Pacific Northwest NATIONAL LABORATORY

Cybersecurity for Marine Renewable Energy Systems

2/18/2020

Marine Energy Council Webinar

U.S. DEPARTMENT OF ENERGY BATTELLE

PNNL is operated by Battelle for the U.S. Department of Energy

PNNL-SA-151251

U.S. DEPARTMENT OF ENERGY

Energy Efficiency & Renewable Energy

DOE's Strategy for Energy Sector Cybersecurity

"…energy sector cybersecurity is imperative for national security and economic prosperity."

- Bruce J. Walker, Assistant Secretary

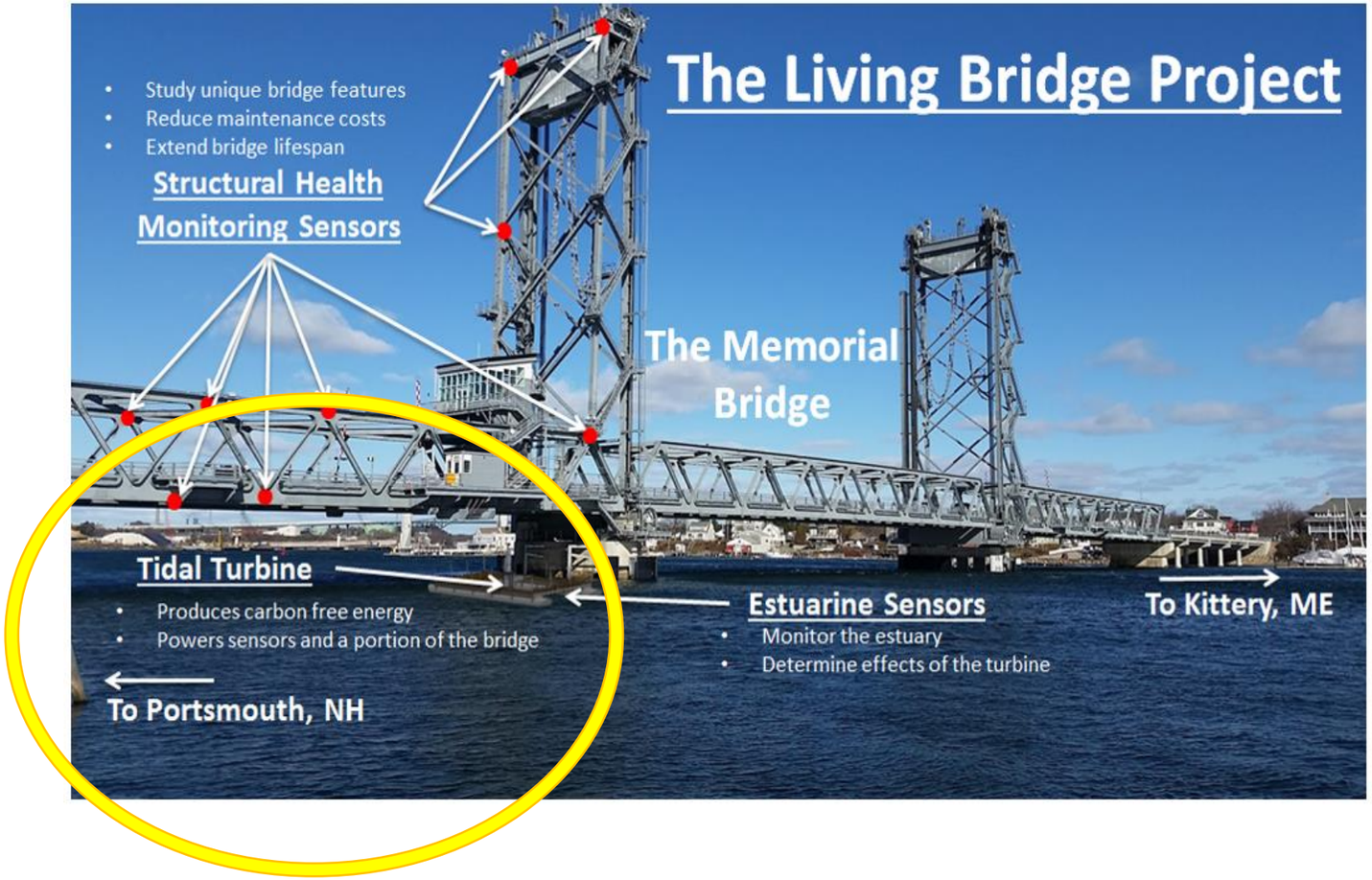
Office of Electricity Delivery and Energy Reliability

