The bridge to possible

Future-ready Shopfloor Architecture and How You Can Get to It

Step by Step

Henning Loeser, Head of Audi P-Lab
Arun Siddeswaran, Director IoT Solution Engineering
Thomas Hopfgartner, Technical Solutions Architect

Content from Tilman Taubert, EMEA IoT Manufacturing Lead

Cisco Webex App

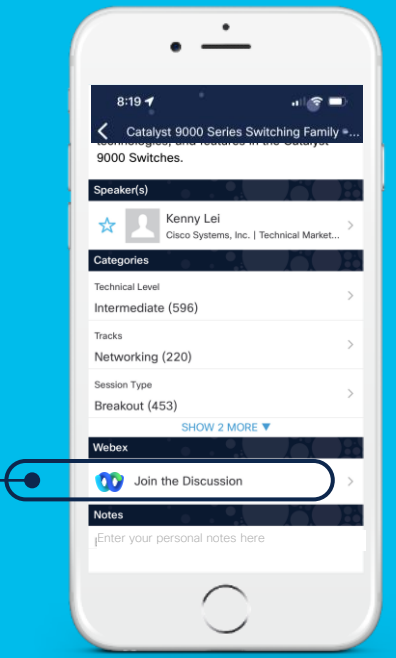
Questions?

Use Cisco Webex App to chat
with the speaker after the session

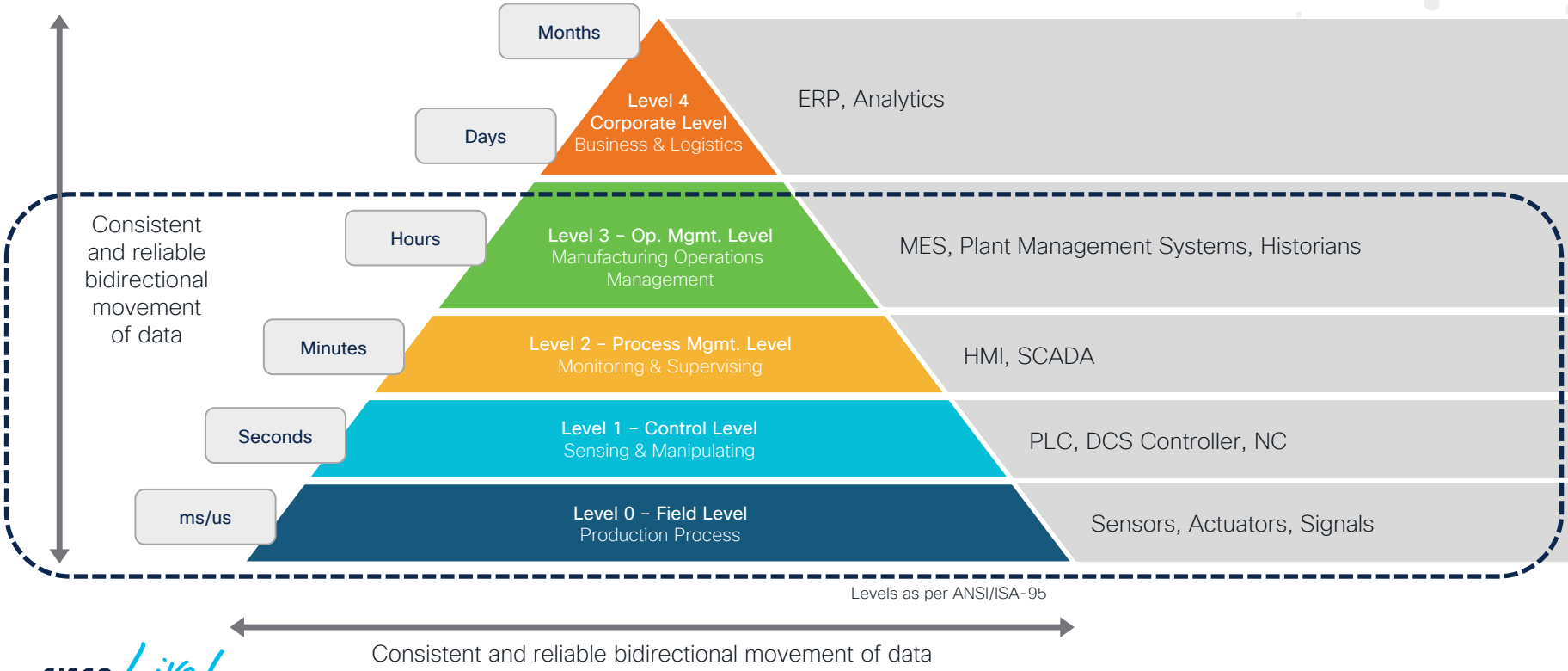
How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated until February 24, 2023.



Scope of this Session



Agenda

1. **Momentum**
   Why do you care?
2. **Organization**
   Who's topic is it ?
3. **Capabilities**
   What you need to plan for?
4. **Time**
   How to get started ?
5. **Take Away**
   Summary

Momentum

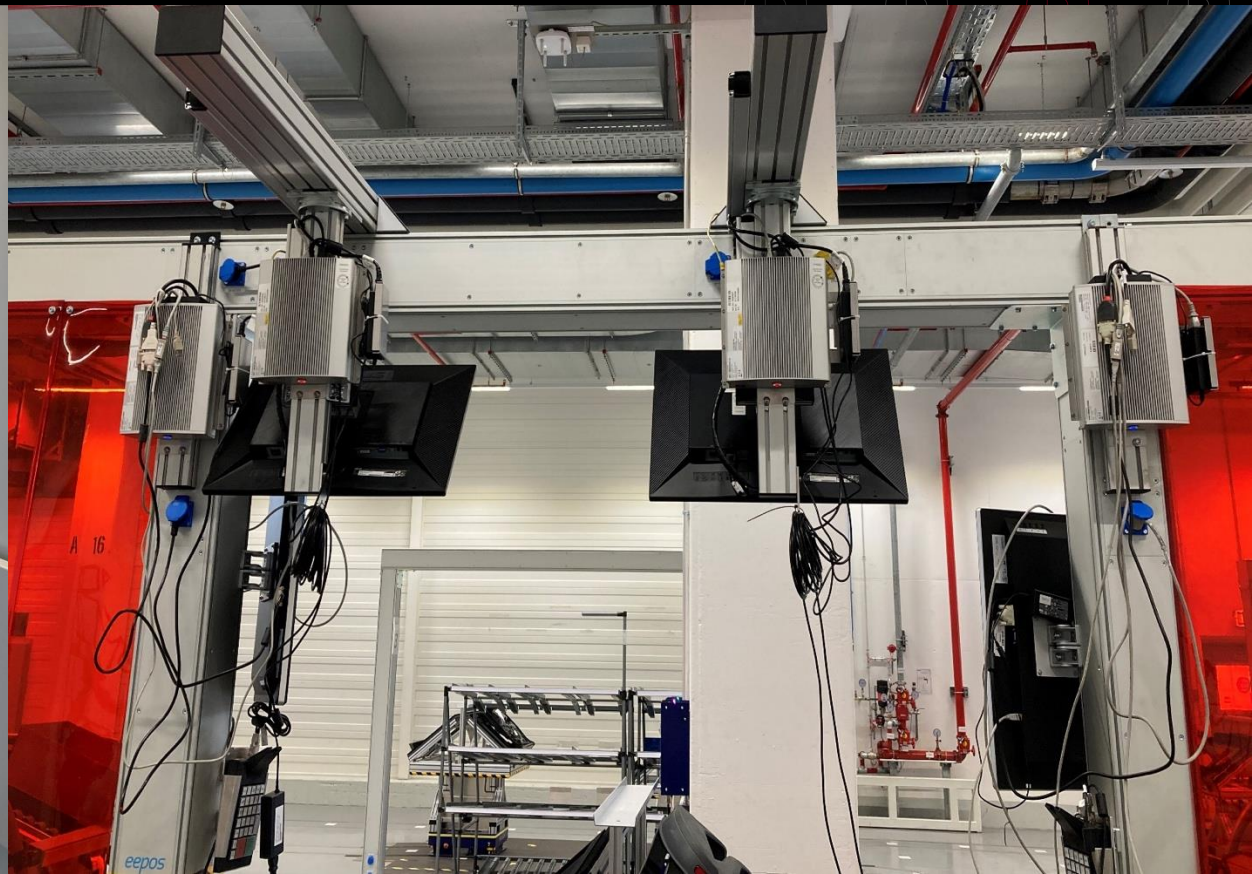
cisco Live!

