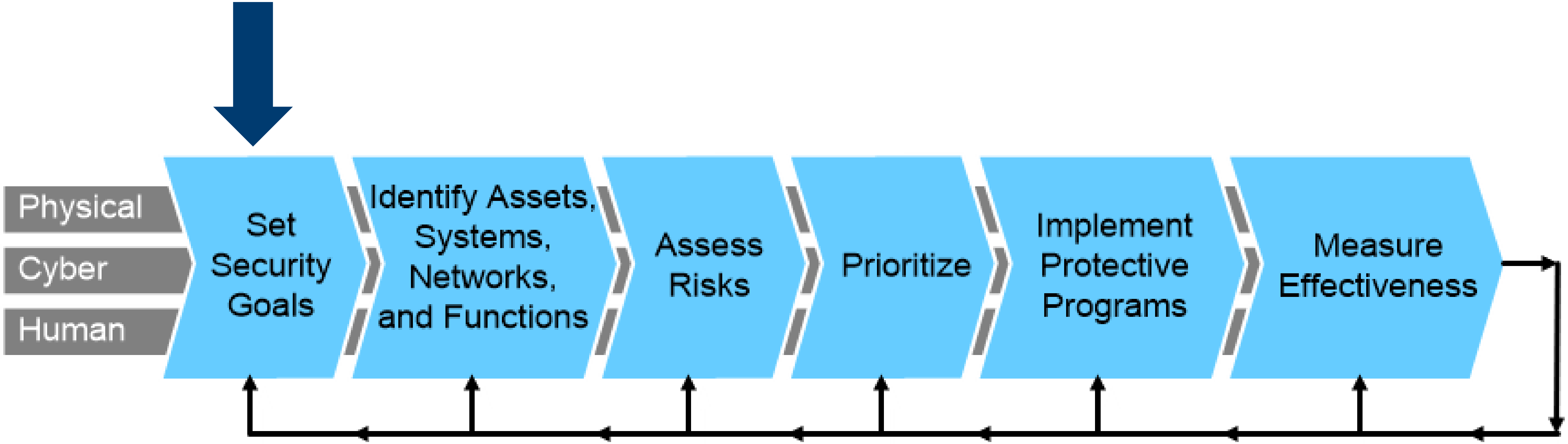
Learning Objectives

- Learn Industrial Control System Basics
- Understand Cybersecurity Goals in Industrial Control Systems
- Introduce Energy System Cybersecurity Driving Factors
- Discuss Current Solutions and Trends

Risk Management in ICS



Risk Management in ICS

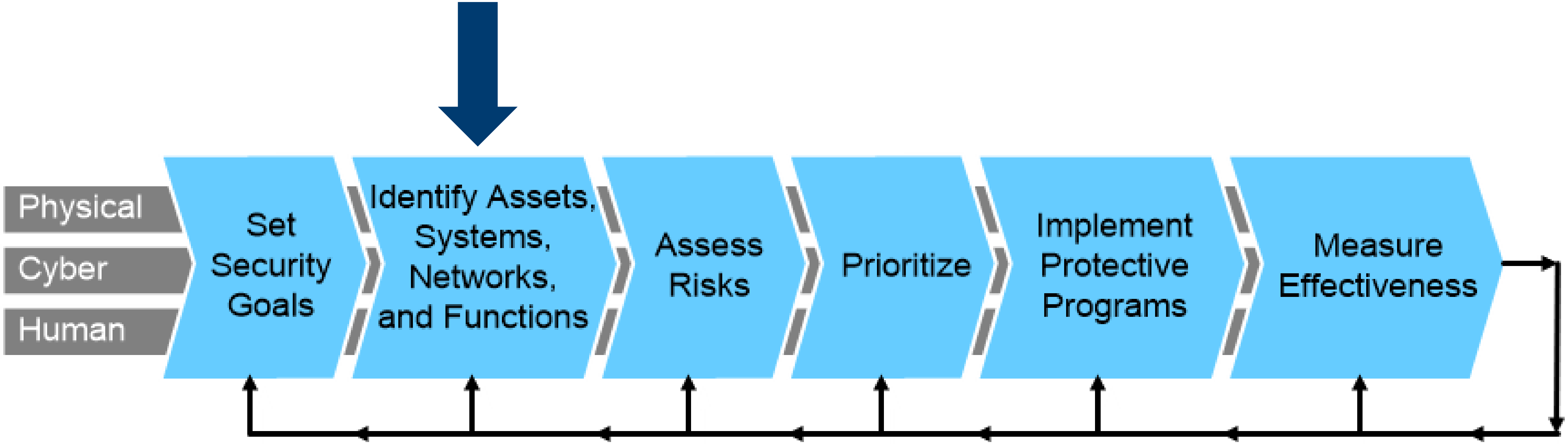


Our goal as defenders

Reduce probability of a successful attack campaign that is material to the business, organization, or system…

