

An abstract digital graphic on the left side of the slide. It features several blue, three-dimensional cubes of varying sizes. The surfaces of these cubes are covered in a pattern of small, glowing blue dots, resembling binary code or data points. Some of the cubes have internal light sources, creating a bright blue glow. A few small, glowing red and green dots are scattered around the cubes, and a thin blue line with a red dot at its end extends from one of the cubes.

Cybersecurity in Industrial Control Systems

Nathan Kipp
Engineering Manager
Infrastructure Defense Product Development

Learning Objectives



Learn Industrial Control System Basics



Understand Cybersecurity Goals in Industrial Control Systems



Introduce Energy System Cybersecurity Driving Factors

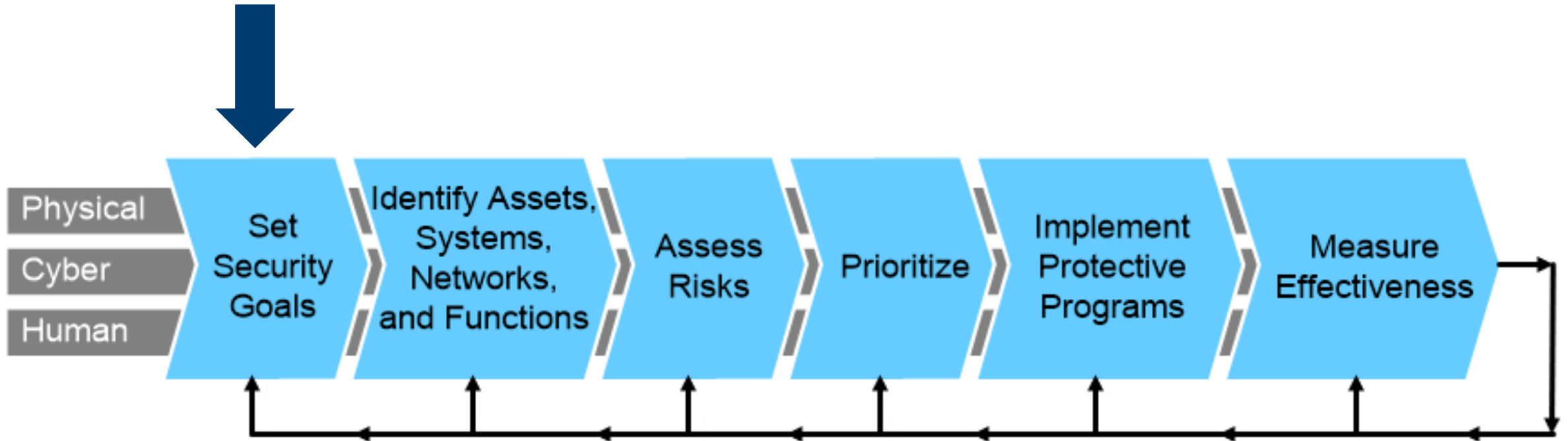


Discuss Current Solutions and Trends

Risk Management in ICS



Risk Management in ICS



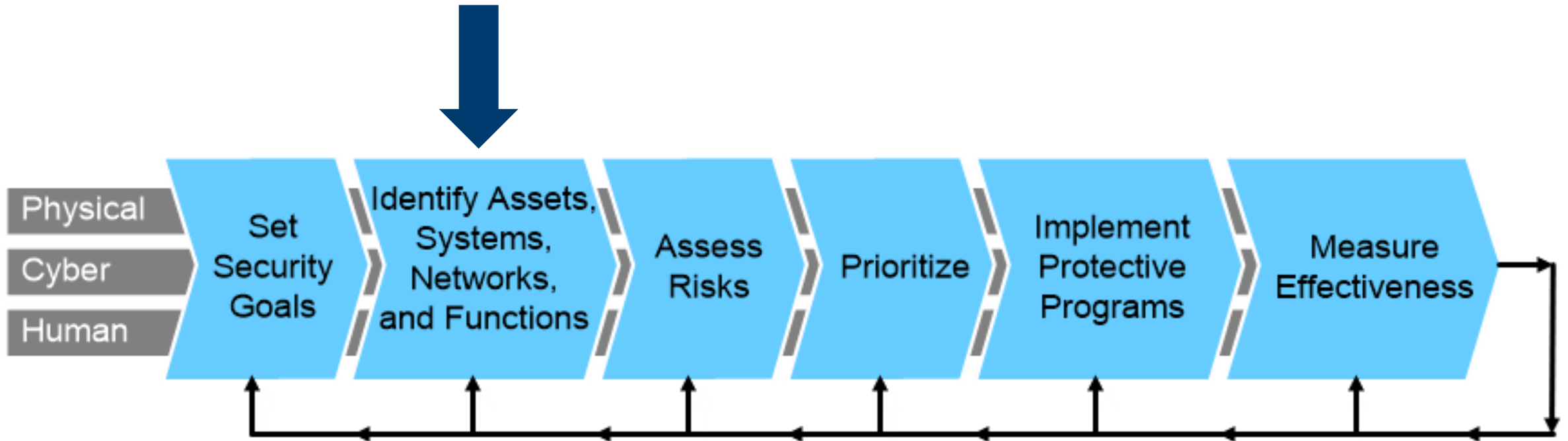


Our goal as defenders

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

Temperature Sensor



Thermostat



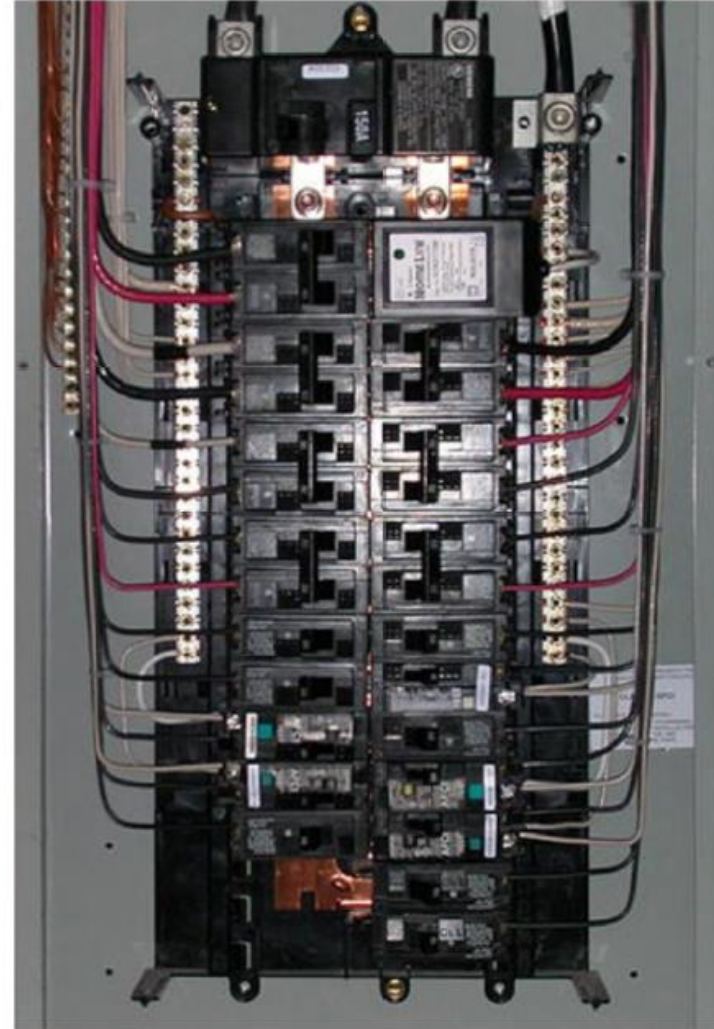
HVAC



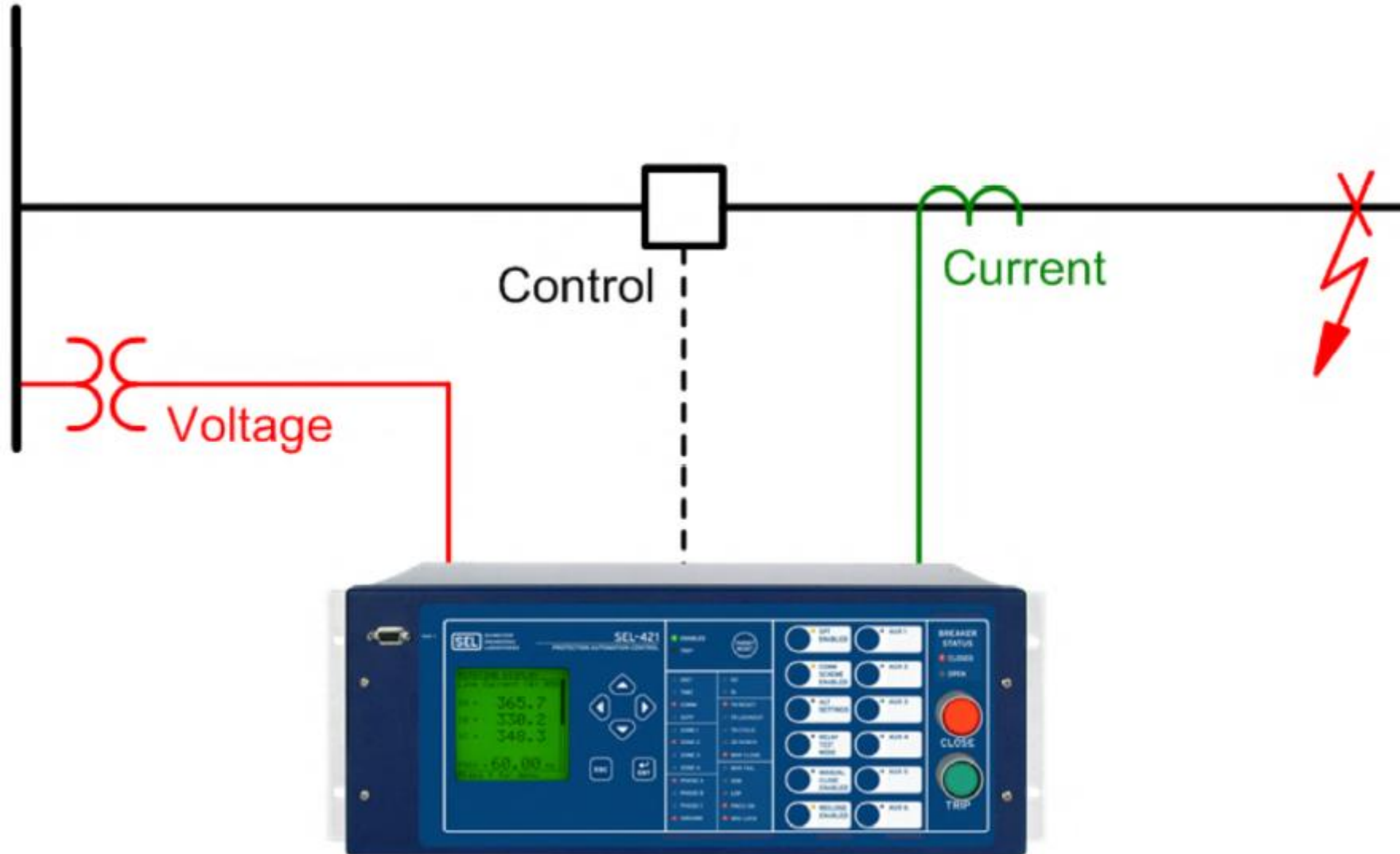
Temperature
Settings
(Up/Down)

