INDUSTRY CHALLENGES
Design, Construction, and Operation of SBIoT Systems
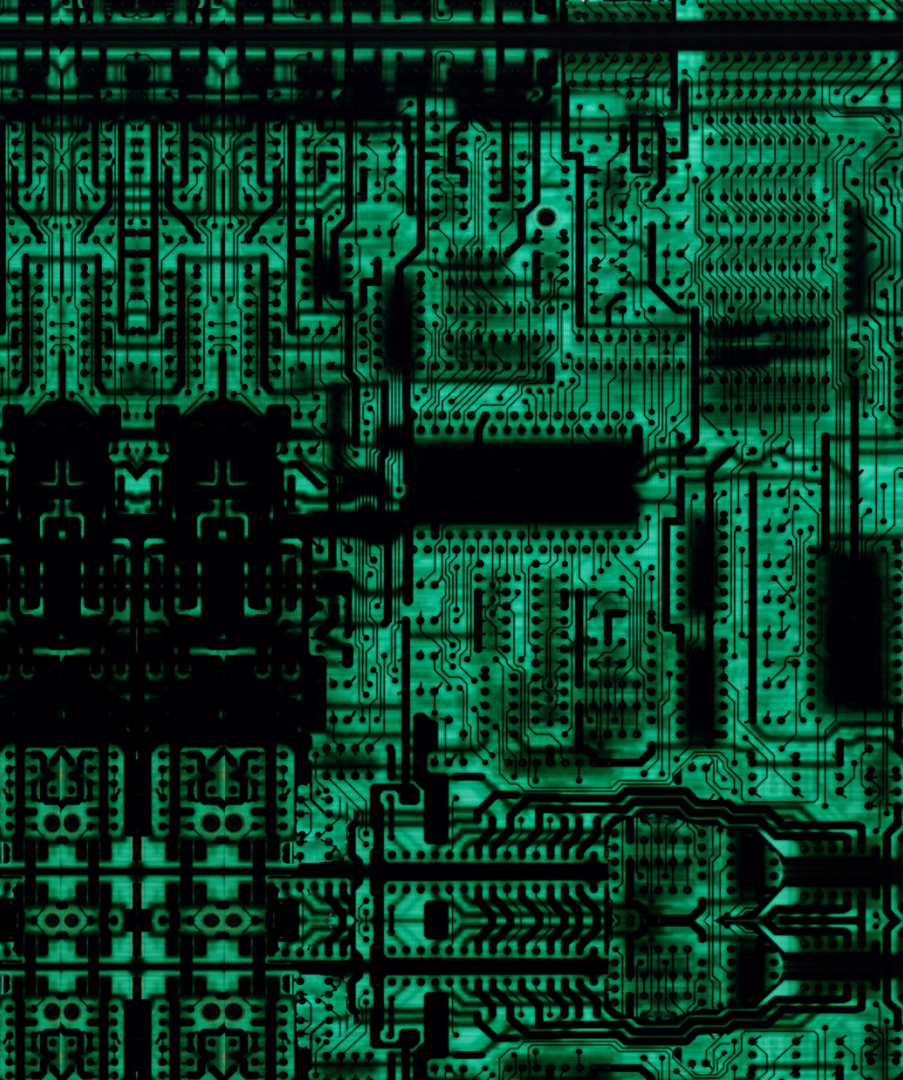
BENEFITS

SBIoT Today

- Through the Integration of Field Sensors -- Data Analytics -- Field Controllers, we can provide a more Safe and Efficient environment for people.

- Field Sensors, Controllers, and the Systems they report to may be referred to as "Operational Technology"

WHAT IS OPERATIONAL TECHNOLOGY (OT)?