EC4P

Dr. Henning Löser

February 9th, 2023

Audi production today…



Many systems within our production

Torque Software

MES

Manufacturing Execution System

Diagnosis- and Quality Control System

PLC

Programmable Logic Controller

How we handle data

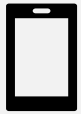
In the past

In the future

…at home




Music CD | Calendar | Camera | Calculator

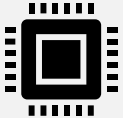


Smartphone with own cloud

…in the car




Control unit 1…n

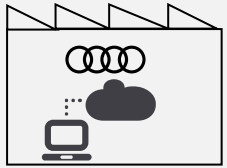


Central control unit

…in the production




Local computers 1…n | local PLCs 1…n



Edge Cloud 4 Production

Audi production tomorrow:
a smart factory not a maintenance nightmare

A continuous technology alignment

For almost two decades, IT and OT technologies have started to converge towards a common technology platform.

1980 - 2000

Two separate networks
Different technologies and approaches

Yesterday

Increased adoption and proliferation of IT based technologies in industrial information systems
IP based communication, software, hardware, cyber security

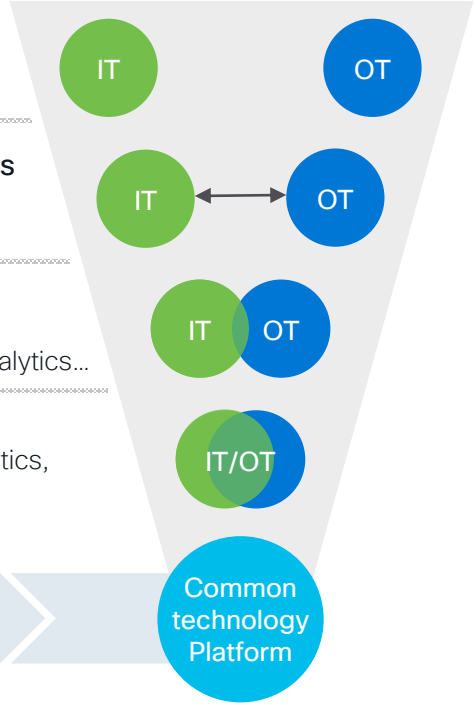
Today

Strong need for integration of business and operational data to gain insights
Cloud, wireless, Big Data, smart sensors, Industrial IoT, predictive analytics…

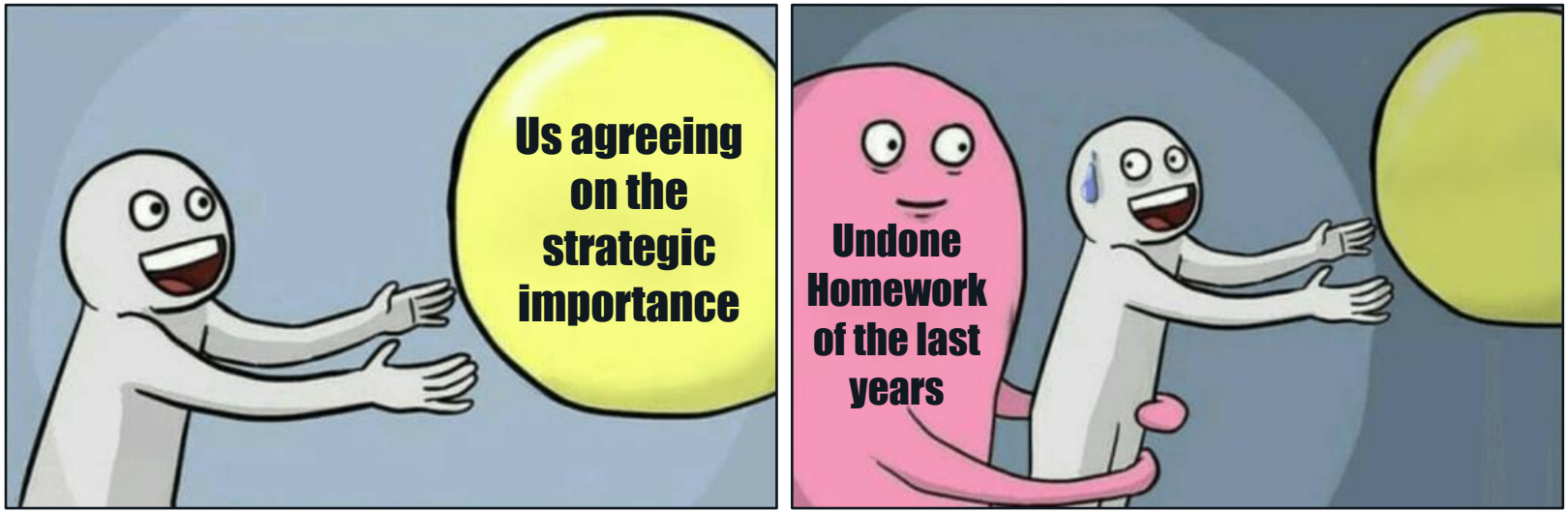
Tomorrow

Advent of Industry 4.0
Digital Twin, smart robots, cyber physical systems, prescriptive analytics, augmented reality, adaptive manufacturing

Fully connected enterprise and factory
Vertical and horizontal integration of the entire value chain