Temperature
Display

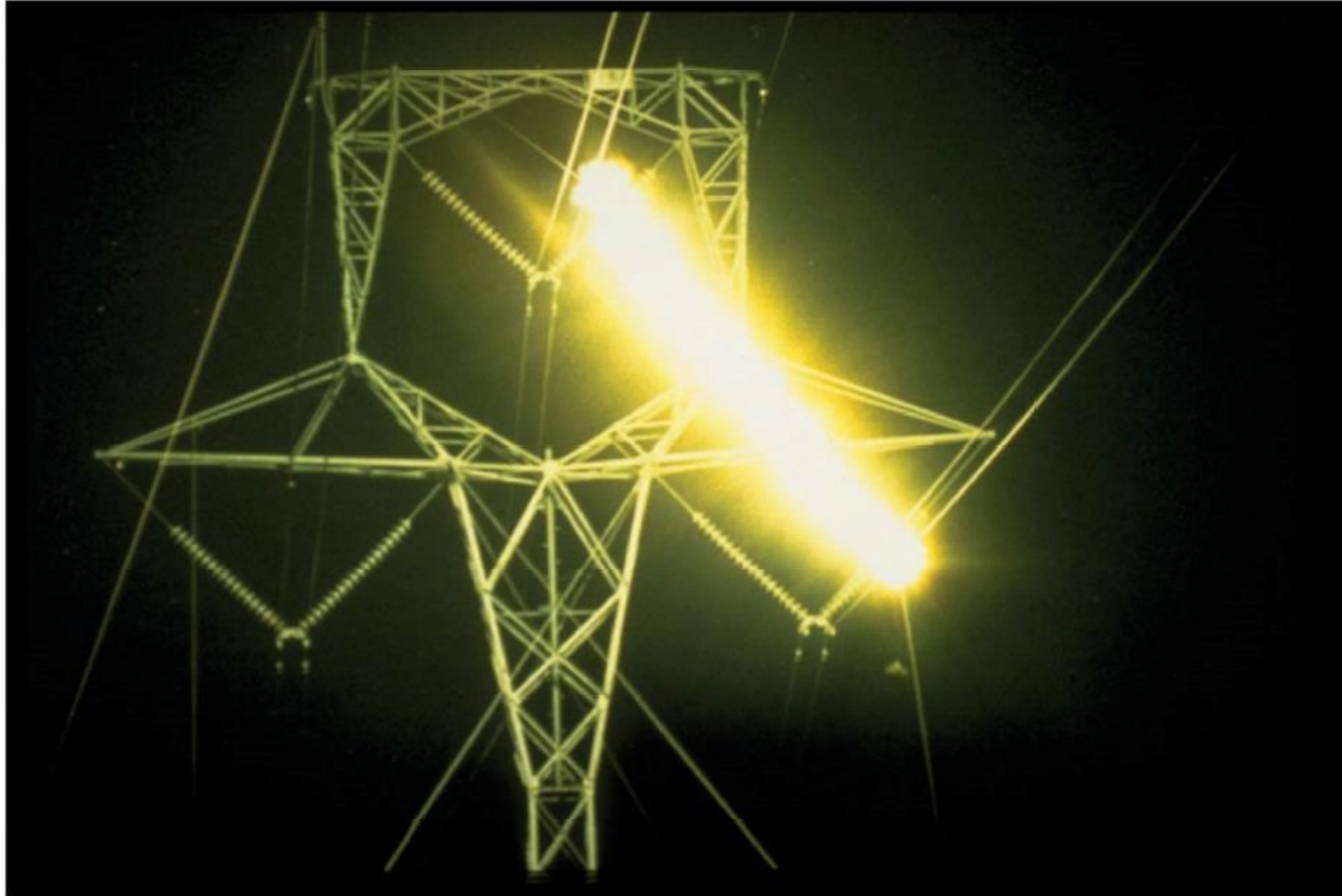
Protecting Your House



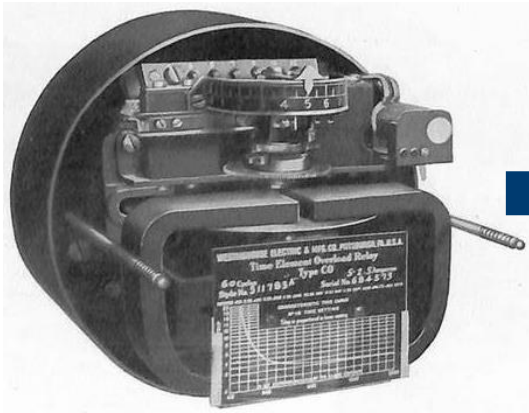
Protective Relays Clear Faults



What is a Fault?



