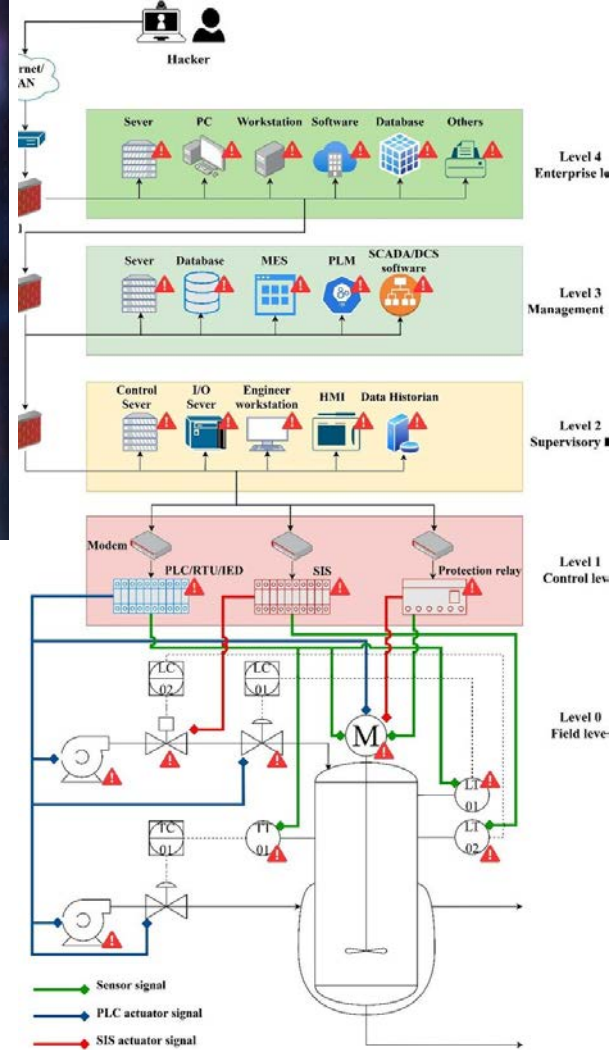
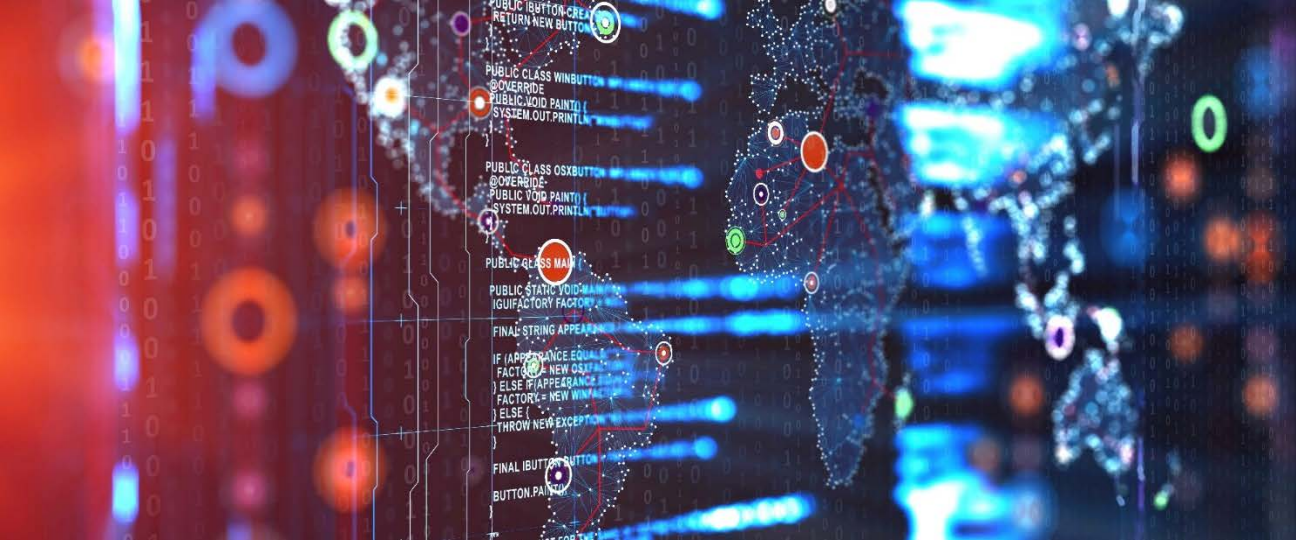




Cybersecurity – Bridging the Engineering Gap

Presenter



Jeff Monforton

Senior Cybersecurity Specialist

jeffrey.monforton@hdrinc.com

Office: 205.635.9017

Cell: 850.293.6999



Learning Objectives

- Why is this Important during the Design Phase?
- How Does it Work?
- How are the QMP requirements Different from the Typical QC Process?
- What Does it Require?



