HDR

Mitigating Healthcare MEP Cyber Risk

HDR

10/5/2023

Speakers

David Brearley, CISM, GICSP, PMP

Operational Technology Cybersecurity Director

David.Brearley@hdrinc.com

Scott Klawitter, PE, LEED AP BD+C

Sr Electrical Engineer/Electrical Section Lead

Scott.Klawitter@hdrinc.com

Tim Koch, PE

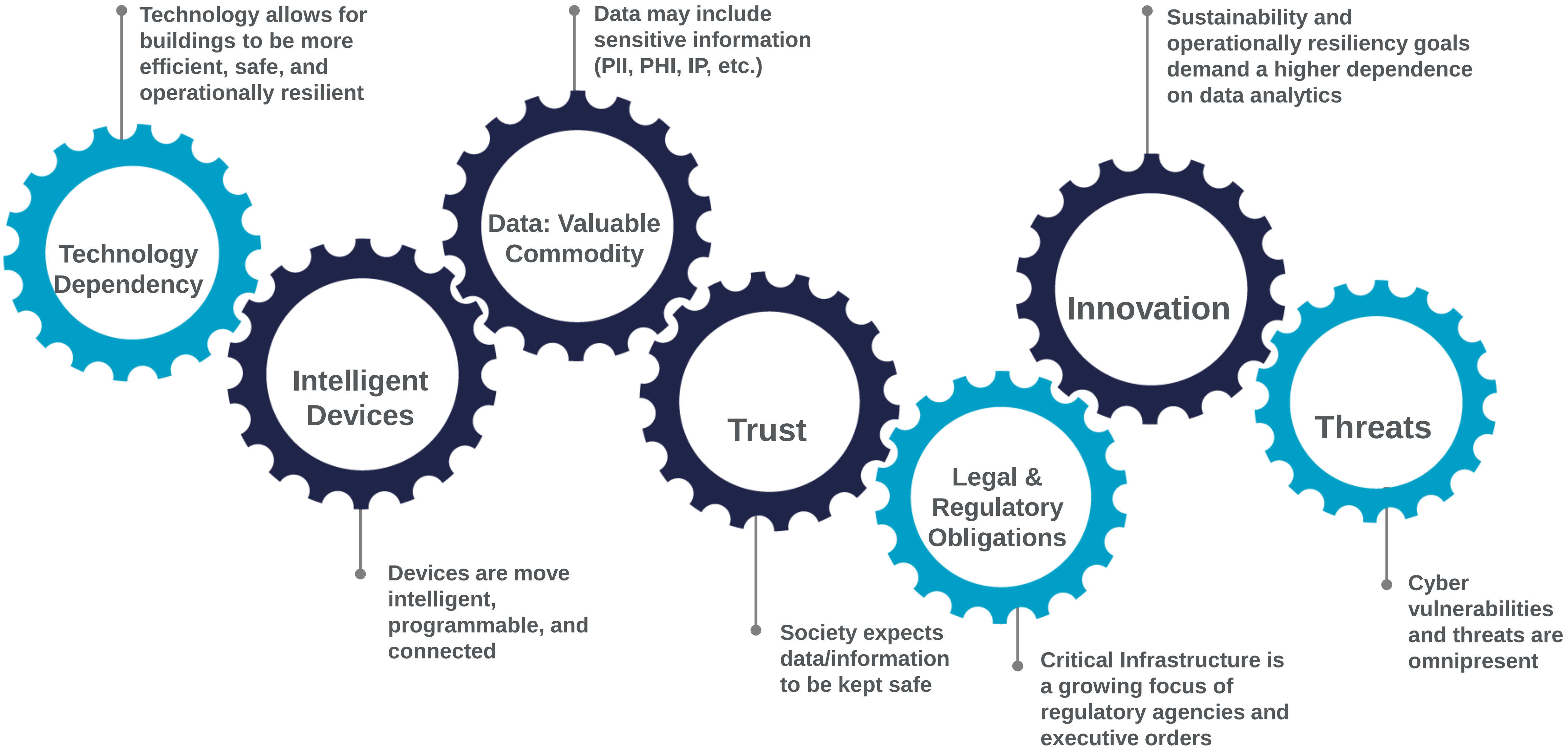
Engineering Principal

Tim.Koch@hdrinc.com

Agenda

1. Impact of Cybersecurity on Design
2. MEP vs. Cyber Design Effort
3. Framework for Inclusion of Cyber In Design
4. Q&A / Panel Discussion