1 Strengthen today's cyber systems and risk management capabilities

2 Develop innovative solutions for tomorrow's inherently secure and resilient systems

Securing Marine Renewable Energy (MRE) Systems from Cyber Attacks Improves Resiliency

Goal:
Incorporate cybersecurity into design and operations of MRE systems and end-use applications



Marine Energy Industry Drivers

Seeks to:

- **Understand the power requirement** of emerging coastal and maritime markets
- **Advance technologies** that could integrate MRE
- **Relieve power constraints**
- **Promote economic growth**

Increased technology advancement

↓

Accelerated MRE development

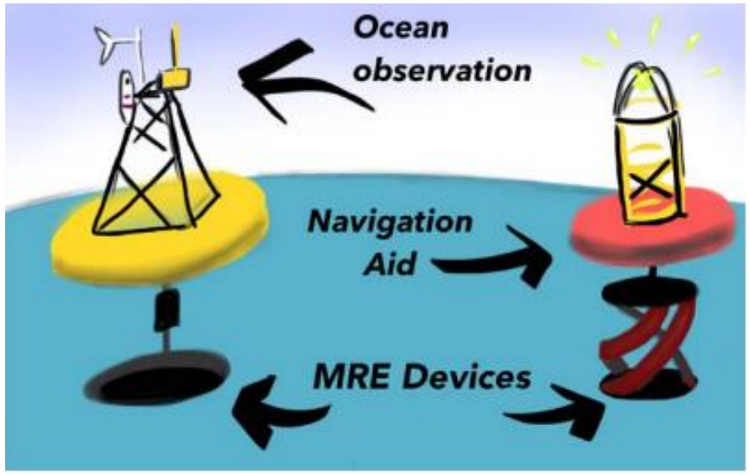
↓

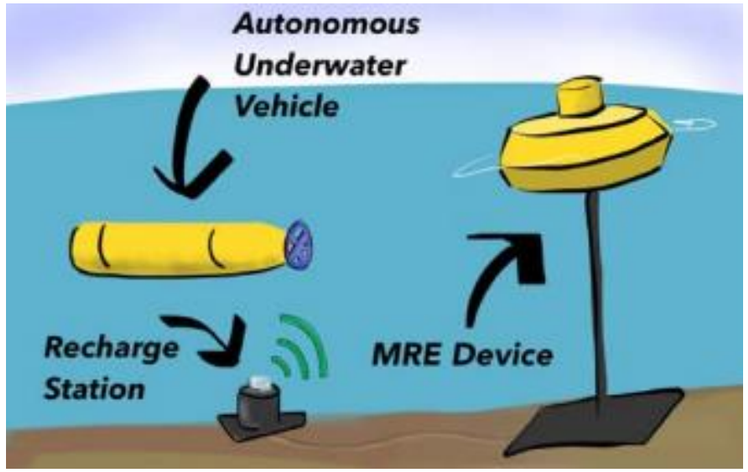
Increased cyber risk

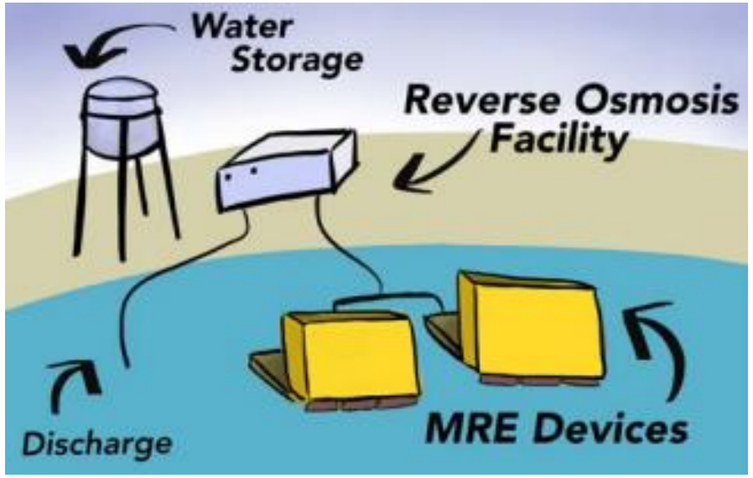
↓

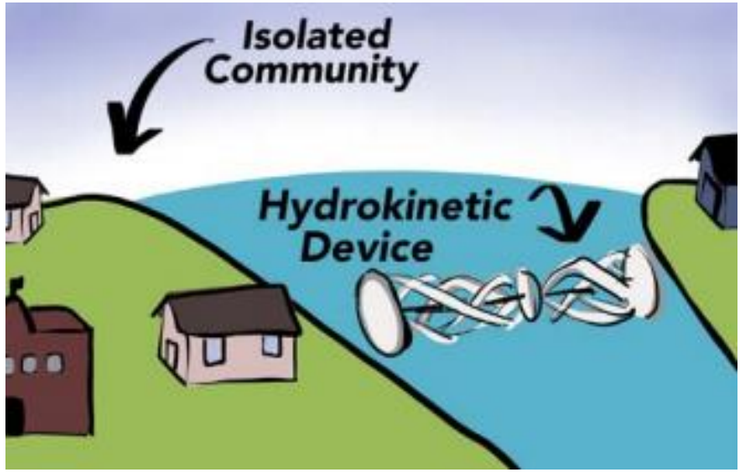
Severity of cyber attack depends on MRE end use