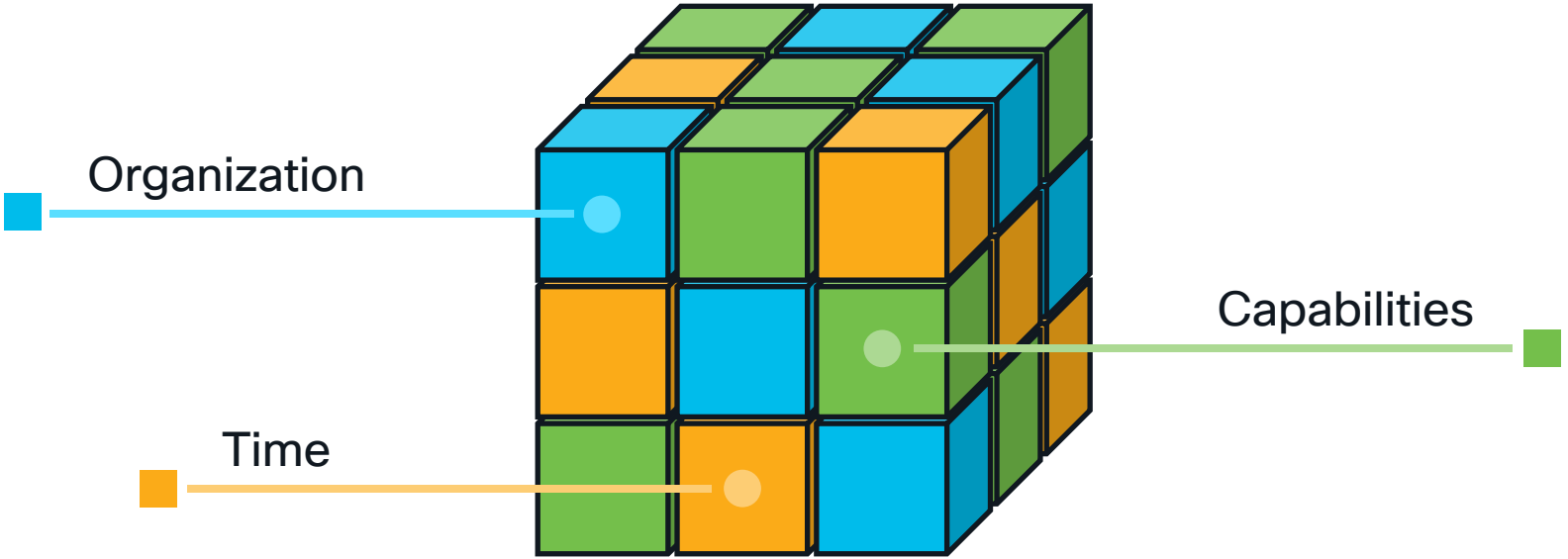


Reality check



Resolving this, needs more than just technology

Three key areas of focus



Organization

The human aspect

Common objectives and a healthy exchange will help to bridge the divide

IT

Believe that Operations don't know IT best practice

Often lack specific knowledge and experience with real-time, OT solutions/systems

Better understanding of global business vision as well as core technology skills (networks, operating systems, DBs, etc.)

But, CIO is typically accountable for cyber security and risk

OT

Believe that IT don't know practical Engineering & Operations

Support mission critical systems where availability and integrity are key

Understand how to support Operational workers in a 24x7 environment

And OT solutions and Infrastructure are becoming more like IT

Different culture, skills, know-how and risk drivers

IT/OT Convergence models

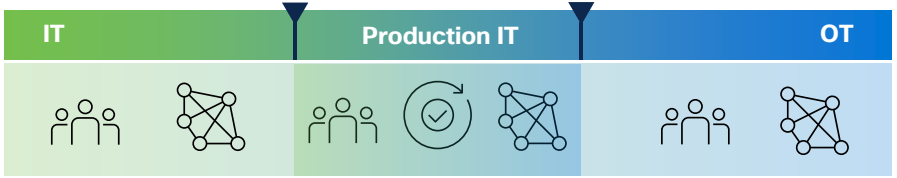
Organization Processes Technology

Unification model

- Standardized technology and business processes
- Centralized management and decision making for OT infrastructure
- IT providing infrastructure services and monitoring to OT

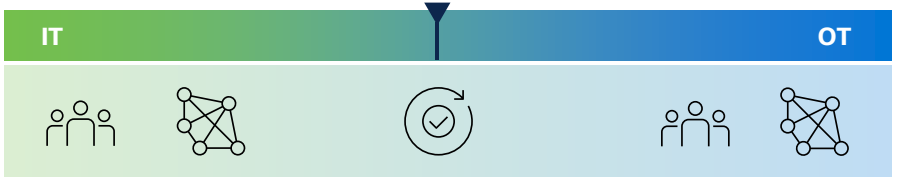
Three-Tier Model

- Organization divides responsibility between traditional IT and automation organizations.
- Service-oriented IT and Production IT emerges
- Specspecialized centers of excellence for OT related topics



Replication/Coordination model

- Shared processes among IT and OT
- Procedures involve cooperation between IT and OT
- Beginning of technical integration



Diversification model

- Roles and responsibilities for application, infrastructure and security are duplicated within IT & OT organization with little standardization & integration
- Separate procedures exist for IT and OT area
- Technically separated IT and OT environments