Cyber Risk Increases with our Dependence on Building Technology



Technology Dependency

Technology allows for buildings to be more efficient, safe, and operationally resilient

Intelligent Devices

Devices are move intelligent, programmable, and connected

Data: Valuable Commodity

Data may include sensitive information (PII, PHI, IP, etc.)

Trust

Society expects data/information to be kept safe

Legal & Regulatory Obligations

Critical Infrastructure is a growing focus of regulatory agencies and executive orders

Innovation

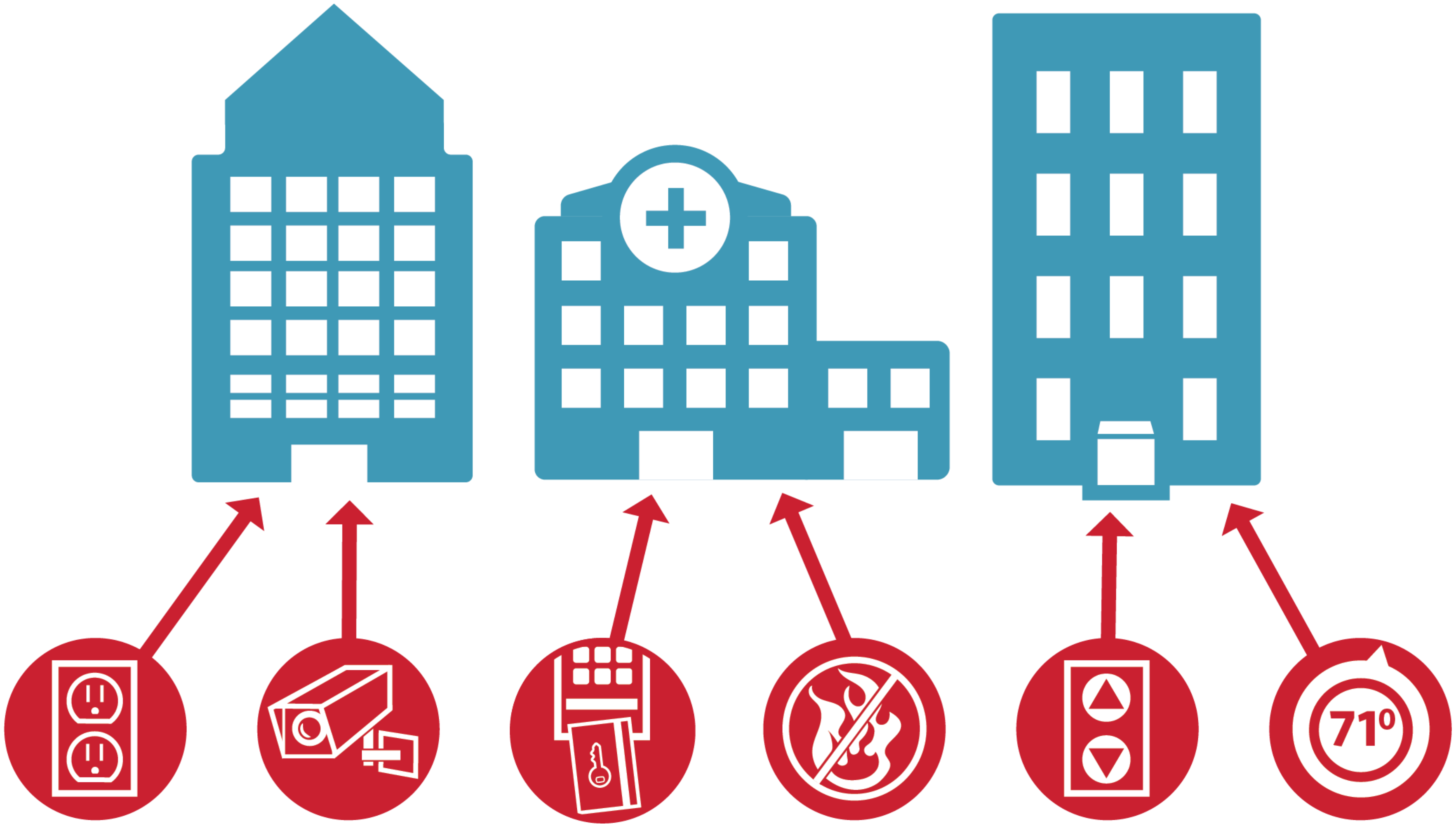
Sustainability and operationally resiliency goals demand a higher dependence on data analytics