Impact of Cyber Attack Depends on MRE End Use



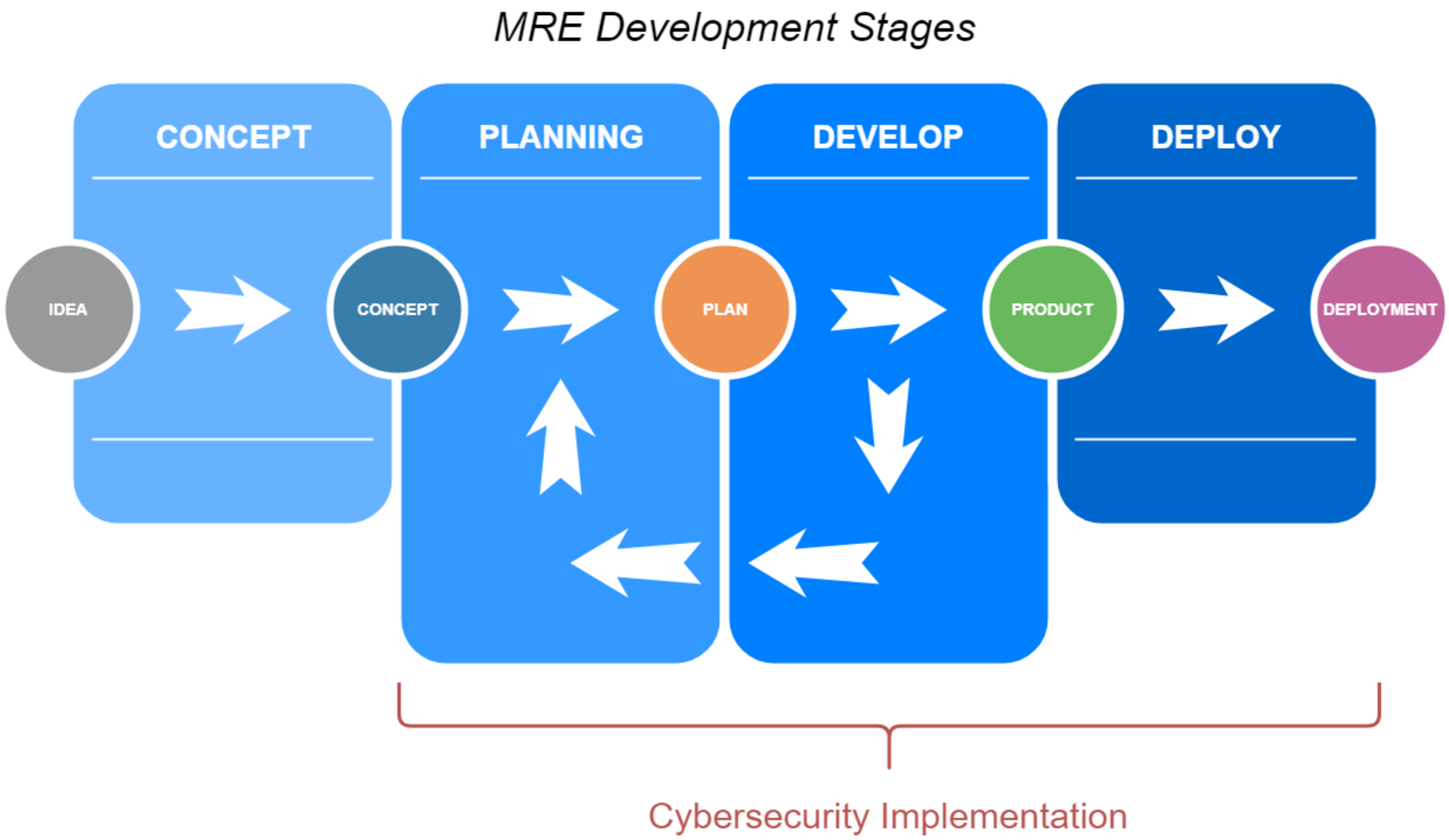






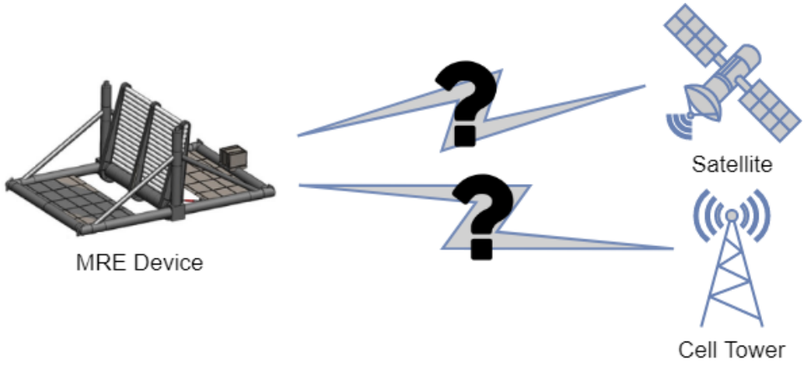
Photos courtesy of Molly Grear of PNNL

Cybersecurity Should Be Implemented Within the Development Cycle

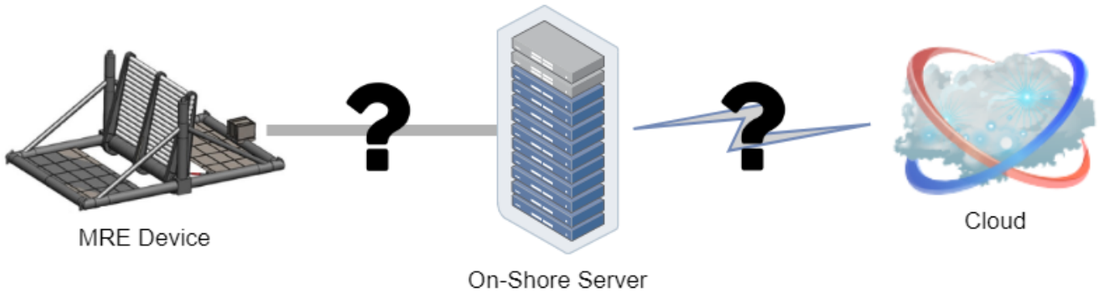


MRE System Operational and Communication Knowledge Gaps