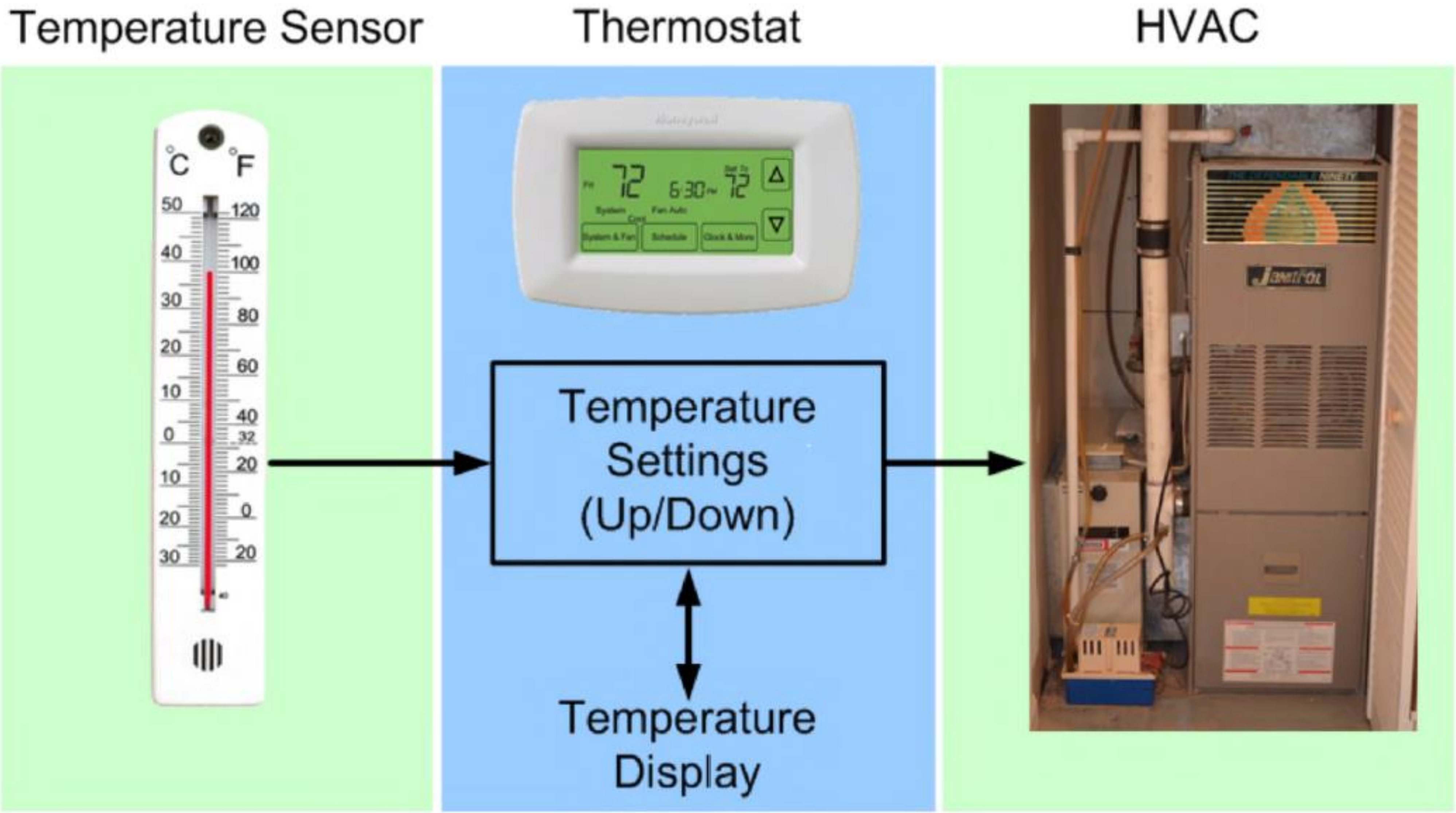
A material issue has a major impact on the financial, economic, reputational, and legal aspects of an organization…