Threats

Cyber vulnerabilities and threats are omnipresent

More Technology = Wider Threat Surface = More to Monitor, Defend & Maintain

Cybersecurity Threats to Facilities



- Medical Gas
- Wayfinding
- Wastewater Treatment
- Emergency Generators
- Rainwater Harvesting
- Automated Blinds
- Photovoltaic Systems
- Occupancy Controls
- Geolocating / Tracking
- AGVs
- Lighting
- Nurse Call
- Paging
- Pneumatic Tube
- Digital Signage
- Fume Hood
- Water Purification
- Leak Detection
- Parking Systems

- Many more…

Confidential Client Example

Market Sector: Healthcare

Cyber Identified as Tier-2 Risk

2,000,000 Attacks/Day on Firewalls

- 250+ per second
- Over 700,000,000 attempts per year

Risks Identified:

- Patient Records
- Patient Orders and Ordering Systems
- Billing Systems

Purpose

Cyber Design and Cyber-Ready Design mitigates risk

Cybersecurity is risk management; we cannot eliminate risks, but these processes are put in place to assist owners to mitigate their risks.

A cyber ready design includes the necessary information for a cyber protection engineer to put cybersecurity measures in place, note;

- ➢Cybersecurity is life safety; consider a cyber disabled fire protection, medical gas, or emergency generator system
- ➢Cybersecurity protects facility operations; consider a cyber disabled elevator bank, food service, or water system

Cyber Terminology

- **Operational Technology (OT);** any building component/system that can be programmed

- **Data-Flow**; shared data between two devices

- **Use-Case**; a statement (business case) to identify the purpose for data flow between two building systems

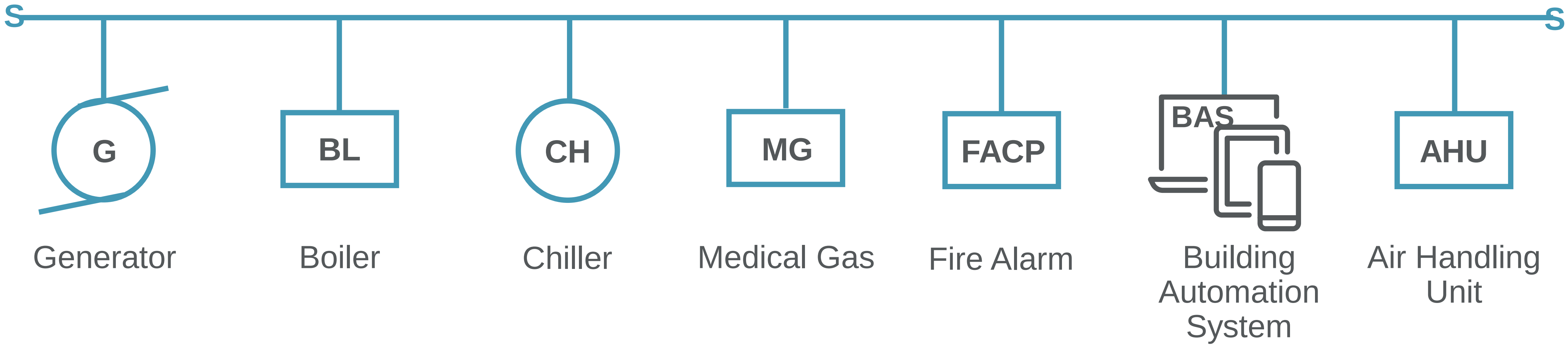
- **Outcome**; a set of use-cases to achieve an energy efficient, safe, and operationally resilient building