CYBERSECURITY – What is it for?

- Preventing Unauthorized Access
- Protecting Data and Privacy
- Mitigating Risks
- Securing Critical Infrastructure

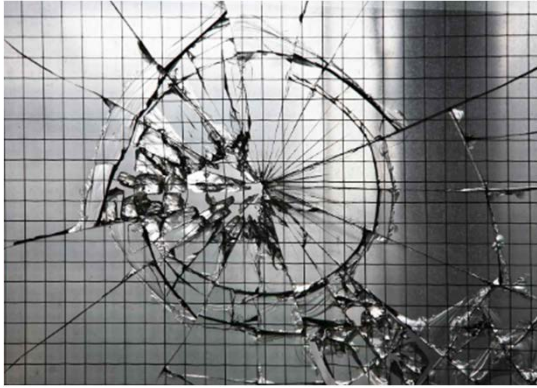
To name a few...

In Summary, it is essential for protecting digital assets, ensuring integrity and availability of information, and maintaining trust of individuals and organizations in the digital world



CYBERSECURITY – What is it for?

In the 'Real World' what are the things that an adversary is looking for?



Cybersecurity is looking for the cracks in the system.

Places where joints don't meet



Typical Design Approach

Mechanical, Controls, Electrical, Fire & Life Safety (FLS), Telecom, & security often perform their designs in a silo.



However, these designs are also dependent on one another.

- Telecomm provides design of the backbone (WAN) for the Controls Network.
- Electrical provides the design to power field systems/devices for all other systems.
- Mechanical designs the HVAC, Plumbing, etc.
- Controls designs for the monitoring and control of all systems, whether isolated or interconnected. This often includes a connection to a campus wide UMCS.
- Security designs for IDS, ACS, alarms, etc.
- Cybersecurity must design for HOLISTIC protection of ALL of these systems.
Often with little shared info on the systems under design.

Ways That Systems Interconnect/Interact That Are Not Always Obvious or Communicated

- ❖ The Fire Life Safety System (FLS) affects control over the HVAC during active alarms to provide ventilation or control circulation based on alarm zones.
- ❖ The Electrical System may have AMI which is part of the UMCS
- ❖ The FLS connects/interacts with the Telecom system to send alarm status to fire department (Often separate from the normal WAN path, may be wireless or cellular)
- ❖ The Electronic Security System (ESS) may interact with the Telecom systems to send text or email alerts to key staff.
- ❖ Etc.



In Design – What often Happens?

Meters are called out, but not connected to Controls or AMI systems.

Critical drop locations are missed.

Device connections are not indicated.

Devices are not defined in tables for the UMCS.

Designs are often copied from “something close”.

Design elements are left for the contractor to work out as Deferred Design.



In Construction – What Happens?

Contractors issue RFIs – This impacts delivery time.

Contractors work it out themselves – The Path of Least Resistance is generally chosen.

From an Engineering perspective - Do they always choose the BEST path?

Without guidance, are all Implementation Details captured on the drawings?

What becomes Tribal Knowledge?

Information is simply Lost.

There is a cybersecurity tenant –

“You can ONLY protect what you know you HAVE.”



How can Some of these conditions be Addressed?

Engineers / Designers – Via Internal Procedures

Engineers / Designers – Quality Control processes

Multiple Designers/AEs – Through strict coordination via Leads and
Project Managers

Officially– Via UFC (Unified Facility Criteria)



New Requirements – Via UFC

Requirements have been changes and expanded in **UFC 4-010-06** (change 2).
Refer to section 5-3 “*Coordination with Other Disciplines.*”

Cybersecurity is now required to coordinate with all disciplines.

The HOW is not Defined.

