TRIDIUM

NS2022

ACCELERATING INNOVATION

TRIDIUM

Architect and Maintain a Cyber-Secure BAS OT Framework

NS2022
ACCELERATING INNOVATION

FRED GORDY
DIRECTOR OF CYBERSECURITY – INTELLIGENT BUILDINGS

Fred Gordy is a SmartBuilding industry expert and thought leader with over 20 years of experience in secure control system development and implementation for Fortune 500 companies throughout the US and abroad. He is one of the first in the SmartBuilding industry to address the inherent risk that control system technology poses.

Fred has developed control system cybersecurity assessment methodologies and tools. He is currently a member Building Cyber Security which has been building a cybersecurity framework for building control systems based on ISA/IEC 62443.

Fred has authored over 100 articles and white papers on building control cybersecurity with industry magazines as well as the Wall Street Journal, CNBC, and Healthcare publications. In additional to publishing articles, he has been a passionate speaker and teacher, on the subject of building control cybersecurity.

NS2022
ACCELERATING INNOVATION

BILL SMITH
LEAD SOFTWARE ARCHITECT – HONEYWELL CONNECTED ENTERPRISE

Bill Smith is a lead software engineer that specialized in the Niagara product line. Bill has been a Niagara developer with Tridium/Honeywell for over 21 years and has spent the last 10+ years focusing on the cybersecurity posture of the Niagara Framework.

In addition to focusing on Niagara, Bill frequently helps by consulting for other teams and sharing his experience gained from working on Niagara. Bill is also an active member of the Honeywell Product Security Incident Response Team (PSIRT).

Bill often presents at the Niagara Summit and Niagara Forum and participates in cybersecurity discussions with local universities and focal groups.

MIREL SEHIC
GLOBAL DIRECTOR CYBERSECURITY – HONEYWELL BUILDING TECHNOLOGIES

Mirel Sehic is the Global Director Cybersecurity for Honeywell Building Technologies (HBT). Mirel has global experience working with engineering, operations, solution engineering and sales teams across various Major Hazard Facilities (MHFs) as well as critical infrastructure.

Mirel is dedicated to addressing challenges and driving new growth opportunities, capabilities, efficiencies and promoting best practice excellence ensuring productivity and performance improvements integrating Digital Operations, ICT and Cybersecurity.

Mirel is based out of Atlanta, USA and holds a Bachelor of Engineering (Mechatronics and Robotics) with Honours, and Bachelor of Science (Mathematical Modelling) with Honours from Deakin University, Australia.