Protective Relay Evolution



1902



1984



2021



Operator's Perspective



ICS Communications

Serial

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

Frame Relay

PoTS Dial-up

Leased Line

SONET/SDH

Ethernet

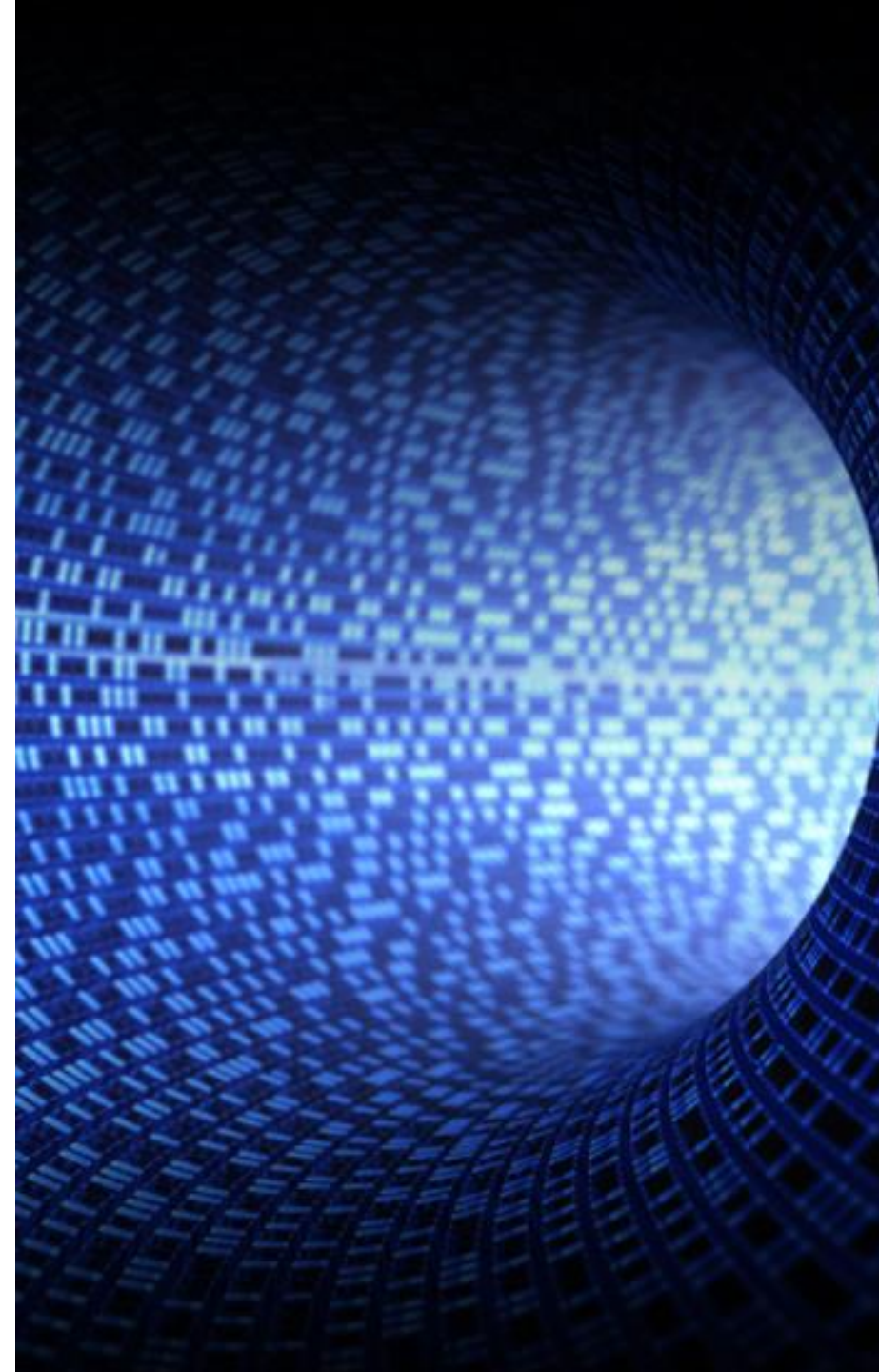
Copper

Fiber

Radio

Satellite

Cell



Two Families of Technology

Information Technology

Highly dynamic environment

Tech lifespan of 3-5 years