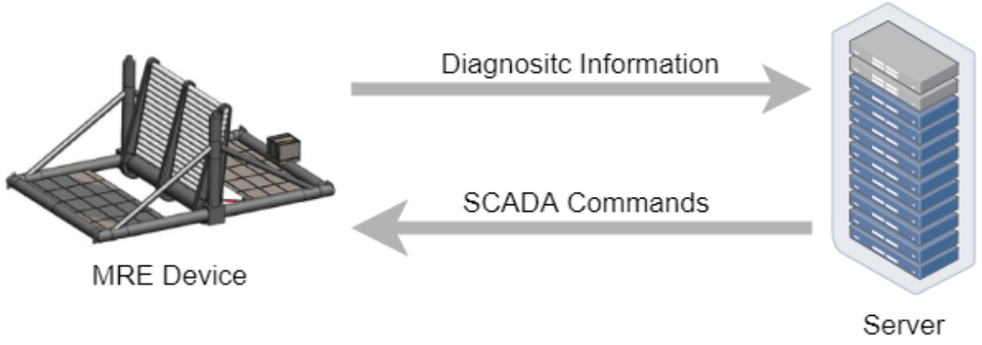
- Wireless networking systems? What kind?
  - ✓ Satellite?
  - ✓ Cell tower?
  - ✓ Short-wave Radio-frequency?



- Wired networking to shore? What next?
  - ✓ Delivered to Cloud?
  - ✓ Delivered to End-User systems?
  - ✓ Any in-between steps?