This places Cybersecurity “In The Mix”. {An ingredient without a measure}

§5-3.2 UFGS Coordination Issues

User Interfaces. Where will they be located? Which, if any, will be privileged? How will they be secured?

Specific requirements for Fire Protection systems.

Submittal Review. Specific requirements, inventory reporting.

Hardware and software requirements: Ethernet switches and device & equipment power.

User Authentication.



So....Where & When Cybersecurity Engage?

There are two Reasonable Engagement Points -
Design & Quality Control



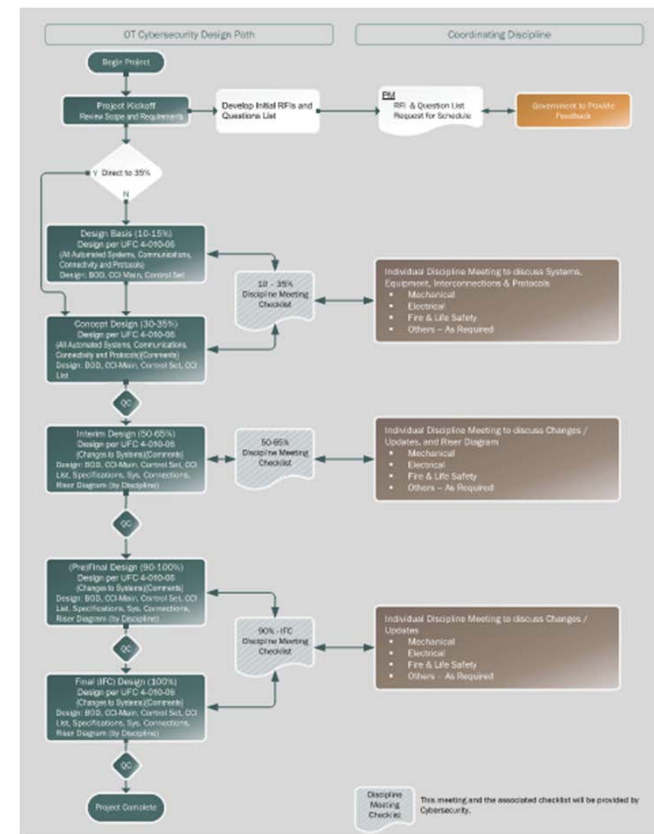
During Design

Employ a Formal Process that results in Interdisciplinary Engagement

Open discussion of the design at various stages.

Discuss the information being supplied to Cybersecurity from other Disciplines

Share the meeting minutes with ALL Disciplines.
No secrets!



During Design

Create dynamic documents that are updated as the project progresses.

Discuss relationships of systems during Update meetings.

Be ‘Nosey’. Ask Who, What, When, Why, Where, & How.

Again: Share the meeting minutes with ALL Disciplines. No secrets!

Caveat – “You can lead a horse to water, but you can’t make them drink!”

Category		Usage / Info		Additional Information
GENERAL	Facility Classification :	MISSION ESSENTIAL		
	Mechanical Lead :			
	Additional Engineers & Area :			
	ASHRAE 90.1 Applicable :			
	Riser Diagram Discussed :		(Req. @ Interim)	
SYSTEMS	(Specification indicates one exists)			
	Heating, Ventilation, & A/C (HVAC)			
	Computer Room AHUs (CRAC/CRAH)			
	Chilled Water Systems (CWS)			
	Cooling Towers (CT)			
	Hot Water Systems (HWS)			
	Compressed Air Systems (CAS)			
	Meters [Water & NG] (MTR)			
	Meters connected to DDC?			
CONTROLS	Additional Systems			
	Supervisory/Controller			
	Level 1-2 Communications Media			
	Level 1 Communication Protocol :			
	Level 2 Communication Protocol :			
M&CS	Allowable Ethernet Ports :			
	Monitoring and Control System			
	Existing Systems / Details ?			
	New/Existing Front End ?			
			SYSTEM Network Name :	
			Who Configures? :	
	Local HMI Station Required :			



During the QC Cycle

Cybersecurity STARTS with the Design from the Other Disciplines.