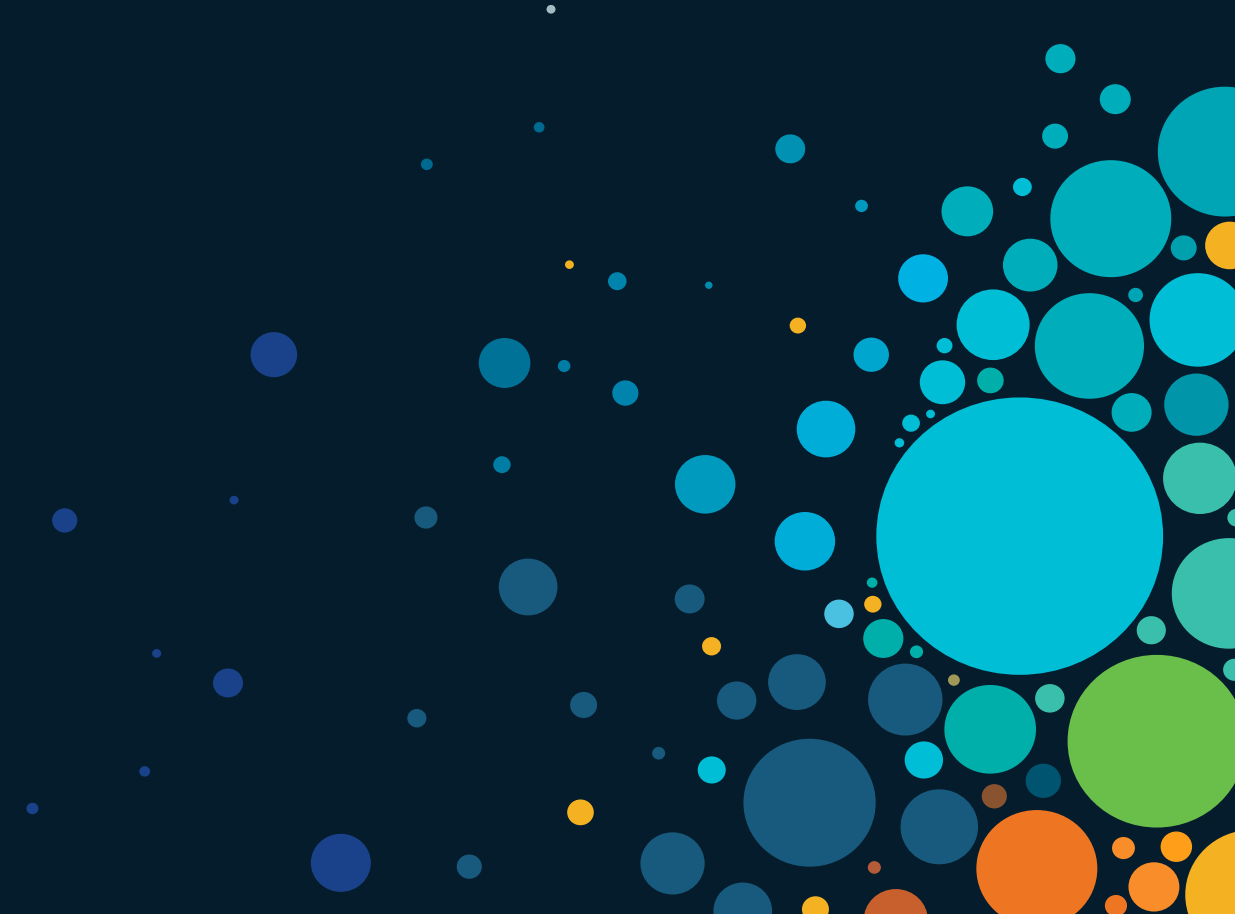
Operations Model

Finding the model, that supports every stakeholders needs

	IT	OT
Roles	• Plan, Build and Run of IT infrastructure like Network, Compute/Storage, Hyper-visors, Operating Systems, Infrastructure Services like DNS, DHCP and Active Directory • Operate Network- and Systems Management	• Plan, build and run of Application related technology like PLCs, DCS, I/O, NC, Drives, HMIs, SCADA, Historians, MES, etc. • Operate the production platform
Responsibilities	• Define supported standards, versions and configuration • Provide Security Policies and Posture • Provide Delegation-portals and monitoring-information to OT • Configure IT system components (initial, change) • Install and maintain Hardware in the datacenter setting	• Define application requirements and profiles • Maintain Life-cycle related information within Security Policies (Assets, Groups of Assets) • Install and maintain Hardware in the industrial setting (install new, replace faulty device, etc,)

This Example of an Operations Model is based on **Unification** IT/OT convergence approach

Capabilities




The 90’s have called. They want their tech back.

Common Requirements

What do we need to plan for ?

More Bandwidth and Processing

Video, AGVs, Real-time sensing for Digital Twin's and Machine Vision drive increased need

Low Latency, Resilient Communications & Rich Data

Real-time control of machinery. Secure, context rich (time, location) data delivered to IoT apps

Cyber Security

Explosive growth in connected devices increases expansion of the threat surface

Simplified Scale

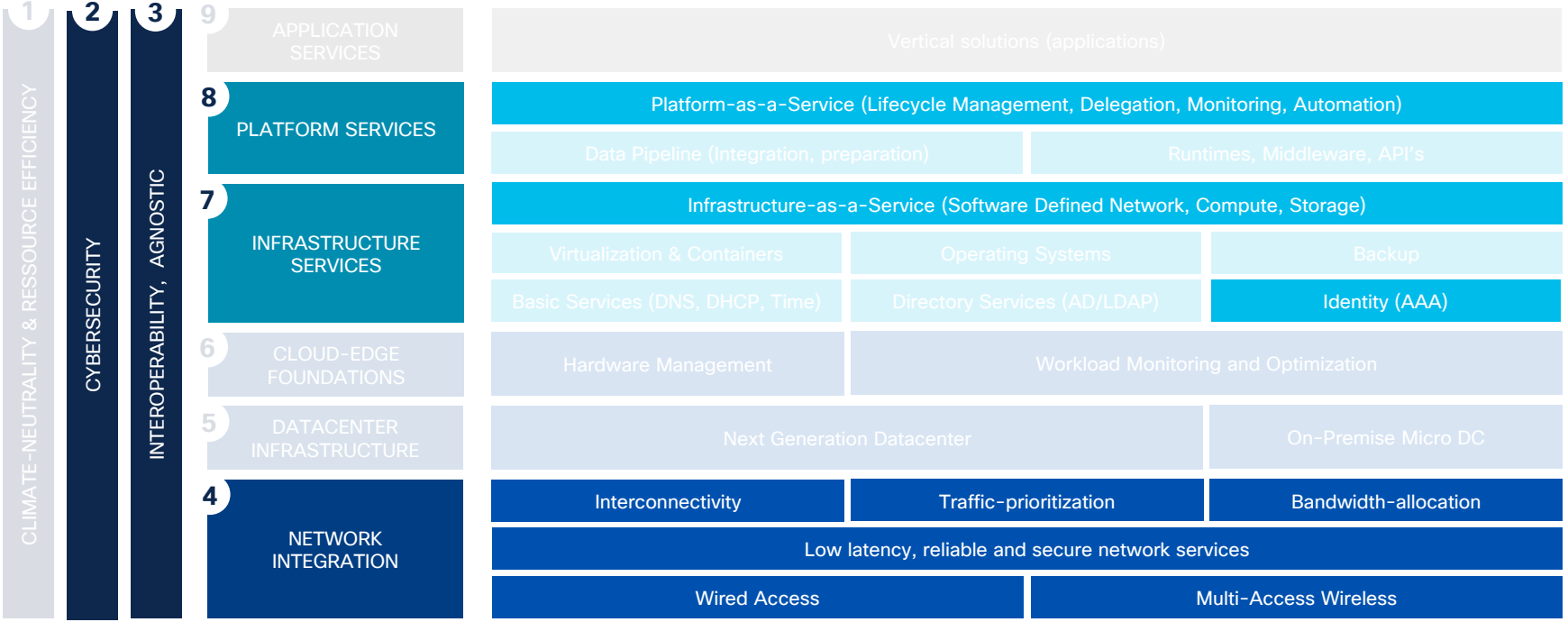
Deploy & manage more devices across more locations with the same resources

Edge Computing

Process and act on data faster when it is closer to its source. Maintain compliance. Save costs.

Technology Stack

How could a common technology platform look like ?