Risk Management in ICS

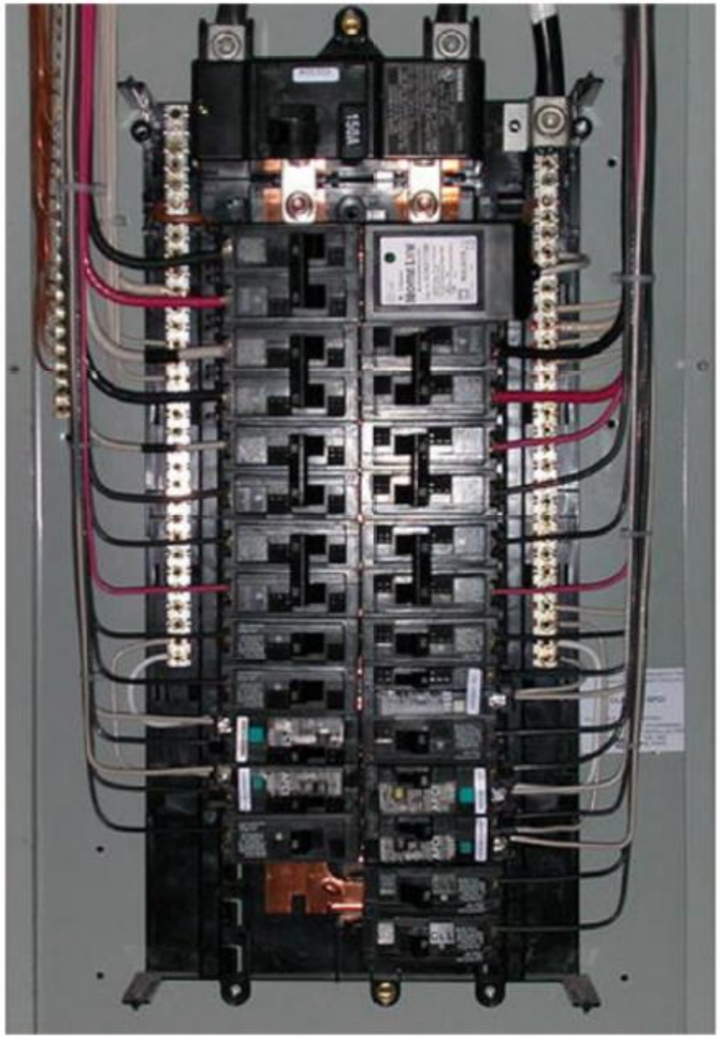


Industrial Control Systems are All Around Us

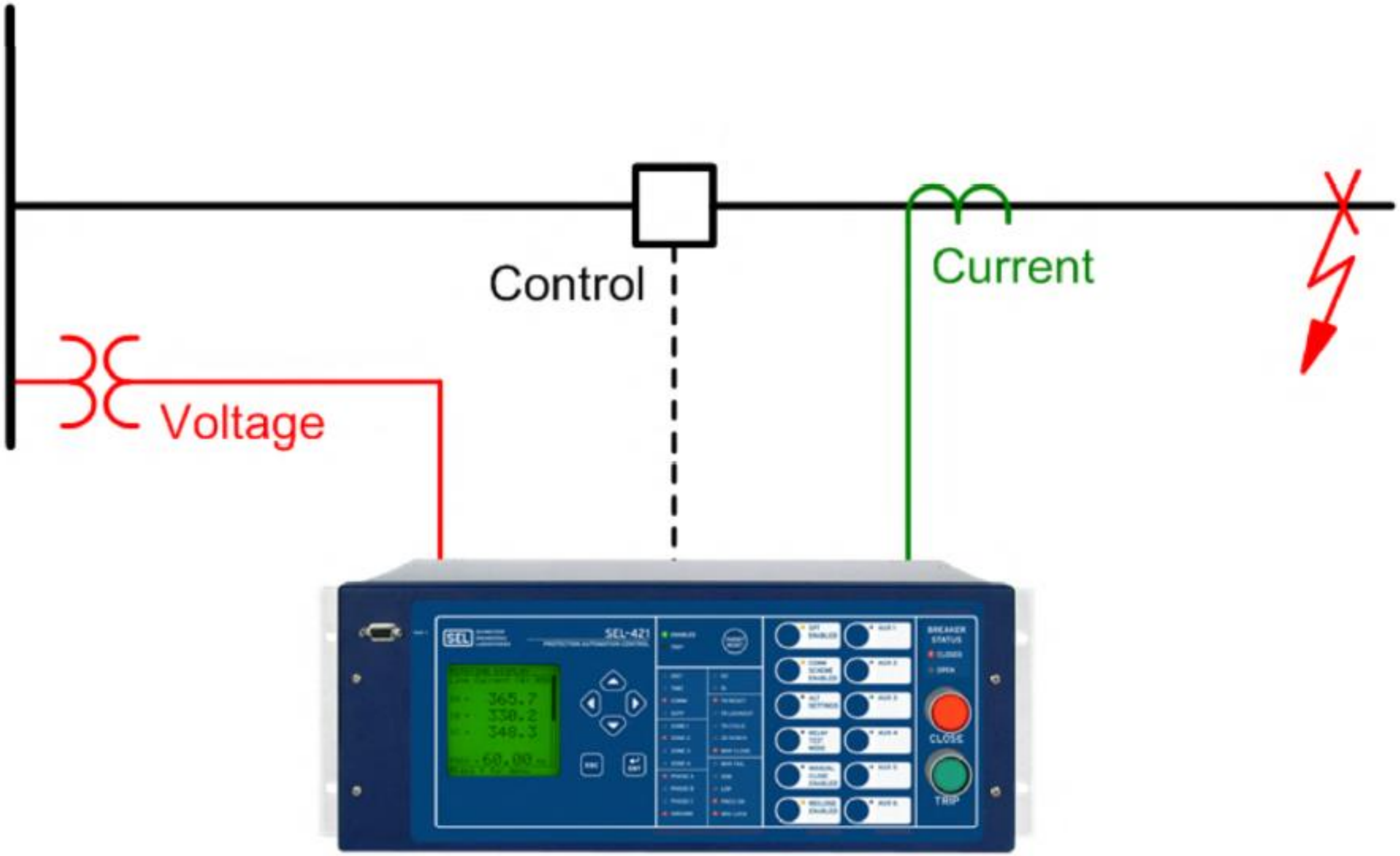
Simple Control System



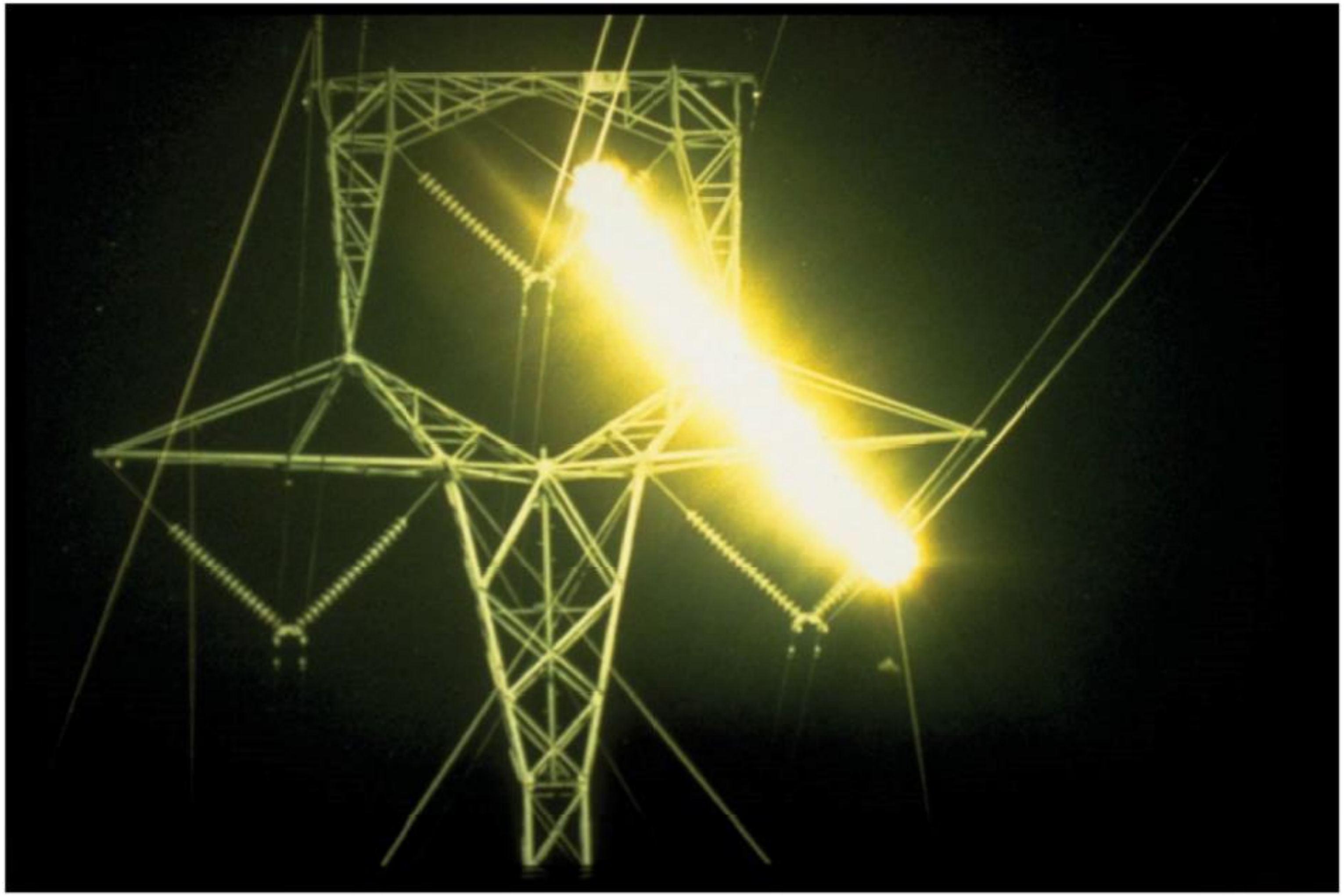
Protecting Your House



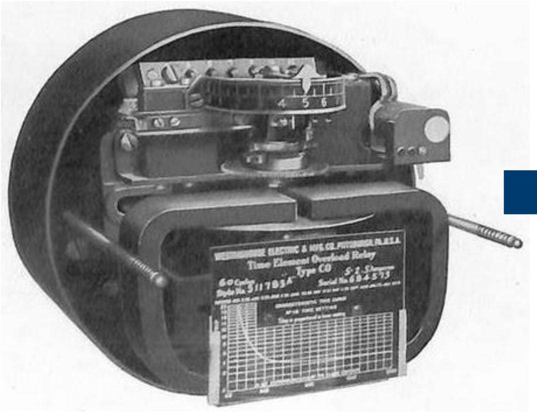
Protective Relays Clear Faults



What is a Fault?



