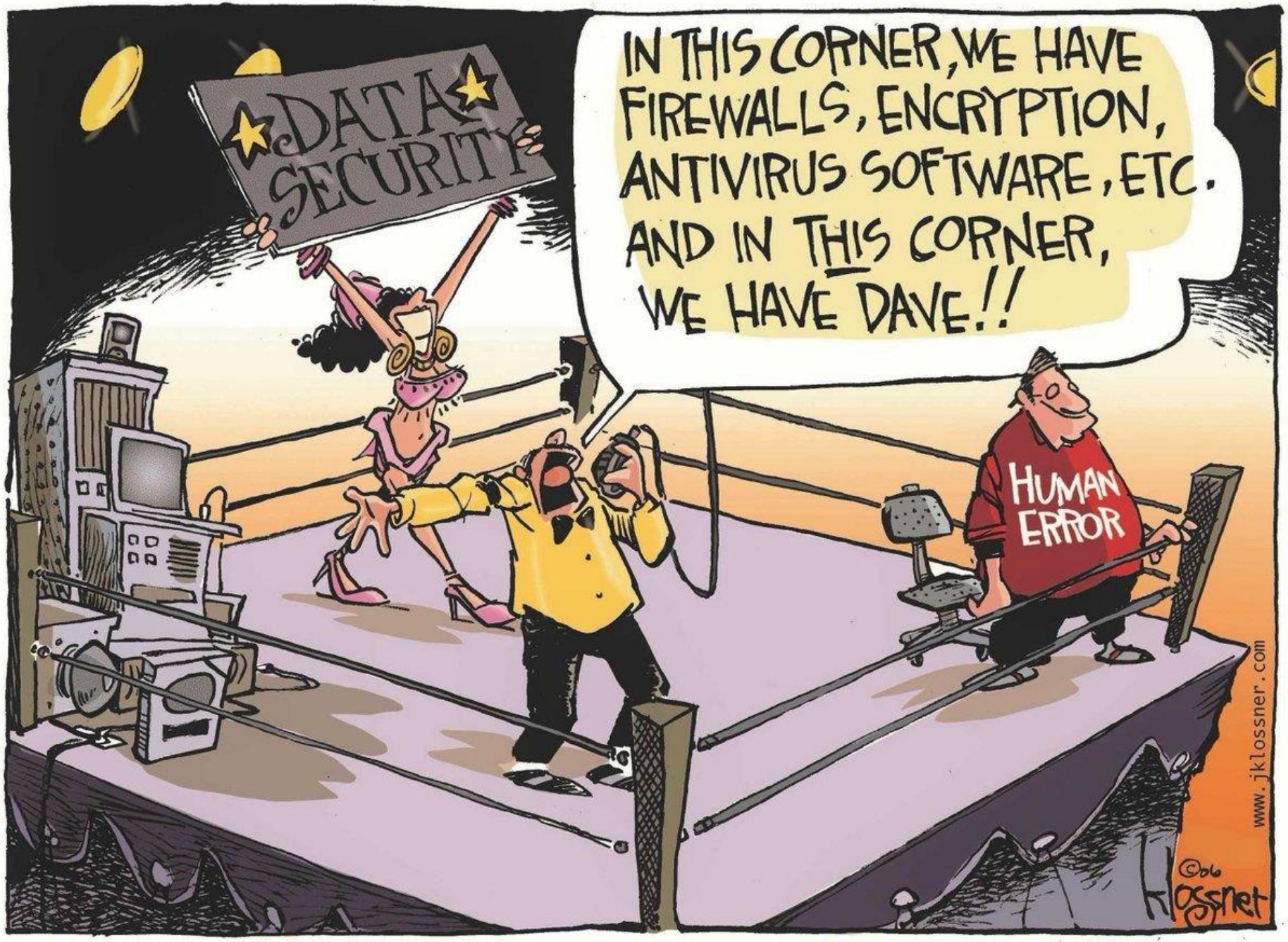
Industrial Control System Cybersecurity Risk Management

Nathan Kipp
Engineering Manager
Infrastructure Defense Product Development

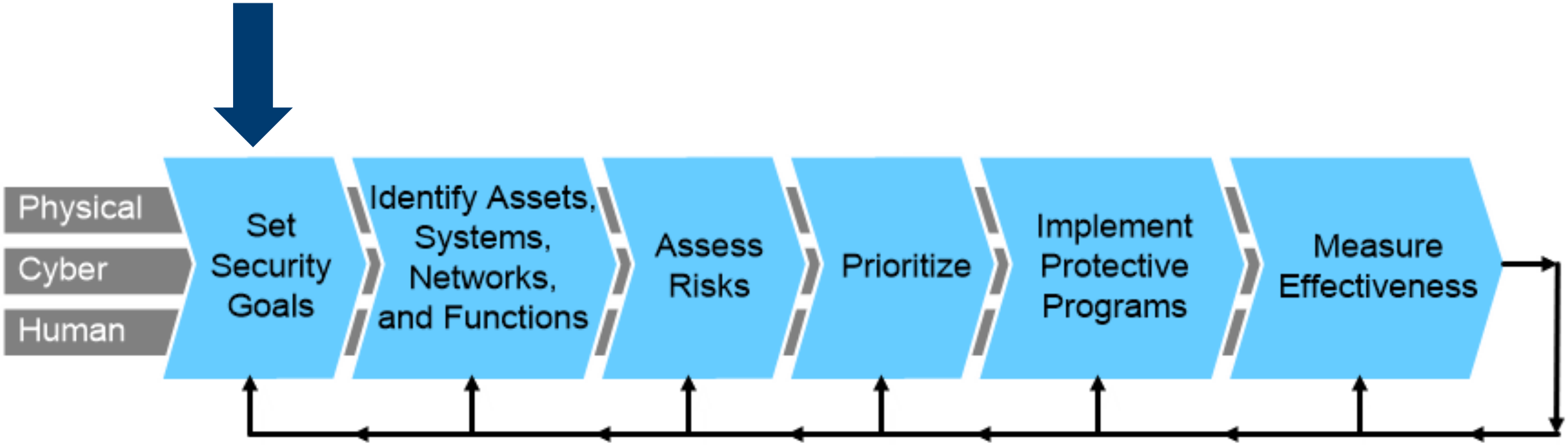
Learning Objectives

- 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


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC.
AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
©06
Klossner