TRIDIUM

NS2022
ACCELERATING INNOVATION

CYBER THREATS ARE INCREASING BY THE HOUR

Professional hackers

Accidental insiders

Script kiddies

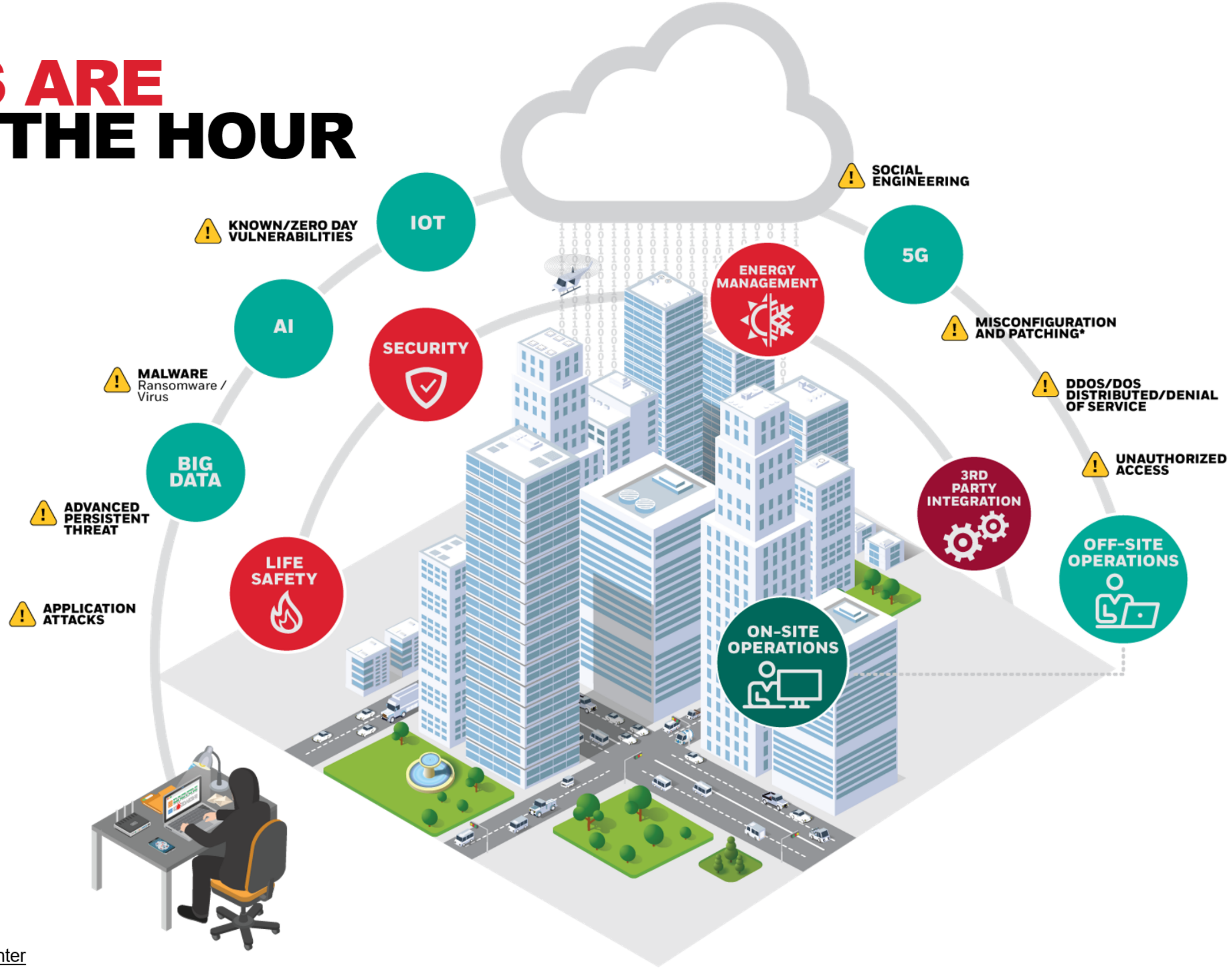
Corporate spies

Ideological hackers

Malicious insiders

Criminal hackers

Disgruntled employees



Source - Four types of Cyber attack that can take down your data center

*Misconfiguration/Patching are not types of attacks but systems that have not been updated correctly, making them vulnerable