Protective Relay Evolution


Westinghouse Electric & Mfg. Co. Pittsburgh, Pa. U.S.A.
Time Element Overload Relay
Type CO

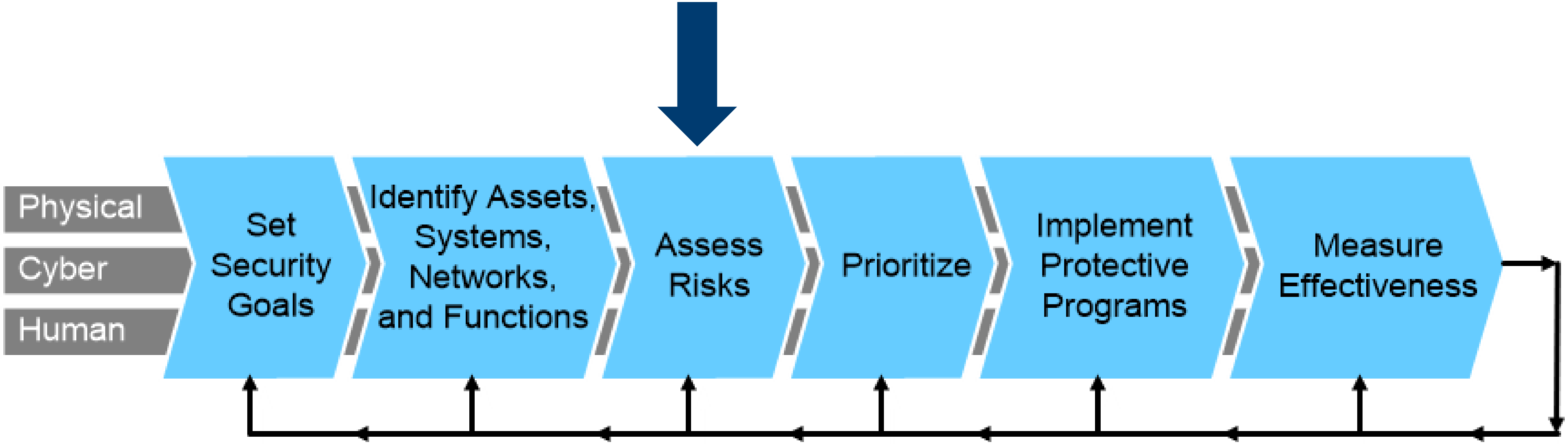
1902 1984 2021

Operator’s Perspective

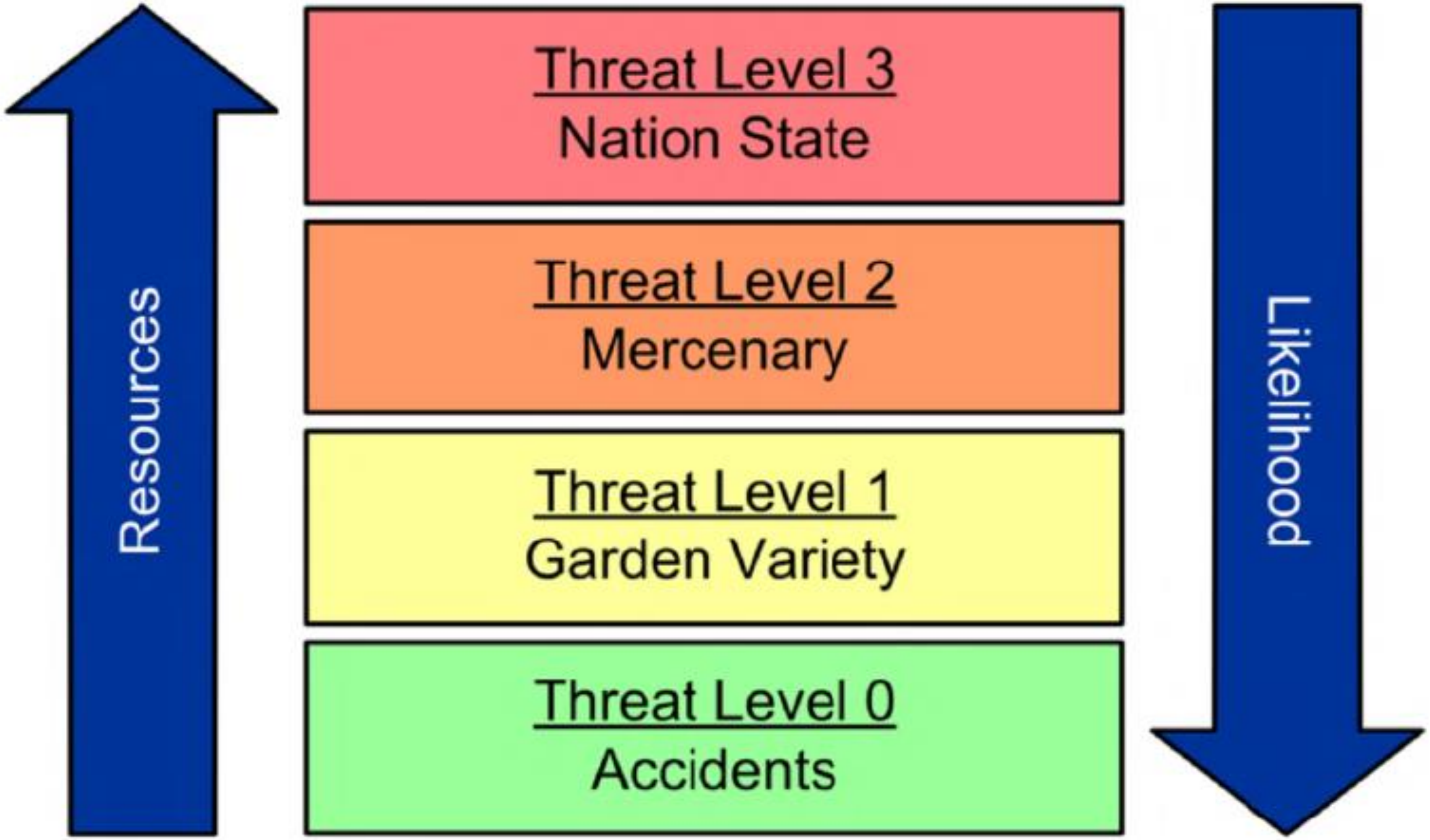
Two Families of Technology

Information Technology	Operations Technology
Highly dynamic environment	Highly static environment
Tech lifespan of 3-5 years	Tech lifespan of 10-60 years
Best attempt	Failure intolerant
Data driven	Machine Driven
Controlled environments	Uncontrolled environments