Risk Management in ICS

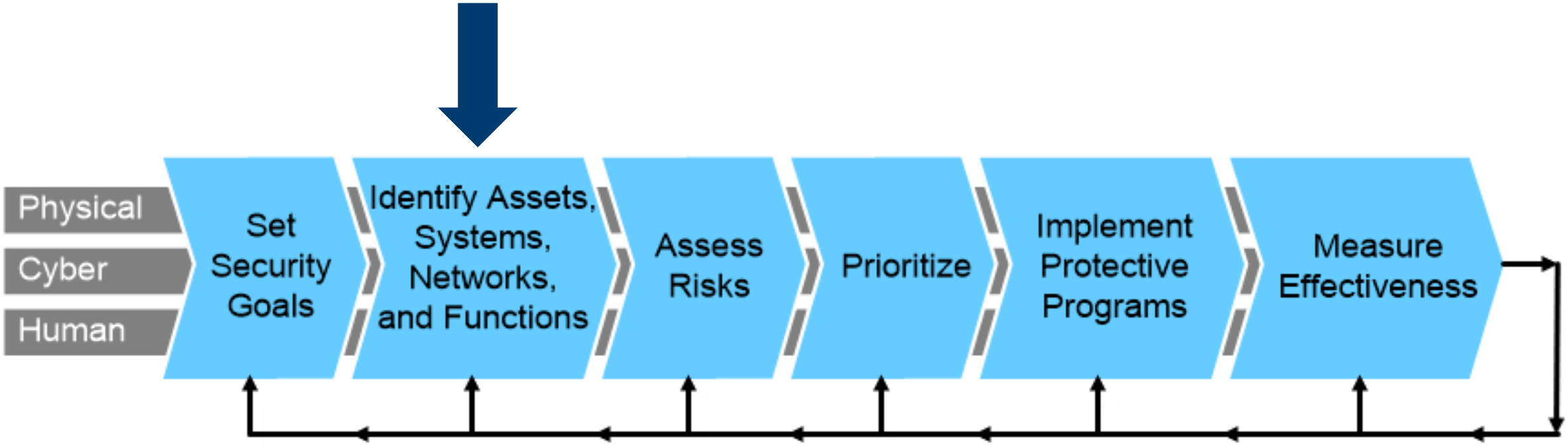


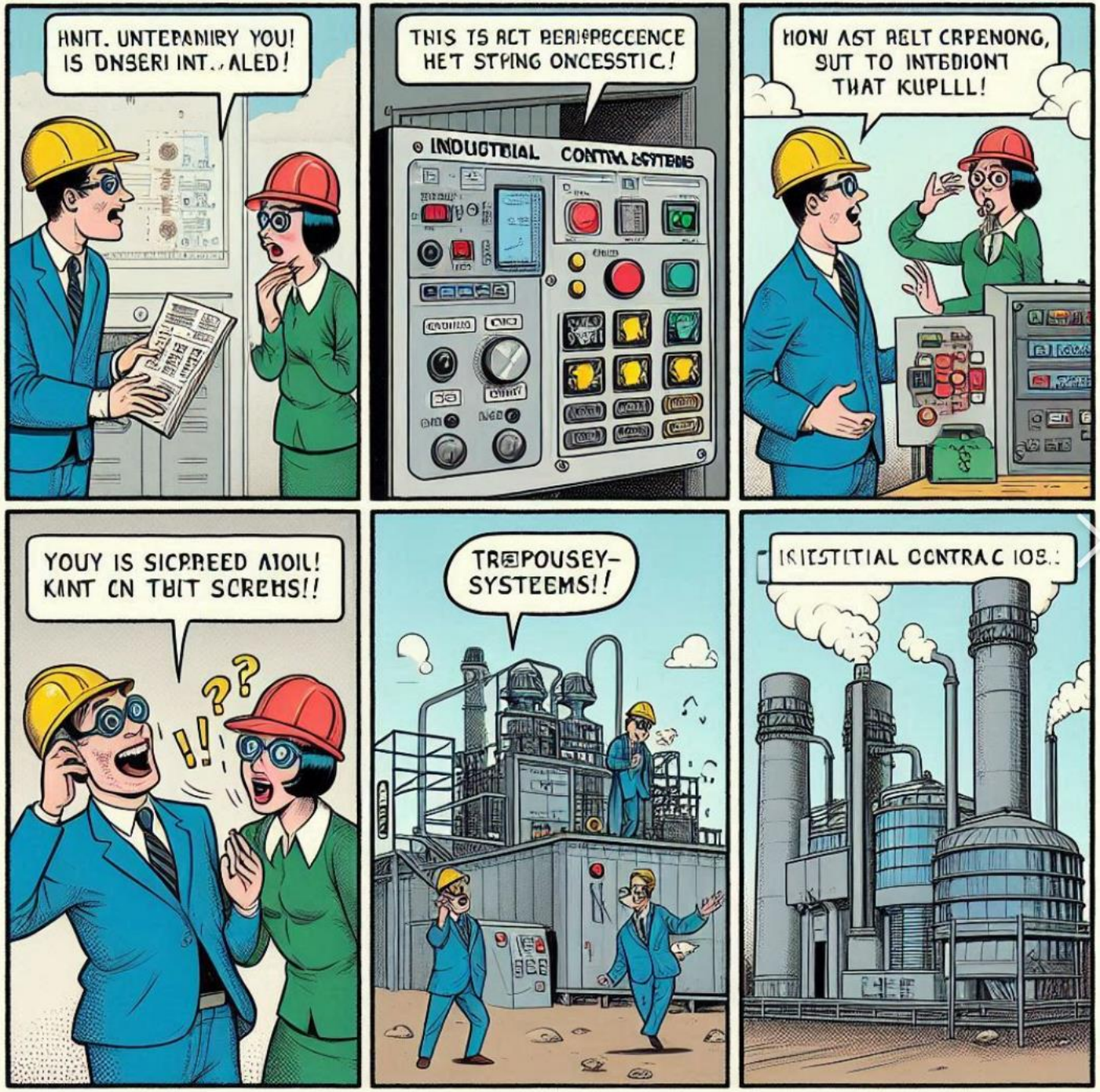
Our goal as defenders

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…

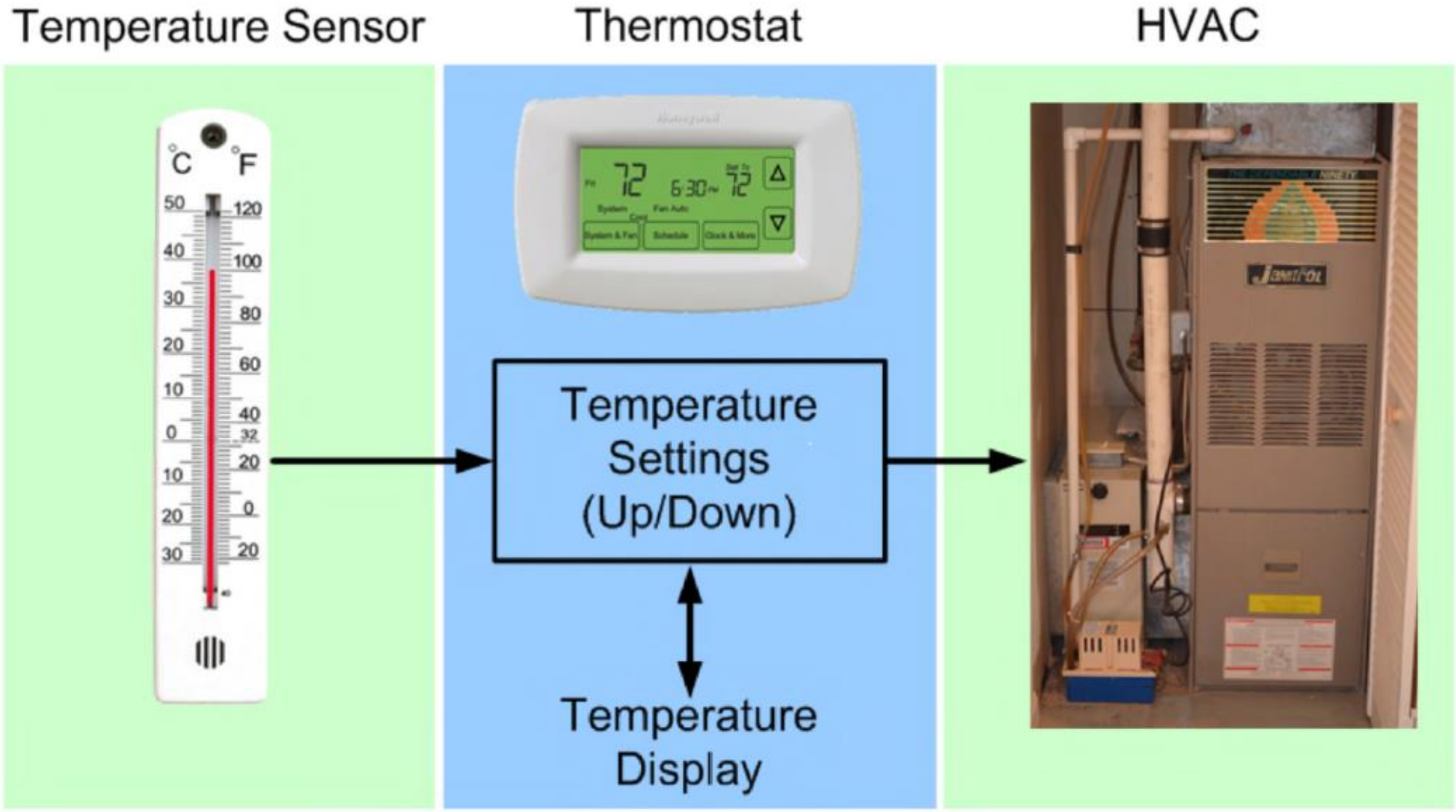
Risk Management in ICS



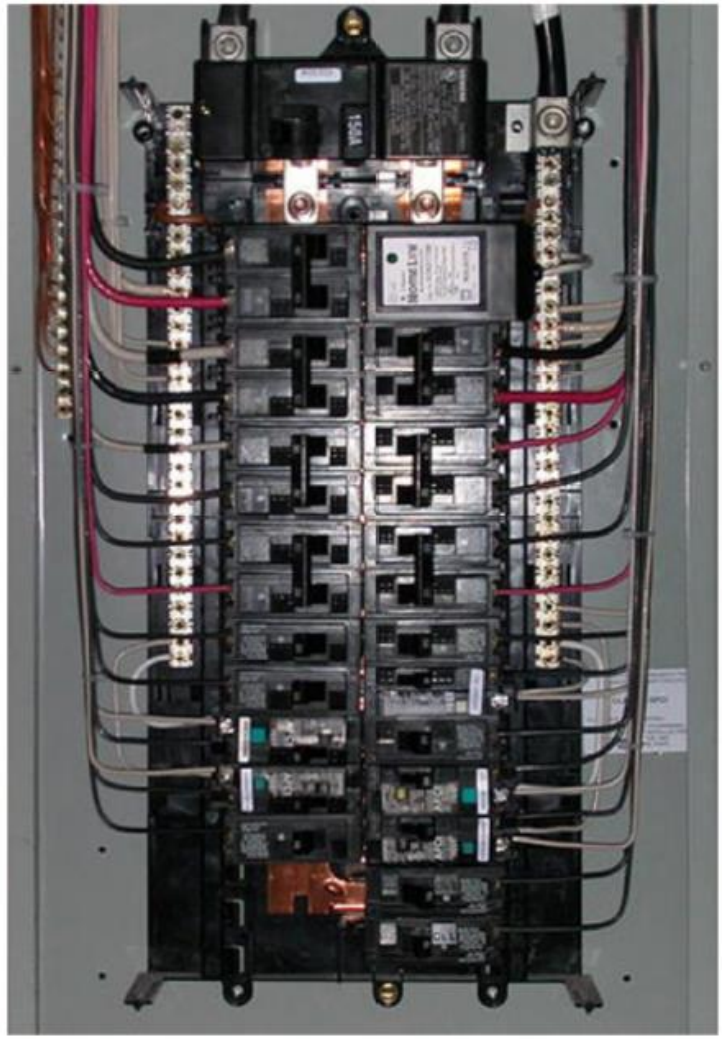

HNIT. UNTERANIRY YOU!
IS DNSERI INT.. ALED!
THIS TS ACT BERIPECCENCE
HET STPING ONCESSTIC!
INDUCTRIAL CONTIN SYSTEMS
HONI AST RELT CRPENONG,
SUT TO INTEDIONT
THAT KUPLLL!
YOUY IS SICPREED AIOIL!
KINT CN THIT SCREHS!!
TROPOUSEY-
SYSTEEMS!!
ISITSTITIAL CONTRAC IOS.:

Industrial Control Systems are All Around Us

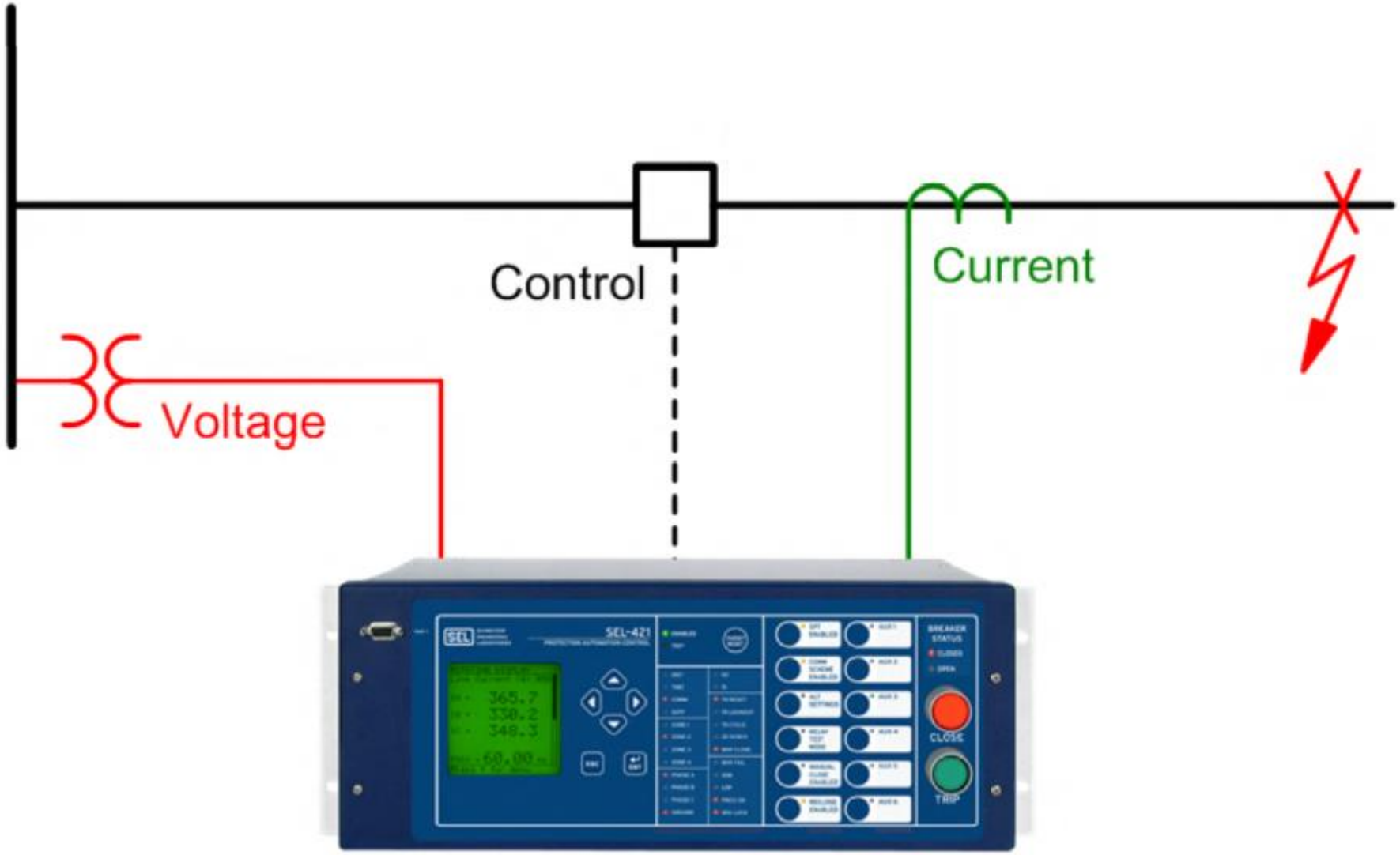
Simple Control System



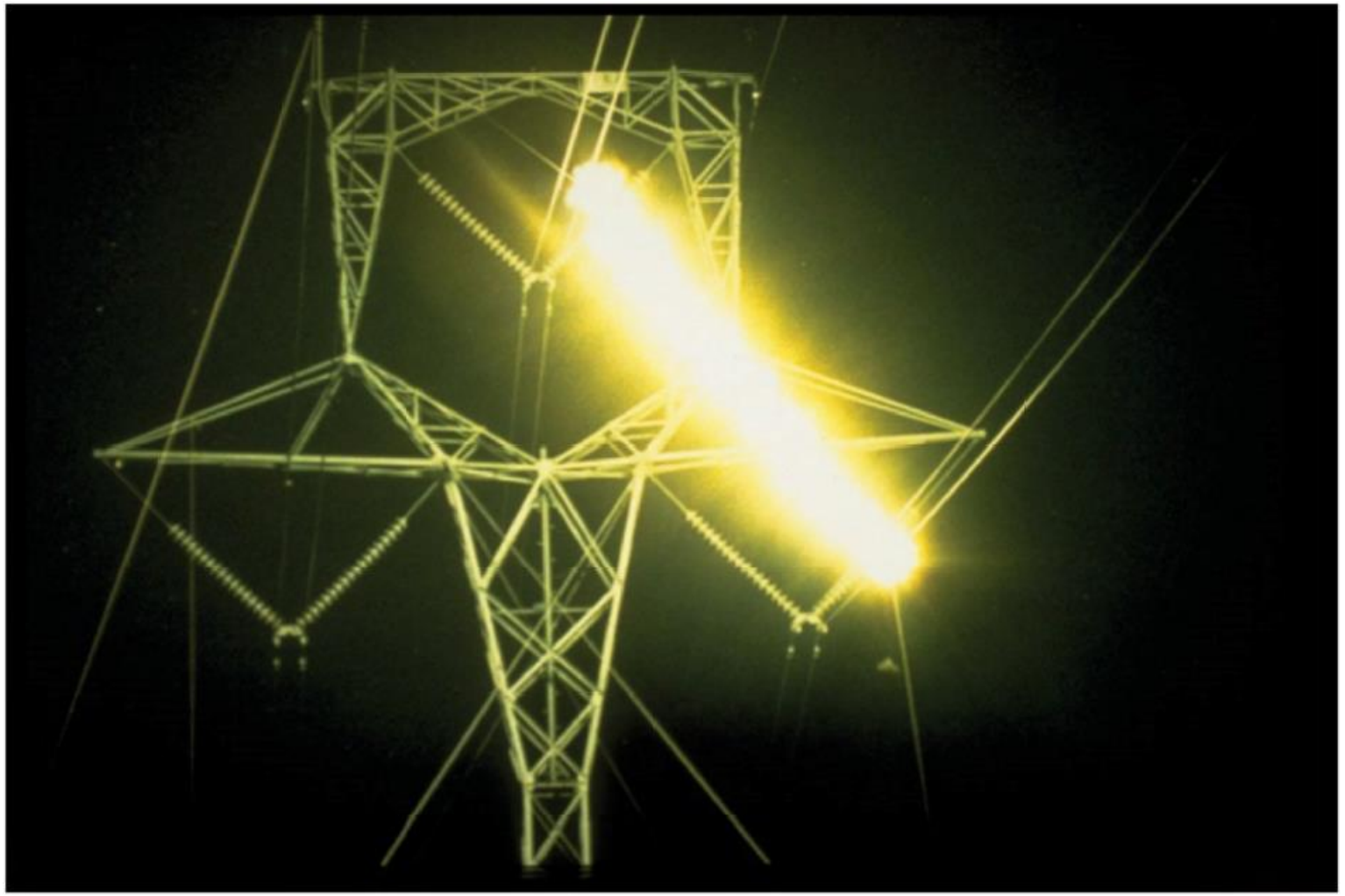
Protecting Your House



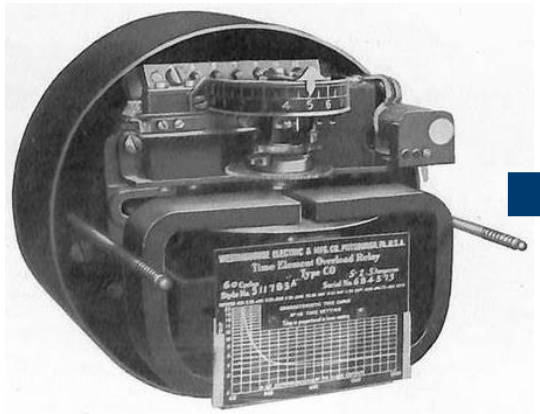
Protective Relays Clear Faults



What is a Fault?



