INSTITUTE FOR DEFENSE ANALYSES

Challenges and Recommendations: Operational Cyber Testing of Hull, Mechanical, and Electrical (HM&E) / Industrial Control Systems (ICS)

Dr. Mark R. Herrera, Project Leader

Dr. Mark R. Herrera

March 2022

Approved for Public Release.

Distribution Unlimited.

IDA Document D-32986

Log: H 2022-000064

INSTITUTE FOR DEFENSE ANALYSES
730 East Glebe Road
Alexandria, Virginia 22305

The Institute for Defense Analyses is a nonprofit corporation that operates three Federally Funded Research and Development Centers. Its mission is to answer the most challenging U.S. security and science policy questions with objective analysis, leveraging extraordinary scientific, technical, and analytic expertise.

About This Publication
This work was conducted by the Institute for Defense Analyses (IDA) under contract HQ0034-19-D-0001, BD-09-2299.09.93, "Cyber - Naval," for the Office of the Director, Operational Test and Evaluation. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

Acknowledgments
The IDA Technical Review Committee was chaired by Mr. Robert R. Soule and consisted of Dr. Brian Vickers; Dr. Gregory Khoury ; Dr. Jason Husted; Dr. Robert Huekstaedt; Dr. Robert Atkins; Dr. Tye Botting from the Operational Evaluation Division, and Dr. Richard White from the IDA.

For more information:
Mark R. Herrera, Project Leader
mherrera@ida.org • (703) 578-2762

Robert R. Soule, Director, Operational Evaluation Division
rsoule@ida.org • (703) 845-2482

Rigorous Analysis | Trusted Expertise | Service to the Nation

INSTITUTE FOR DEFENSE ANALYSES

IDA Document D-32986

Challenges and Recommendations: Operational Cyber Testing of Hull, Mechanical, and Electrical (HM&E) / Industrial Control Systems (ICS)

Dr. Mark R. Herrera, Project Leader

Dr. Mark R. Herrera

Executive Summary

This test and evaluation concept proposes IDA's general evaluation approach for assessing the cybersecurity posture of Hull, Mechanical, and Electrical (HM&E) systems aboard U.S. Navy platforms. HM&E systems, also described as Industrial Control Systems (ICS), allow operators and maintainers to control critical ship functions. For the purposes of this test concept, we will use the terms HM&E and ICS interchangeably.

DOT&E guidance states that "test agencies must continue to use all available tools and resources to assess these [HM&E/ICS] systems." However, to date, no Navy platform on DOT&E oversight has included on-ship testing of HM&E/ICS as part of cyber operational testing for several reasons: (1) the Navy's Operational Test and Evaluation Force (OPTEVFOR) has lacked tools and expertise in HM&E/ICS-specific technologies and (2) system owners are concerned that testing of HM&E/ICS networks could cause unforeseen disruption or damage to critical systems.

To overcome these challenges, this test concept outlines an integrated methodology using passive data collection techniques, engineering-based risk assessments, laboratory-based demonstrations, and focused on-ship operational testing to help DOT&E assess these critically important but so far unassessed systems.

A. System Description

HM&E/ICS networks allow a computer network to physically monitor, interact, and control physical processes. In the context of shipboard Navy systems, common examples include:

- Electrical power and distribution
- Steering propulsion
- Damage control
- Heating, ventilation, and air conditioning
- Auxiliary functions (e.g. degaussing)

Similar types of hardware and software are also found in large-scale industrial processes. Field-level devices, such as programmable logical controllers or remote terminal units serve as the interface between the computer and physical control

systems (e.g. switches, relays, valves). A notional HM&E/ICS network and its segmented interface with the rest of a ship's systems is shown in Figure 1.