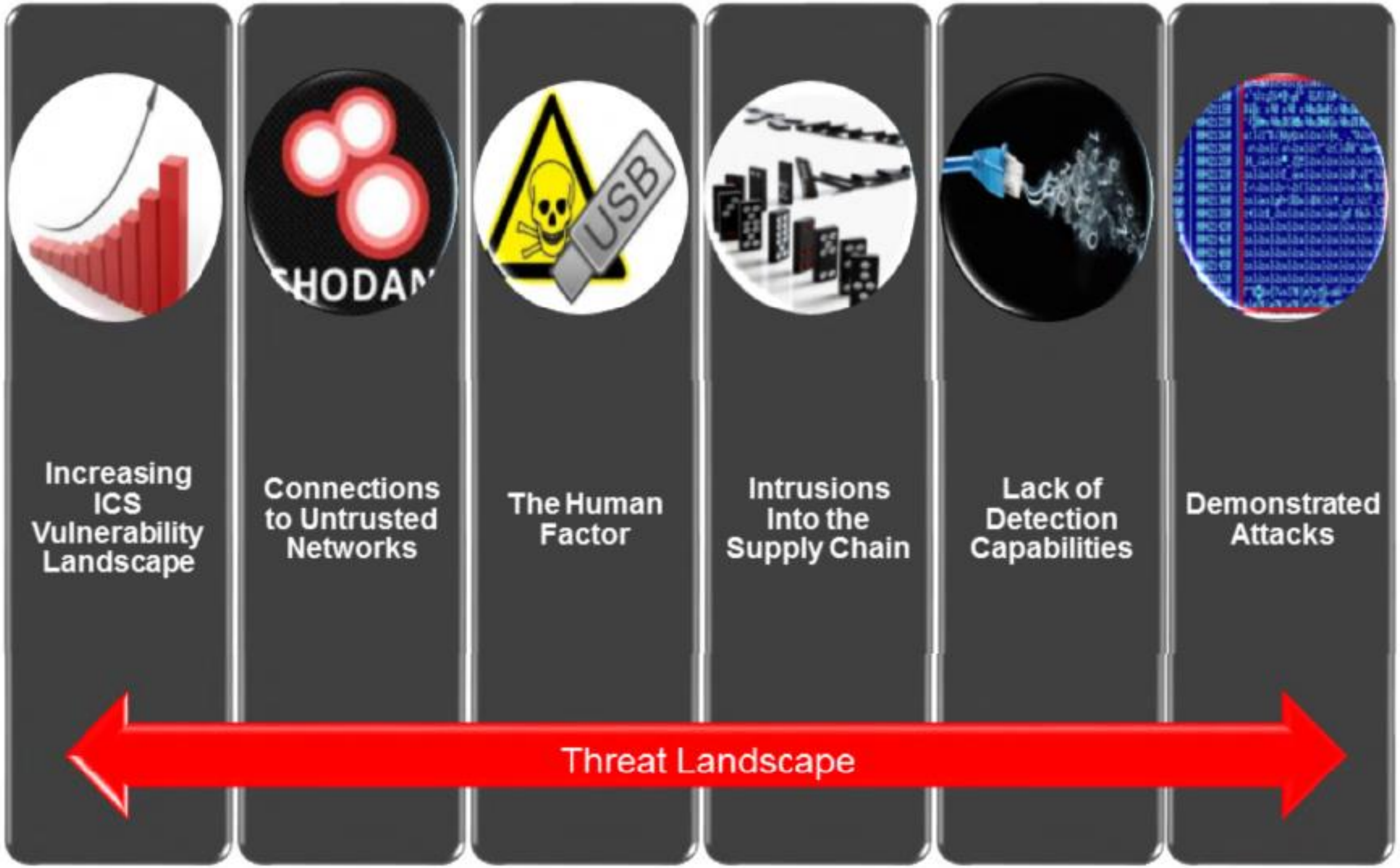
Risk Management in ICS



Threats Against ICS



Key Risk Factors


SHODAN
USB
Increasing ICS Vulnerability Landscape
Connections to Untrusted Networks
The Human Factor
Intrusions Into the Supply Chain
Lack of Detection Capabilities
Demonstrated Attacks
Threat Landscape

