ISA Italy Section

Cyber security - why and how

Frankfurt, 14 June 2018

ACHEMA

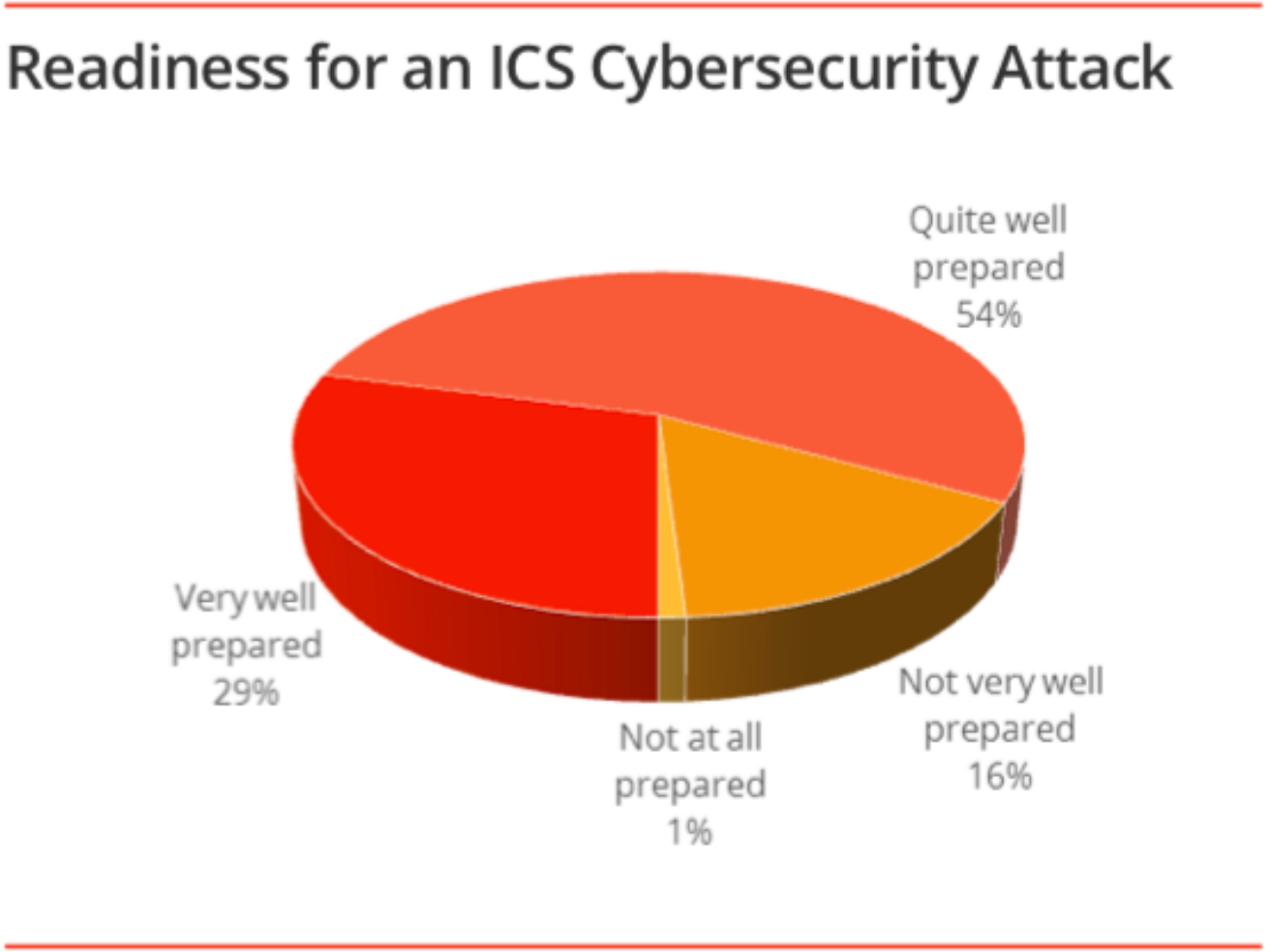
PANDUIT®

Cybersecurity for Industrial Network Infrastructure

Hayo Volker Hasenfus, Dir. Industrial Accounts and IoT Business EMEA

PANDUIT™

Where do you see yourself?



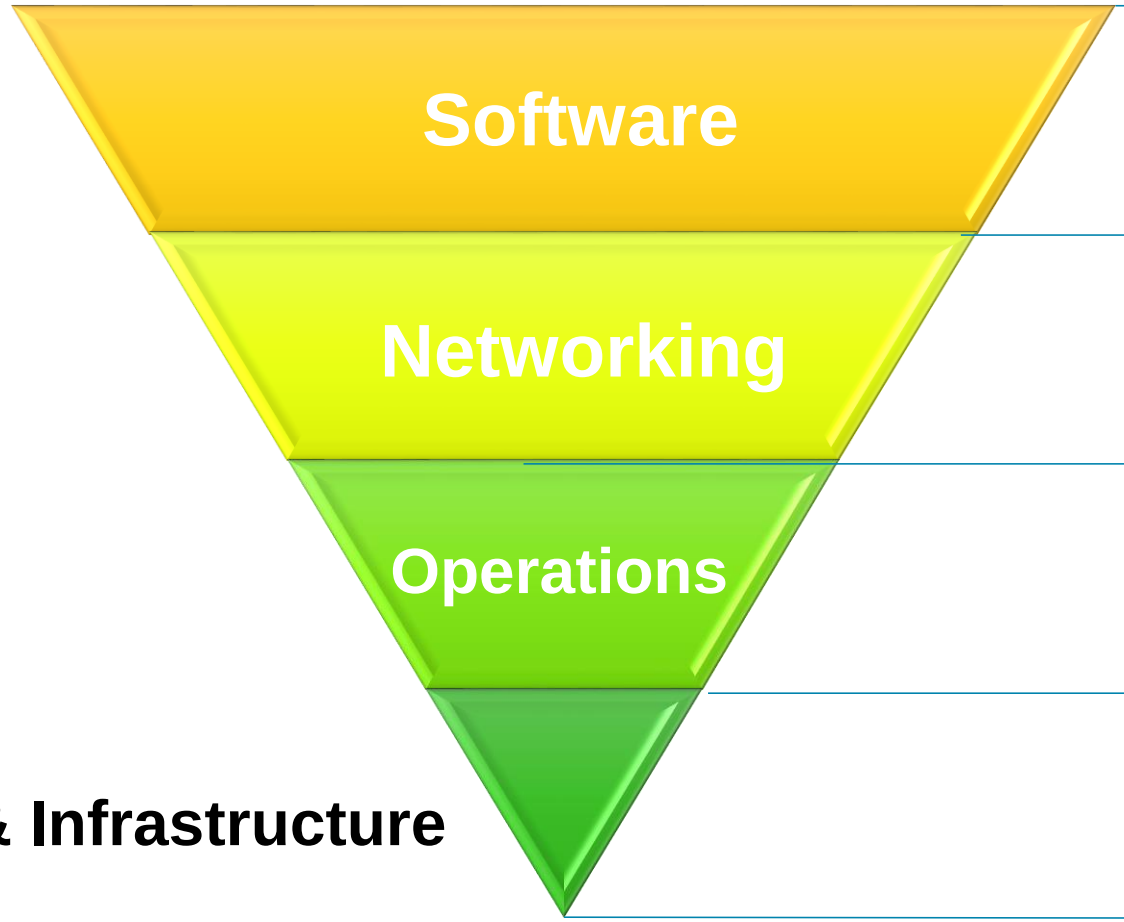
"We don't have any breaches on the industrial side as far as we know. I know we can never be 100% sure, but it is more antiquated equipment than cyber threat [causing problems] and we do monitor downtime."

Head of IT, Chemicals Manufacturing, UK

Importance of Industrial Networks

- Control and communicate the status of your ***profit-making assets***
- Impacts ***workforce productivity*** significantly
- Outages and slowdowns are ***extremely visible*** and ***readily monetized***

Overall Network Cost Distribution



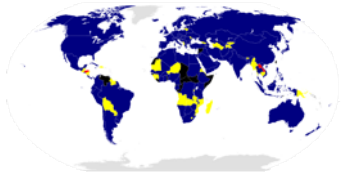
Asset Life = 2 to 5 years
60% of project budget

Asset Life = 5 years
23% of project budget

Asset Life = 5 years
10% of project budget

Asset Life = 20+ years
7% of project budget

By the way: Cybersecurity Standards



Data Center	Office	Plant Floor
ISO/IEC 27000	ISO/IEC 27000	ISO/IEC 62443

- Ensure to build on standards and building blocks for manageable cybersecurity
- Adapt standards to balance access limitation, interoperability and (IoT) technology enablement

