PHYSICAL SECURITY TECHNOLOGY UPDATE
- ASSESSING NEW THREATS

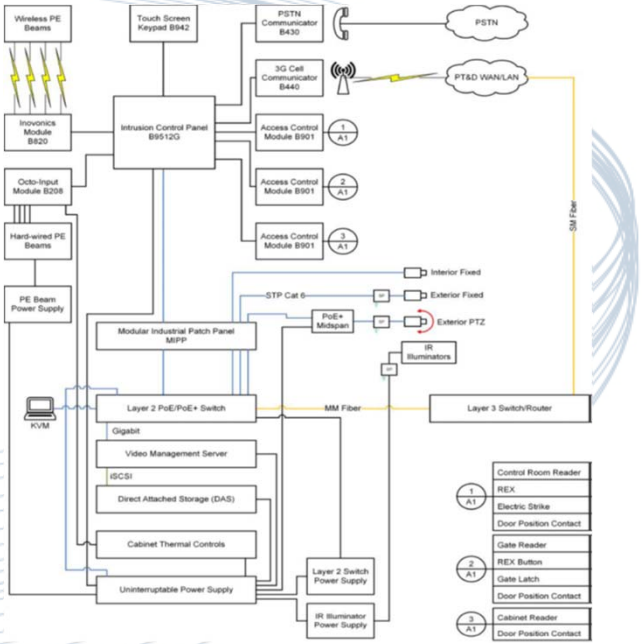
Jörgen Strandberg, RCDD

ANIXTER

BICSI

COMPLEX SOLUTION | PT&D UTILITIES

- Sample of a reference architecture for PT&D Utilities
  - Multiple subsystems
  - Physical Infrastructure
  - Hardened IT infrastructure
  - Video analytics
  - Cybersecurity
  - Lighting integration
- Defense in depth approach
  - Perimeter to cabinet



ACCESS CONTROL SYSTEM ARCHITECTURE MOVEMENT

PC-based Analog	Network Based (IP)	Interfacing (Open) Architecture	Standards Based
Peripherals	Peripherals	Peripherals	
Door	Door	Door	
Controller	Controller	Controller M = A, Controller M = B, Controller M = C	
Computer	IP Network	IP Network	
	Proprietary Software with AC Server	Integrated Software with AC Server	
	Workstations/Clients	Workstations/Clients	
		IMRON CORPORATION	ONVIF

ACaaS – Management in the cloud (Programing, Access records, Profile DB, RMR)

Bicsi

PACS – HOW THE MARKET DEVELOPS

- **System technologies evolve at a slow rate**
  - EAC system lifespan is long
  - Change is driven by the end user
  - Manufacturers develop technology based on end user demand
  - Integrators follow proven technologies
  - Distributors successfully support established technology

CREDENTIALS & READER TRENDS

Proximity Readers & Credentials

- 1-way unencrypted communication
- Wiegand Protocol
- Unsecure technology

Smart Card Readers & Credentials

- 2-way encrypted/secured communication
- Wiegand Protocol or OSDP
- Multi-application memory
- Multi-technology readers
- Secure technology

Mobile Enabled Readers & Credentials

- 2-way encrypted/secured communication
- Wiegand Protocol or OSDP
- Multi-application memory (Card)
- Multi-technology readers
- BLE & NFC Mobile Devices
- Increased Security
- Adjustable Read Range
- Secure technology

Biometrics

- Positive authentication
- No credential cost
- High security
- Multi-layer authentication
- Hands free capabilities
- Multi-modal authentication

Today

CREDENTIALS TECHNOLOGY MIGRATION

- Proximity cards – 50% of new installations
  - Proximity is no longer a secure technology
  - Produced an immediate demand for a new technology
- Contactless Smart Cards – 50% of new installations
  - High demand from end users and Integrators
  - Pricing similarly to proximity technology
- Mobile Credentials
  - Uses existing Bluetooth on IOS and Android mobile phones
  - Has a pre-installed adoption path
  - 20% of all credentials will be mobile by 2020
  - 50% commercial market will be mobile by 2020