ICS Attack Potential Impact

ICS Attack Potential Impact

ICS Attack Examples

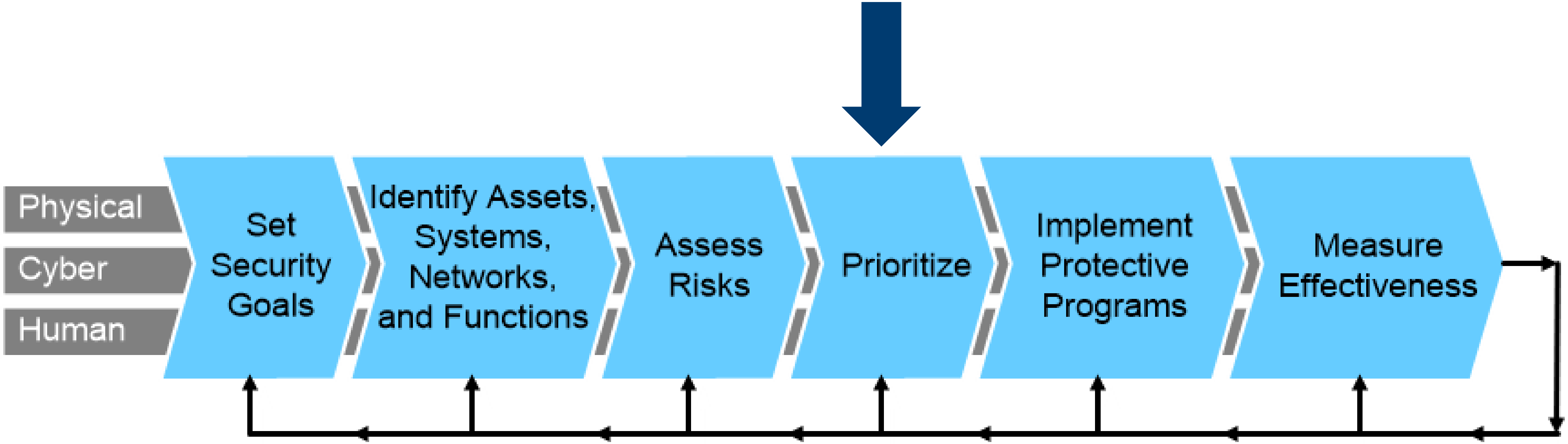
Maroochy Shire

Stuxnet

Metcalf

Ukraine

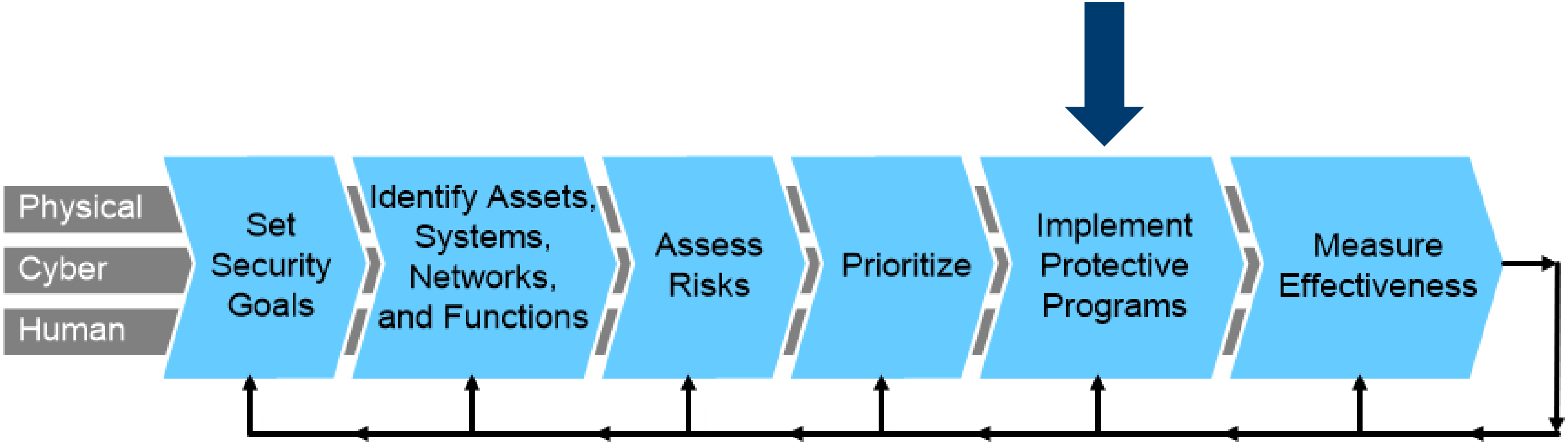
Risk Management in ICS



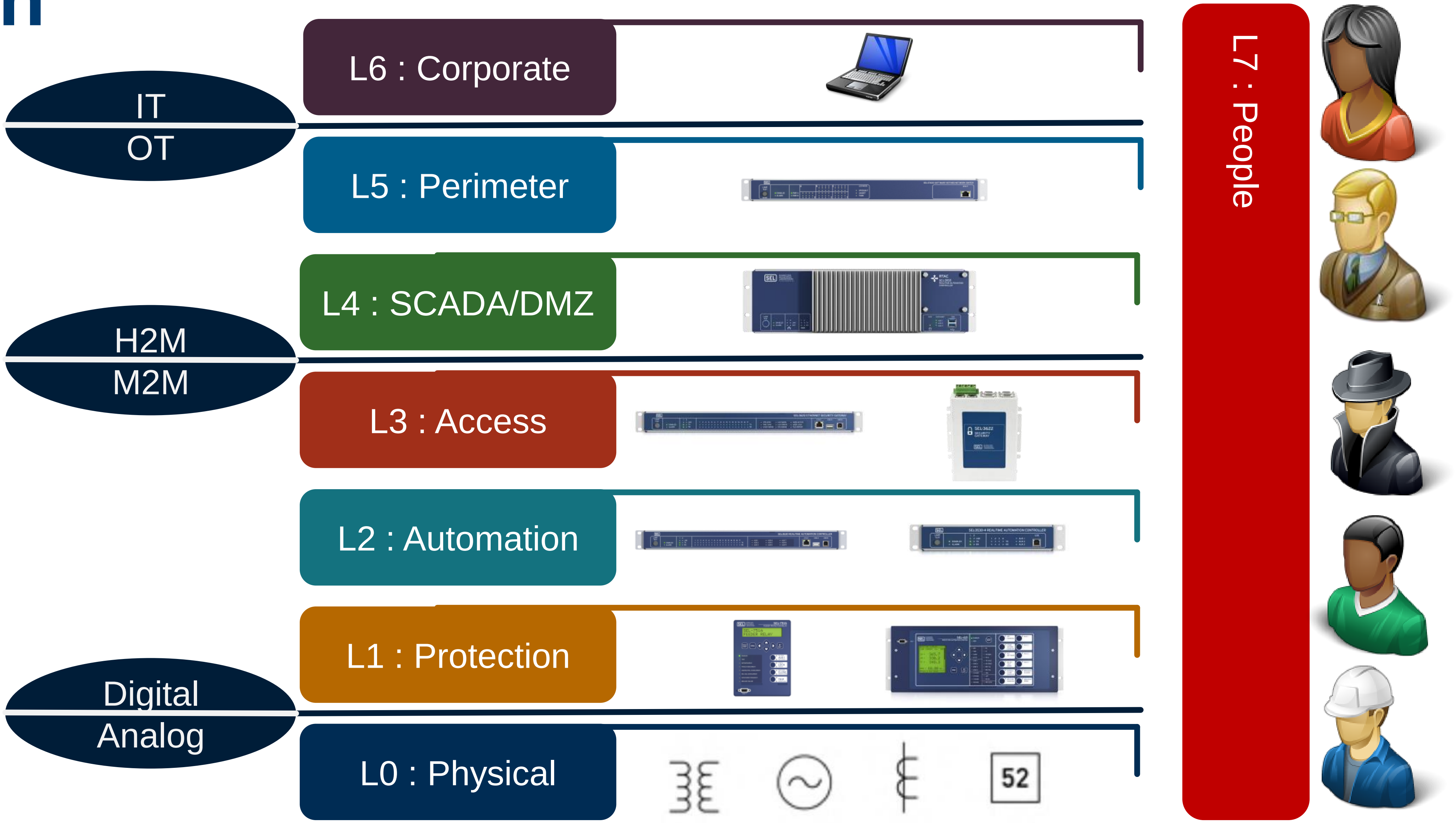
Prioritize

	Urgent	Not Urgent
Important	🟦	🟧
Not Important	🟥	🟩

Risk Management in ICS



System Level Approach



IT

OT

H2M

M2M

Digital

Analog

L6 : Corporate

L5 : Perimeter

L4 : SCADA/DMZ

L3 : Access