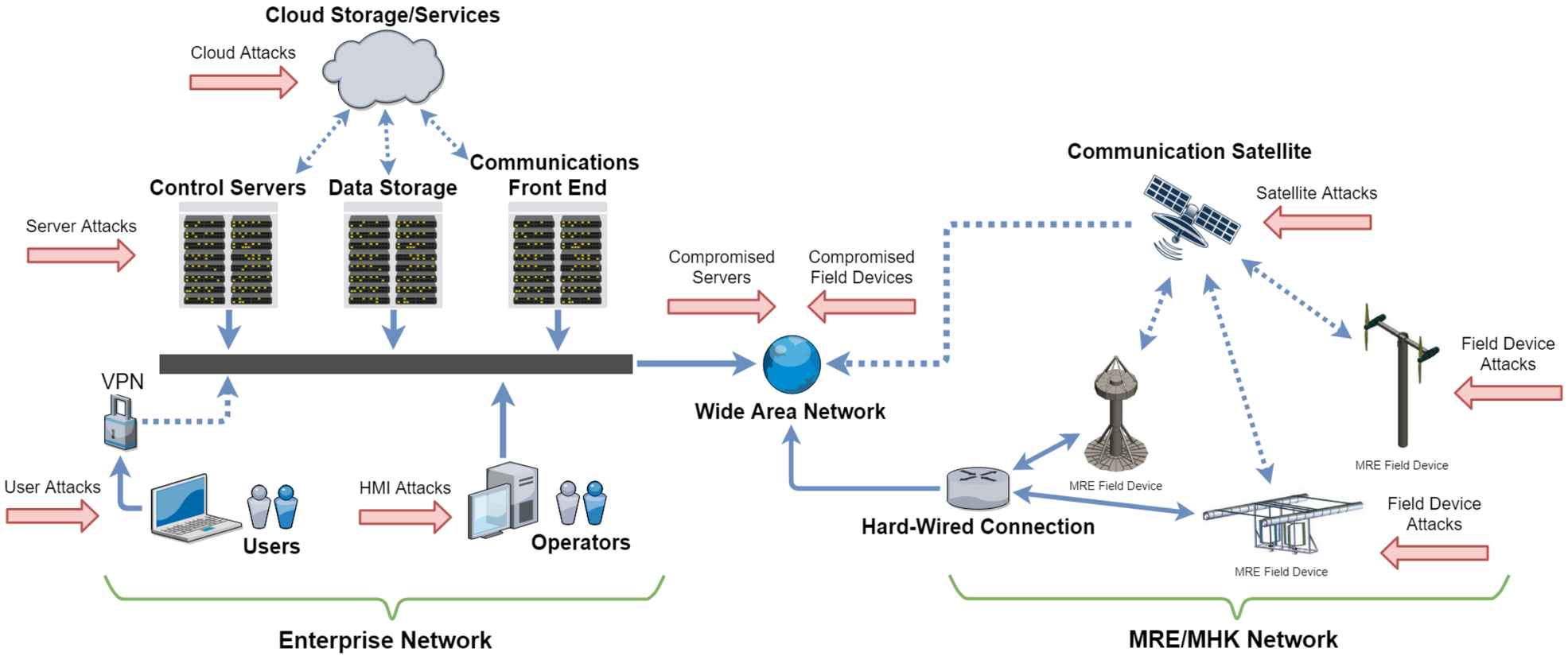


- Type of data being communicated?
  - ✓ Onboard machine status?
  - ✓ Weather and temperature reports?
  - ✓ Active braking or SCADA commands?



Threat Actors Attack Vulnerabilities in IT/OT System Configurations and Operational Processes