ISA/IEC-62443 Overview

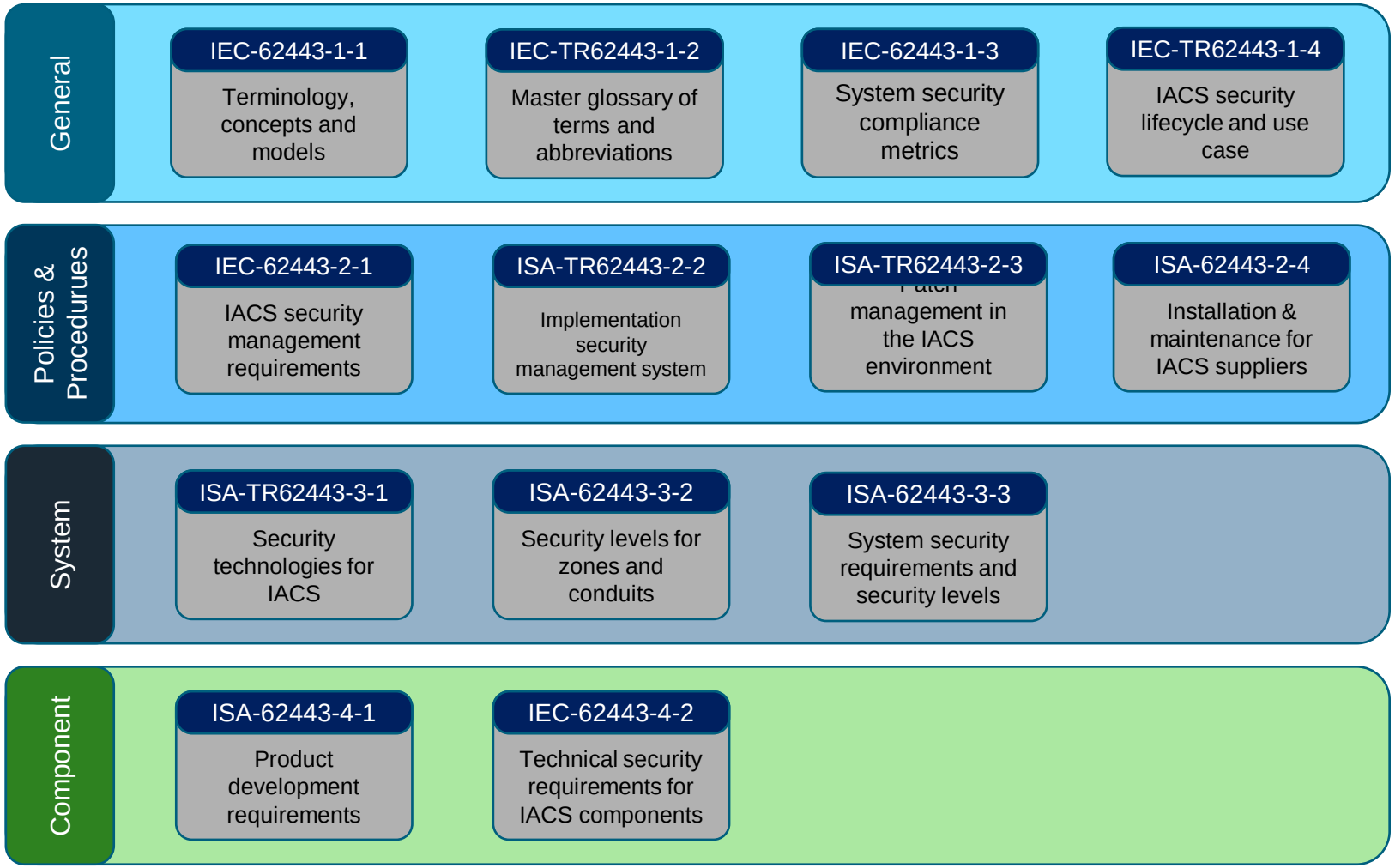
- Series of standards that defines secure *industrial automation and control systems* (IACS)

- Applies for stakeholders
  - designing
  - manufacturing
  - implementing
  - managing

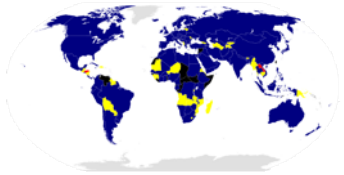
  industrial control systems:

  end-users, system integrators, security practitioners, technology providers and systems vendors

ISA/IEC-62443 Overview



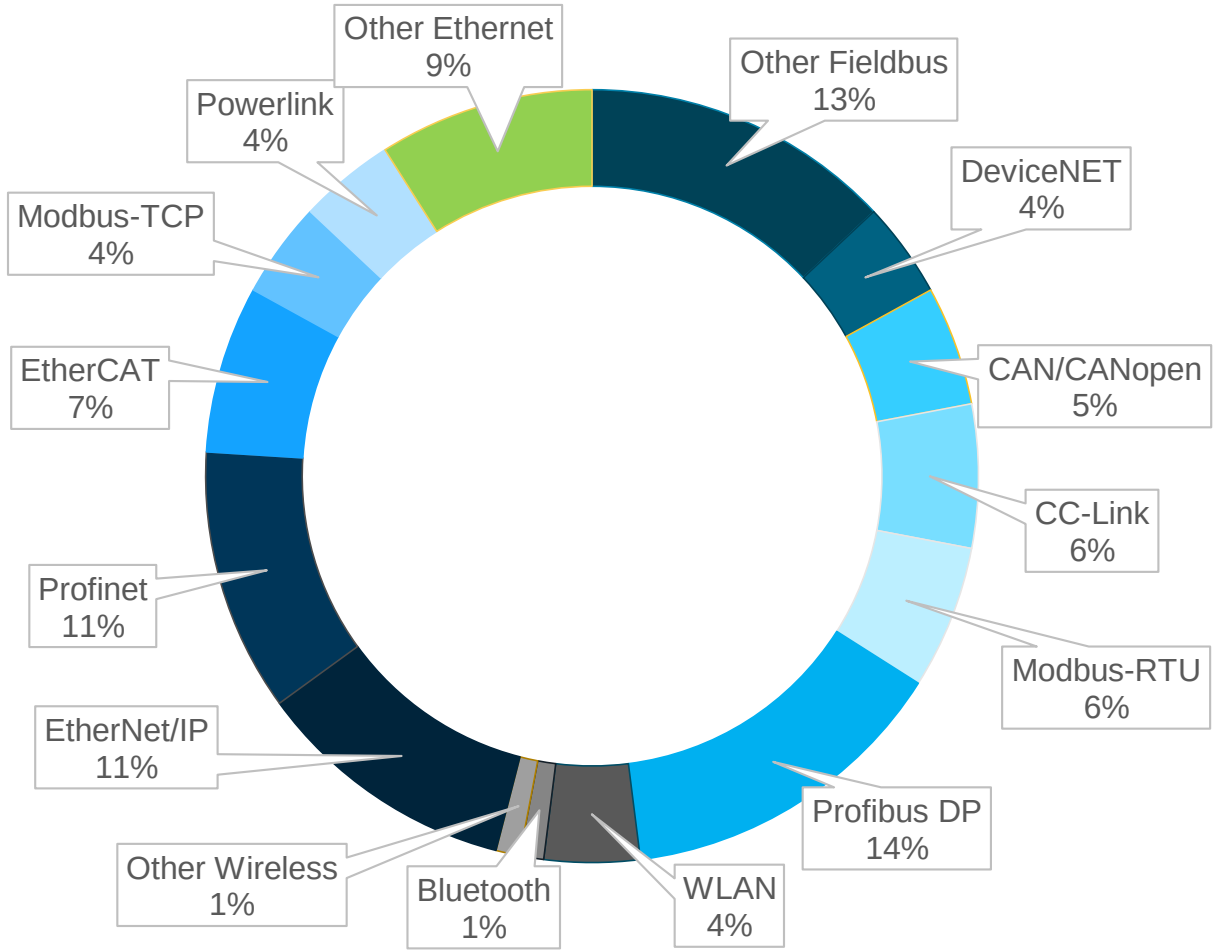
Are you global? Telco Cabling Standards



Data Center	Office	Plant Floor
ISO/IEC 24764 now: ISO/IEC 11801-5	ISO/IEC 11801	ISO/IEC 24702 now: ISO/IEC 11801-3
EN 50173-1 EN 50173-5	EN 50173-1 EN 50173-2	EN 50173-1 EN 50173-3
ANSI/TIA 942	ANSI/TIA 568-C	ANSI/TIA 1005

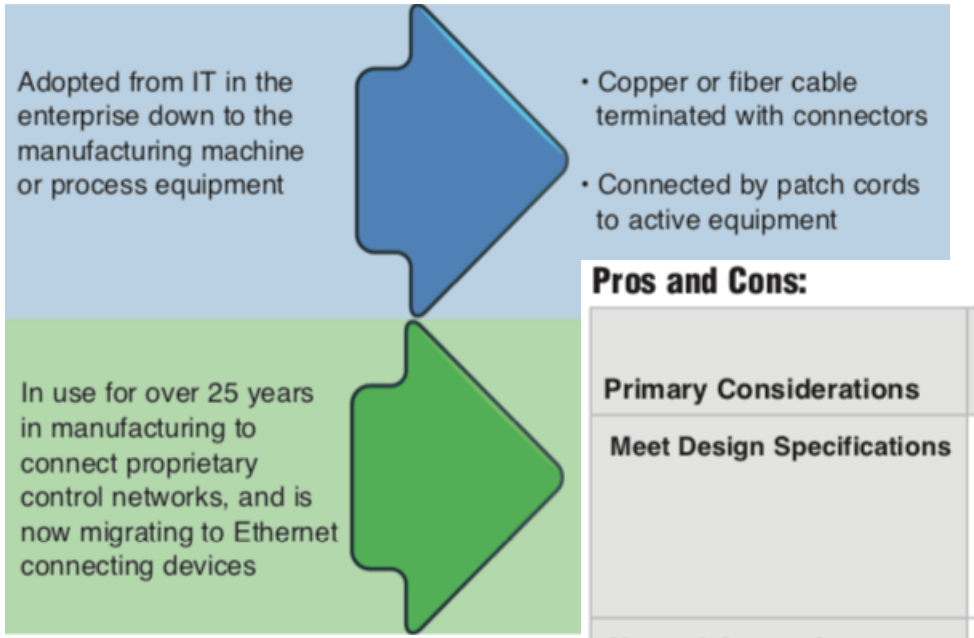
Network Planning & Management

- Legacy Protocol Migration
  - Key output of the site assessment
  - Your industrial network is *not* all the same age
  - Some elements need to retire
- Industrial Network Refresh Rate
  - need for succession planning
- Which new (IoT) services do you need to plan for?