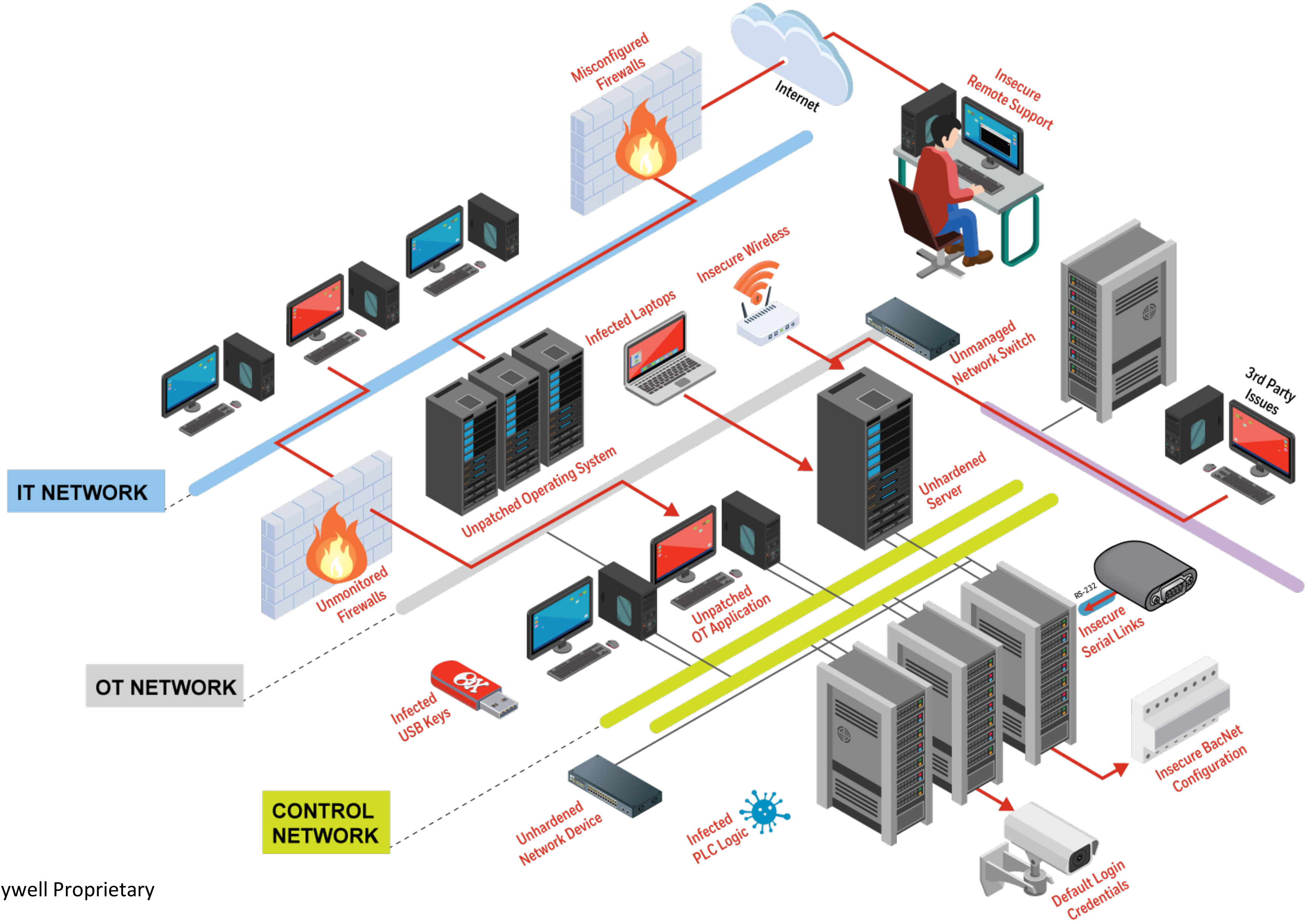
WHAT IS OPERATIONAL TECHNOLOGY (OT)?

Does Things
Controls Things
Monitors Things

OPERATIONAL TECHNOLOGY	INFORMATION TECHNOLOGY
PERFORMANCE PRIORITIES	
Low Bandwidth	High Bandwidth
Real-Time	Delay Tolerant
AVAILABILITY	
Outages: Not Acceptable	Rebooting: Bad But Doable
Redundancy Required	Retrievable Back-up Acceptable
RISK	
Human Safety	Data Integrity
Property Safety	Data Security
OPERATORS	
Control Engineers With Content Skills	IT Staff With Systems Skills
Network Design By Process Engineers	Dedicated Network Designers
CONSTRAINTS	
More Specific Hardware	Flexible Hardware
Security Not Primary	Easy Security Updates
Specialized Communications Protocols	Industry Standard – TCP/IP
MAINTENANCE	
Single Vendor Support	Multiple Support Sources
10 to 15 Year Component Life	3 to 5 Year Component Life
Remote Components, Hidden Access	Modular, Accessible Components
Updates Carefully Planned and Tested	Frequent Patches And Updates
No Full-Time Dedicated IT Staff	IT Staff or Service Contract In Place
SECURITY PRIORITY	
Availability, Integrity, Confidentiality	Confidentiality, Integrity, Availability

Protects Data
Stores Data
Manipulates Data

Source:
[1] Frontiercomputercorp.com/industrial-iot



Honeywell Proprietary

11:25 AM Eastern

WHY TARGET OT SYSTEMS?