Protective Relay Evolution



1902 1984 2024

Operator’s Perspective

ICS Communications

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

Frame Relay

PoTS Dial-up

Leased Line

SONET/SDH

Ethernet

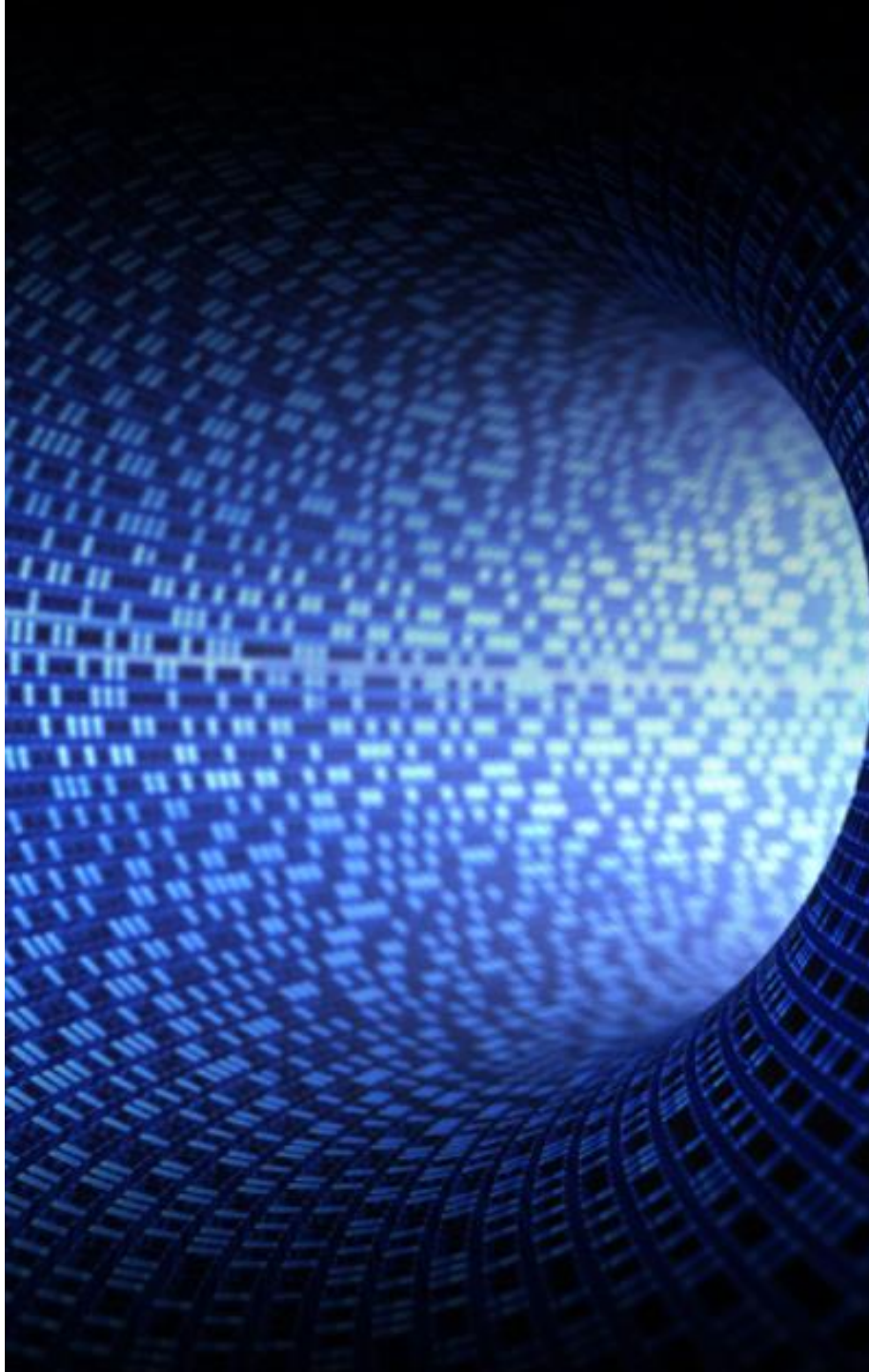
Copper

Fiber

Radio

Satellite

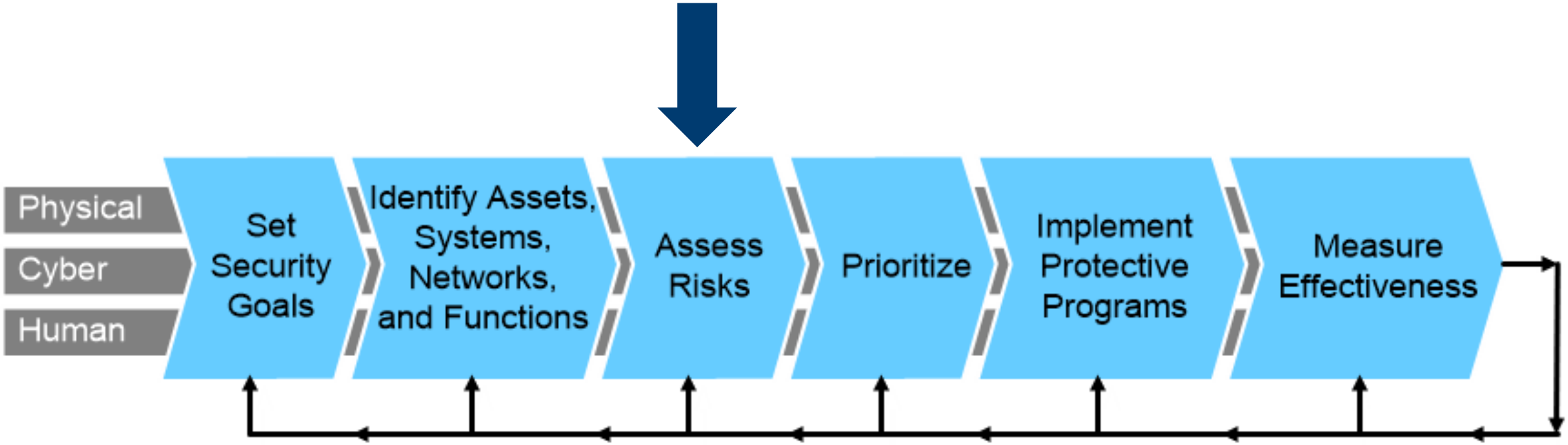
Cell



Two Families of Technology

Information Technology	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