Source: HMS Industrial Networks

Structured Cabling <<<>>> Point-to-Point Cabling



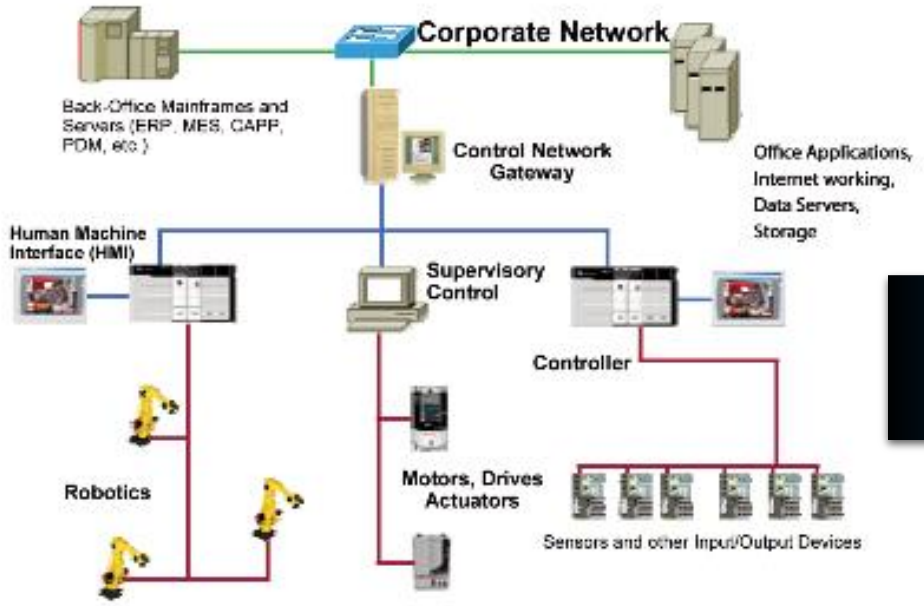
source: http://www.panduit.com/heiler/ProductBulletins/D-NCCB66--SA-ENG-IndustEthntPhysLayerSoluts-W.pdf

Pros and Cons:

Primary Considerations	Structured Cabling	Point-to-Point Cabling
Meet Design Specifications	• High cable density – many cables from panel to panel • Testability at the panel can provide assurance for commissioning new ports and may yield potentially longer warranty terms	• Low cable density – few cables from panel to machine • Ring or linear topology using copper cabling where distance between connections is < 100 meters • PCF for long reach or noise mitigation
Network Longevity (Future Proof)	• Designed in spare ports (no need to re-pull new cables for 'adds') • Fiber backbones with higher grade fiber such as OM3 or OM4	• Impractical to have spare cable runs laying loose and/or unprotected • Higher performance with fewer connectors
Maintainability (Moves, Adds, and Changes)	• Environments with multiple changes occurring • Cable slack is required	• Environments with minimal changes occurring • Slack cabling is undesired and precise cable lengths are required
Installation	• Multiple points of connectivity • Backbone and horizontal cabling is largely untouched	• Quick installation • Use where tight bends or moderate flexing is required • Use in areas where it is impractical or impossible to mount a patch panel or other cable connector interface

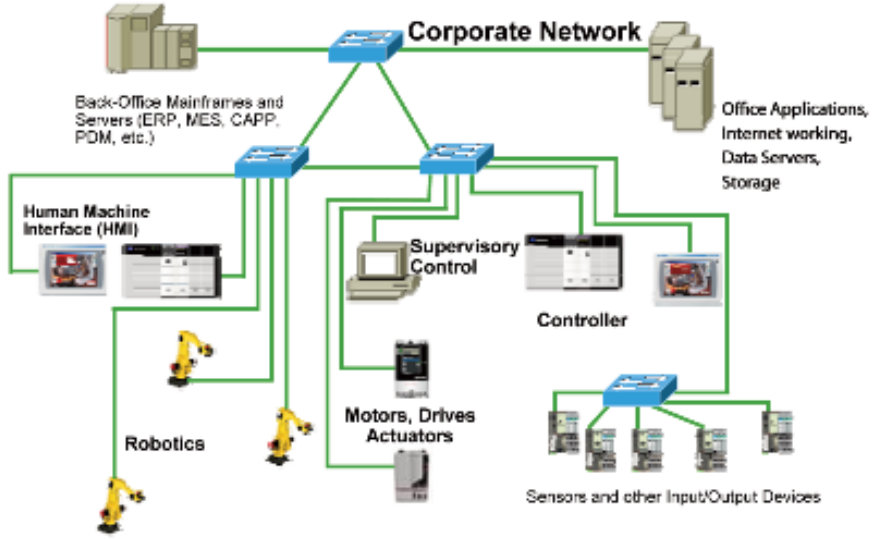
Evolution of Industrial Ethernet Reference Architecture

3-Tier (Old)



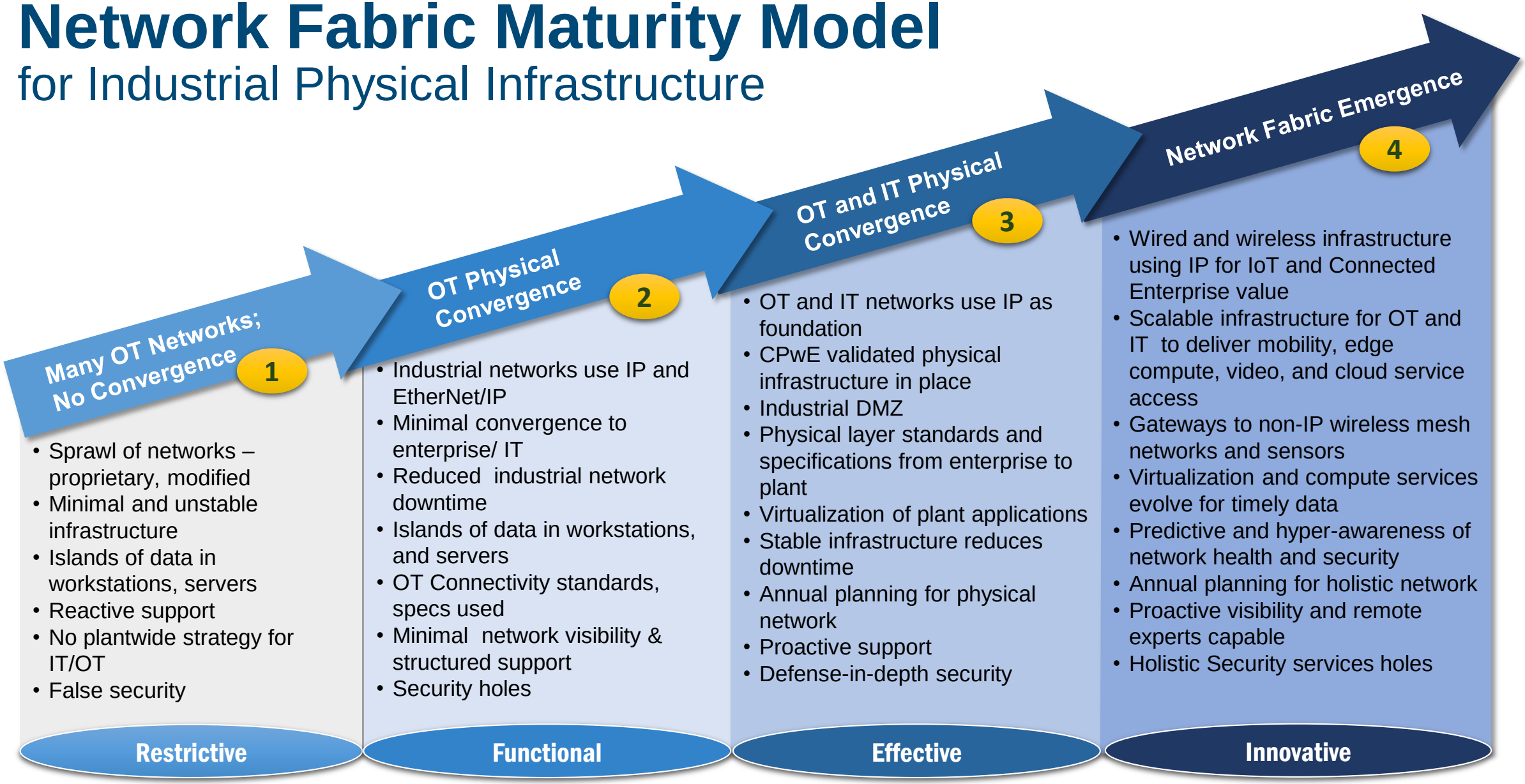
- Natural segmentation
- Natural security
- Requires mapping between layers

Converged (New)