- **Integrated / Smart Building**; sharing OT data to achieve building system outcomes at any level

Integrated Building

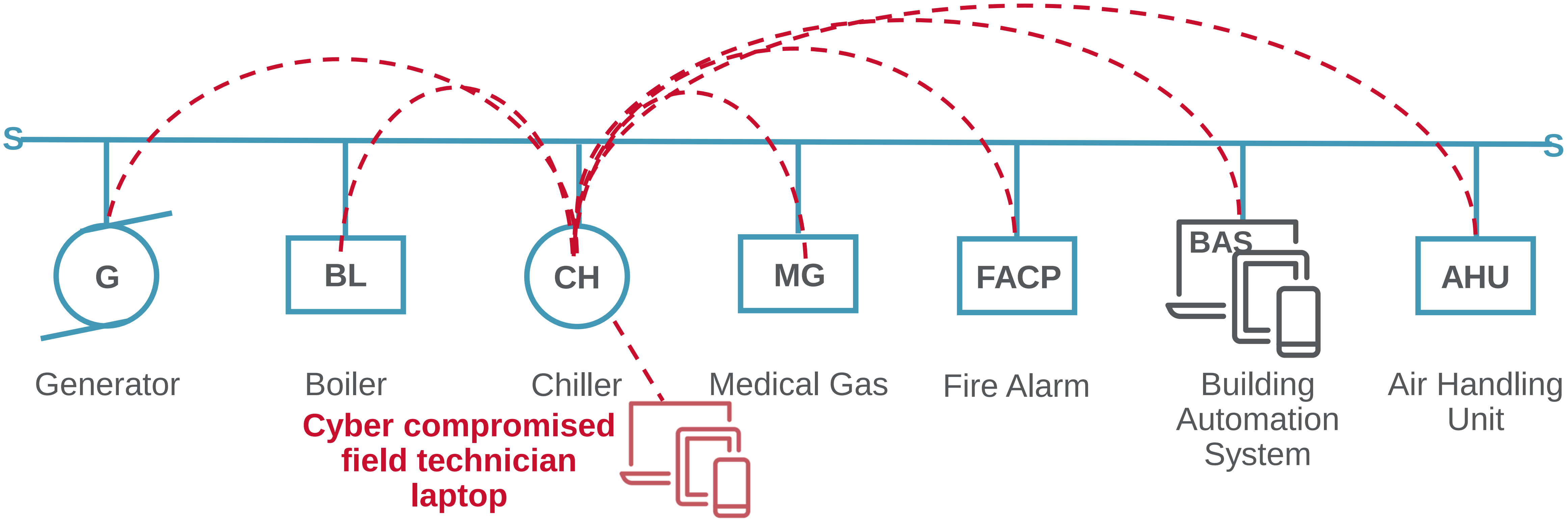
Today's buildings share data over the Operational Technology (OT) network to achieve outcomes necessary for an energy efficient, safe, and operationally resilient building

Example of a flat (or open) OT network



Integrated Building

Example of a **cyber compromised** flat (or open) OT network*



Malware from a field technicians' laptop can pivot through the Chiller control panel and has access to any other system on the flat (or open) OT network.
The malware may install ransomware, disable life safety systems, silently collect data, etc.

Standardized Approach

Planning

- Establish stakeholders, roles and responsibilities
- Establish a vision for project cyber requirements (cyber project plan)

Schematic Design

- Identify Operational Technology Systems
- Develop Use-Cases

Design Development

- Finalize Use-Cases
- Procurement Requirements
- Specifications to support cyber mitigations, configuration and documentation

Construction

- Shop Drawings: Asset Inventory, Network Diagrams, IP Addresses, etc
- Test Bed Environment – shop test
- Defined coordination with stakeholders

Substantial Completion

- System Back-ups
- Training
- Integration with Owner Monitoring and Maintenance Systems
- Cyber Commissioning – validation of security and network configuration