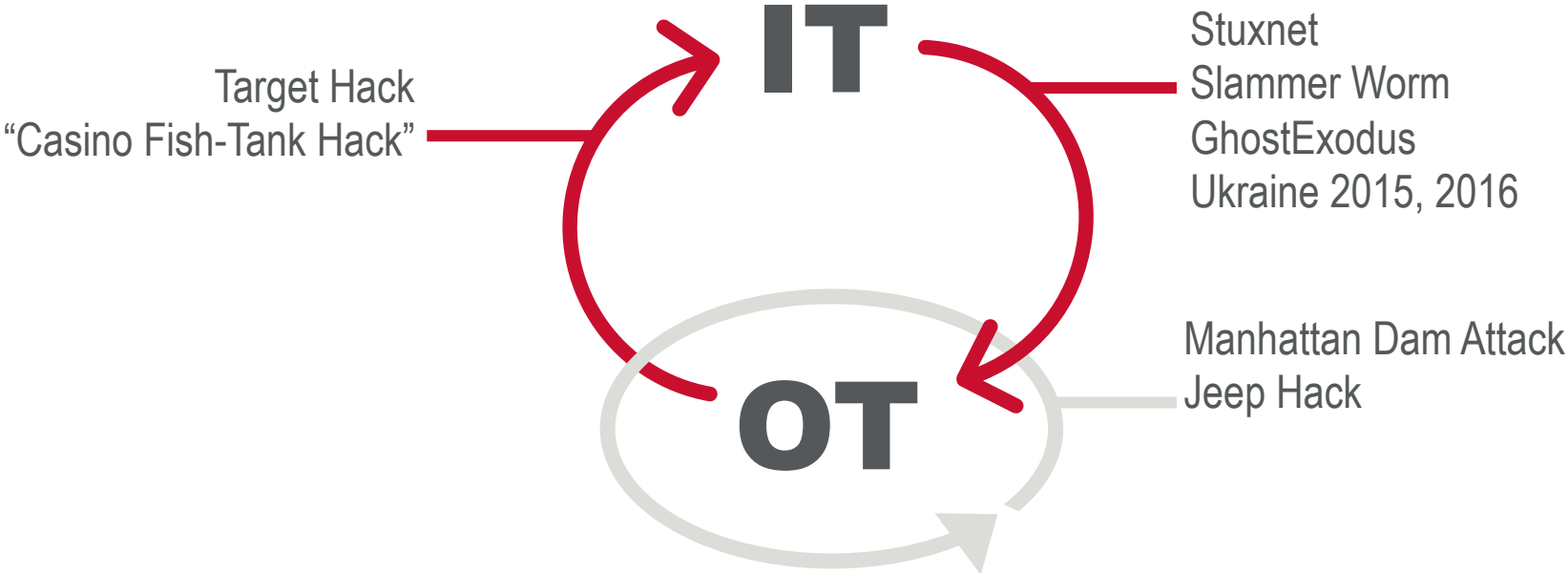*Technology which controls or operates the Physical Environment*

1. Building Management Systems (BMS or BAS)
2. Chilled Water System, Air Handling Units, VFDs, Boiler Control
3. Physical Security; Access Control and Cameras
4. Site or Building Lighting Control
5. Fire Alarm, Fire Protection, Mass Notification
6. Generator, PSG, Automatic Transfer Equipment
7. UPS, Energy Management System, Switchgear
8. Elevators, Pneumatic Tube
9. Medical Equipment (MRI, CT-Scan, Da Vinci, etc.)
10. Fuel Storage or Pumping Stations
11. SCADA, DCS, PLC, Protective Relays
12. Cars, Military Vehicles
13. Diagnostic Test & Calibration Equipment

IT AND OT DIFFERENCES

	Information Technology	Operational Technology
Protocols & Encryption	Standards	Numerous open serial protocols
Component Locations	Typically Accessible	May be poorly accessible
Support	Open	Vendor representative
Risk Management (CIA)	Data Confidentiality	Human safety, system Availability
Component Lifetime	3-5 years	10-15 years
Availability	"…server will be down 12a-6a…"	Outages planned weeks in advance
Change Management	SOP	Focus on operations
Cyber Security Awareness & Tools	Inherent	No serial based tools
Approved Cyber Component List	Typical	None

IT AND OT HAVE RELATED CYBER RISK

(SIMPLIFIED)

IT

OT

Target Hack
"Casino Fish-Tank Hack"