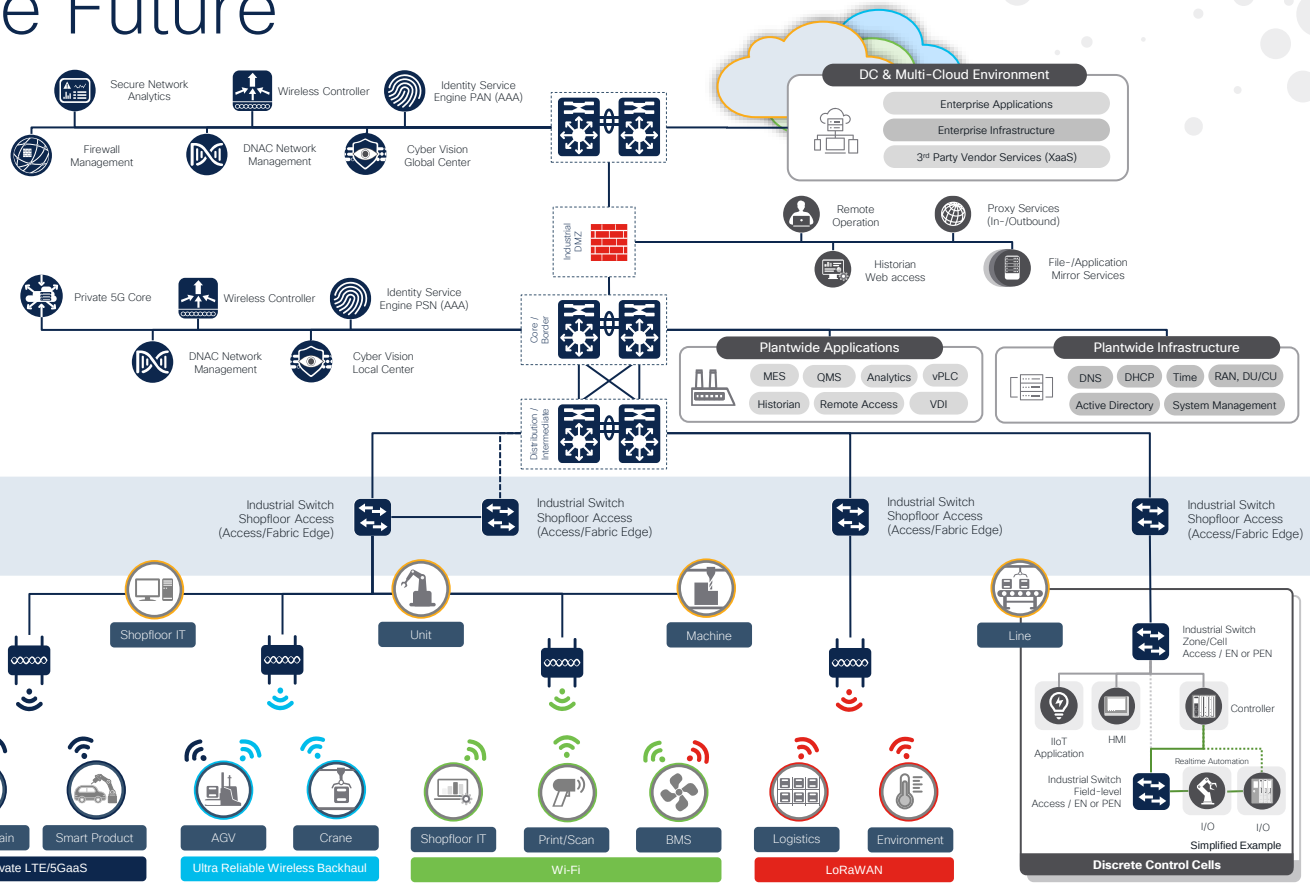
Value and use-cases for Manufacturing Operation

Take a business-centric focus to build the architecture

	Flexible	Secure	Agnostic
Benefits	▪ Increased Efficiency in Setup and Change (Reduced Turnaround Time) ▪ Reduced failure potential (Human Error) ▪ Improved overall Time-to-fix	▪ Minimize risk for property, people and equipment damages ▪ Reduce lost production and labor hours ▪ Reach Compliance requirements	▪ Increased Efficiency in Operation ▪ Availability of technology Experts (existing internal/external Know-how) ▪ Lower OPEX Cost
Use-case	▪ Provision, deploy & manage network infrastructure on scale ▪ Simplified and flexible changes ▪ Automation of common Tasks	▪ Visibility into Assets and Communication Flow ▪ Prevention of lateral Movement ▪ Rapid Threat Containment	▪ Harmonization of Standards ▪ Global replication ▪ Building Blocks to fit multiple site sizes
Capabilities	▪ Centralized seamless Management incl. Zero-touch Provisioning ▪ Workflow Automation (Intent-based) ▪ Integration into existing Processes and Tool-chain	▪ Insights through Network Traffic Analysis ▪ Identity-based policy enforcement with Dynamic assignment (Central Control) ▪ Macro-/Micro segmentation	▪ Automation-vendor neutral Network architecture ▪ One technology within a given domain

Factory of the Future

High-Level Architecture



Best practice & Design principles

Scoping

Best practice & Design principles

- Proper Requirements Engineering
- Industrial Automation Systems can become very complex in depth
- Profiling of Application(s) with the business helps to be clear on expectations and meet them
- Building a User Requirements Summary is suggested

Application Profile

Application Description ?
Automation Vendor ?
Product/Solution Name ?

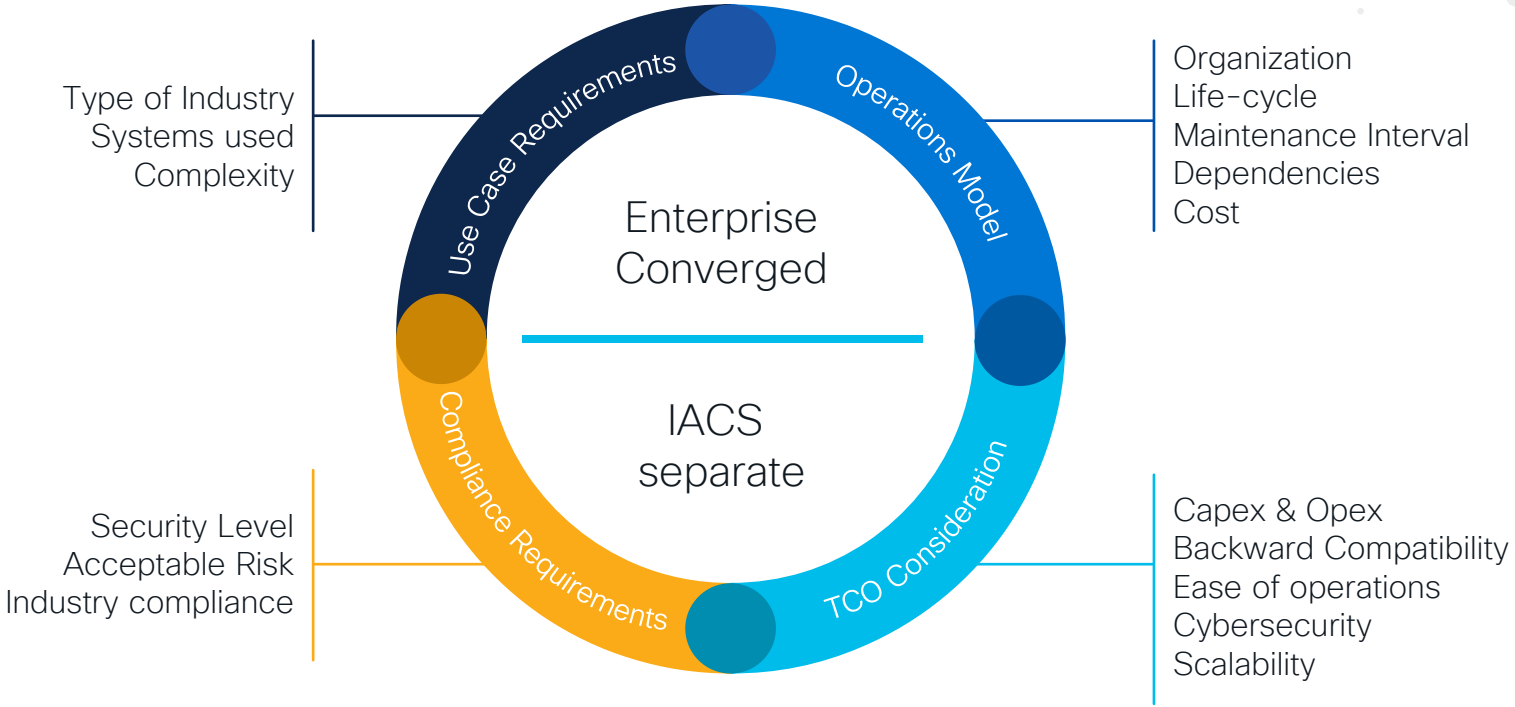
Safety-relevant ?
External SIS or Integrated ?