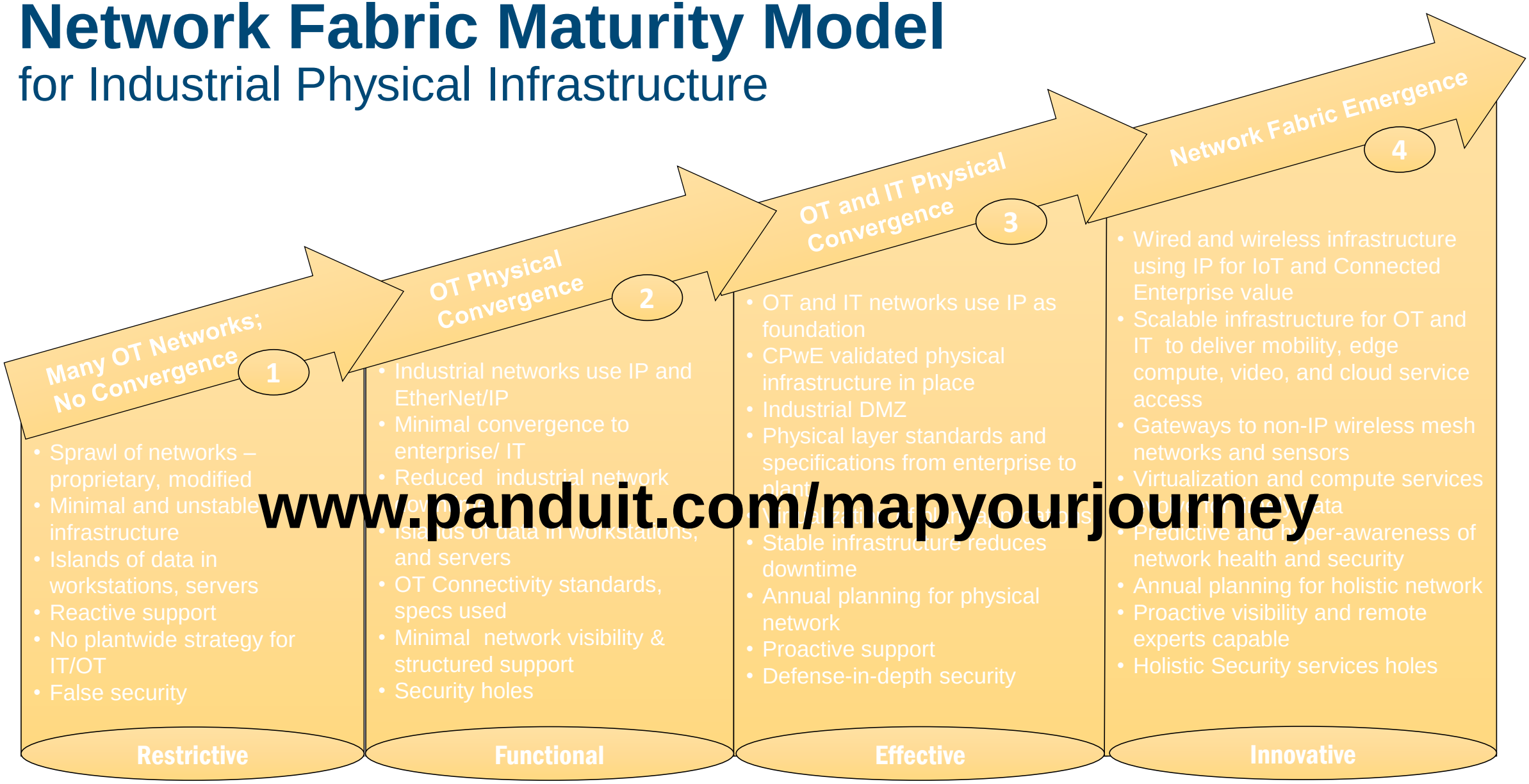
- Gateway eliminated
- Data from anywhere
- Needs more security

Network Fabric Maturity Model
for Industrial Physical Infrastructure



Network Fabric Maturity Model

for Industrial Physical Infrastructure

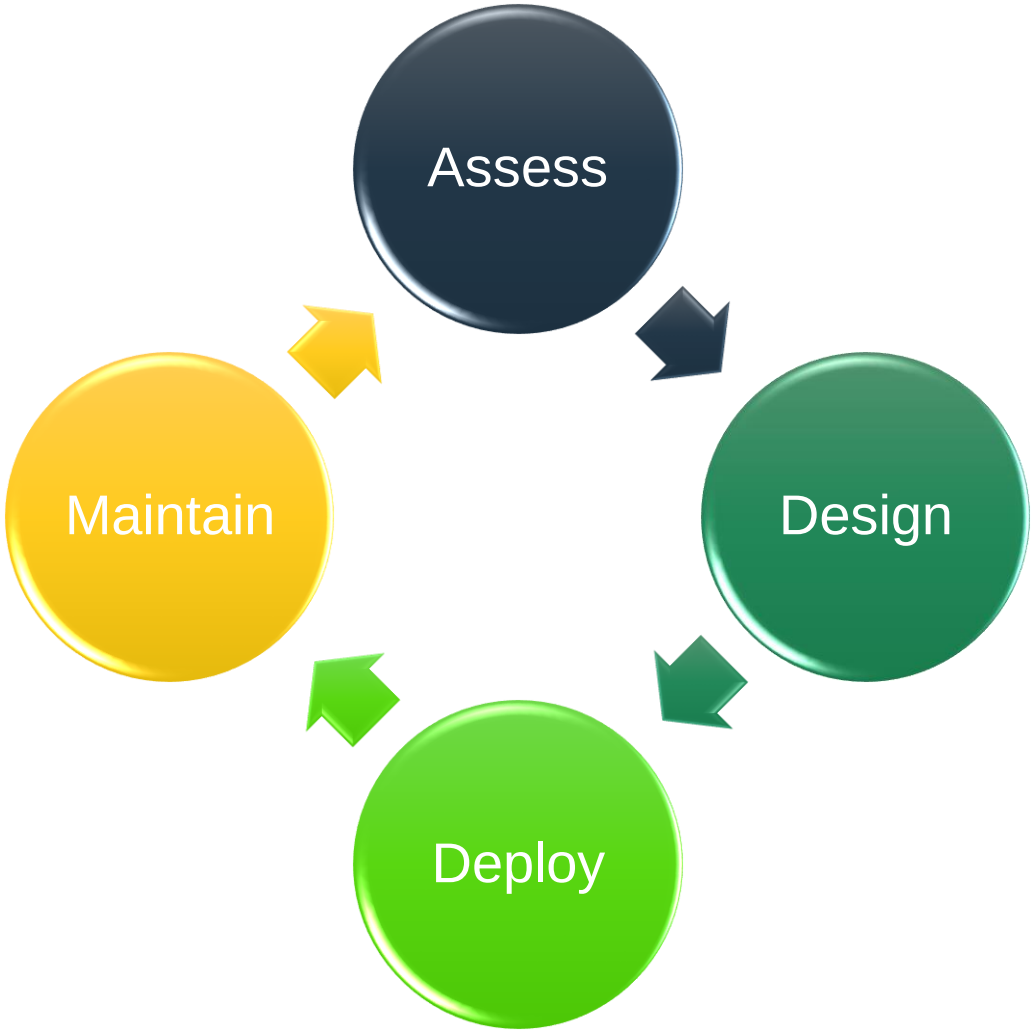


www.panduit.com/mapyourjourney

Where do I start?

- Network assessment and documentation
- Mitigation plan for impending problems
- Network M&O strategy
- Future looking plans for your current network; ***i.e. legacy protocol migration, IoT readiness***

Rigor around Networks



- Replicate and effectively maintain network infrastructure across complete enterprise footprint
- Quickly respond to changes or incidents with minimal lost motion
- Optimal network evolution over time, ready for new services
- A repeatable high quality process ensures these desirable results

You can only secure when you know what is out there?

Assess with Network Management Systems

- Functional Needs
  - Documentation of current state of network
  - Monitor network readiness
  - Gauge network performance
  - Find faults or misconfigurations
  - Uncover network traffic problems
  - All through a common view, aka “Single Pane of Glass”
  - Topology view and physical location details

NMS Feature Set

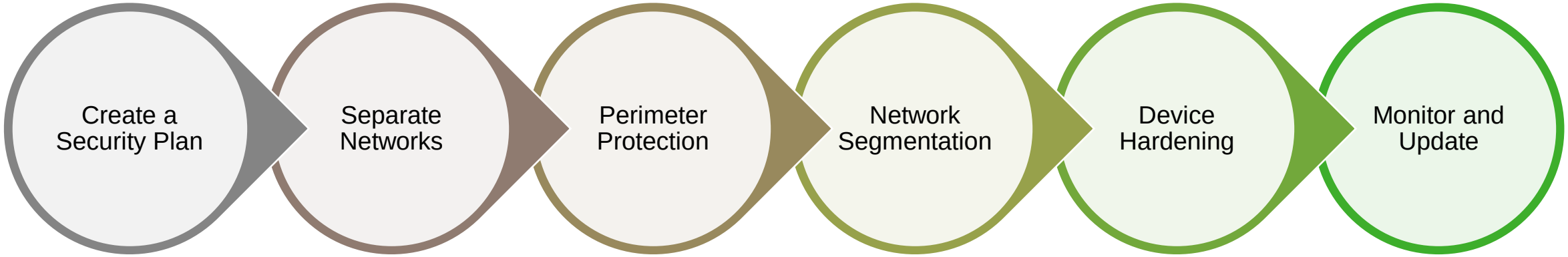
	BASELINE FEATURE SET	IDEAL FEATURE SET
Automatic Topology Map of Field Devices	X	X
Vendor Neutral Diagnostics	X	X
Live Health Monitor for Field Devices	X	X
Live Event Logs	X	X
Graphical Bandwidth Analysis	X	X
Key Performance Indicator (KPI) Reporting	X	X
Activity Monitoring Dashboard		X
Remote Assessment of Plant Network		X
Supervisory Function for Global Plant Visibility		X