ELECTRONIC DOOR HARDWARE INNOVATIONS

Electronic Cylinders

- No power required in the cylinder
- Powered by smart credential / key
- Cylinder and credential record access activity
- Self-contained EAC
- Multiple cylinder types
- Integrates with mechanical high security cylinder

Integrated Electronic Locks

- Combines Electrified Lock, Reader, Request to Exit and Door Monitoring on the door
- Multi-technology readers with BLE
- Single cable run
- Modular connected cables
- Reduces hardware installation time and installation errors
- Wireless options

ACCESS CONTROL INTEGRATION TRENDS

- Integration Options
  - No longer 1-way integration with EAC
  - Access control to VMS integration
  - Intrusion integration
  - Mobile device interaction
  - Wireless integrated locks
- Demand for Proven Technology
  - Disparate systems & applications drive complexity
  - ONVIF is making progress (Profiles C, X, X)
  - Slows adoption of open architecture platforms

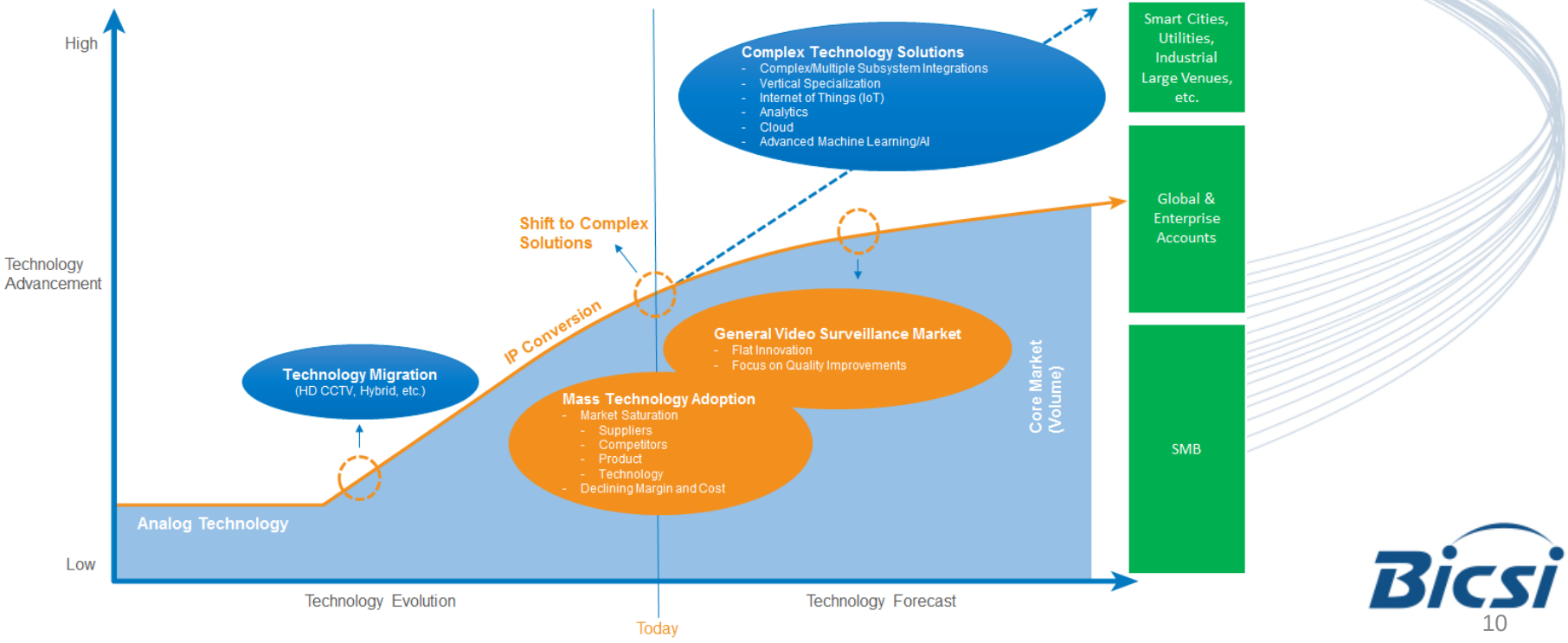
Challenges:

1. Cost of Integration
2. Integrator Skillset
3. Internal Ownership
4. One-off Integrations
5. System maintenance

ADDITIONAL KEY ACCESS CONTROL TRENDS

- Compliance
  - Data center cabinet security | Expanded locking solutions
  - Regulatory & Certification Requirements
- Entrance Protection | Perimeter Hardening
- Identity Management | Predictive Analytics
- Big Data & Internet of Things (IoT)

FOCUS POINTS FOR VIDEO SURVEILLANCE



LIGHTING FOR SECURITY

- Better quality lighting, not more lighting helps reduce cost to the customer as well
- Upgrading a customers lighting system to LED offers more control functions such as dimming, occupancy sensing, diagnostics, & communication
- Long life than traditional light sources
  - LED >100,000 hours
  - Metal Halide 10,000 – 20,000 hours
  - High Pressure Sodium 24,000 hours

- LED offer a higher Color Rendering Index (CRI) than traditional light sources allowing the security cameras to pick up more detail

IMPACT OF ADVANCEMENTS IN COMPRESSION

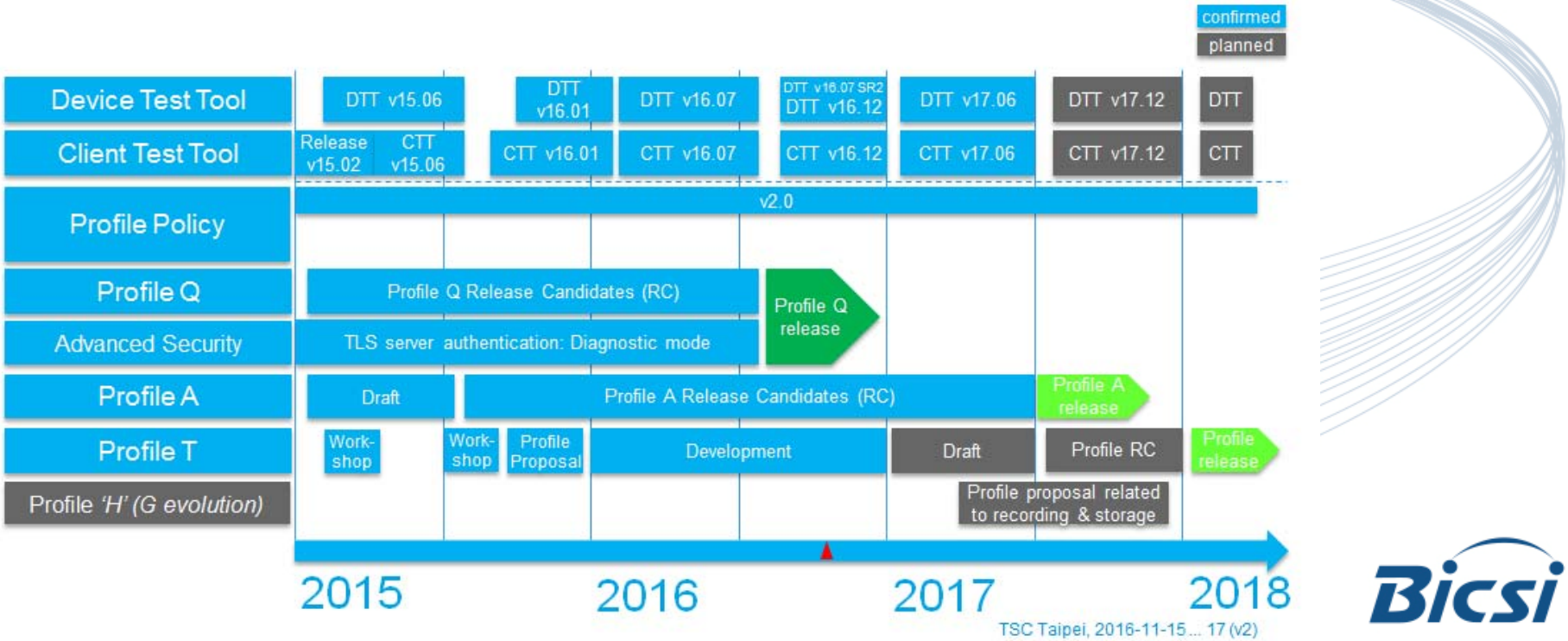
- Compression Algorithms
  - Impact on LAN and WAN
    - Remote monitoring
  - Cloud Enablement (VSaaS)
  - Impact on Enterprise Storage & Compute
- Resolution
  - Mainstream HD 720 & 1080
  - 4K, 8K, 12K…
- Market Adoption