Technical requirements

Protocols been used ? (Include Controller and field-level)
Components and Communication ?
IP Schema ?
NAT been used (PAT/1:1 NAT/L2NAT ?
Cycle Times ?
Retry Timer (Safety) ?

Type of Deployment

Best practice & Design principles



Wireless Access Technology

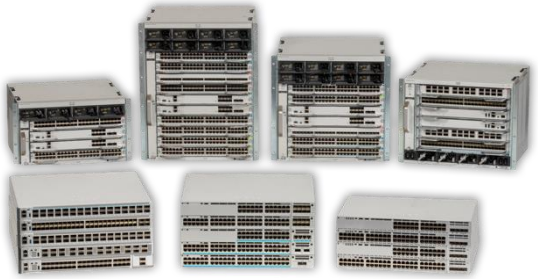
Best practice & Design principles

Private LTE/5GaaS	CURWB	WiFi 6 (802.11ax)
Broad geographic coverage	Zero loss – sub ms latency and seamless roaming	Applications focused on capacity, client density, mobility, “guest” access, BYOD
	Mission Critical Applications	
Wide Area Coverage	Process Automation	Autonomous applications	Fixed Backhaul	Remote Expert	Digital Campus

Performance | IIoT Scale | Capacity | Security

Hardware

Best practice & Design principles



Purpose-built for ‘clean’ environment
Density, bandwidth, PoE power-budget

Purpose-built for Industrial environment
Temperature, industrial standards, vibration, shock and surge, and electrical noise immunity

Ease-of-Use
SD-Card, Alarm I/O (Analog relays)

Industry specific Features and Functionality
PROFINET, Ethernet/IP, Modbus TCP, MRP, DLR, RP, HSR, L2NAT

Operating System (Cisco IOS XE)

Network Management (Cisco DNA Center)

Availability and Resiliency

Best practice & Design principles

Resiliency Protocol	Mixed Vendor	Ring	Redundant Star	Net Conv > 250 ms	Net Conv 50-100ms	Net Conv < 0-10 ms	Layer 3	Layer 2
STP (802.1D)	◉	◉	◉					◉
RSTP (802.1w)	◉	◉	◉	◉				◉
MSTP (802.1s)	◉	◉	◉	◉				◉
PVST+		◉	◉	◉				◉
REP/REP Fast		◉			◉			◉
EtherChannel (LACP 802.3ad)	◉		◉		◉			◉
MRP (IEC 62439-2)	◉	◉		◉	◉			◉
Flex Links			◉		◉			◉
PRP/HSR (IEC 62439-3)	◉	◉	◉			◉		◉
DLR	◉	◉				◉		◉
StackWise		◉	◉	◉			◉	
HSRP		◉	◉	◉			◉	
VRRP (IETF RFC 3768)	◉	◉	◉	◉			◉	

Cyber Security Consideration

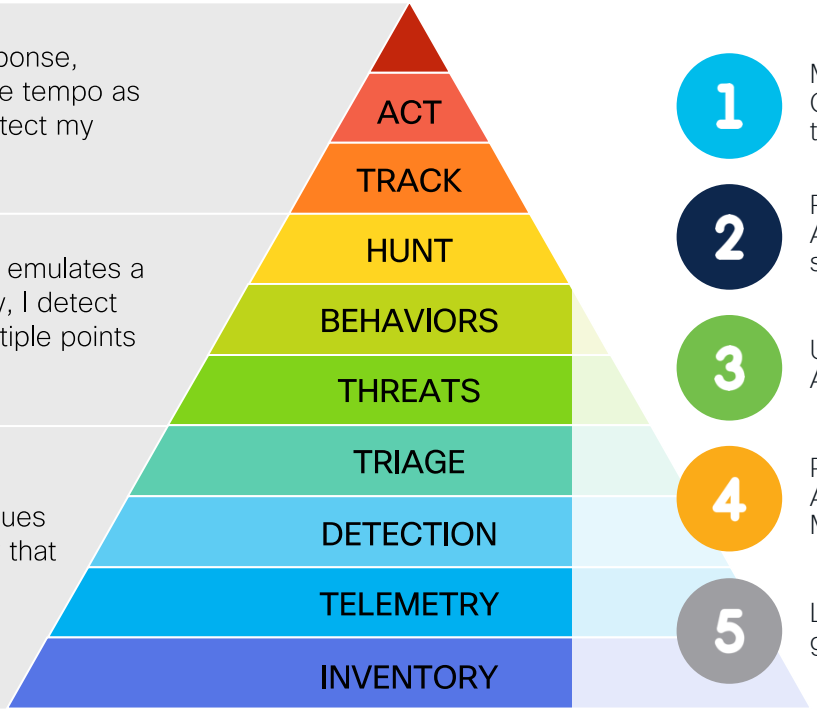
Best practice & Design principles

The incident response hierarchy of needs

"During incident response, I operate at the same tempo as the adversary to protect my business assets."

"When my red team emulates a real-world adversary, I detect their intrusion at multiple points along the kill chain."

"I detect hygiene issues and operator activity that does not follow best practices."



1. Mitigate risk from Unpatchable systems, both IT and OT assets and these assets associated business risk to the Manufacturing operation.
2. Rapid Visibility of IACS System Threats, ensuring the Ability to Detect both IT and OT malware within the shopfloor environment.
3. Up-to-date complete Inventory of IACS system Assets with details per Asset
4. Protect Manufacturing Platform and Applications from Attack. Protect from both Known and Unknown Malware.
5. Limit Network Traffic and Network Path leveraged to get to Critical Manufacturing Systems.