Best attempt

Data driven

Controlled environments

Operations Technology

Highly static environment

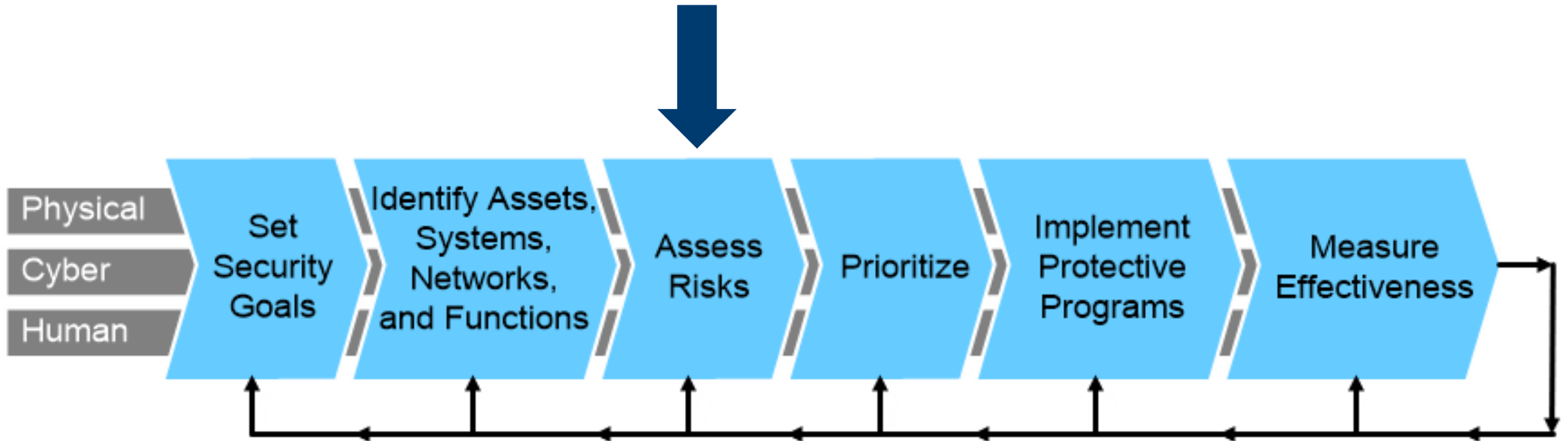
Tech lifespan of 10-60 years

Failure intolerant

Machine Driven

Uncontrolled environments

Risk Management in ICS



Components of Risk

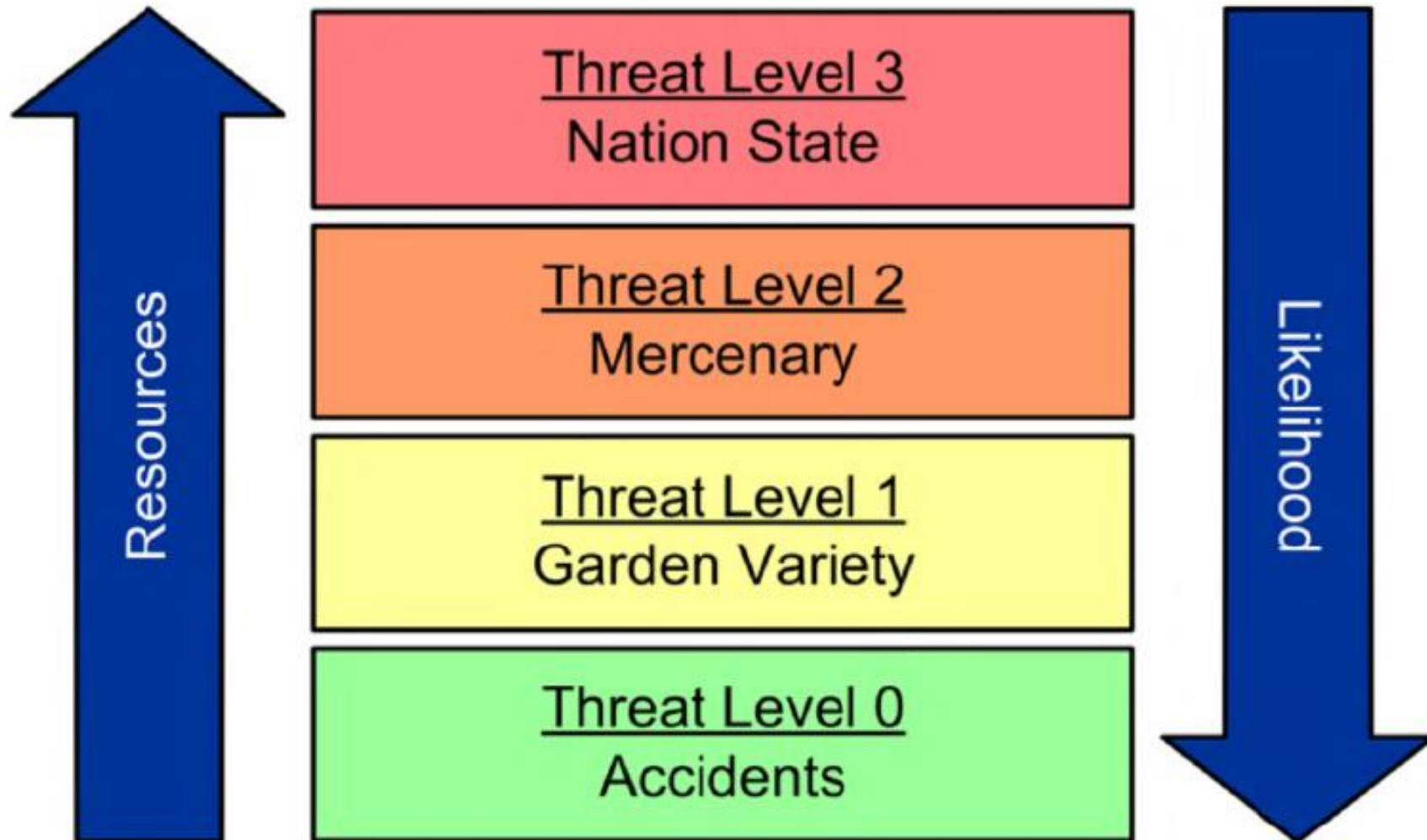


Threat

Consequence

Probability

Threat Levels



Threat Landscape



ICS Attack Potential Impact