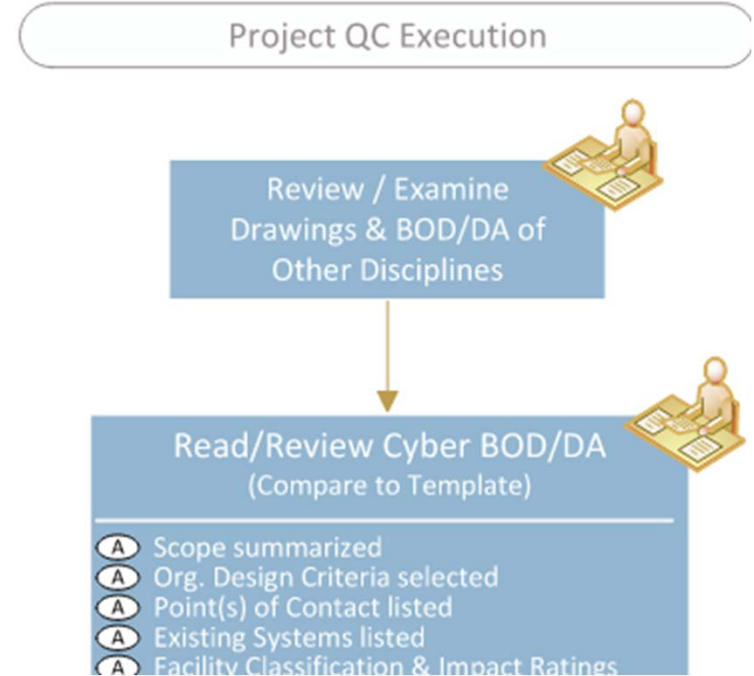
QC Reviewer

Looking for Systems/Elements in the external Design

How are those Systems/Elements reflected in the Cyber Design?

Lead Cyber Designer

Looking for Changes from Cyber Design



During the QC Cycle

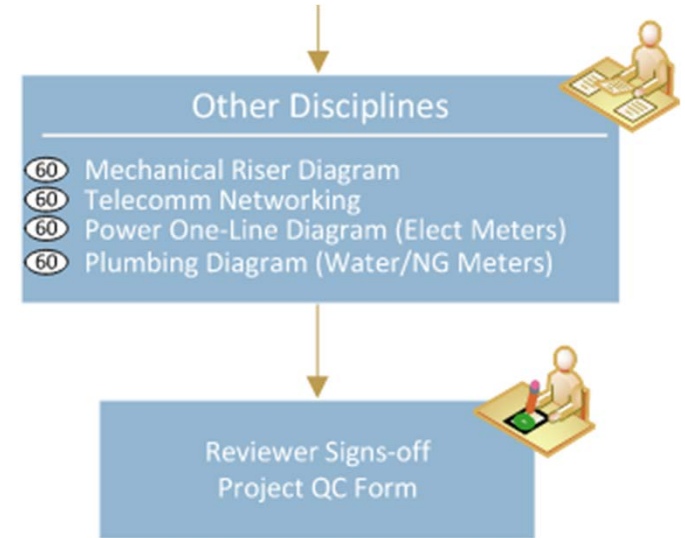
Cybersecurity FINISHES with the Design from the Other Disciplines.

QC Reviewer

Looking for Required connections / designs required by the Cyber Design.

Lead Cyber Designer

Looking for loose-ends in the Other Disciplines design.



During the QC Cycle

Examples:

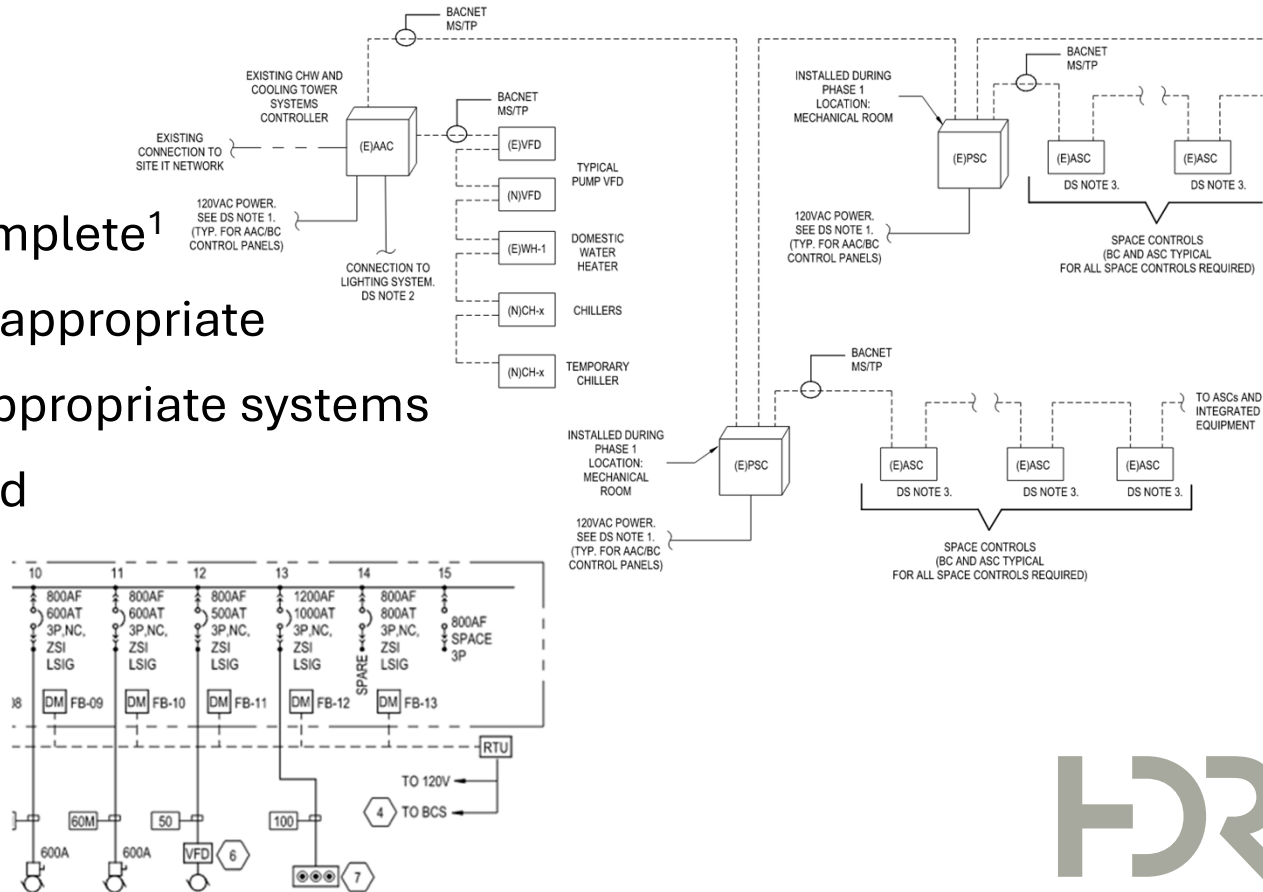
Riser Diagrams are Complete¹

Telecomm Networking appropriate

Meters connected to appropriate systems

Major Systems Checked

Point Tables reviewed.



¹ UFC 4-010-06 Change 2, 2023;
Section 5-4.3 “Riser Diagrams”

What does it take to **MAKE** this Happen?

What are the requirements?

An Open, Cooperative Environment

Cybersecurity Familiarity with Other Discipline UFCs

BUT – Not an Expert

Cybersecurity Limiting Comments in the QC Process

Stay on Point and Limit to the Cyber Requirements

Discuss Comments/Questions in Interdisciplinary meetings

This is your best opportunity for dialogue, discovering issues during QC cost us money and potentially missed deadlines.



Summary

This approach is NOT limited to Cybersecurity

- Encourage other disciplines to engage with each other

Cybersecurity is excellently positioned for this due to our role in Design

- We are responsible for security of all implemented electronic systems

Cybersecurity must delve into the Gaps to ensure that they are addressed for security purposes

This addresses and fulfills requirements in the recent version of UFC 4-010-06



Final Thought

This only works when ALL disciplines work as a Team

“For millions of years, mankind lived just like the animals. Then something happened which unleashed the power of our imagination. We learned to talk, and we learned to listen. Speech has allowed the communication of ideas, enabling human beings to work together to build the impossible. Mankind's greatest achievements have come about by talking, and its greatest failures by not talking. It doesn't have to be like this. Our greatest hopes could become reality in the future. With the technology at our disposal, the possibilities are unbounded. **All we need to do is make sure we keep talking.**”

Steven Hawking