Cyber Security Considerations

Best practice & Design principles

Discover

- Discover Devices (Assets) in the network
- Discover Communication between Assets

Segment

- Network Segmentation
- Perimeter Security
- Access Control
  - Authentication
  - Authorization
  - Accounting

Detect

- Detect Baseline Differences
  - Device (Asset) changes
  - Changes in Communication between Assets (another Protocol)
  - changed Communication behavior (Variables within Application)
- Anomaly Detection (Pattern based, IDS)
- Vulnerability Reporting

Respond

- SIEM / SOC Integration
- Prevention & Remediation
  - Change of Authorization (CoA)
  - IPS

Accepted Standards like IEC 62443 and NIST Framework driving the agenda.

Segmentation Strategies

Best practice & Design principles

- Use dynamic classification where possible (802.1x and MAB)
- Use static assignment where needed
- Private VLANs could be an intermediate but immediate step for simple use-cases
- Keep the policy simple but effective

Example TrustSec Matrix

KEEP
CALM
AND
DON’T REINVENT
THE WHEEL

Resources for your consumption

Best practice & Design principles

Cisco Validated Design

Tested Implemented Proven

[Networking and Security in Industrial Automation Environments Design and Implementation Guide]

[Cisco DNA Center for Industrial Automation Design Guide]

BRKIOT-2720 - Connected Factory Architecture

[Industrial Security Design Guide]

BRKIOT-2882 - Implementing Segmentation in Industrial Networks

End-End Architecture

CVDs start with the customer use cases and architecture from the edge device to the application, validating the key Cisco and 3rd party components

Best Practices

Document best practices so you can confidently set performance expectations

Reliability

Reduce risk products won't work together or perform as promised

Comprehensive

Provide tested system designs and configuration instructions

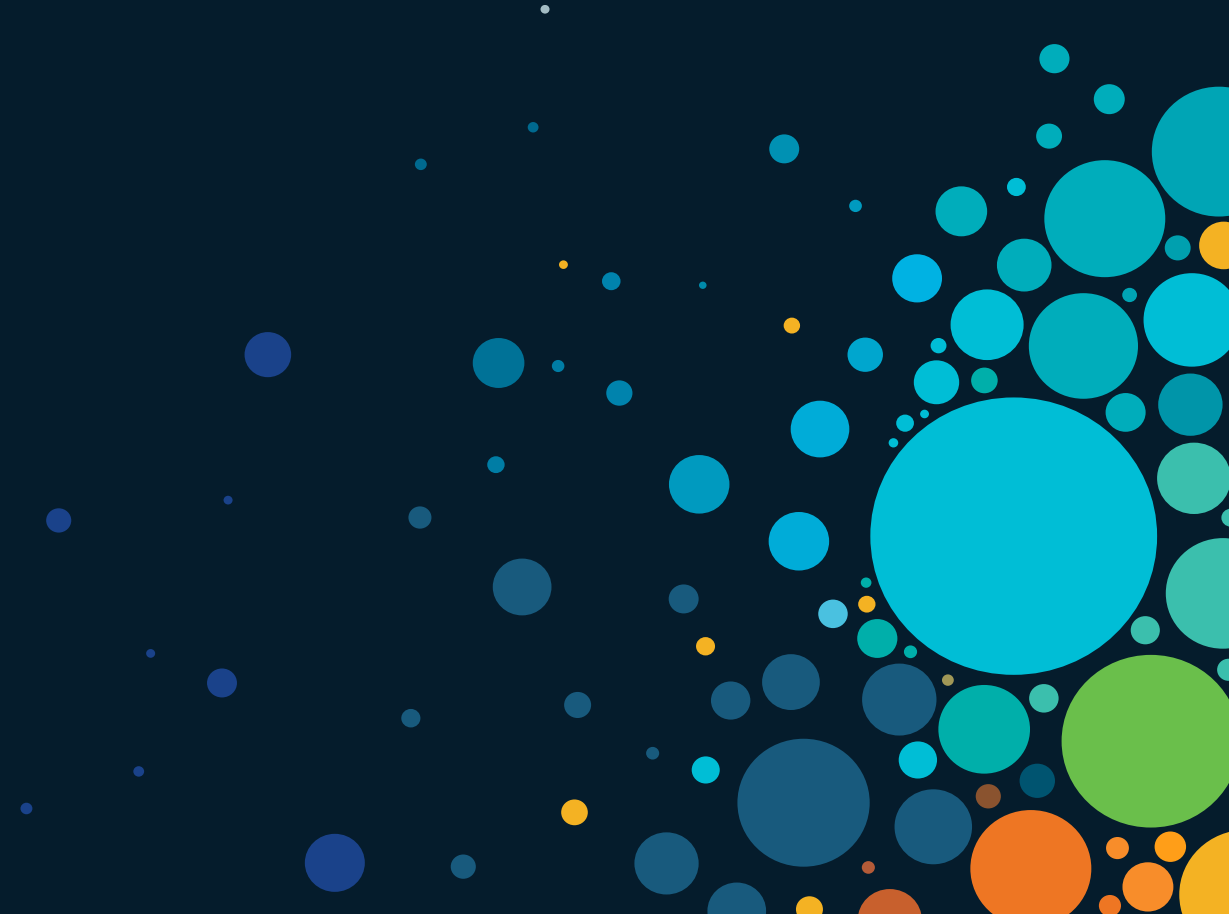
Outlook

Technical Journey

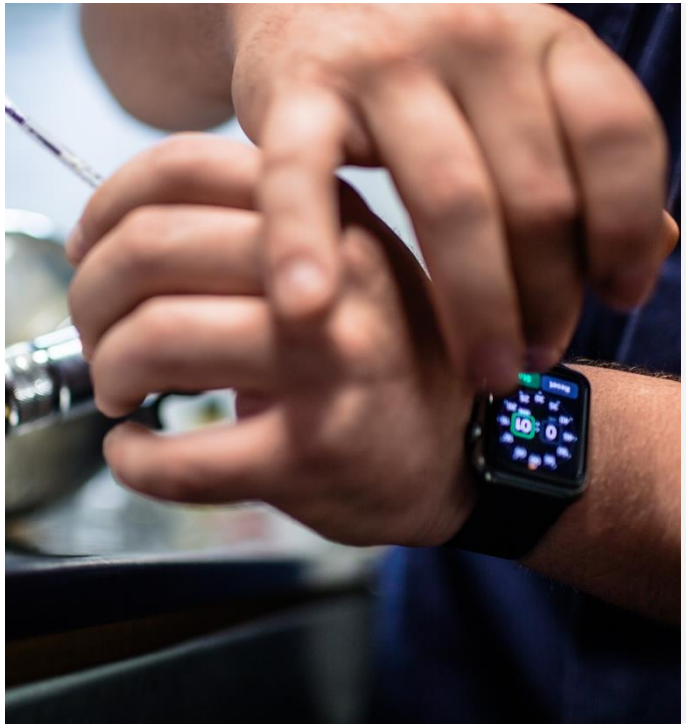
Intent-based Networking

- Automation Use Cases
- Assurance Use Cases
- ISE Use Cases
- SDA Use Cases

Time



Bringing it to life



- Executive/Senior Leadership Sponsorship is a Must-have
- Change process needs time
- A release strategy can help
- Don’t overengineer