TRENDING INTELLIGENCE

- A discussion on Analytics
  - Simple
  - Complex-METADATA
- Why do people want them?

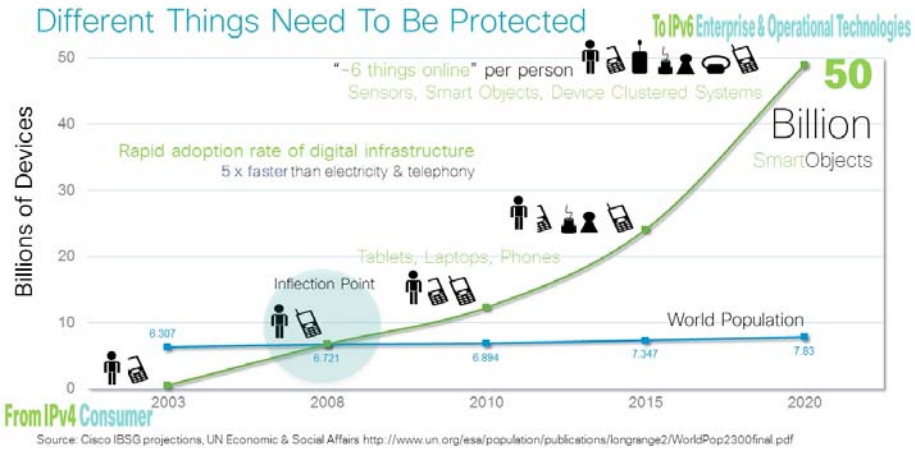
ACTIONABLE EVENTS

ONVIF TSC ROADMAP | TEST TOOLS & PROFILES



CYBERSECURITY AND IoT

- Internet has moved from the digital world to the physical world
  - OT shifting from closed systems into IP-based systems
    - Physical Security
    - Industrial Automation
    - Building Automation
- Challenges with IoT and OT
  - Multiple Protocols & Operating Systems
  - Policies & Procedures
  - Attack Surface
  - Speed of Adoption | Density
  - Maintenance