Basic Services Requirements (The “What”)

- Comprehensive Asset Inventory (Hardware/Software)
- Firmware Updates prior to commissioning
- Default Username and Password Updates (coordinated with owner)
- Graphical / Interactive Displays – password protected for functionality
- Documented Turn-over of Backups (software, configurations, etc – necessary for recovery)
- Specification and Plan Requirements

Plans and Specifications

Specifications with cyber language

- OT network and network component guidelines (25.10.00)
- Cyber hygiene requirements (in MEP specs with programmable devices)
- OT inventory-of-device list (25.55.00 attachment)

A data-flow tool (use-cases) (On plan sheet)

- Consider a use-case matrix or section dedicated to use-cases
- Confirm best practices data flow methods (data diodes, hard wired, etc.)

Developing Use-Cases for System Interactions

	25 55 00 Integrated Building Technology																			
	--- Use-Case Matrix																			
		Fire	Plumbing	Fuel Oil	Fan Coil	Medical	Smoke	HVAC		Feedwater			Cooling	Energy	Air	ATU	BMS	CO		Bldg
		Protection	Pumps	System	Unit	Gas	Damper	Pumps	Fans	System	Boilers	Chiller	Tower	Recovery	Handlers		Equipment	Control	VFD	Mgmt Sys
		21.10.00	22 11 23	23 12 00	23 82 39	22 60 00	23 31 13	23 21 23	23 35 00	23 54 16	23 52 00	23 64 16	23 65 13	23 72 00	23 73 00	23 36 00	25 30 00	25 21 00	25 23 00	25 50 00
		FP	P Pmps	FO	FCU	MG	SD	Pmps	Fans	FW	Blrs	Ch	CT	ERV	AHU	ATU	Mon	CO	VFD	BMS
1	Fire Pumps and Fire Alarm Bells; see FA Matrix	FP																		
2	Plumbing Pumps; see BMS spec		P Pmps																	BMS
3	Medical Gas Alarms; see Med Gas spec					MG														BMS
4	Smoke Damper shutdown; see FA Matrix						SD													
5	Hydronic Pumps; see BMS spec							Pmps												BMS
6	Fan Shutdown; see BMS spec / FA Matrix								Fans											BMS
7	Smoke Control; see BMS spec / FA Matrix																			BMS
8	Boiler Shutdown; see BMS spec										Blrs									BMS
9	Boiler Plant Sequence of Operation; see BMS spec									FW	Blrs									BMS
10	Chiller Shutdown; see BMS spec											Ch								BMS
11	Chiller Sequence of Operation; see BMS spec											Ch								BMS
12	Chiller Sequence of Operation on Generator Power; see BMS spec											Ch								BMS
13	Chiller Sequence of Operation on Reduce Gen Power; see BMS spec											Ch								BMS
14	Cooling Tower Shutdown; see BMS spec												CT							BMS
15	VFD Control; see BMS Spec																		VFD	BMS
16	AHU Control; see BMS Spec														AHU					BMS
17	AHU shutdown; see FA Matrix														AHU					BMS