Stuxnet
Slammer Worm
GhostExodus
Ukraine 2015, 2016

Manhattan Dam Attack
Jeep Hack

HOW DO WE MEASURE SUCCESS INTEGRATING IT AND OT

Of a Smart Building? A Smart City? A Smart Utility System?
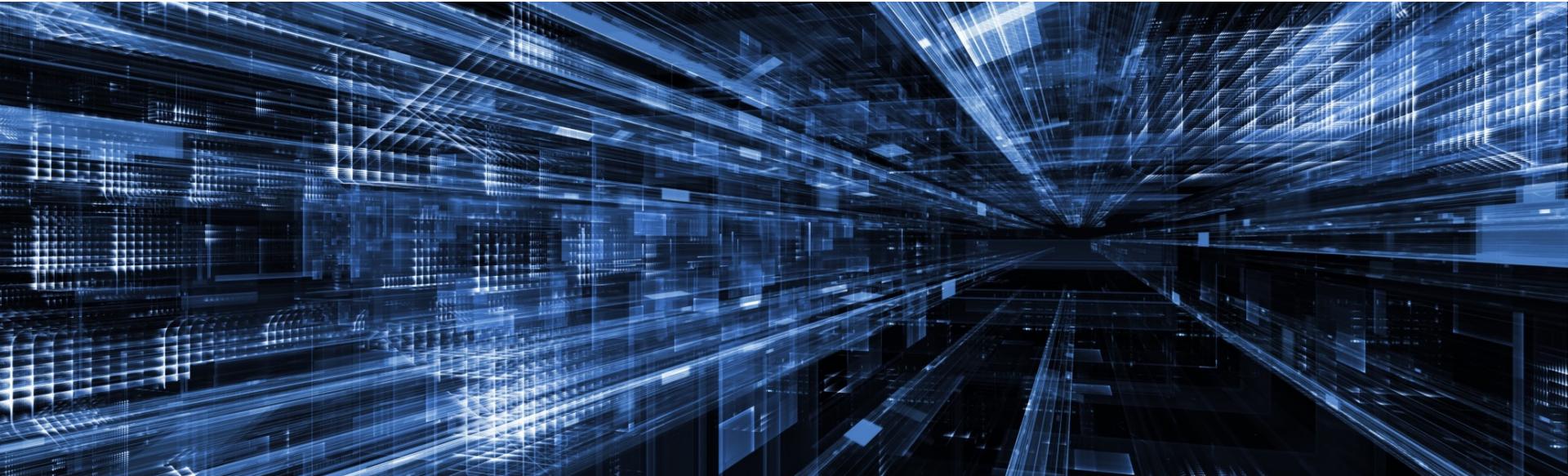
Success may be Measured by:

- The <u>Sustainability</u> of the "Smart" **use-case**
  - Does the outcome meet the expectations of the user's vision / intent / need
  - Does the use-case still work after a generation of technology (2-10 years from now)
- The <u>Cyber Physical</u> protection of the "Smart" **use-case**
  - As OT becomes more IP enabled, the Cyber-risk landscape expands
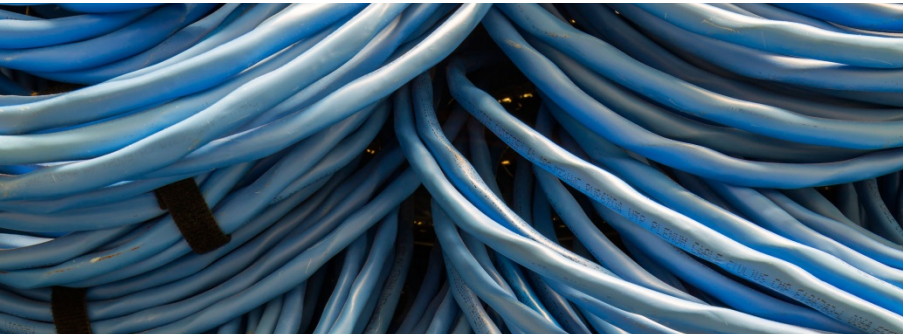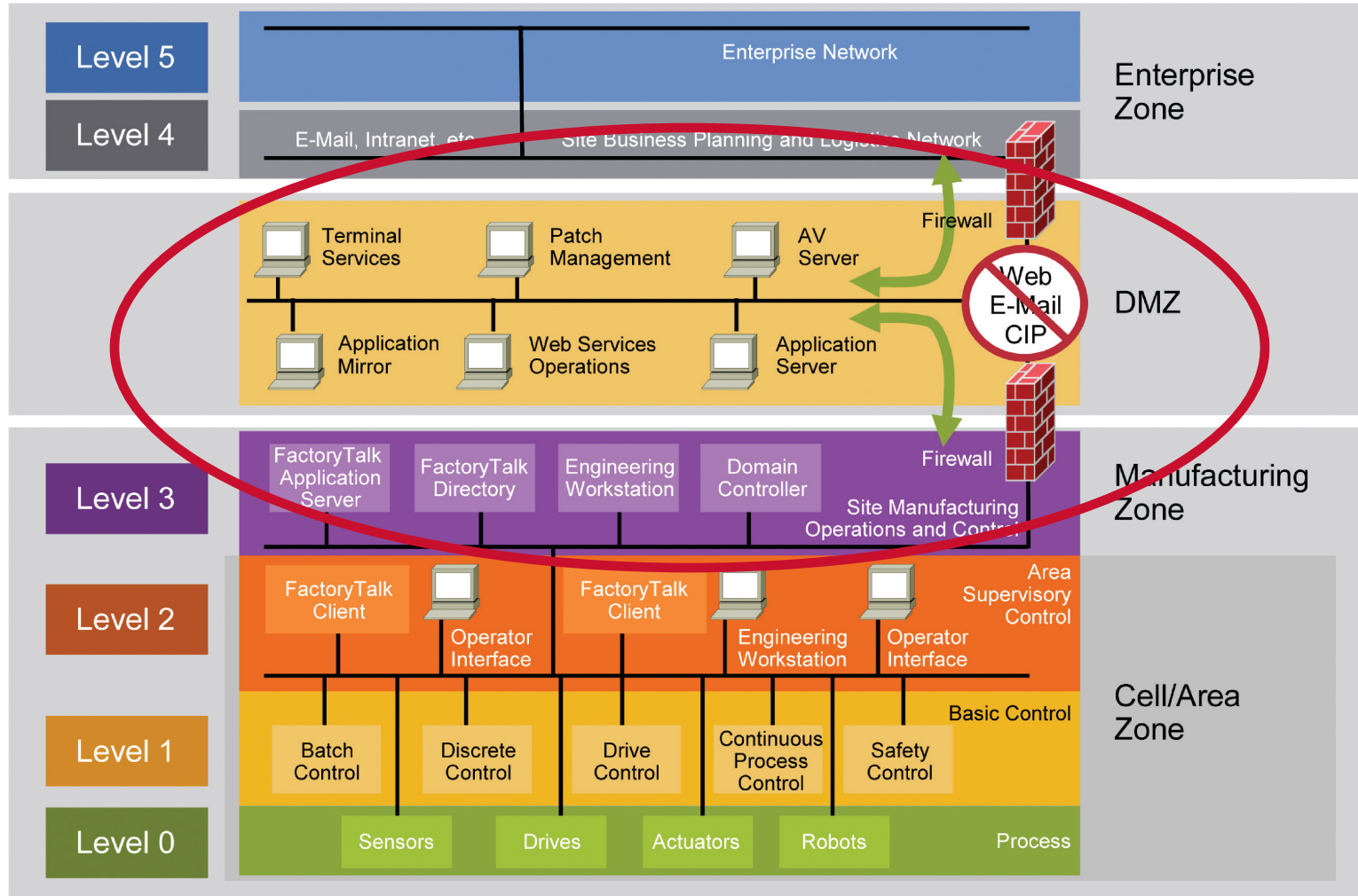
NEXT STEP