LITTLE BOBBY

by Robert M. Lee and Jeff Haas

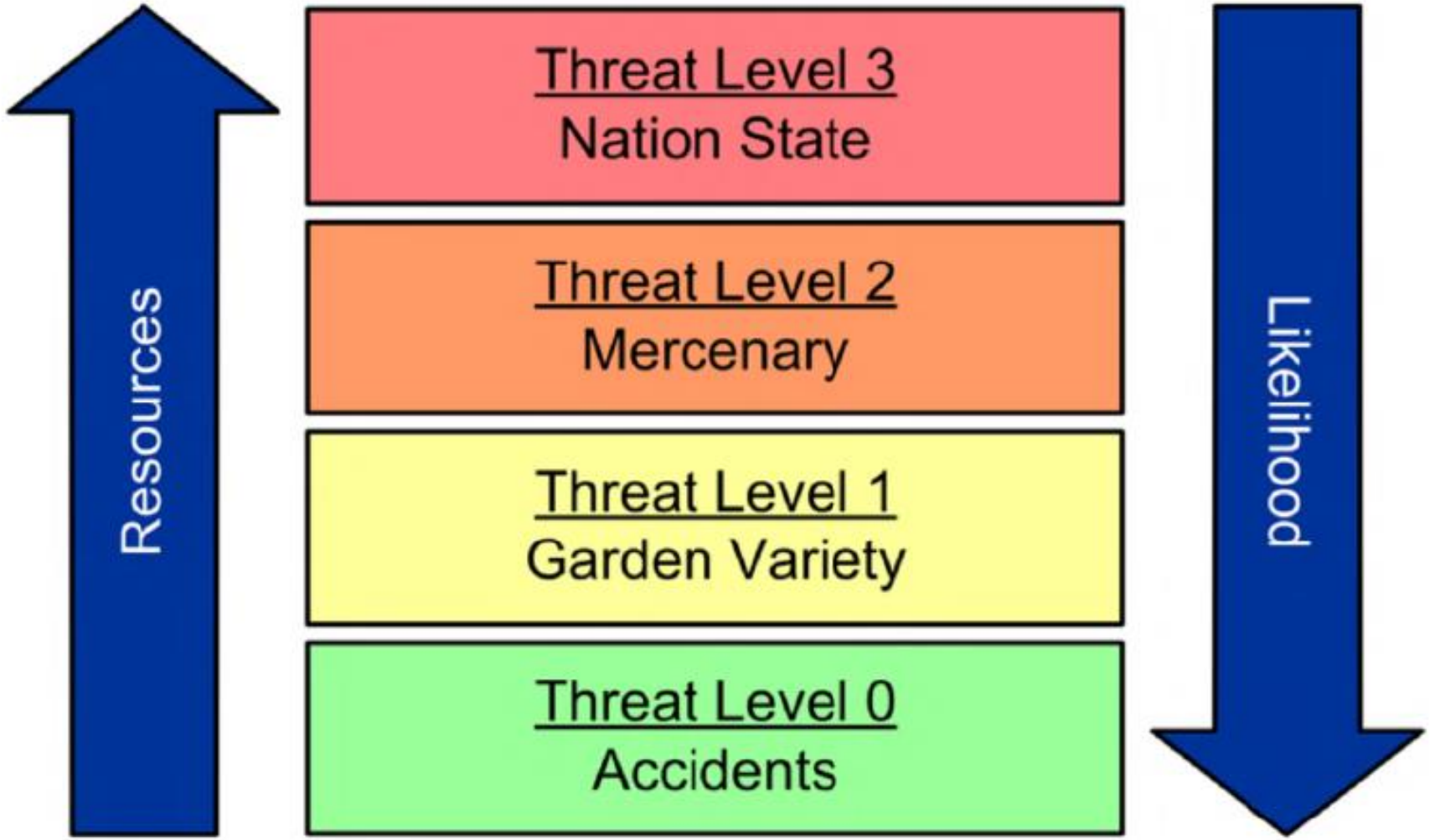
Components of Risk

Threat

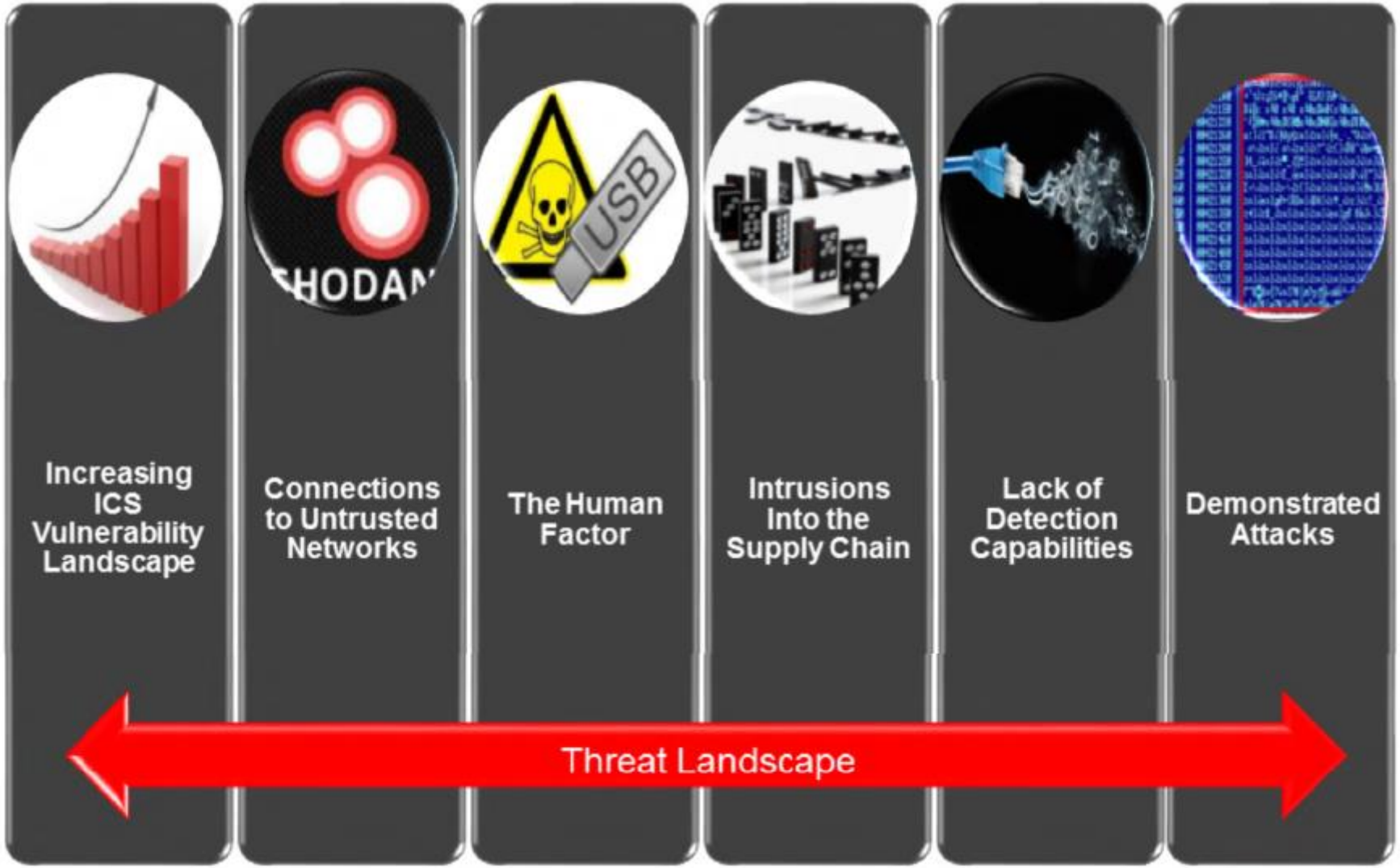
Consequence

Probability

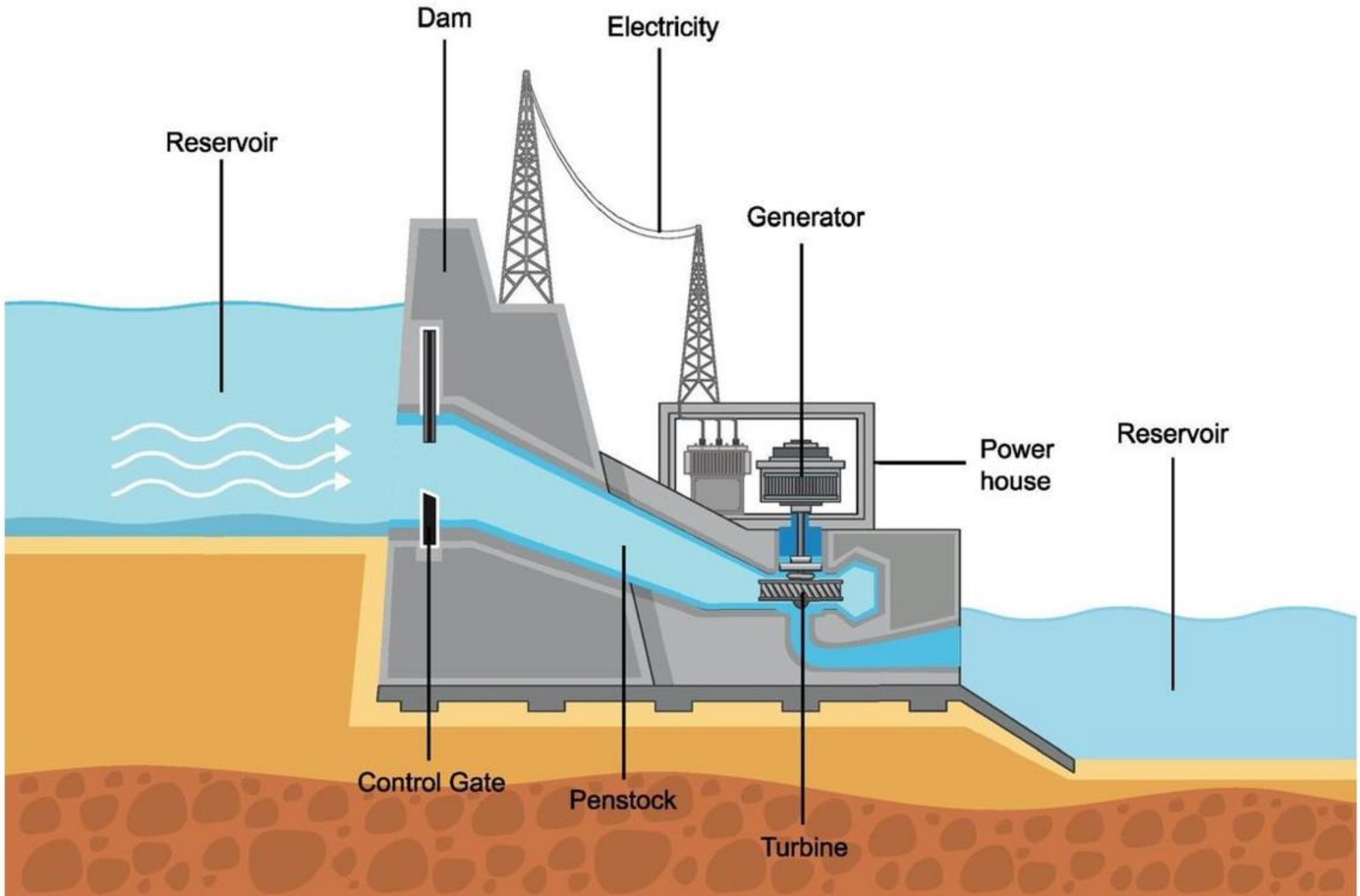
Threat Levels



Threat Landscape



ICS Attack Potential Impact


Dam
Electricity
Reservoir
Generator
Power
house
Reservoir
Control Gate
Penstock
Turbine