Design with Reference Architectures

- Vital requirements
  - Created by domain experts
  - Based on user needs
  - Utilize standard, unmodified Ethernet protocols
  - Validated prior to publication
  - Regression testing as equipment is replaced by newer versions

- Why Reference Architectures?
  - Streamline design and implementation of new or upgraded industrial networks
  - Ensure consistent quality and performance across operations
  - Reduce MTTR during network incidents
  - Enhanced function in concert with enterprise network and business systems, prepared for new technologies and services

IEC 62443 - Defense in Depth

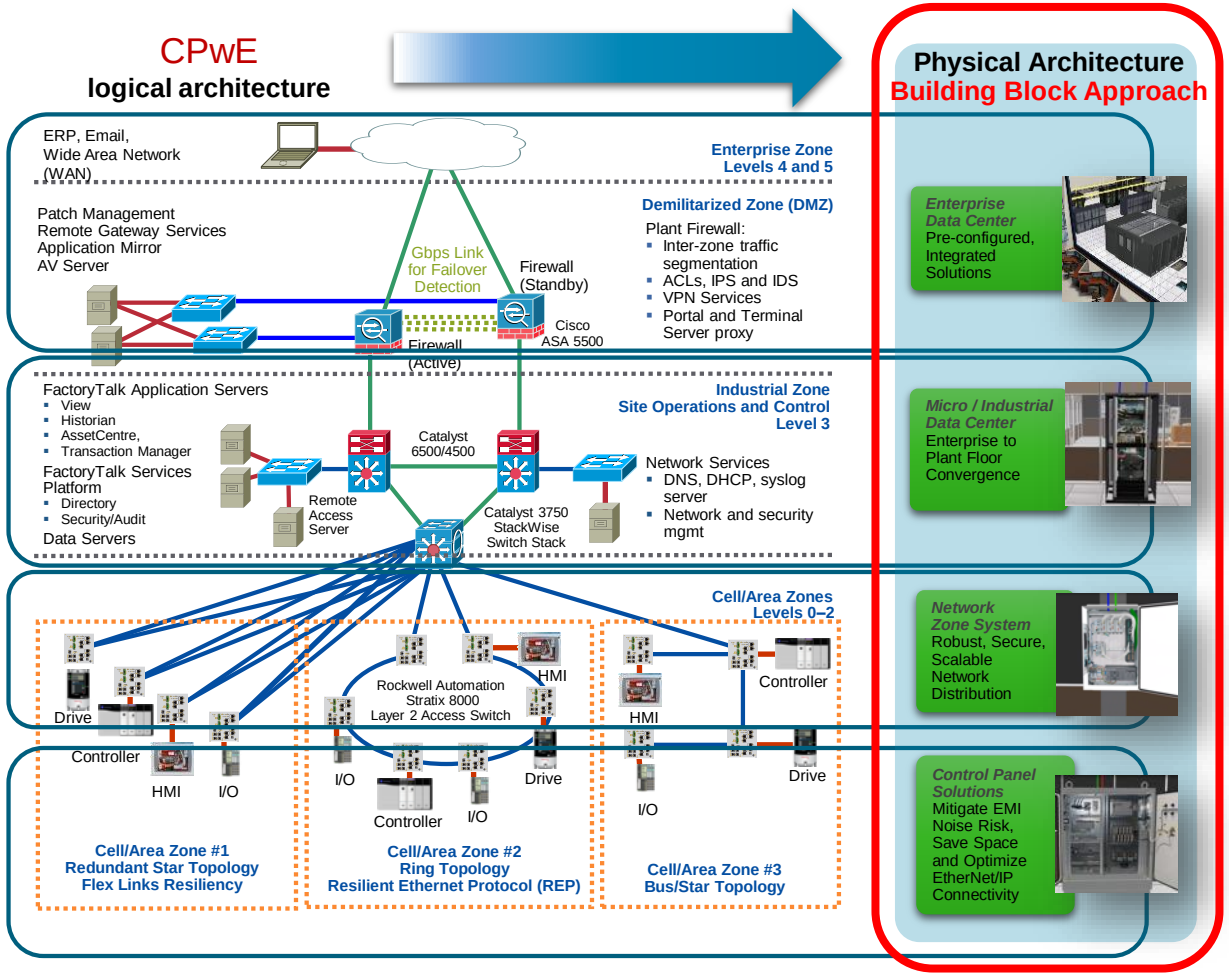


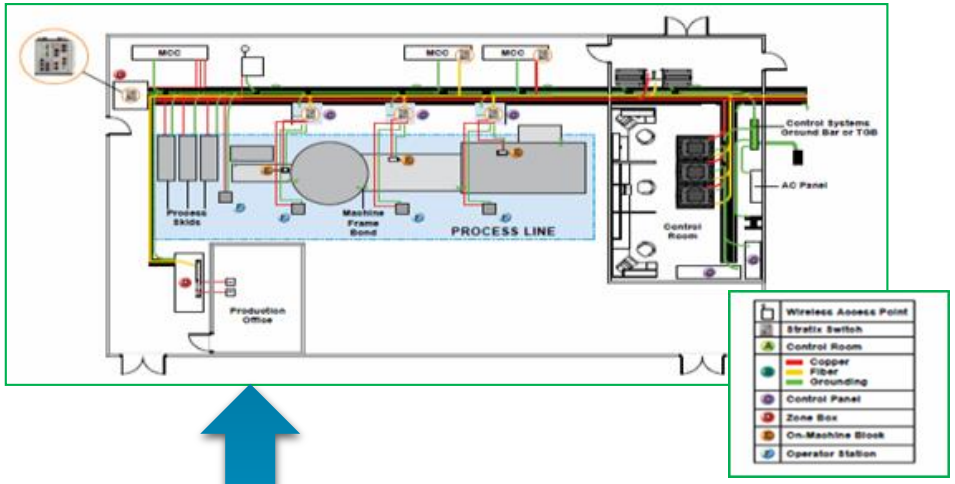
Design on Basis of Converged Plantwide Ethernet

- **TESTED AND VALIDATED REFERENCE ARCHITECTURE**
- A collection of use case driven reference architectures
- Designed to be robust and scalable
- Created by Cisco and Rockwell Automation 10 years ago
- Panduit contributed since 2014, collaboration extension since end of 2017
- Build-in cybersecurity consideration

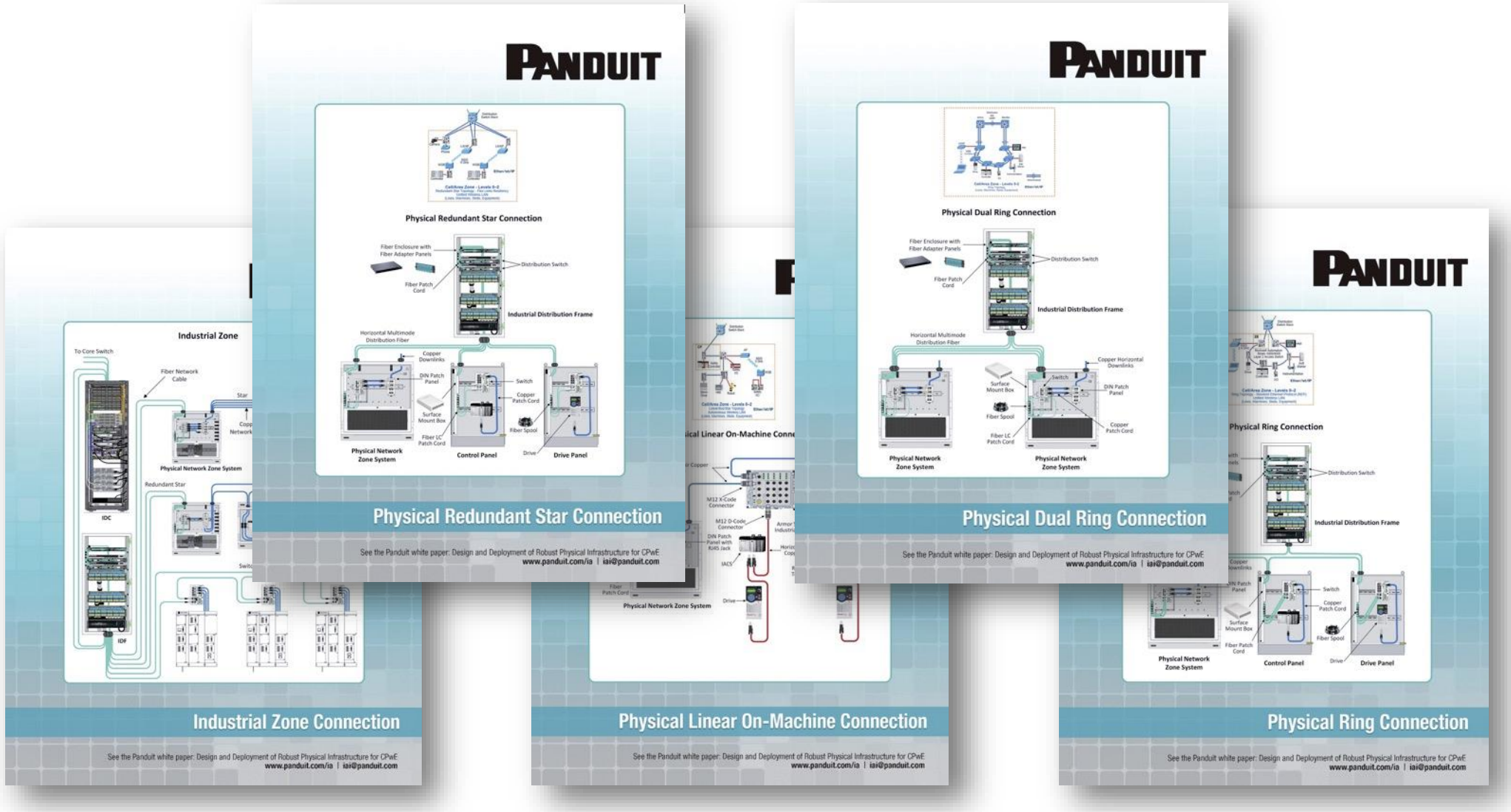
Simplify *Design* and *Develop* from ‚Logical to ‚Physical‘