Cyber Protected Integrated Building

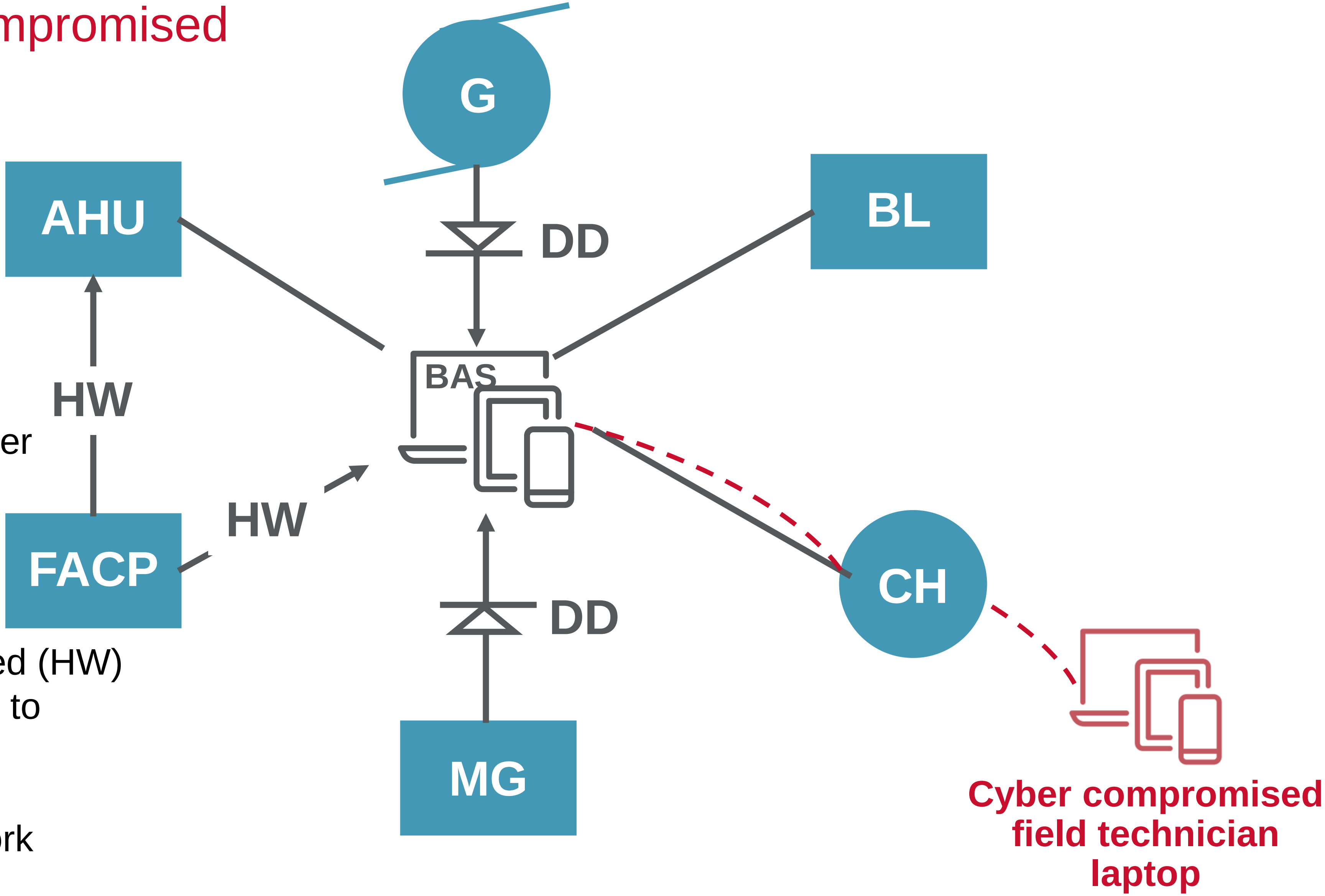
Example of a Cyber Compromised OT network*