THEY ARE OFTEN EASY

- OT Systems have longer lifespan than IT System
- Contains legacy, unsupported and unmaintained systems
- Common communication protocols can potentially be designed without security
- Default accounts and passwords are common
- OT is unsupported by IT hence not updated or protected due to lack of awareness, budgets and know-how

CAN DO A LOT OF DAMAGE

- Disruption of OT systems can cause catastrophic outcomes in business-critical systems
- Often contain a lot of sensitive data (e.g., employee and patient information)
- OT environment can be used to access IT environment (e.g., shared accounts and internal systems)

SOME OF THE **MOST WELL KNOWN CYBER INCIDENTS** RELATE BACK TO CONTROL SYSTEMS

BCS Mission

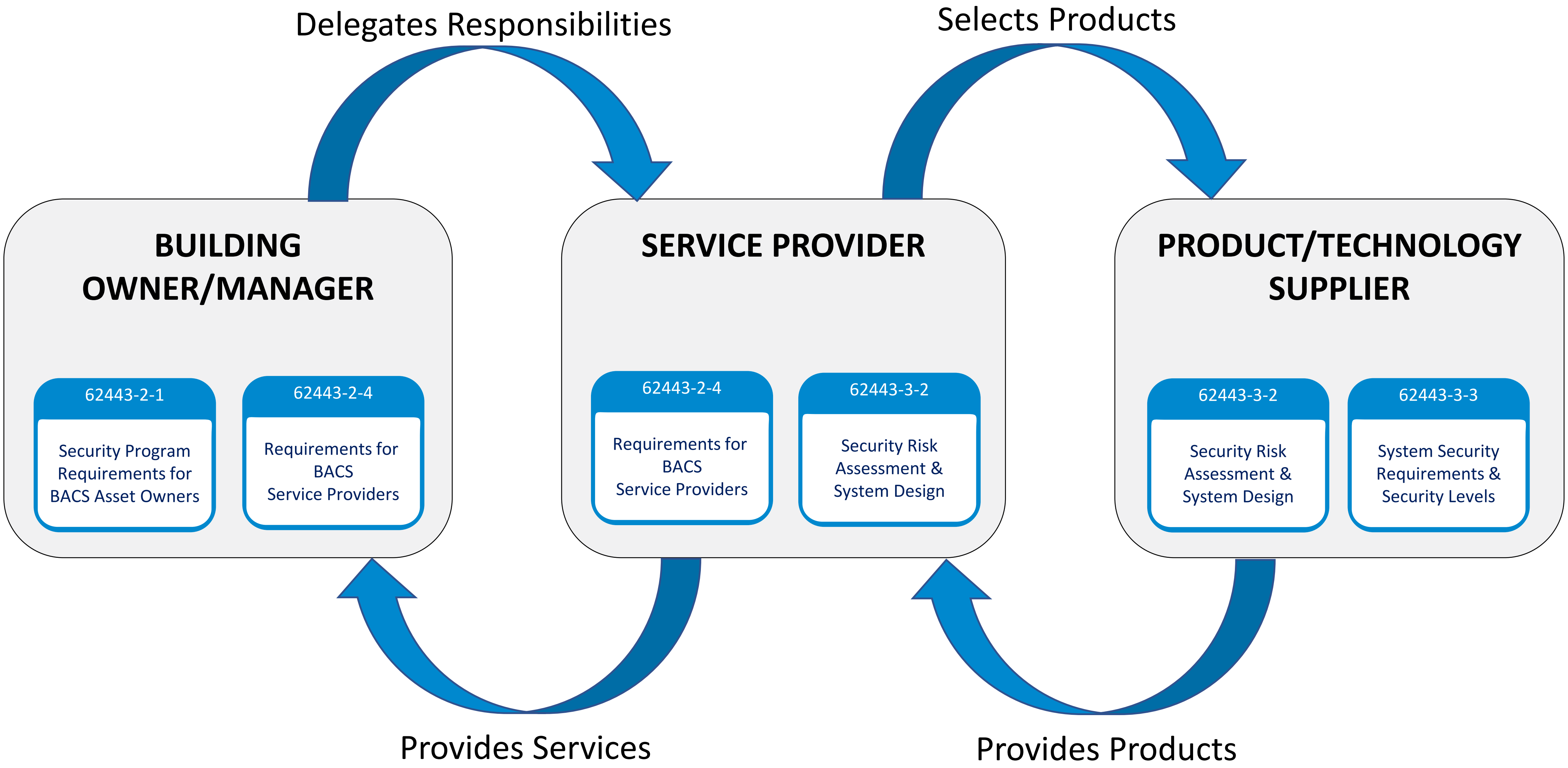
Establish and sustain frameworks developed by stakeholders across multiple sectors and administered by a non-profit organization offering market-driven options to promote cyber protections in controls and devices for enhanced physical security and safety in an increasingly smart world.