ICS Attack Potential Impact





ICS Attack Examples

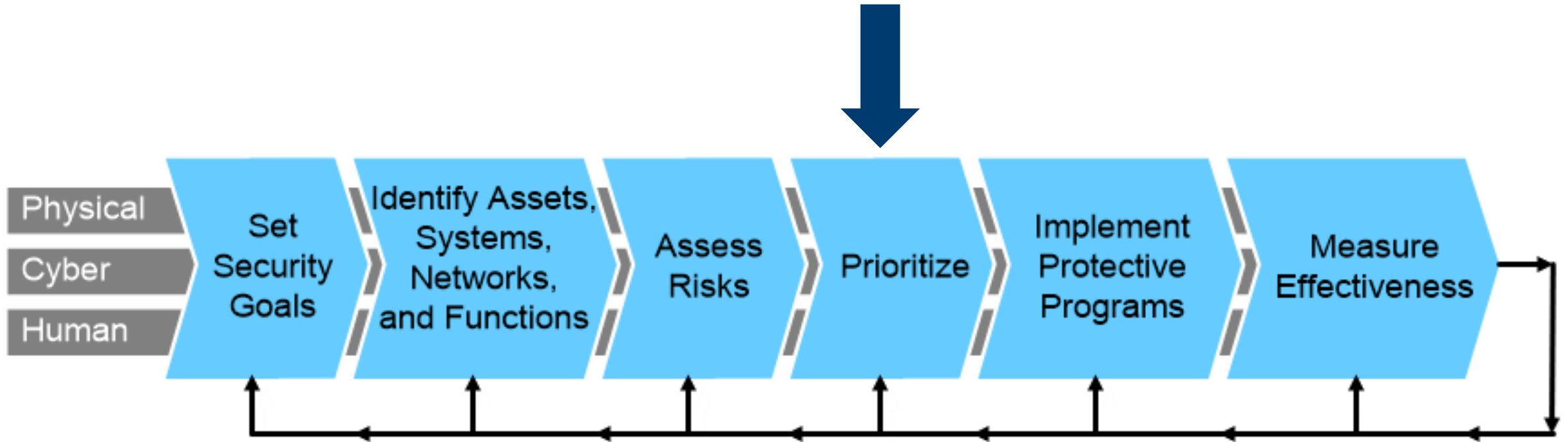
Maroochy Shire

Stuxnet

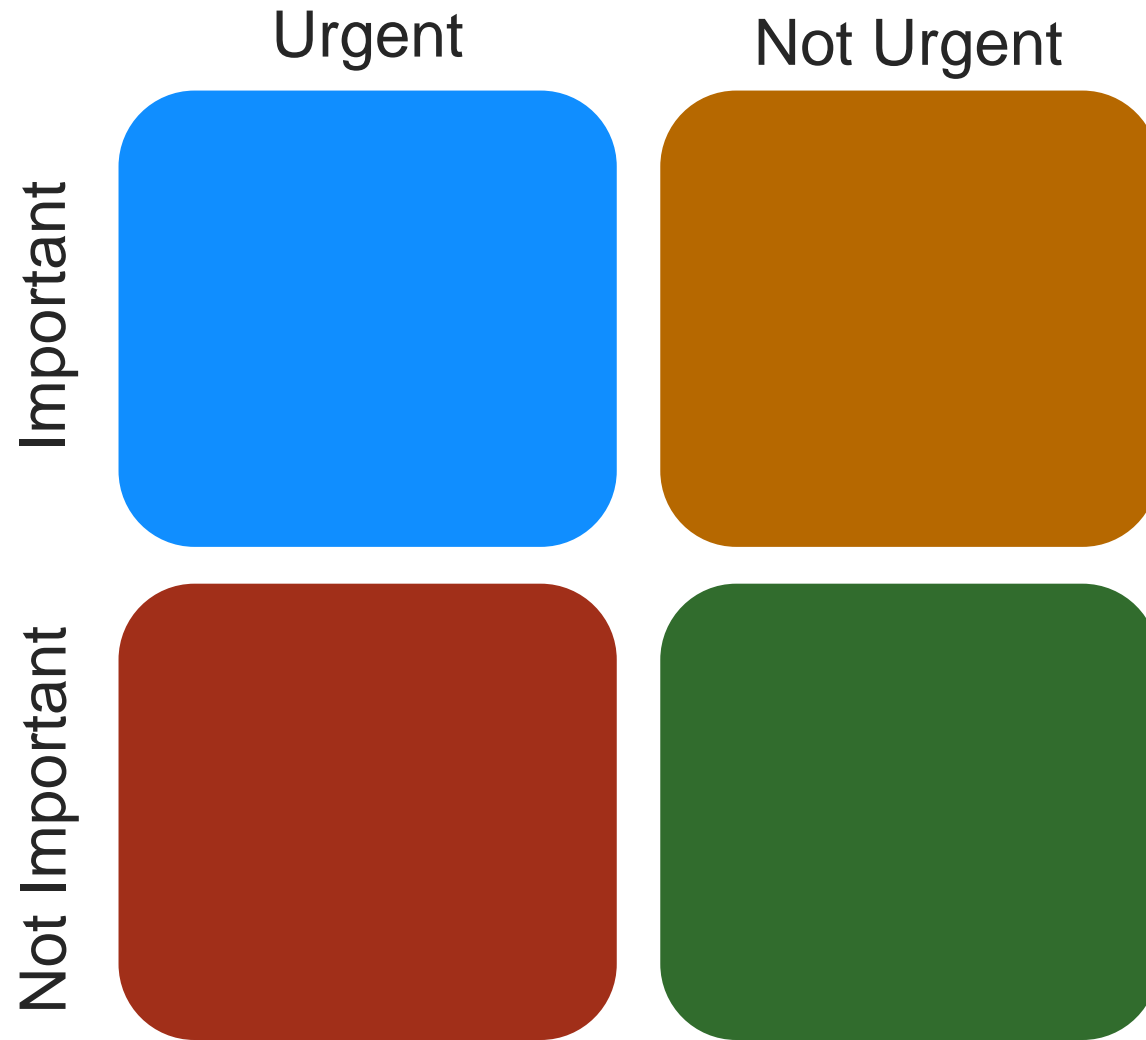
Metcalf

Ukraine

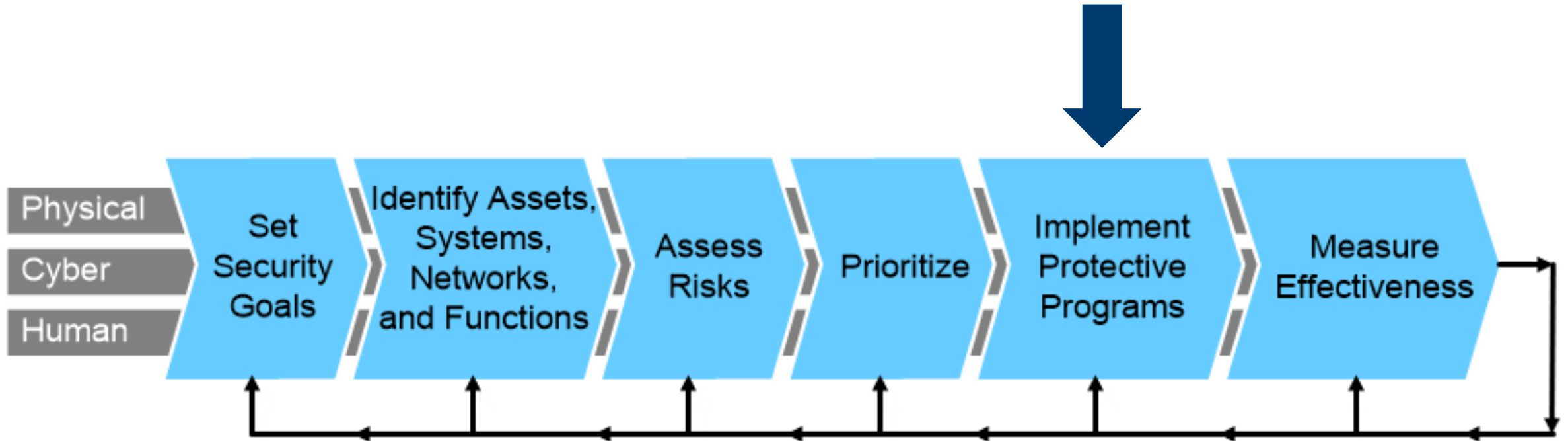
Risk Management in ICS



Prioritize



Risk Management in ICS



Defensive Strategies

Process

Reduce
Attack
Surface

System
Architecture

Redundancy

Monitoring

Data
Correlation