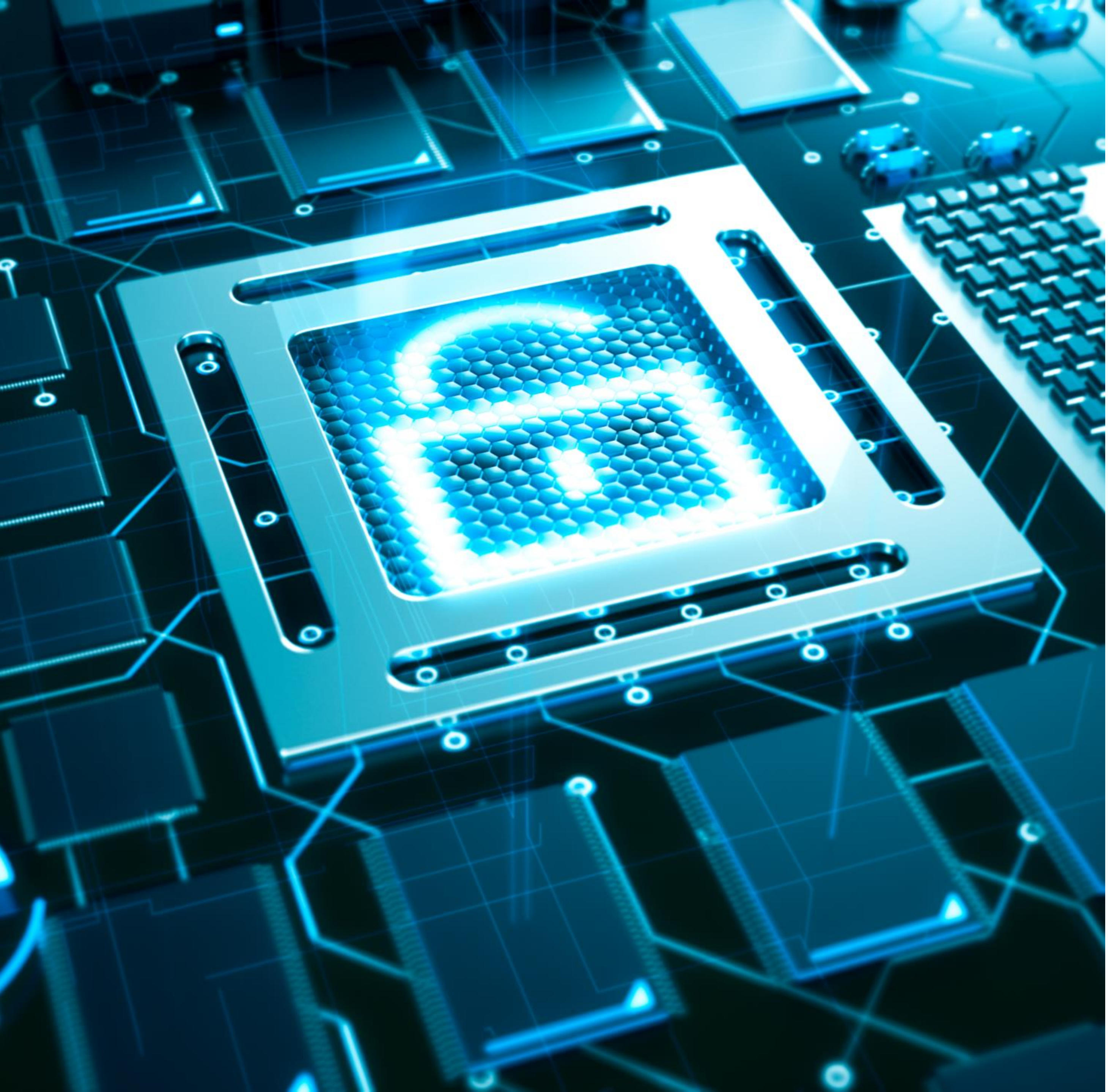
Malware from a field technicians' laptop needs to pivot through Chiller control panel and the BAS to gain access to other Building OT systems

There is no use-case for the chiller to data share with the boiler therefore, there is no direct network connection

Data Diodes (DD) and Hard Wired (HW) do not allow data-write capability to life-safety systems

*Where the BAS is the OT network





Add Services Cyber Scope (The “HOW”)

- Development of specific cybersecurity requirements to adhere to recognized industry standards
- Design of zero-trust solutions
- Risk Management Framework consulting to assist owner with developing a cost/risk balanced solution to OT security
- Validation of installed system (Cyber Cx)

Food for Thought/Takeaways:

- Generators - Stand Alone or Connected to BMS?
- WIFI capable devices. – Disable Bluetooth Capabilities?
- Lighting Control System Integration – Stand Alone or Connected to BMS?
- Power Monitoring Integration – Stand Alone or Connected to BMS?
- UPS Systems – Allow Remote access or Connected to BMS?

Questions & Panel Discussion

David Brearley, CISM, GICSP, PMP

Operational Technology Cybersecurity Director

David.Brearley@hdrinc.com

Scott Klawitter, PE, LEED AP BD+C

Sr Electrical Engineer/Electrical Section Lead

Scott.Klawitter@hdrinc.com

Tim Koch, PE

Engineering Principal

Tim.Koch@hdrinc.com