BCS Vision

Building Cyber Security (BCS) will be the premier global administrator certifying operational technologies, processes, training, and recovery plans for safe, secure use of controls and devices.

BUILDING Cyber Security

ROLES AND RESPONSIBILITIES



Delegates Responsibilities

Selects Products

BUILDING OWNER/MANAGER

62443-2-1

Security Program Requirements for BACS Asset Owners

62443-2-4

Requirements for BACS Service Providers

SERVICE PROVIDER

62443-2-4

Requirements for BACS Service Providers

62443-3-2

Security Risk Assessment & System Design

PRODUCT/TECHNOLOGY SUPPLIER

62443-3-2

Security Risk Assessment & System Design

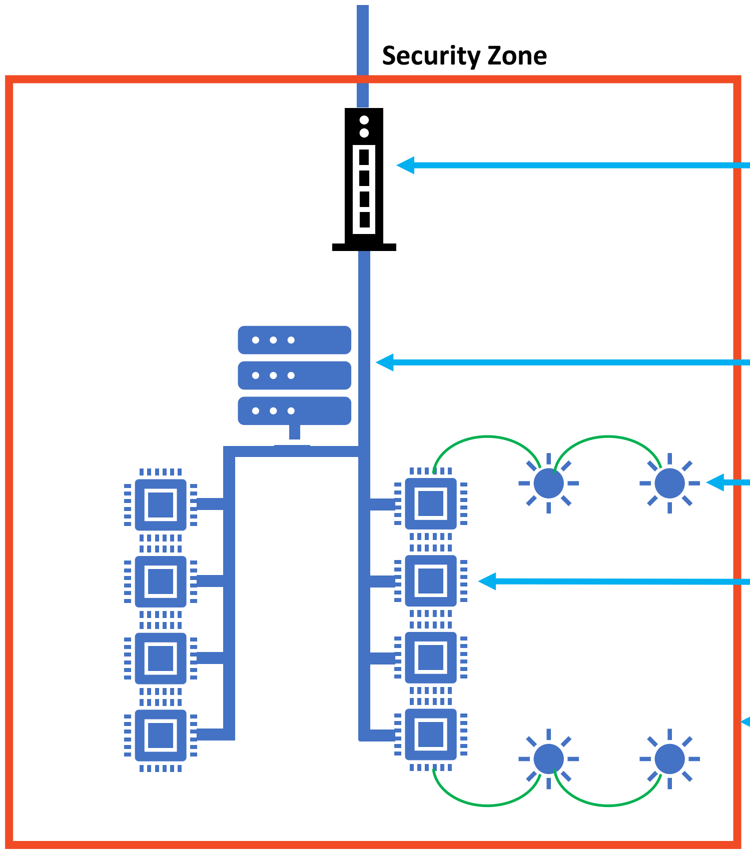
62443-3-3

System Security Requirements & Security Levels

Provides Services

Provides Products

REFERENCE MODEL SECURITY ZONE



Zone Access Point

Accessibility Types

1. Low (e.g. physical access, no network)
2. Moderate (e.g. physical access, network to/from OT zones)
3. High (e.g. physical access, network to/from IT zones)
4. Very High (e.g. physical access, network to/from internet)

Host Device (e.g. Windows/Linux PC/Server) – **Software Application** (e.g. front-end)

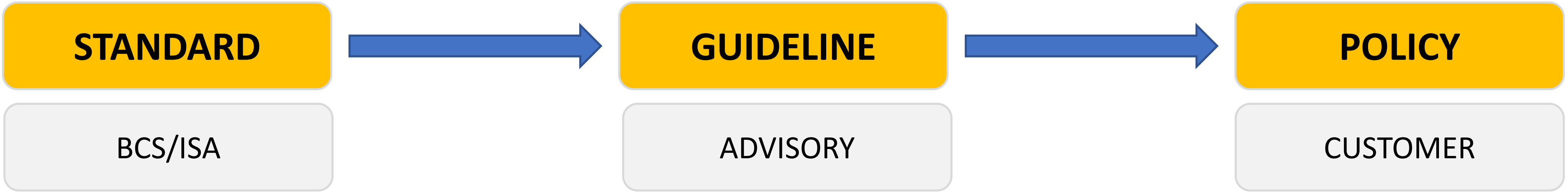
Embedded Device (e.g. field controller)

Network Device (e.g. supervisory controller)

Security Zone

1. Set of assets with common security requirements
2. Similar to network segmentation)

STANDARDS, GUIDELINES, & POLICIES



STANDARD

BCS/ISA

- Cannot be changed except by ISA/BCS
- Not to be shared with customer unless specifically designated in the SOW

GUIDELINE

ADVISORY

- Adaptation of Standard without changing the intent of the Standard