Design and *Deploy* with CPwE Network Building Blocks

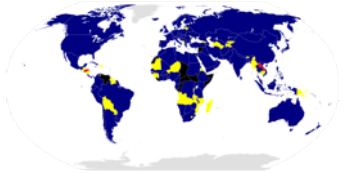




Network topologies designs



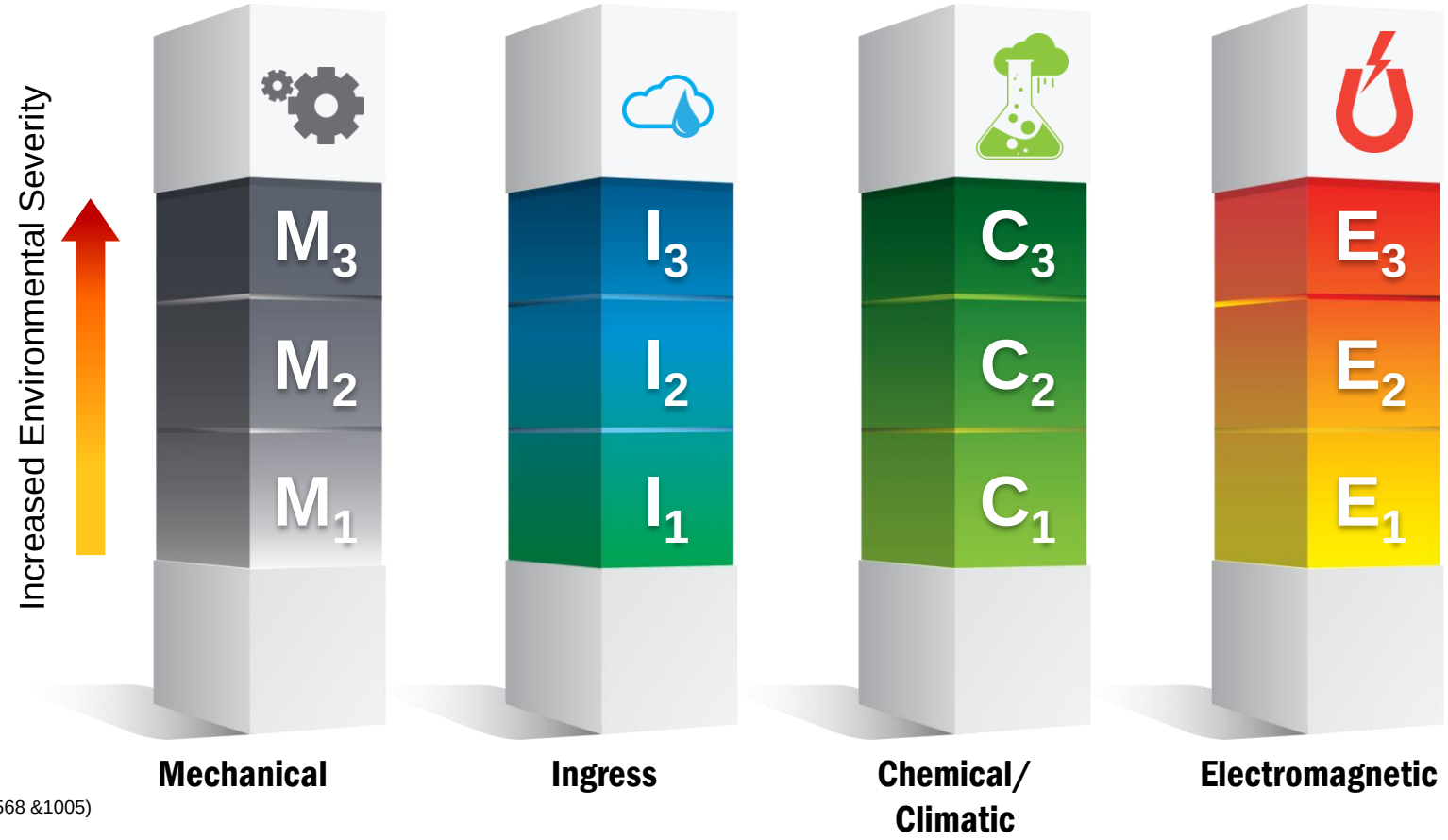
Compliant to (Network) Standards



Data Center	Office	Plant Floor
ISO/IEC 24764 now: ISO/IEC 11801-5	ISO/IEC 11801	ISO/IEC 24702 now: ISO/IEC 11801-3
EN 50173-1 EN 50173-5	EN 50173-1 EN 50173-2	EN 50173-1 EN 50173-3
ANSI/TIA 942	ANSI/TIA 568-C	ANSI/TIA 1005

Common Ground: Environmental M.I.C.E Analysis

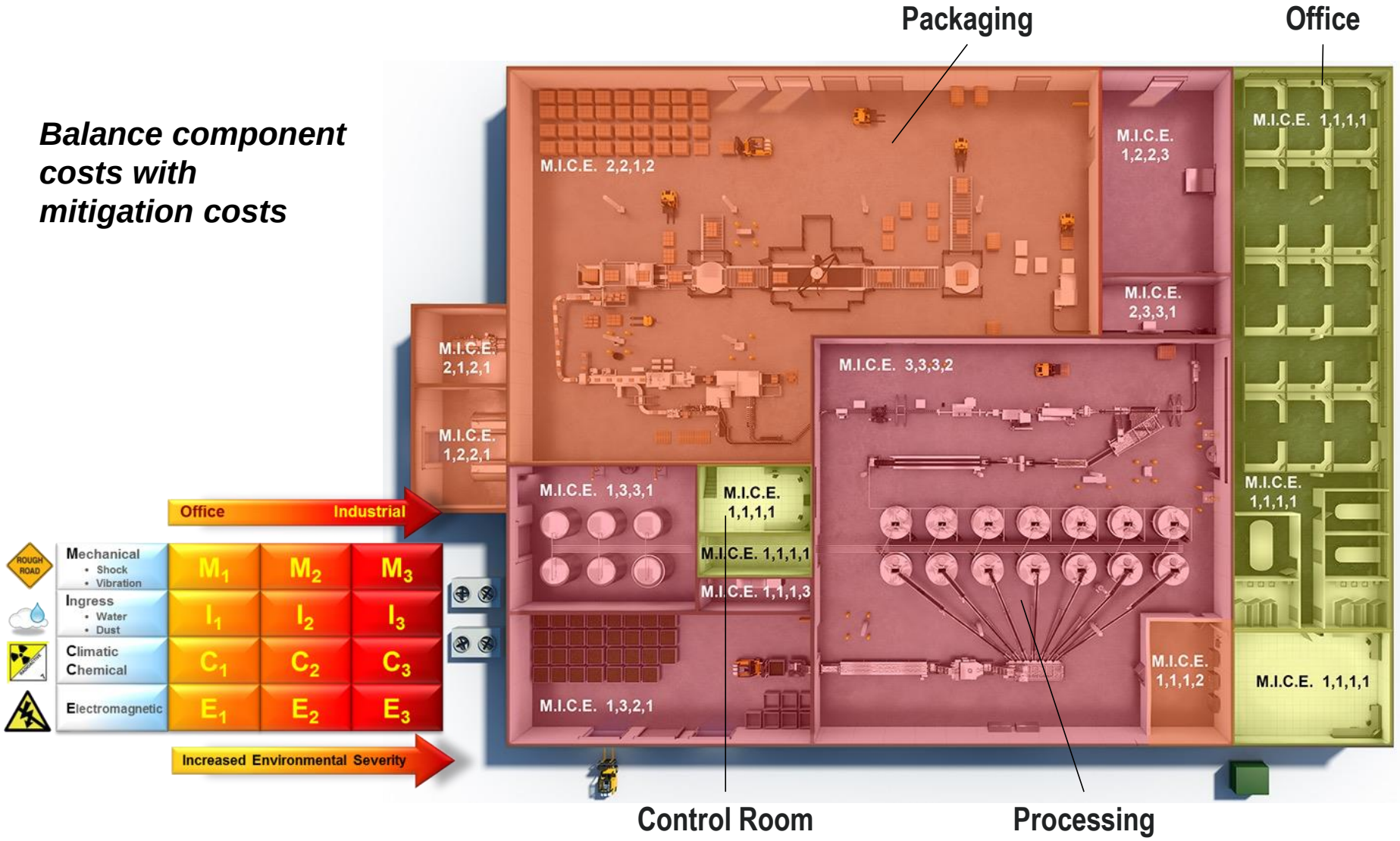
Pg. 11



(ANSI/TIA 568 &1005)