L2 : Automation

L1 : Protection

L0 : Physical

L7 : People

ICS Communications

Serial

- EIA-232
- EIA-422
- EIA-485

Frame Relay

PoTS Dial-up

Leased Line

SONET/SDH

Ethernet

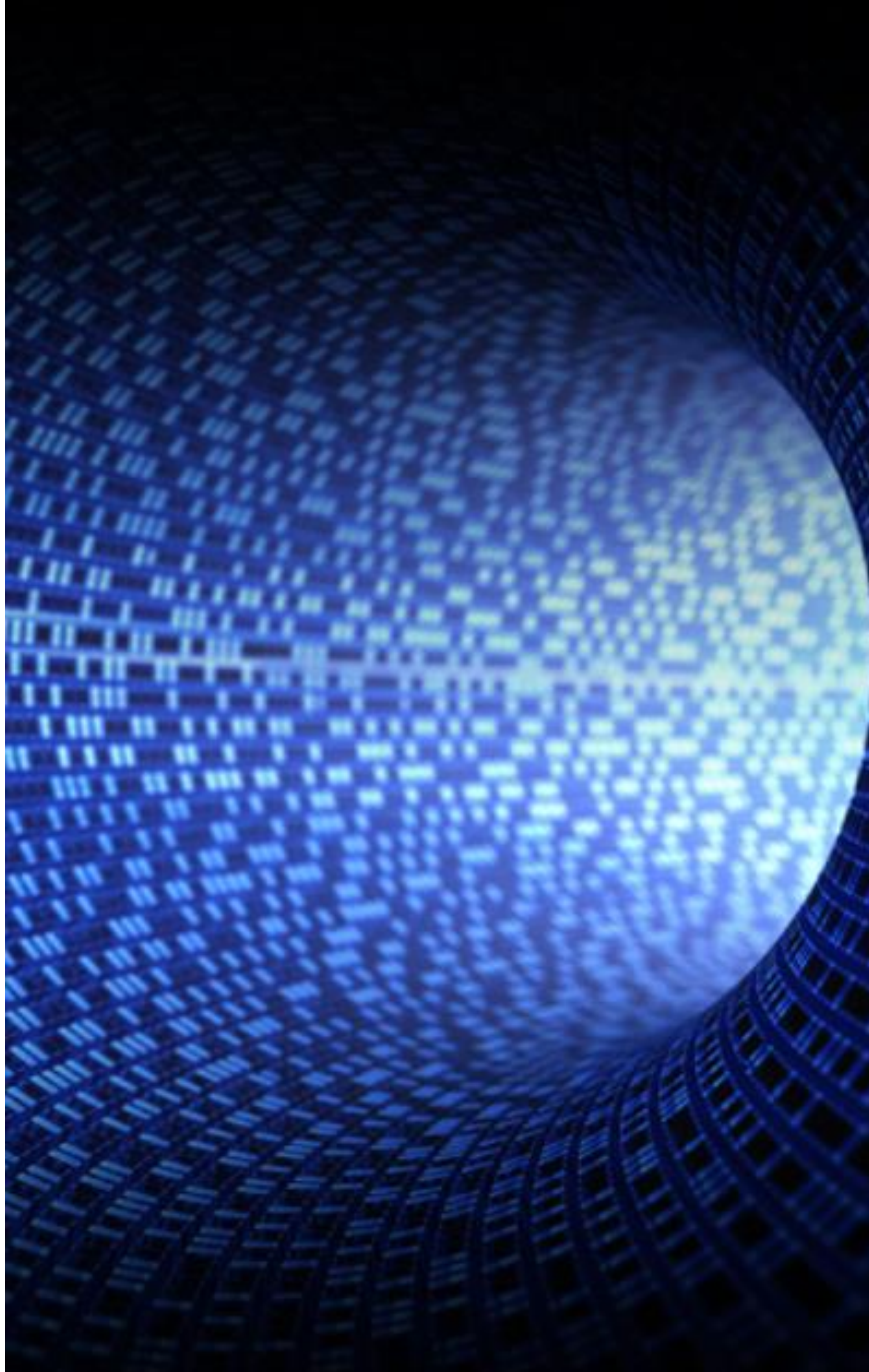
Copper

Fiber

Radio

Satellite

Cell



Defensive Strategies

- Train
- Reduce Attack Surface
- System Architecture
- Redundancy
- Monitoring
- Data Correlation
- Automation
- Cryptography
- Updates
- Access Control
- Process
- Physical
- Backups