- Takes in consideration the needs of the customer
- Customer may not use all requirement groups or individual requirements for their Guidelines

POLICY

CUSTOMER

- Customer responsibility to create and maintain
- Adopts IB provided Guidelines in existing Policy or creates new Policy
- Policy is only relatetable to the Standard if the intent of the Standard is maintained

PRODUCT CYBERSECURITY

Cybersecurity During Development

- Threat Modeling
- Static Code Analysis
- Third Party Component Scanning
- Code Reviews
- Unit Testing / Code Coverage
- Penetration Testing
- What else?

NS2022

ACCELERATING INNOVATION

PRODUCT CYBERSECURITY

What do you do post release?

- Help with customer education
- Periodic internal review (products and processes)
- Response to reported findings
  - Product Security Incident Response Team (PSIRT)
  - Incident review and assessment
  - Planned mitigations
  - ICS-CERT and notifications
- Plan for Product EOL

TRIDIUM

PRODUCT CYBERSECURITY

Engineering Buy In – part of the culture

Customer education

Secure by Default

NS2022

ACCELERATING INNOVATION

CHARLOTTE, NC | APRIL 4-6

Takeaway Recommendations
To Keep Secure

1. Don’t forget about OT cybersecurity
2. Ensure appropriate ICT/Cyber hygiene - AV, Backups, Patch Management, Password Management, Logical Separation, Control Removable Media
3. Look for ‘Unknown’ internet connectivity
4. Raise awareness and educate system users
5. Review OT systems best practices (NIST, ICS-CERT, AUSCert)
6. Recognise the need, and ask more from your OT supplier, ask about your OT Cybersecurity and conduct a Cybersecurity Assessment

TRIDIUM