M.I.C.E Diagramming

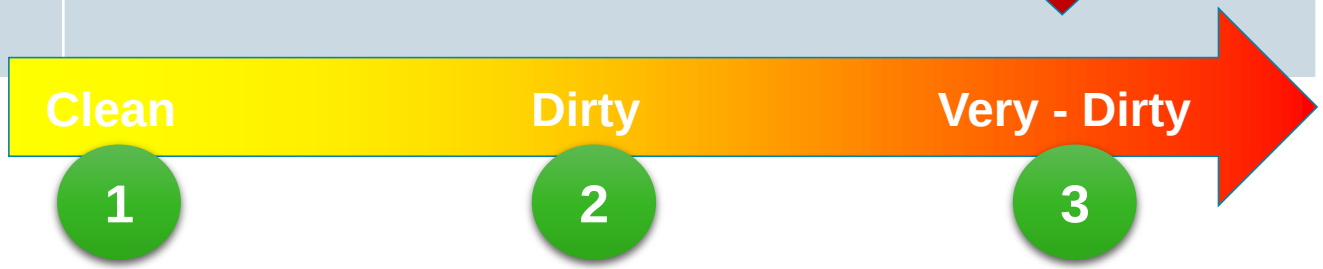
Balance component costs with mitigation costs



How M.I.C.E Can Be Effected By Product Selection

“M.I.C.E” characteristics change as a result of the routing products and methods used.

Route Type	Protected?
Hangers	No X
Trays	No X
Conduit	Yes X
Lay-in Housing	Yes
Pull-thru Housing	Yes X



Helping you in a Simplified Way

Standard and MICE Compliant Product Selection Guide

Deploy with Compliant Network Cabling Systems

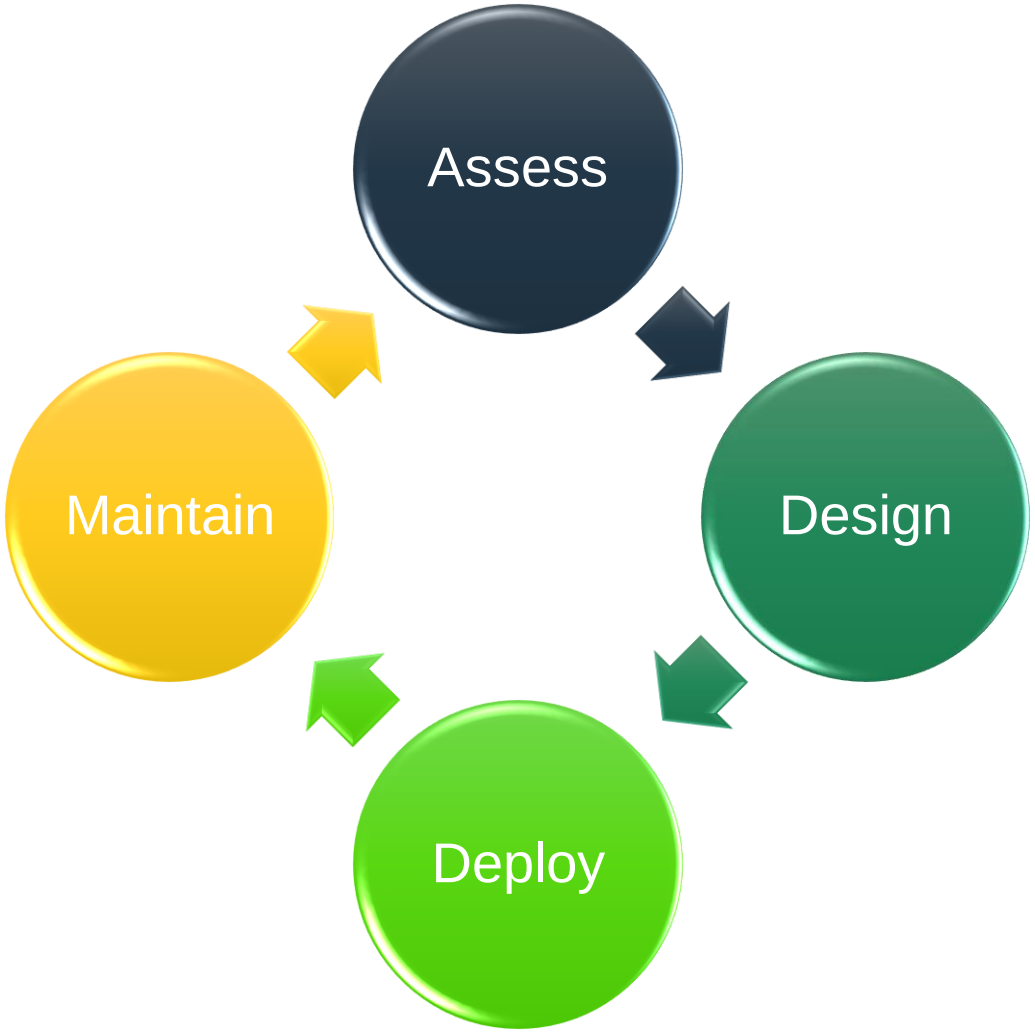
- Fiber and copper cable
- Indoor and outdoor
- Connectivity
- Zone systems
- helpful accessories
- https://pages.panduit.com/rs/349-EQI-366/images/MICE%20Selection%20Guide.pdf

IEC 24702 now 11801-3. And in EU: CPR in addition

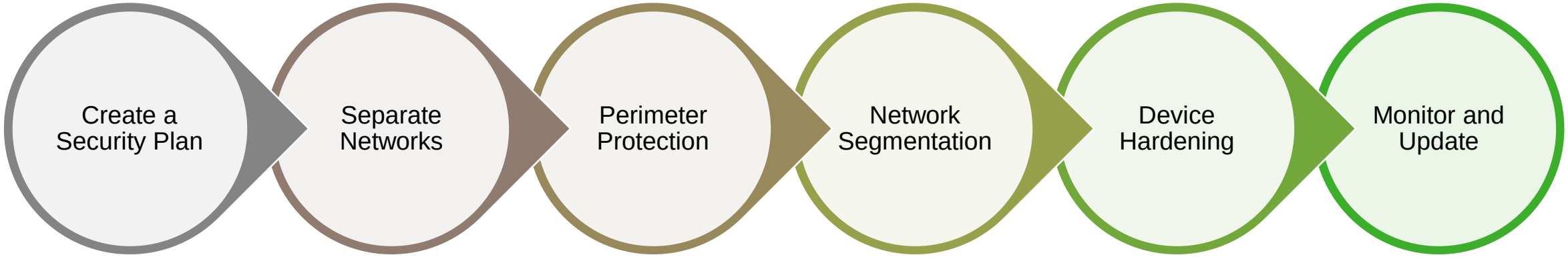
- Ensure that Panduit can help you to get the right type of cabling. There may also be vertical-specific requirements to fulfil, for example in
  - food & beverage
  - pharmaceutical
  - oil & gas…

- **plus: EN 50575:2014 Construction Products Regulation in the EU**
  Since July 1st, 2017 the fixed cabling used needs to comply, power and data cabling.
  Panduit will help you to update your company standard:
  http://www.panduit.com/cpr

Maintain supported by Key Performance Indicators (KPIs)



IEC 62443 - Defense in Depth



Panduit has the Solution for Your Network Management Journey

Continuing Education

With Partners and via Panduit

Panduit ONE

- Develop your competitive edge
- Necessary investment as your network evolves
- Considerable benefits to all team members that touch your network
- Based on roles in the company: design, develop, deploy
- http://partners.panduit.com/