ICS Cybersecurity Guidance

NIST

- Special Publication 800

NERC

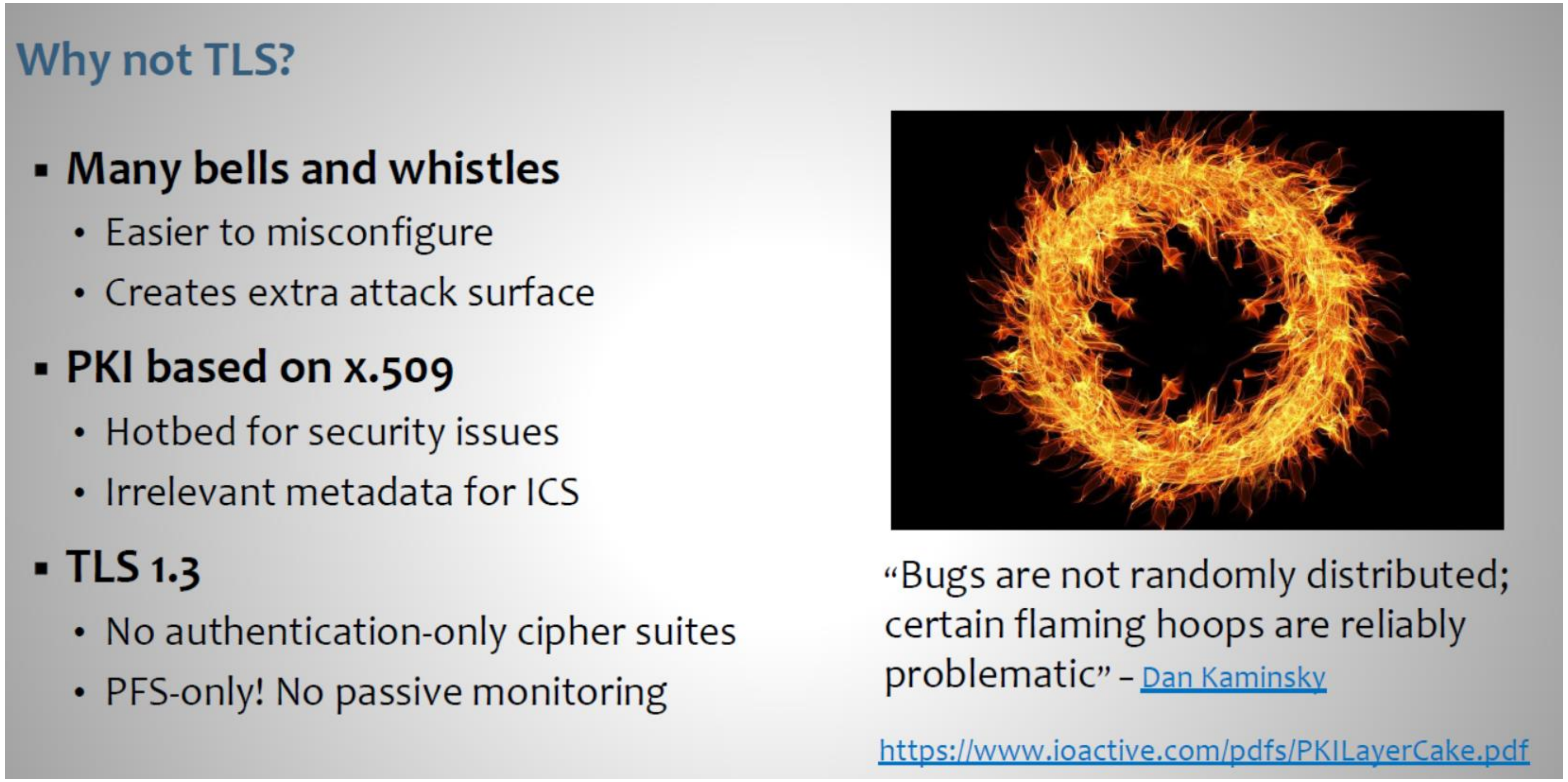
- Critical Infrastructure Protection

ISA/IEC

- 62443
- 62351

Re-Using IT Technology in OT Systems

TLS | X.509 | LDAP | RADIUS | Syslog | SNMP



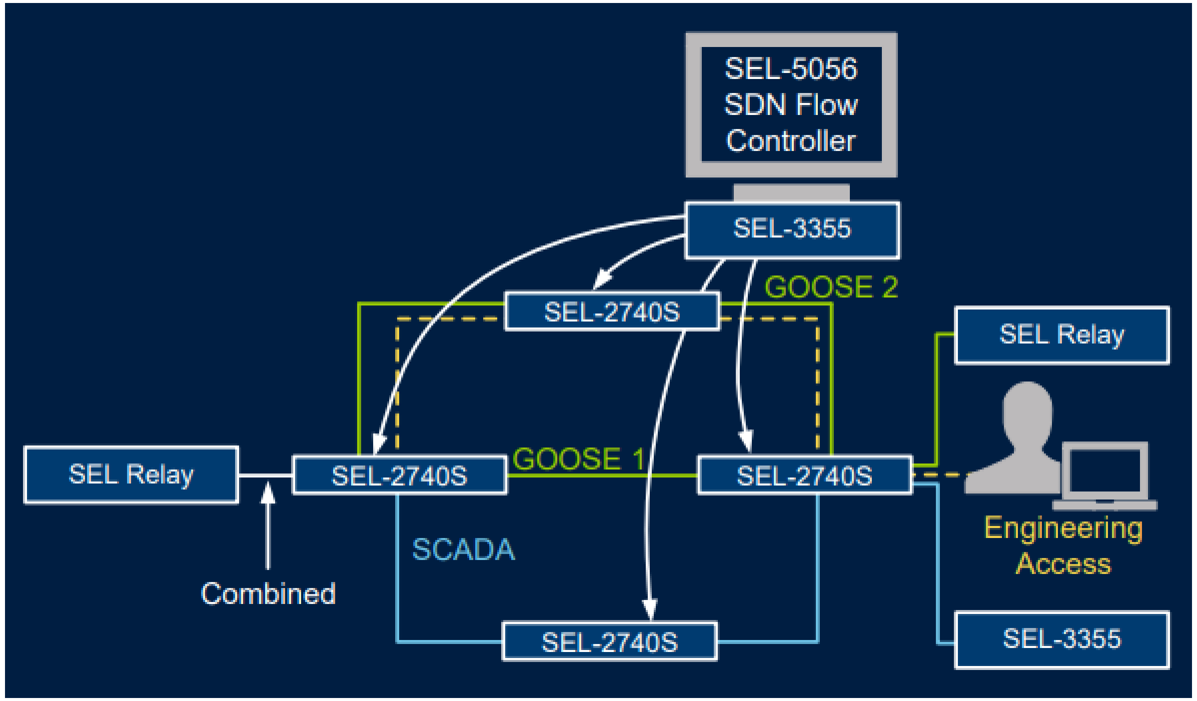
Why not TLS?

- **Many bells and whistles**
  - Easier to misconfigure
  - Creates extra attack surface
- **PKI based on x.509**
  - Hotbed for security issues
  - Irrelevant metadata for ICS
- **TLS 1.3**
  - No authentication-only cipher suites
  - PFS-only! No passive monitoring

"Bugs are not randomly distributed; certain flaming hoops are reliably problematic" – Dan Kaminsky

https://www.ioactive.com/pdfs/PKILayerCake.pdf

Reinventing IT Technologies for ICS



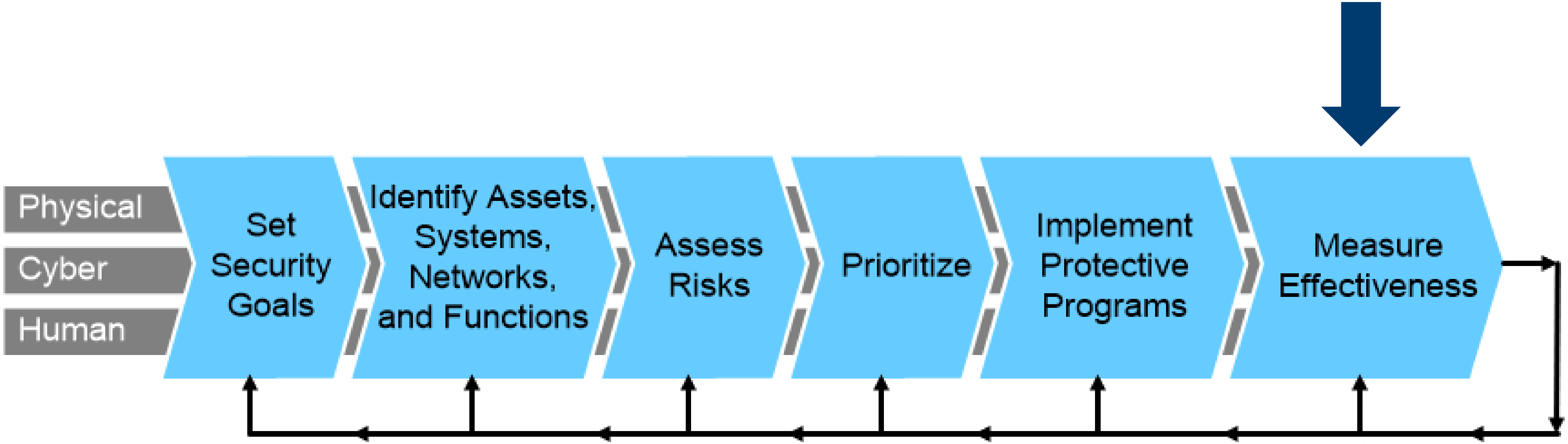
Software Defined Networking

IPsec

MACsec

OAuth

Risk Management in ICS



Physical

Cyber

Human

Set Security Goals

Identify Assets, Systems, Networks, and Functions

Assess Risks

Prioritize

Implement Protective Programs

Measure Effectiveness

Test

Table Top Exercises

Failure/Recovery Exercises

Penetration Test (NOT ON A LIVE SYSTEM!!!!)

Parting Message

ICS cybersecurity has unique considerations

Application awareness is key

Challenging environment for cybersecurity

Tremendous room for innovation

Questions?