ICS Attack Potential Impact

ICS Attack Examples

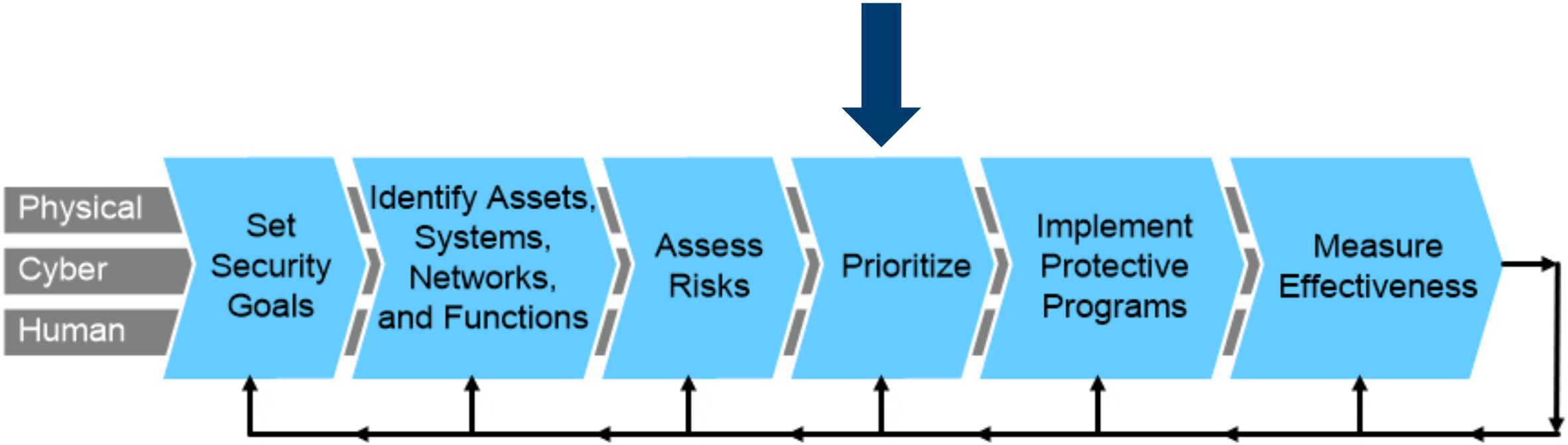
Maroochy Shire

Stuxnet

Metcalf

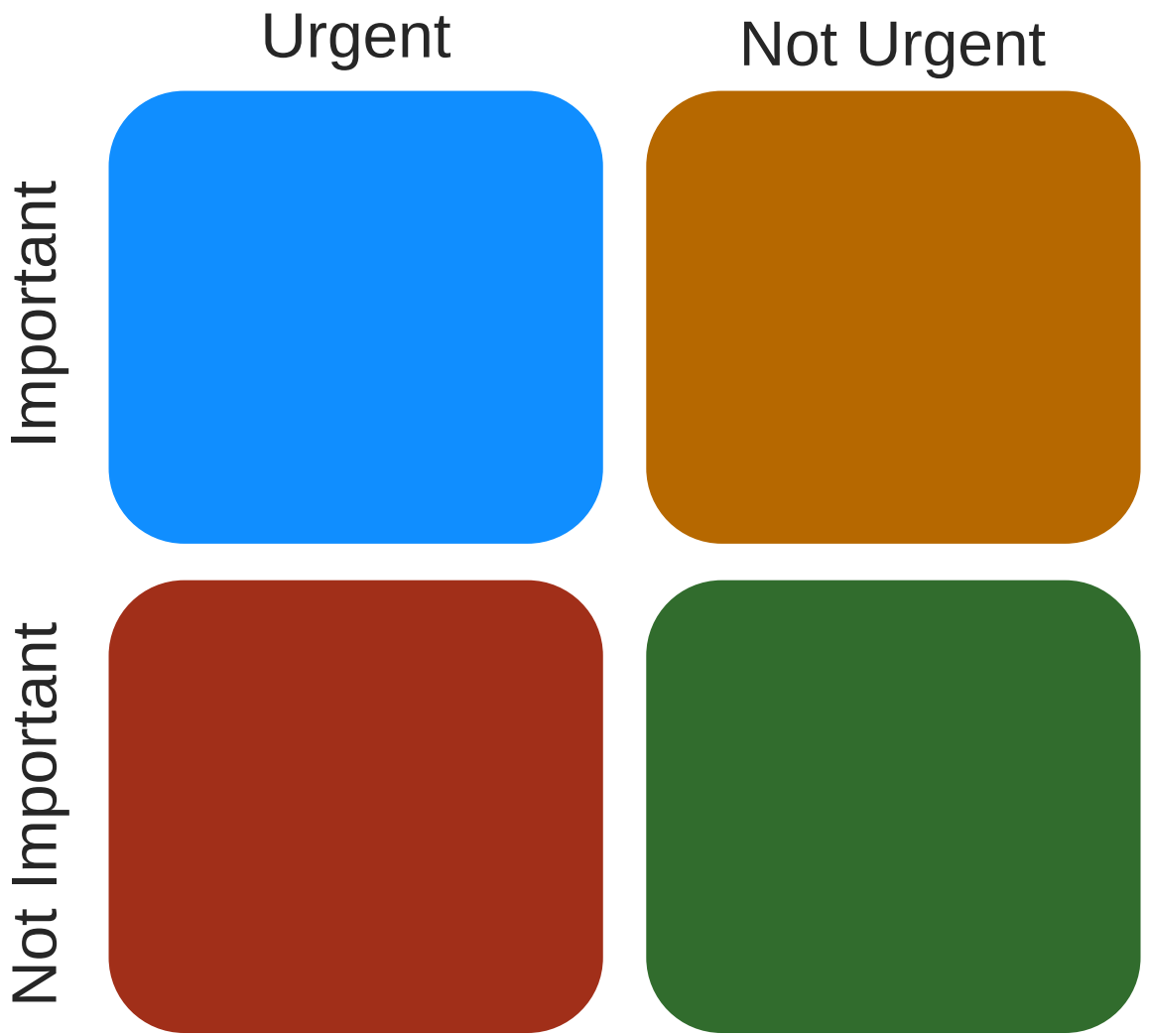
Ukraine – Dec 23 2015

Risk Management in ICS

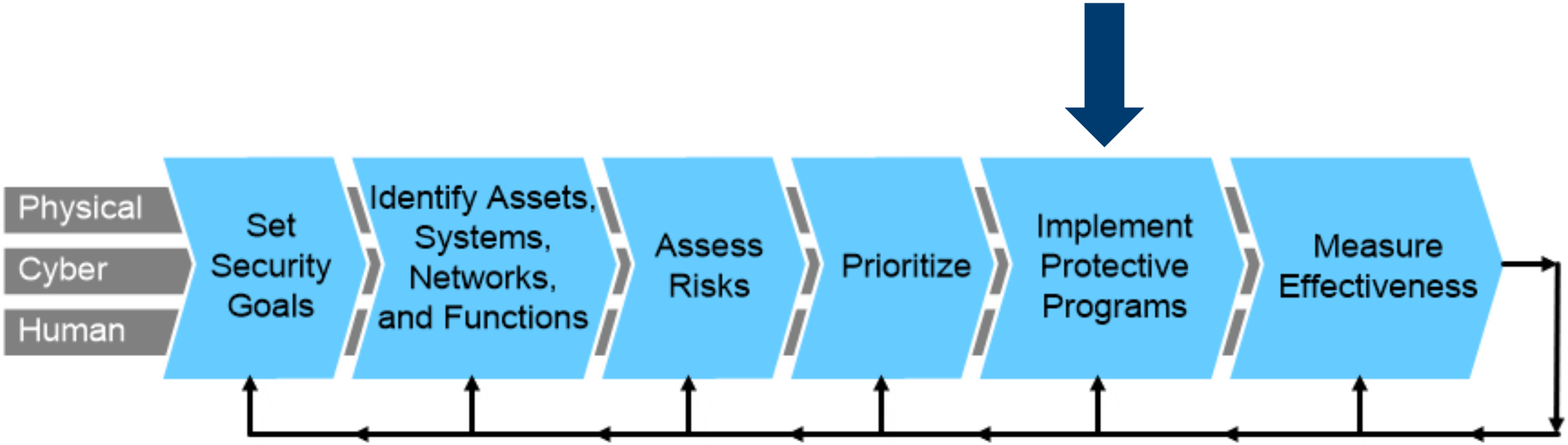



I'M OVERWORKED BECAUSE I DON'T KNOW HOW TO SET PRIORITIES.
Dilbert.com @ScottAdamsSays
TRY RANKING YOUR TASKS BY HOW MUCH YOU HATE THE PEOPLE WHO ASKED FOR YOUR HELP.
WHAT IF I DON'T HATE ANYONE?
THAT PROBLEM SOLVES ITSELF OVER TIME.
8-15-16 © 2016 Scott Adams, Inc. /Dist. by Universal Uclick