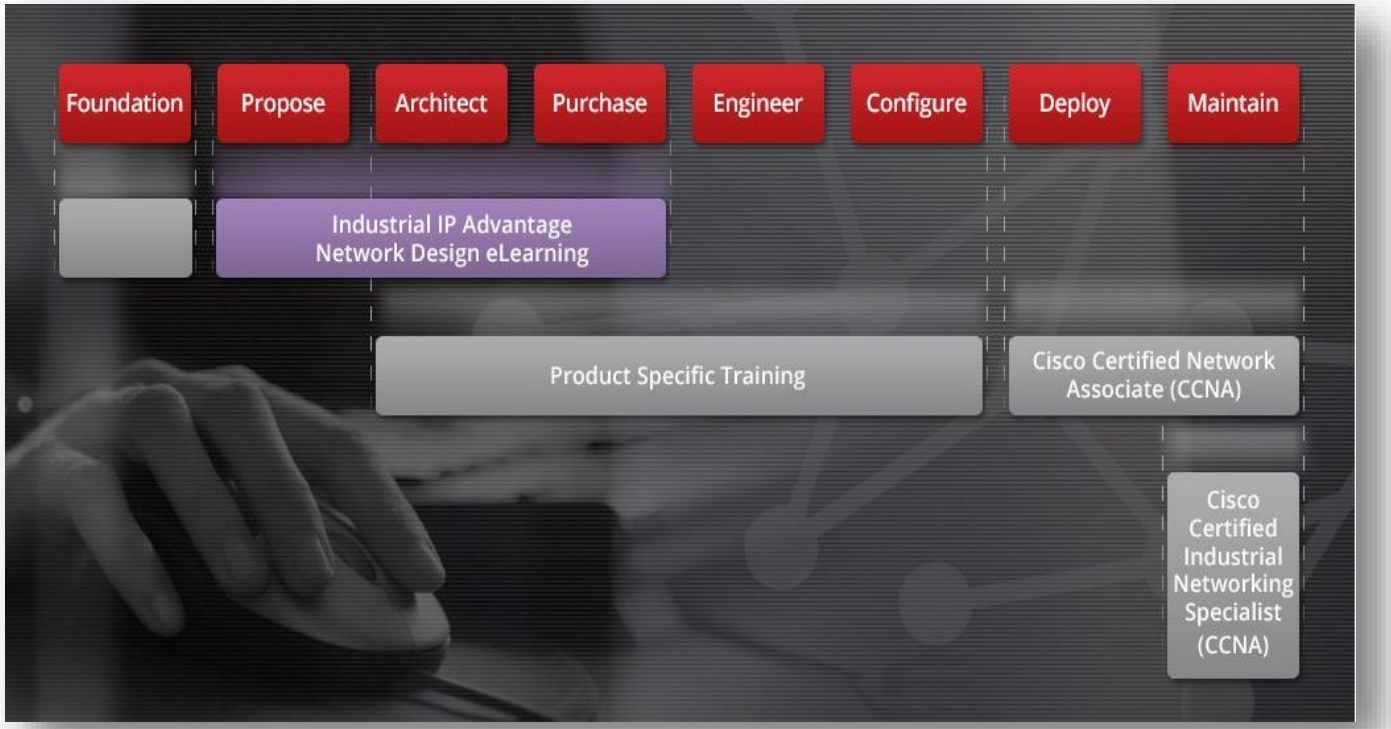
Industrial IP Advantage

- Founded by Cisco, Panduit and Rockwell Automation
- http://www.industrial-ip.org

Industrial IP Advantage (IIPA)

- Mix of instructor-led and e-learning courses
- Developed network design e-learning through collaboration of IIPA partner companies
- Who should attend: control engineers, network engineers and plant IT personnel

Earn digital badges, certificates & PDHs



IIPA – Build your Skills and Stay Engaged

Visit www.industrial-ip.org

- Trends, developments, and implementation advice on the use of IP in industrial applications

Sign up for the monthly newsletter

- Latest news and technology trends

Join in the discussion

- Twitter, Facebook and/or LinkedIn

Interested in e-learning?

- Register at www.industrial-ip.org/register

Panduit offers FREE Training for Partners

- North America: PPNX7QFQ
- Latin America: PPLXZ73Q
- Asia Pacific: PPAMERSW
- **EMEA: PPEQHL83**

Recommended Resources

ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

Our mission is to reduce the Nation's risk of systemic cybersecurity and communications challenges.

- Information Products
- Training
- Assessments
- Recommended Practices
- Standards & References

Converged Plantwide Ethernet

- Validated Reference Architectures
- https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/CPwE_DIG/CPwE_chapter6.pdf
- http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td002_-en-p.pdf

Planning Considerations

Technologies to Monitor

Power over Ethernet

- Delivers DC power along the same conductors that carry Ethernet traffic
- Network switch negotiates with end device to automatically provide the right power
- Created to enable VoIP telephony to succeed
- Not a new idea but there is an enabling IEEE standard

- Industrial Network Impact?
  - DC control power infrastructure will evolve
  - End device power and control simplified
  - Troubleshooting simplified

Property	PoE IEEE 802.3af	PoE+ IEEE 802.3at	4PPoE IEEE 802.3bt	PoE++ IEEE 802.3bt
PSE Power	15.4W	30.0W	60W	100W
PD Power	12.95W	25.5W	51W	71W
Power Management	Power class levels, negotiated at initial connection or 0.1W steps negotiated continuously			

Power-sourcing equipment (PSE)
Powered device (PD)

Single Pair Ethernet

- What is it?
  - Ethernet transmission over a twisted pair at distances up to 1000 meters with optional power delivery
- Where is it needed?
  - Automotive – on vehicle applications like telematics and real time diagnostics
  - Industrial – connectivity at the network edge
  - Digital Building – possible applications due to similarity to some legacy Industrial protocols (still being evaluated)
- Media
  - Industrial – 18AWG shielded twisted pair
    - IP-67 and IP-20 connectors
  - Automotive – 18 AWG twisted but not always shielded
    - Proprietary automotive industry connectors
- Status
  - In task group IEEE 802.3cg, target for specification early 2019

Main Global Ind. Ethernet Technology

Ethernet	PROFINET	ETHERNET/IP	Modbus-IP
ISO/IEC 11801	ISO/IEC 11801-3	ISO/IEC 11801-3	ISO/IEC 11801-3
[redacted]	IEC 61784-2 CPF3	IEC 61784-2 CPF2/2	IEC 61784-2 CPF15

TSN – Time Sensitive Networking

- IEEE802.1 suite of standards
- “tools” in the suite
  - IEEE 802.1 AS for time synchronization
  - IEEE 802.1 Qbv on scheduling and traffic shaping
  - IEEE 802.1 Qcc as enhancements for scheduled traffic
- Enhances communication by adding mechanisms to ensure timely delivery with soft and hard real-time requirements

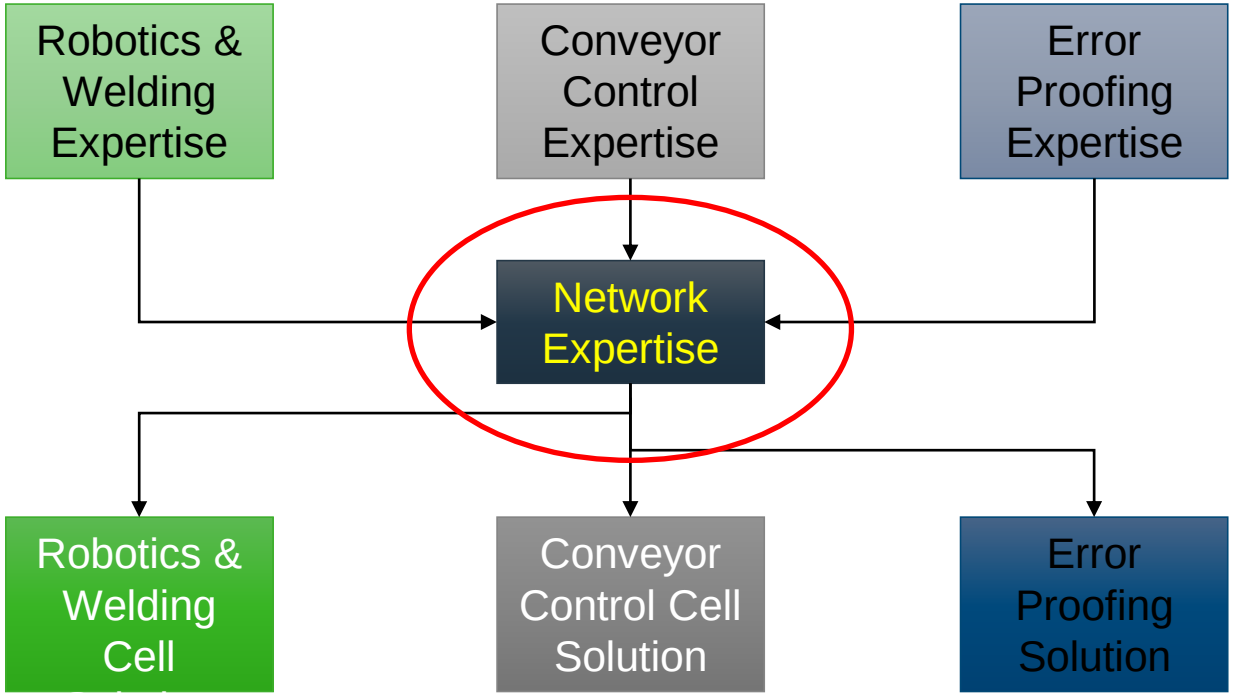
- IEEE802.1 started for professional audio/visual needs
- Future application benefits for:
  - Industrial control
  - Automotive
  - Industrial Internet of Things
- Key elements to monitor
  - IEEE802.1
  - AVNU Alliance

Is your infrastructure TSN-ready? Are the company infrastructure standards sufficient to support TSN?

SDN – Software Defined Networking

- **Software-defined networking** (**SDN**) is an approach to networking that allows network services to be managed through abstraction of lower level functionality

- What to monitor:
  - IEEE and ODVA
  - Progressive network equipment manufacturers



Let us know if you come across this – we're happy to help ☺

Thank you.
Which questions do you have?

Contact us

emea-customerservices@panduit.com
TechSupportEMEA@panduit.com

Hayo V. Hasenfus: d-hvh@panduit.com, +49 (173) 8881050

UK +44 (208) 6017-219	Belgium +32 (2) 7143142	Norway +47 (800) 13602
Germany +49 (69) 95096129	Spain +34 (91) 3778107	Sweden +46 (85) 8536737
France +33 (1) 41918572	Portugal +351 (213) 665 279	Denmark +45 (38) 322923
Holland +31 (20) 4874581	Italy +39 (02) 69633270	ME-A +971 (4) 361-6933