Example Network Architecture and Communication Methods

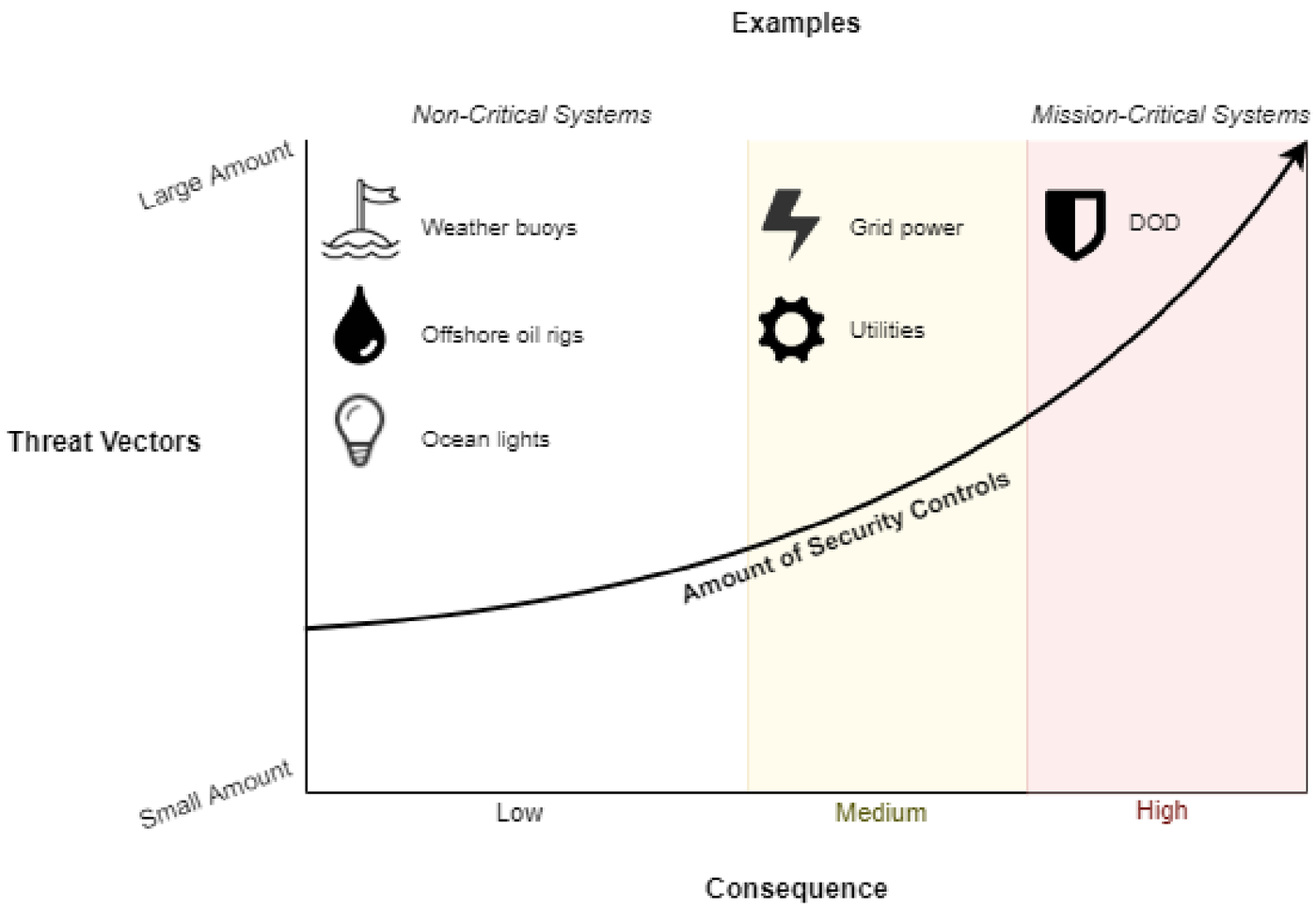


Data collected from developers will be handled as Business Sensitive/Official Use Only

Results of Request for Information (RFI)

- Types of Applications/Markets
  - Large Scale/Moderate Scale Grid power
  - Commercial power/recreational platform
  - Power for underwater vehicles/devices
- General System and Network Architecture
  - Programmable Logic Controllers (monitoring, diagnostics, data collection)
  - Wireless connection or Local Area Networks (maintenance, remote monitoring/reporting, equipment diagnostic data)
  - Cloud-based data storage
  - Satellite communication
- Current Cybersecurity Considerations
  - Hardware firewall
  - Virtual Private Networks
  - Hardware and Software Access/Account/Session Management
  - Intrusion Detection

Focus 1 – Identify Cybersecurity Vulnerabilities



Cybersecurity Risk = Probability x Consequence

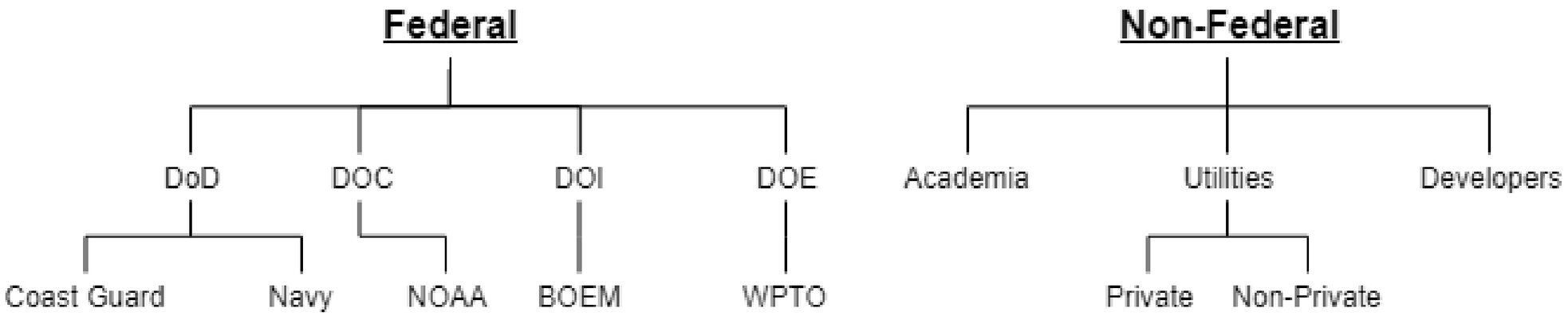
Cybersecurity Threat Analysis

- System –based approach
  - Knowledge of IT/OT networks and architectures (e.g., operational and enterprise)
  - Identify cyber vulnerabilities with those systems