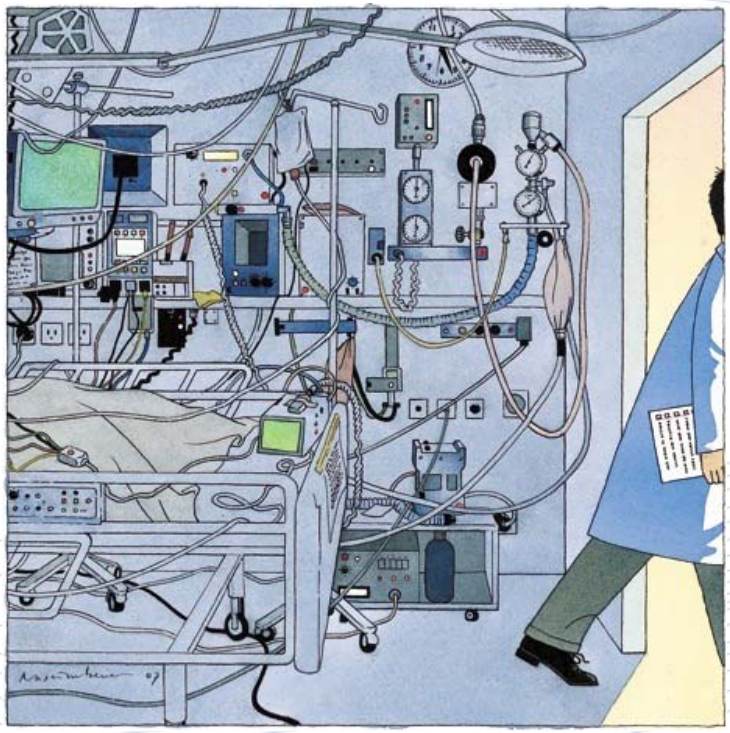


CYBERSECURITY AND PHYSICAL SECURITY

- Inherent Challenges – Breeding Ground for Cyber Attacks
  - Lack of vendor logical security awareness
  - Ownership (Operations or IT)
  - Architecture: standalone or parallel networks
  - Adoption of IT policies and procedures
  - Rapid growth in network attached devices
  - Lack of Maintenance
  - One-off Integrations
- Types of Attacks
  - Denial of Service (DoS) and DDoS
  - Malicious Data
  - Malware
  - Viruses
  - Botnets

***Mirai**, a now open-source malware strain that scans the Internet for routers, cameras, digital video recorders and other Internet of Things "IoT" devices protected only by the factory-default passwords.*