Prioritize



Risk Management in ICS



LITTLE BOBBY **by Robert M. Lee and Jeff Haas**

ICS Cybersecurity Guidance

NIST

- Special Publication 800

NERC

- Critical Infrastructure Protection

ISA/IEC

- 62443
- 62351

Defensive Strategies

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

Re-Using IT Technology in OT Systems

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

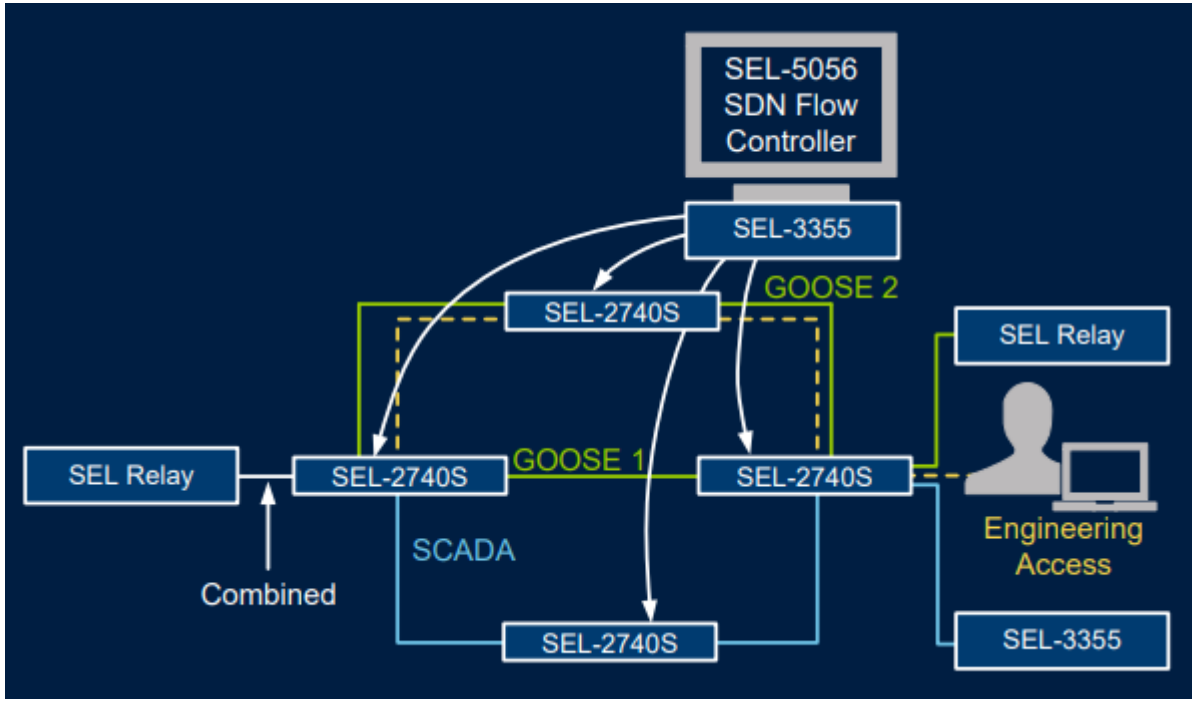
Why not TLS?

- **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

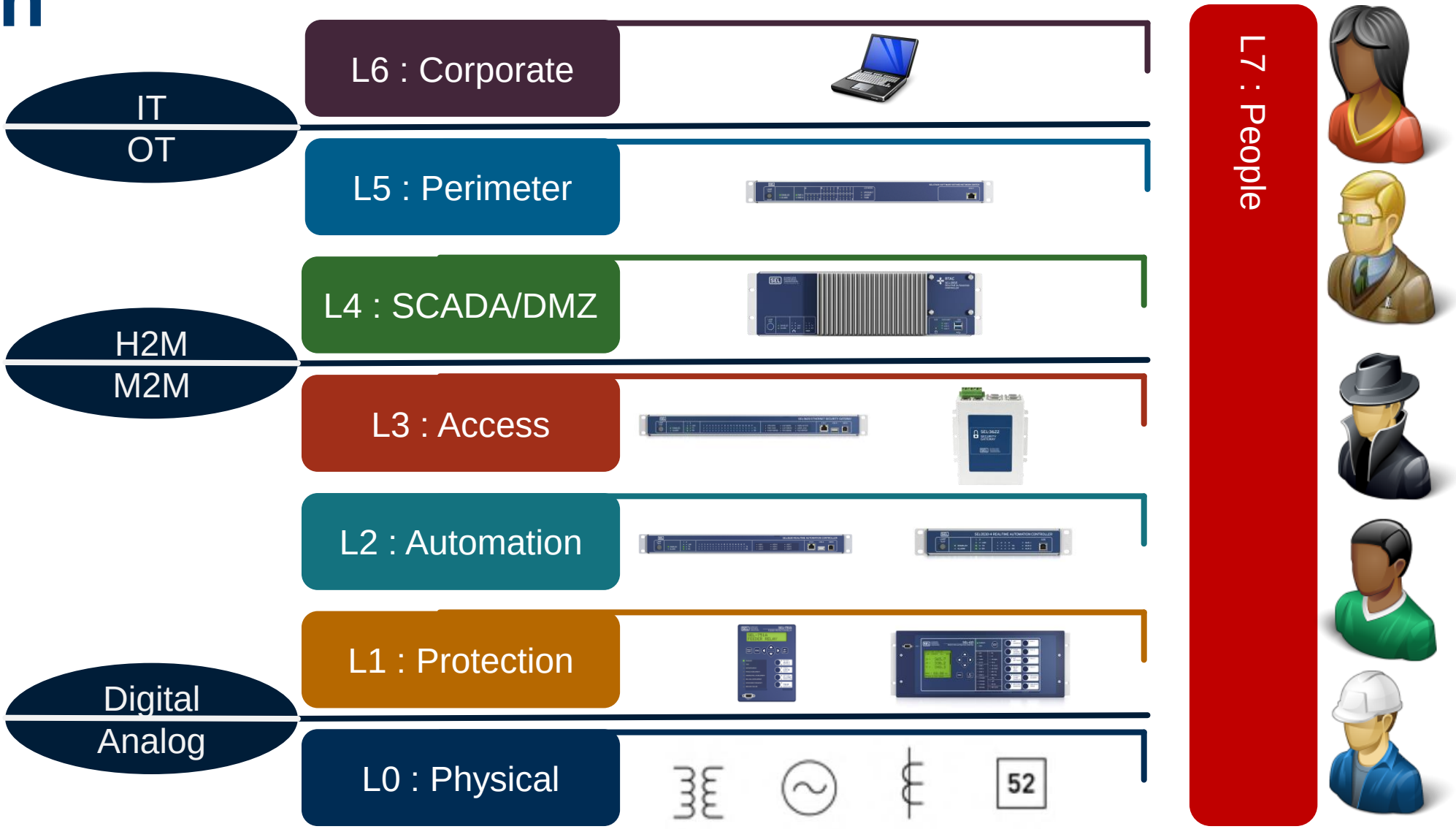
https://www.ioactive.com/pdfs/PKILayerCake.pdf

Reinventing IT Technologies for ICS

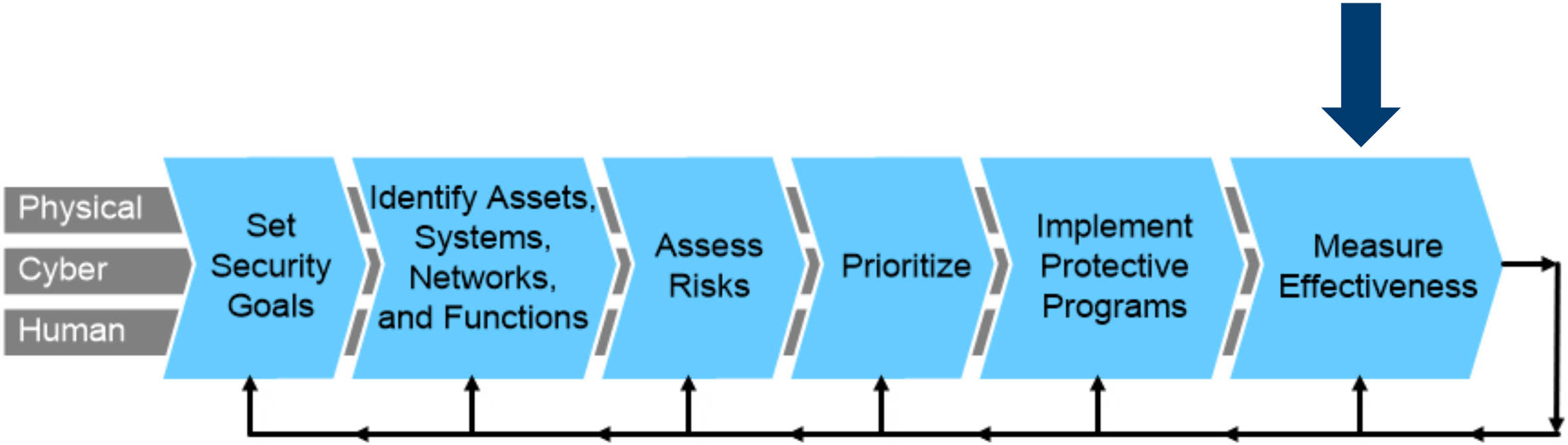


- Software Defined Networking
- IPsec
- MACsec
- OAuth

System Level Approach



Risk Management in ICS




DID YOU SAY
WE ARE
MEETING GOAL?
memes.com

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?