- How do we properly converge the IT and OT Networks, realizing the desired outcomes of Sustainable and Secure **Use-Cases**?
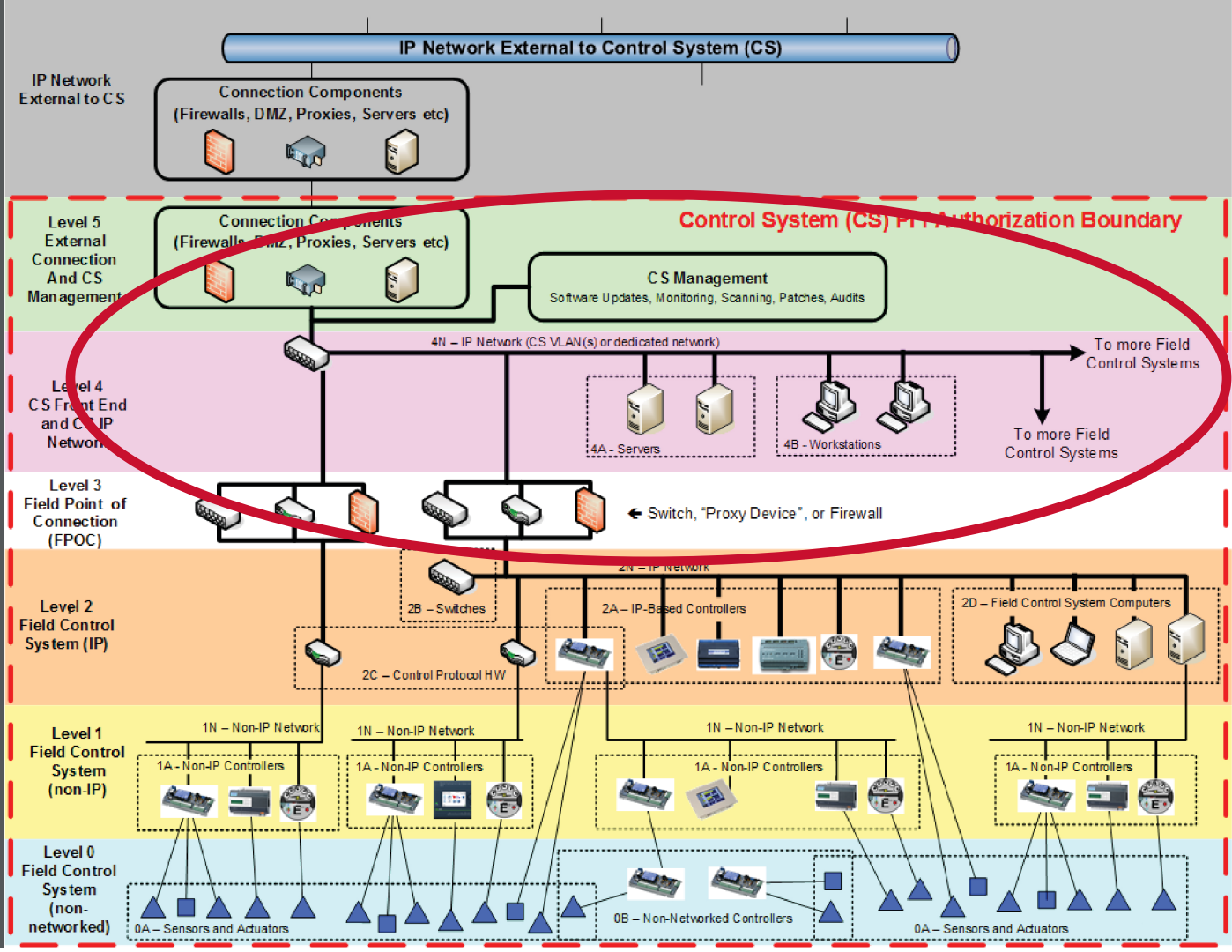 - Taking advantage of IP enabled OT devices

THE "GAP"

Level 5 — Enterprise Network
Level 4 — E-Mail, Intranet, etc. — Site Business Planning and Logistics Network
Enterprise Zone

Firewall

DMZ
- Terminal Services
- Patch Management
- AV Server
- Application Mirror
- Web Services Operations
- Application Server
- Web E-Mail CIP (prohibited)

Firewall

Level 3 — Site Manufacturing Operations and Control
- FactoryTalk Application Server
- FactoryTalk Directory
- Engineering Workstation
- Domain Controller
Manufacturing Zone

Level 2 — Area Supervisory Control
- FactoryTalk Client
- Operator Interface
- FactoryTalk Client
- Engineering Workstation
- Operator Interface

Cell/Area Zone

Level 1 — Basic Control
- Batch Control
- Discrete Control
- Drive Control
- Continuous Process Control
- Safety Control

Level 0 — Process
- Sensors
- Drives
- Actuators
- Robots

Cisco; Top 10 Recommendation for Plant-wide Ethernet/IP Deployments

THE "GAP"

UFC 4-010-06 Fig 2-1

THE CHALLENGE = THE "GAP"

The Gap is finding qualified people to Design, Build, and Operate SBIoT systems

Designer

- Finding People with the understanding of how to <u>correctly scope</u> SBIoT integrated technology use-cases, which meet user requests, and in a way which can realistically be competitively bid.