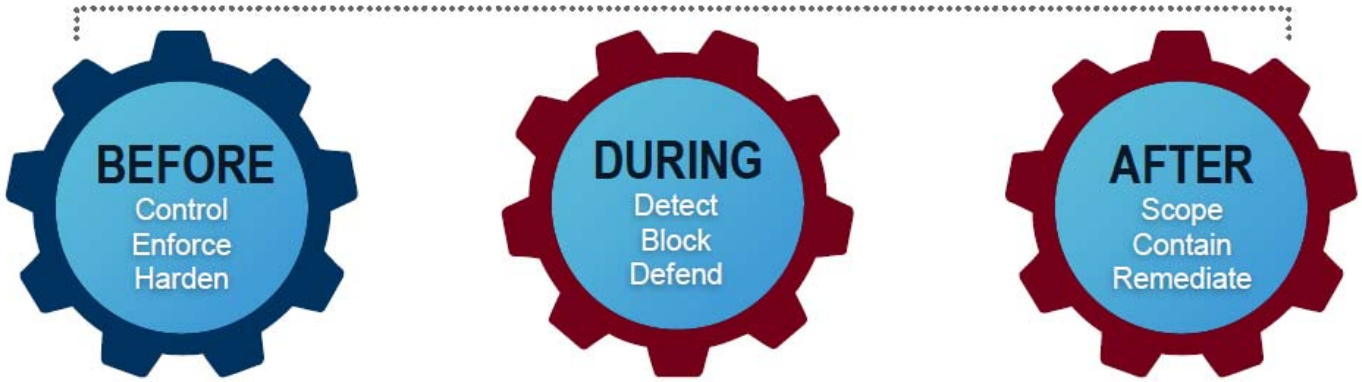
INFECTIOUS DISEASE



CYBERSECURITY

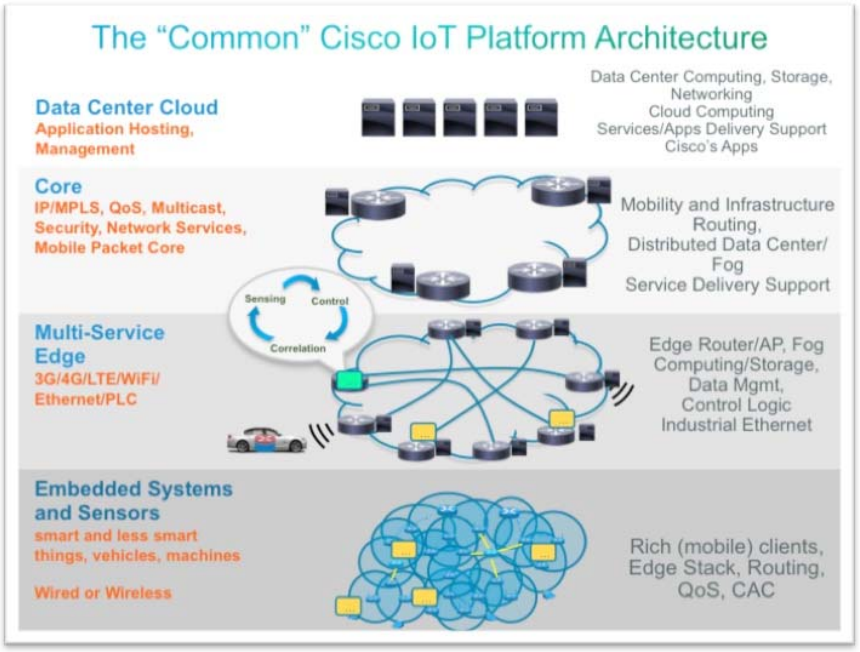
- Hardening Guides - Cameras
  - Password
  - Firmware
  - User permissions
  - Review/Reconfigure Basic network settings
  - Disable Audio as applicable
  - Enable Encryption/SSL certificates
  - Video Client Account
  - Disable IT functions
  - Set IP Address Filter
  - Configure SNMP
- Hardening of Servers, Storage, Switches
- Hardening of Sensors
- Penetration Testing

REQUIRED SECURITY MODEL FOR IoT



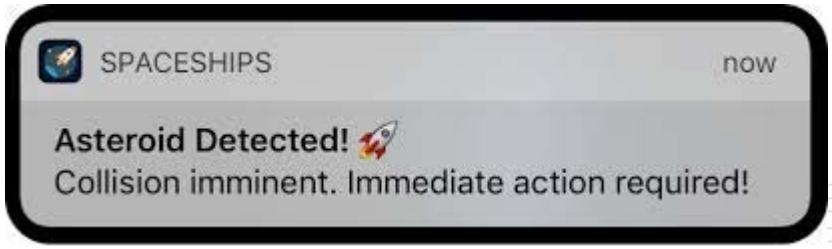
Network as an Enforcer ◀◀ Network as a Sensor ▶▶ Network as a Mitigation Accelerator

IOT


The “Common” Cisco IoT Platform Architecture
Data Center Cloud
Application Hosting,
Management
Data Center Computing, Storage, Networking
Cloud Computing
Services/Apps Delivery Support
Cisco’s Apps
Core
IP/MPLS, QoS, Multicast,
Security, Network Services,
Mobile Packet Core
Mobility and Infrastructure Routing,
Distributed Data Center/ Fog
Service Delivery Support
Sensing
Control
Correlation
Multi-Service Edge
3G/4G/LTE/WiFi/
Ethernet/PLC
Edge Router/AP, Fog Computing/Storage,
Data Mgmt,
Control Logic
Industrial Ethernet
Embedded Systems and Sensors
smart and less smart
things, vehicles, machines
Wired or Wireless
Rich (mobile) clients,
Edge Stack, Routing,
QoS, CAC

MASS NOTIFICATION

- Something is happening-what should you do?



- Ties multiple technology opportunities together

Thanks!