Automation

Cryptography

Updates

Access
Control

Train

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?

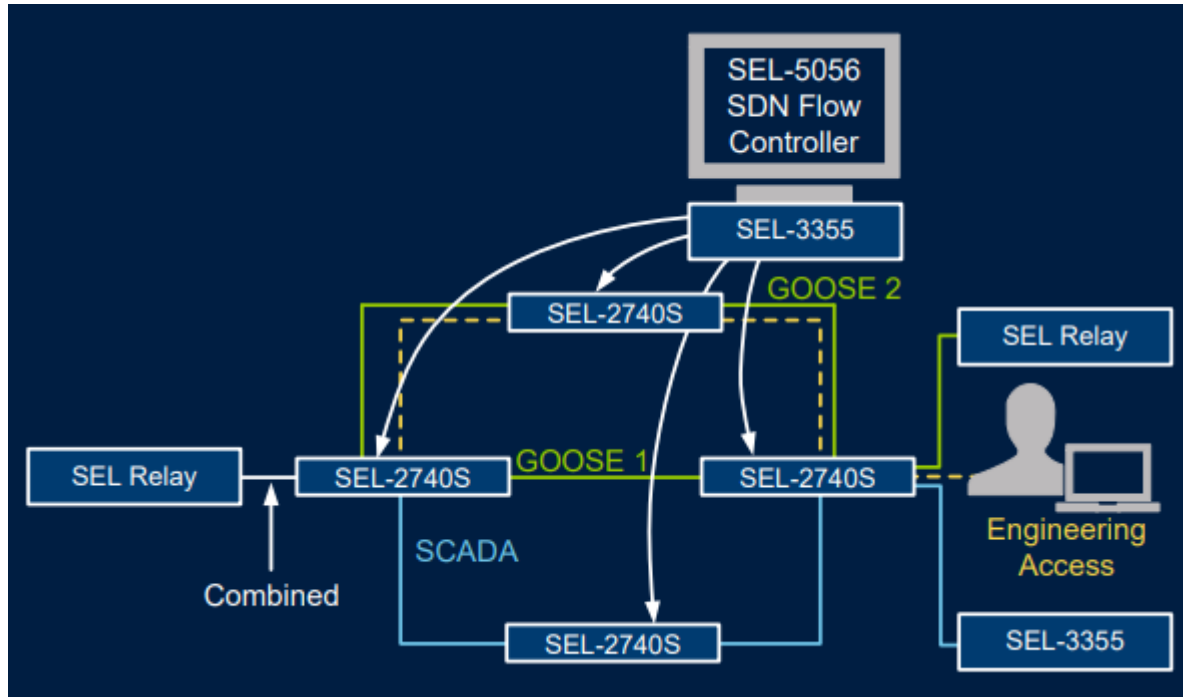
- **Many bells and whistles**
 - Easier to misconfigure
 - Creates extra attack surface
- **PKI based on x.509**
 - Hotbed for security issues
 - Irrelevant metadata for ICS
- **TLS 1.3**
 - No authentication-only cipher suites
 - PFS-only! No passive monitoring