Release Capabilities into Production
Minimum viable product (MVP) approach

MVP 1.0
Initial Release

- Foundational Security
  - Macro Segmentation
  - Perimeter Security (IDMZ)
- Consolidated Hardware Catalogue
- Operation Model (Roles & Responsibilites)
- Configuration Templates
- Basic System Management
- Supply Chain Integration

MVP 1.1
Next sub Release

- Asset Visibility and Inventory
- NAC (Monitoring Mode)
- Foundational Security
  - Macro Segmentation
  - Perimeter Security (IDMZ)
- Consolidated Hardware Catalogue
- Operation Model (Roles & Responsibilites)
- Configuration Templates (+)
- Basic System Management
- Supply Chain Integration

MVP 1.x
Next sub Release

- Enterprise Service Integration
  - Workflow Automation
  - Delegation Portal
- Baselining (Anomaly Detect.)
- Asset Visibility and Inventory
- NAC (Monitoring Mode)
- Foundational Security
  - Macro Segmentation
  - Perimeter Security (IDMZ)
- Consolidated Hardware Catalogue (+)
- Operation Model (Roles & Responsibilites)
- Configuration Templates (+)
- Basic System Management
- Supply Chain Integration

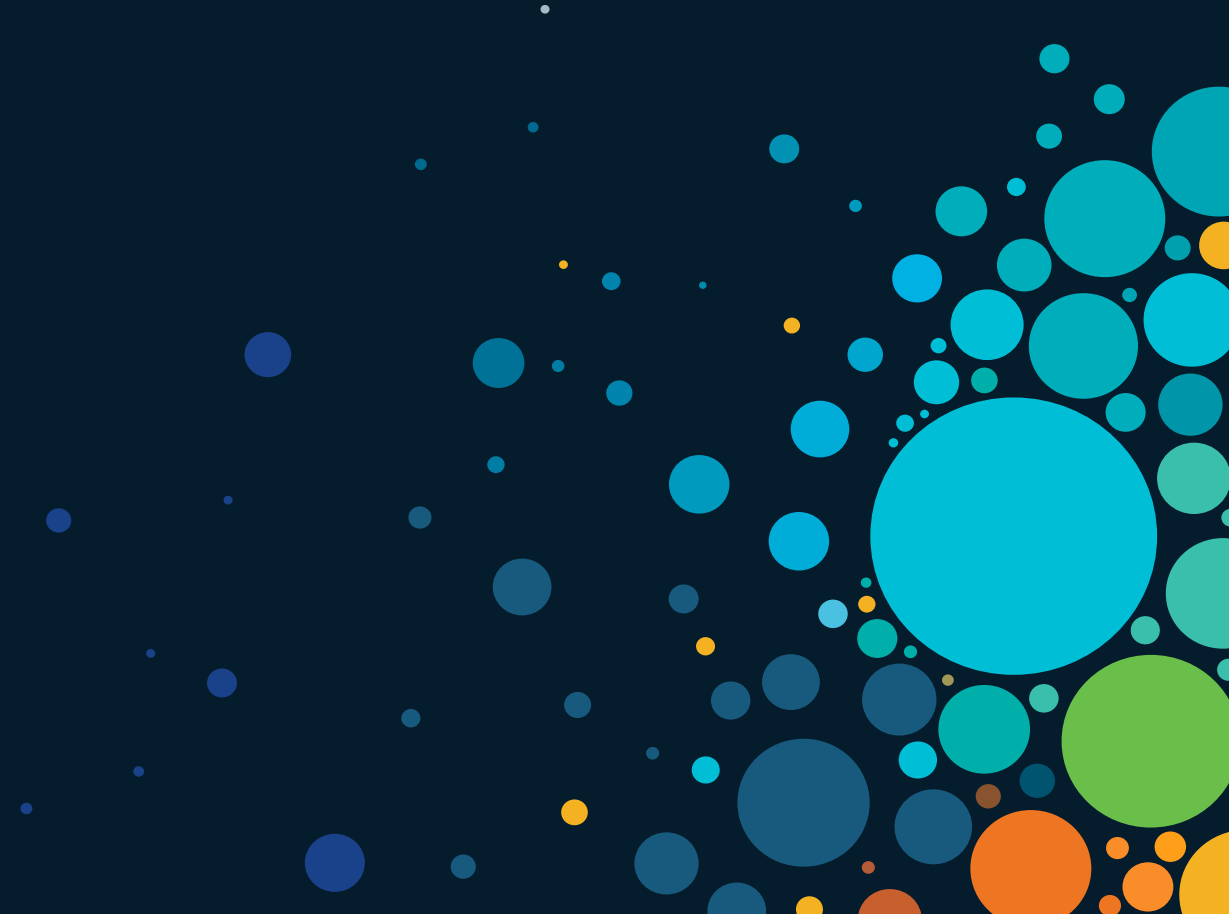
MVP 2.0
Next major Release

- Full Spectrum Security
  - Micro Segmentation
  - Threat Detection
- Enterprise Service Integration
  - Workflow Automation
  - Delegation Portal
- Baselining (Anomaly Detect.)
- Asset Visibility and Inventory
- NAC (Enforcement Mode)
- Foundational Security
  - Macro Segmentation
  - Perimeter Security (IDMZ)
- Consolidated Hardware Catalogue
- Operation Model (Roles & Responsibilites)
- Configuration Templates (+)
- Basic System Management
- Supply Chain Integration

Northstar
Final to-be High-Level Design

- SOC Integration
- Multidomain Integration
- Intrusion Detection
- Full Spectrum Security
  - Micro Segmentation
  - Threat Detection
- Enterprise Service Integration
  - Workflow Automation
  - Delegation Portal
- Baselining (Anomaly Detect.)
- Asset Visibility and Inventory
- NAC (Monitoring Mode)
- Foundational Security
  - Macro Segmentation
  - Perimeter Security (IDMZ)
- Consolidated Hardware Catalogue
- Operation Model (Roles & Responsibilites)
- Configuration Templates
- Basic System Management
- Supply Chain Integration

Wrap up



Key Takeaways

1. **Team up with OT!**
2. **Scope properly**
3. **Use the existing Blueprints**
4. **Get started**

Complete your Session Survey

- Please complete your session survey after each session. Your feedback is important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (open from Thursday) to receive your Cisco Live t-shirt.

- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Session Catalog and clicking the "Attendee Dashboard" at https://www.ciscolive.com/emea/learn/sessions/session-catalog.html

Continue Your Education

Visit the Cisco Showcase for related demos.

Book your one-on-one Meet the Engineer meeting.

Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.

Visit the On-Demand Library for more sessions at ciscolive.com/on-demand.


cisco
The bridge to possible
Thank you
cisco Live!


CISCO Live!
ALL IN