Contractor

- Finding People comfortable working outside of their technology silo's, <u>applying</u> SBIoT <u>available manufacturer technology</u> to correctly achieve use-cases, and interfacing with the Owner IT group.

Owner

- Finding People who can <u>vision</u> the implementation of use-cases, provide and enforce policies and procedures and configuration parameters, and <u>maintain</u> SBIoT use-cases for the life of the building.

THE CHALLENGE = THE "GAP"

The Gap is finding qualified people to Design, Build, and Operate SBIoT systems

Designer

- Finding People with the understanding of how to correctly scope SBIoT integrated technology use-cases, which meet user requests, and in a way which can realistically be competitively bid.
  - "Integration Dreaming" with each Owner <u>user-group</u>
  - "Integration <u>Reality</u>" with Owners leadership
  - Keeping <u>up-to-date</u> with manufacturer offerings
  - Develop <u>specifications</u> standards for successful Network designs
  - Integrated Building Systems (IBS) <u>specification</u> clearly defining contractor / manufacturer responsibility for each use-case
  - <u>Defining</u> OT Test Bed requirements

THE CHALLENGE = THE "GAP"

The Gap is finding qualified people to Design, Build, and Operate SBIoT systems

Contractor

- Finding People comfortable working outside of their technology silo's, applying SBIoT available manufacturer technology to achieve use-cases
  - Taking integration <u>methods</u> to the next level per the IBS specification.
  - Working closely with each use-case component/device <u>manufacturer</u>.
  - <u>Coordinating</u> network connections and protocols.
  - Building use-case efforts into the construction <u>schedule</u>
  - <u>Constructing</u> the OT Test-Bed at each phase of the construction schedule.

THE CHALLENGE = THE "GAP"

The Gap is finding qualified people to Design, Build, and Operate SBIoT systems

Owner

- Finding People who can vision the implementation of use-cases, provide and enforce policies and procedures and configuration parameters, and maintain SBIoT use-cases for the life of the building.
  - Network (IT/OT) rules-of-engagement <u>standards</u> for all IoT devices
  - Developing OT <u>configuration</u> requirements
  - Developing IT <u>policies and procedures</u> when interfacing with OT IP equipment (inventory standards)
  - SOP for OT test-beds, pen testing, and patching <u>procedures</u>
  - <u>Continuous</u> commission use-cases across enterprise network

ADDITIONAL OT SKILL SETS

Finding qualified persons (in addition to Designers, Contractors and Owners) with OT knowledge for:

- Technical Standards Committees
- Safe manufacturer component end-of-life replacement plan
- Manufacturer technical support
- Commissioning Agents
- Industry tool development for network optimization
- OT Network intruder alert, guard rails, and incident response software
- Test and Development Environment (TDE) – Test Bed Development Engineers
- Client based risk and defense-in-depth analysis / solutions,

THE "GAP" SKILLSETS

Embracing the Converged Network.

"…A <u>cross-functional</u> team of control engineers, control system operators, and IT security professionals needs to <u>work closely</u> to <u>understand the possible implications</u> of the installation, operation, and maintenance of security solutions in conjunction with control system operation. <u>IT and OT professionals</u> need to understand the <u>reliability impacts</u> of information security technologies before deployment …"

(part NIST 800-82 rv2)

WHAT IS OUR GOAL?

❖ Explore the benefits of smart buildings, and challenges preventing user adoption.

❖ Identifying curriculum enabling a sustainable and secure SBIoT vision.

Tim Koch

Engineering Principal

HDR

tim.koch@hdrinc.com

402-850-1824