“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



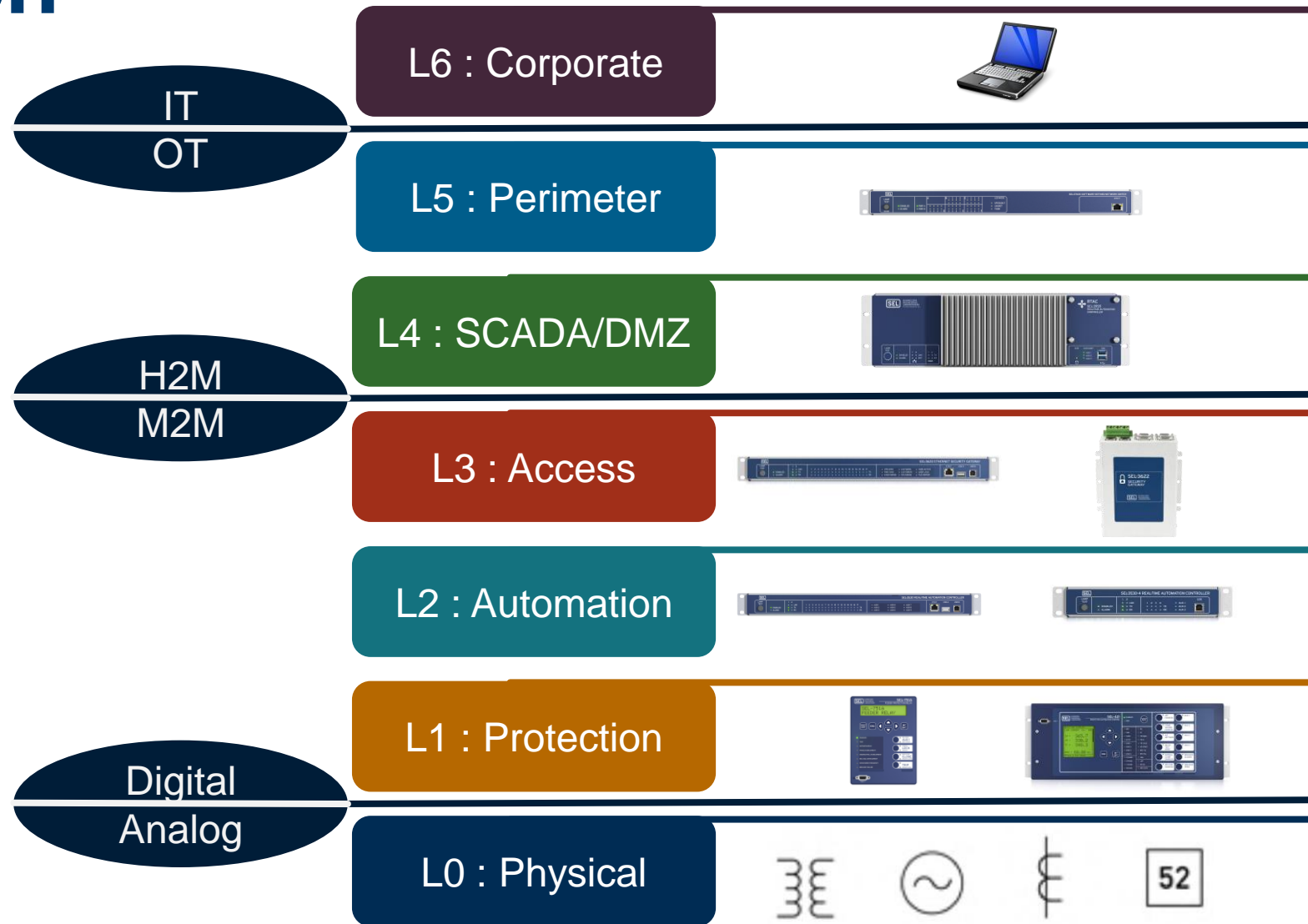
Software Defined Networking

IPsec

MACsec

OAuth

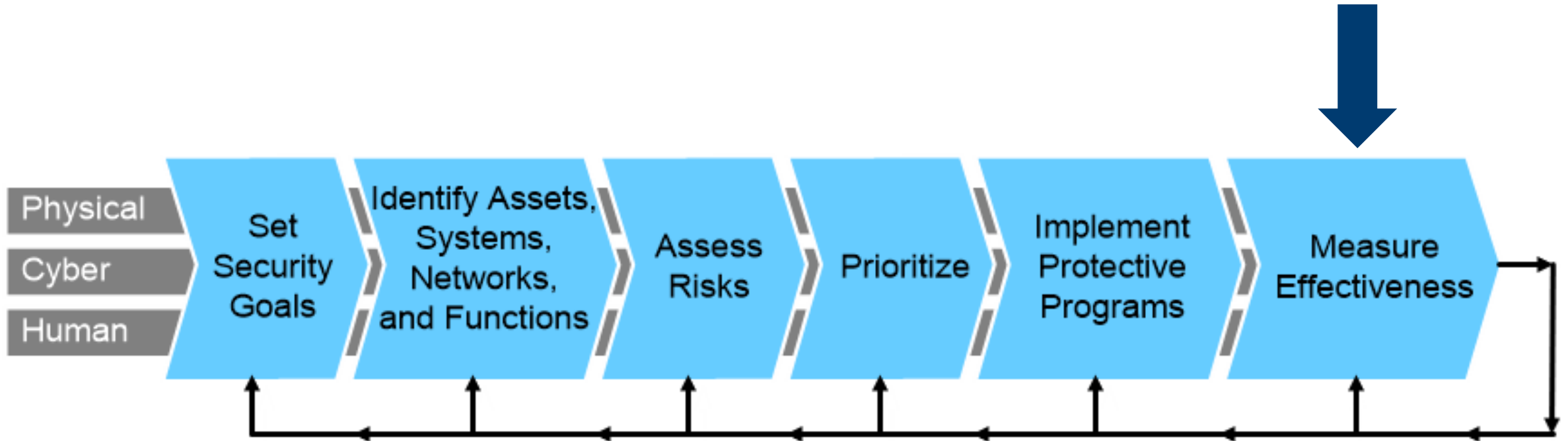
System Level Approach



L7 : People



Risk Management in ICS





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?