- Threat-Based approach
  - Reviewed MITRE ATT&CK Matrix for Enterprise and Industrial Control Systems
  - Identified adversary tactics that MRE systems may potentially experience
  - Determined mitigating techniques for the tactics

Focus 2 – Develop Cybersecurity Guidance

Cybersecurity requirements are mandated by the governance for Different End Users.



BOEM = Bureau of Ocean Energy Management
DOC = Department of Commerce
DoD = Department of Defense
DOE = Department of Energy
DOI = Department of Interior
NOAA = National Oceanic and Atmospheric Administration
WPTO = Water Power Technologies Office

Guidance Identifies Security Controls Commensurate with Risk (Low, Moderate, High)

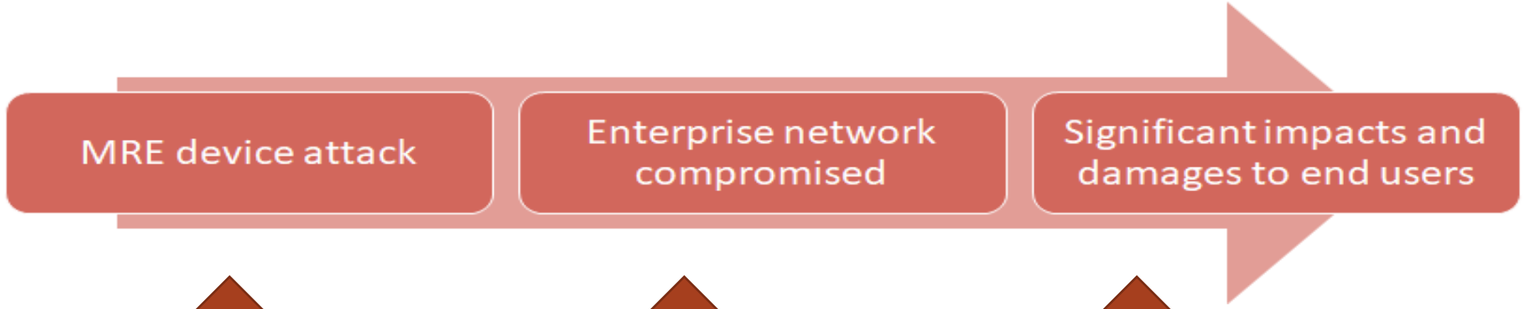
Cybersecurity Function	LOW	MODERATE	HIGH
Identify (ID)	X	X	X
ID-1	X	X	X
ID-2		X	X
ID-3, etc.			X
Protect (PR)	X	X	X
PR-1	X	X	X
PR-2		X	X
PR-3, etc.			X
Detect (DE)	X	X	X
DE-1	X	X	X
DE-2		X	X
DE-3, etc.			X
Etc.	X	X	X
	X	X	X
		X	X
			X

Thank you

For more information please contact:
Fleur de Peralta, P.E.
Pacific Northwest National Laboratory
P.O. Box 999, MS-IN K7-76
Richland, WA 99352
Phone: (509) 375-3323
Email: Fleurdeliza.deperalta@pnnl.gov

Background Slides

Types of Cyber Threats Evaluated for MRE Systems



Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification
Replication Through Removable Media	Project File Infection		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State
Spearphishing Attachment	Scripting					Point & Tag Identification
Supply Chain Compromise	User Execution					Program Upload
Wireless Compromise						Role Identification
						Screen Capture

MITRE ATT&CK Matrix for ICS

How a Cyber Attack Can Impact an MRE System

Adversary completes passive reconnaissance

Adversary exploits external remote services and uses replication through removable media techniques to gain initial access

Spoofing and scripting help adversary with initial execution of tasks

Malware installed on host system

Allows for commands to be executed remotely (e.g.. Injection, exfiltration, control, etc.)

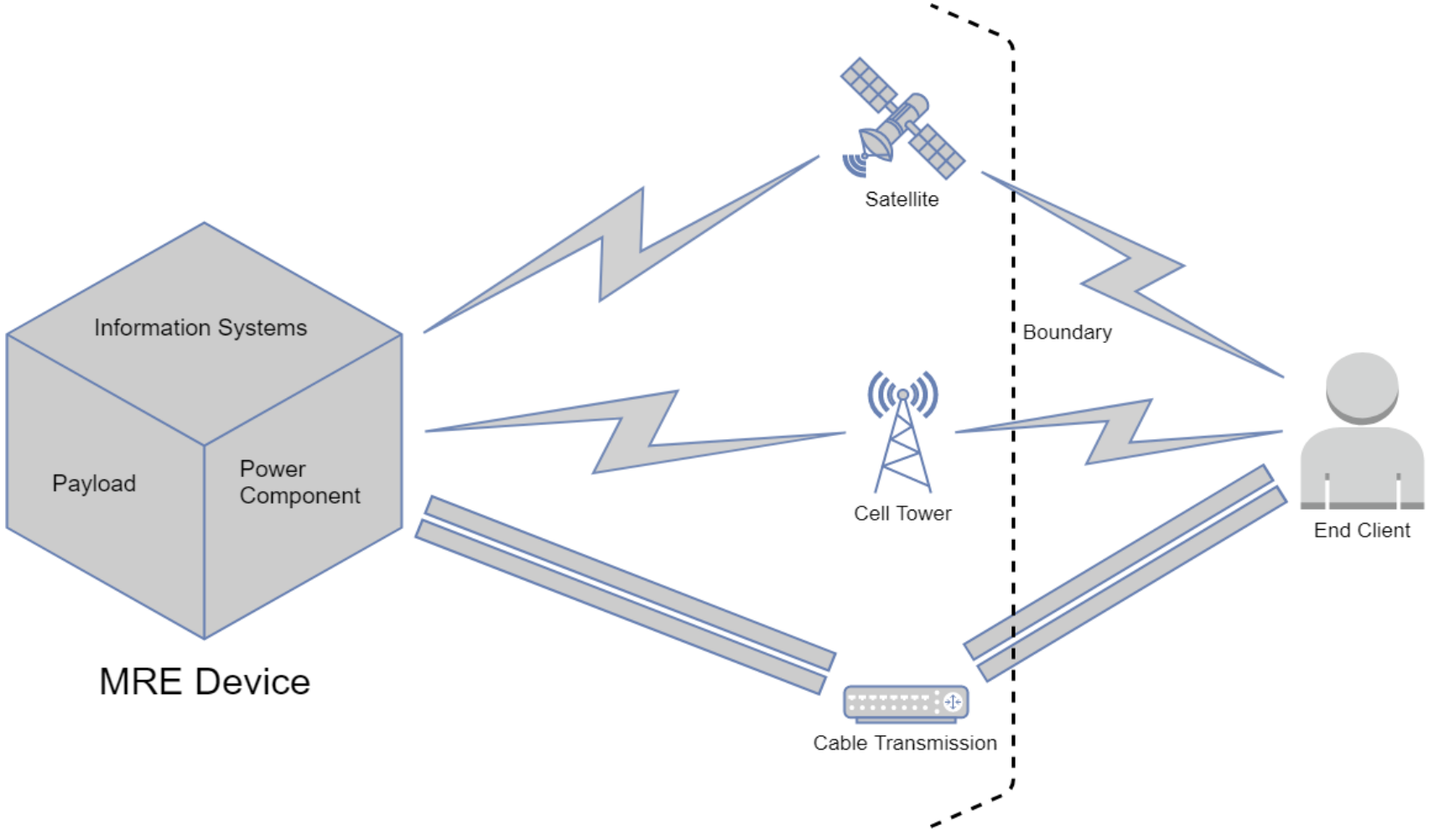
Pivot from initial foothold to targeted systems

Adversary initiatives intended actions (e.g.. denial of service, theft, etc.)

Impacts to optimization, potential damage to equipment, compromise of enterprise network

This is one example of a credible attack chain scenario on MRE devices

MRE Cybersecurity Guidance Document Addresses End-to-End Security



Medium	Protocol
Satellite	SCPS-TP, SCPS-SP
Cell Tower	3G, 4G, LTE
Cable Transmission	Ethernet, FireWire

Information Systems		Payload		Power Component	
MITRE	VirusTotal	MITRE	VirusTotal	MITRE	VirusTot
Technique	Attack Event	Technique	Attack Event	Technique	Attack Event

RSF	CSF	NERC-CIP
Cyber Guidence	Cyber Guidence	Cyber Guidence

Medium -> Protocol Model Diagram