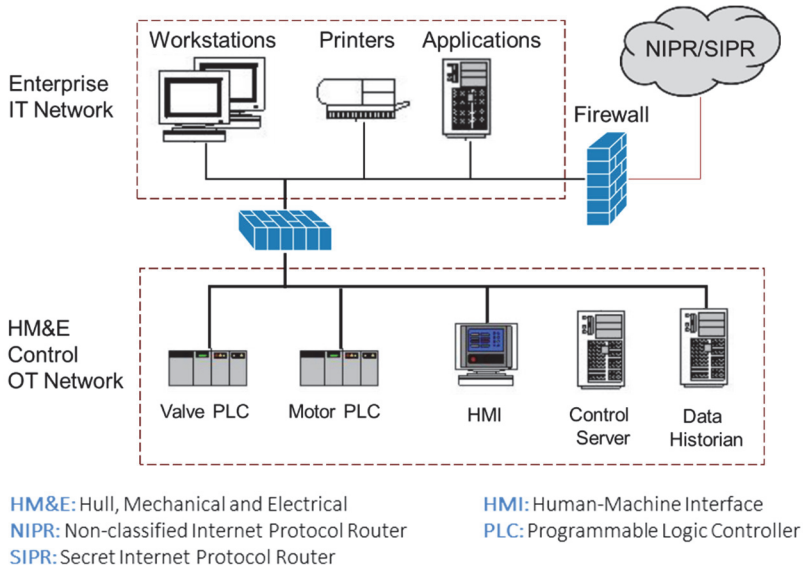


Figure 1. A Notional Diagram of an HM&E/ICS Control Network and Its Segmentation from the Rest of a Ship's Computing Infrastructure

B. Evaluation Approach

We propose an integrated test strategy that leverages developmental testing and other testing activities to form an analytic basis for a cybersecurity assessment. We propose the use of passive data collection techniques, engineering-based risk assessments, laboratory-based demonstrations, and focused, on-ship operational testing. A notional timeline demonstrating how these various events may fit together is shown in Figure 2.

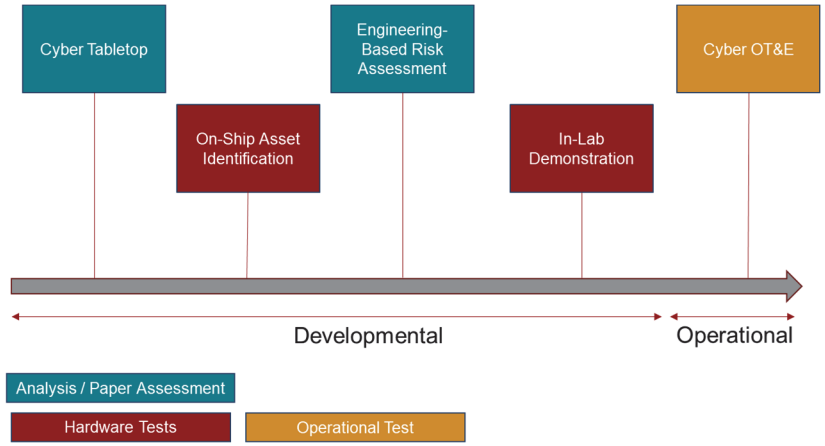


Figure 2. A Notional Timeline Showing Possible Data Sources and How They Relate to Developmental and Operational Testing

1. Passive Data Collection/Enumeration

To develop an accurate representation of the HM&E/ICS network as deployed on a ship (rather than as designed or delivered), IDA recommends the use of passive data collection techniques to increase visibility and asset identification. These methods include:

- Review of configuration files taken from on-ship network infrastructure to verify hardware and access controls

- Physical inspection of on-ship HM&E/ICS systems to discover essential, non-networked components
- Passive collection / traffic sniffing using existing network infrastructure or defensive appliances to observe operational network traffic

Environmental enumeration is essential not only for ensuring the accuracy of any cybersecurity assessment, but also for allowing system owners to develop an adequate cyber defense.

2. Engineering-Based Risk Assessments

Once an accurate representation of a ship's onboard HM&E/ICS networks have been developed, IDA recommends that the test and evaluation community (including developmental testers, operational testers, and program office personnel) develop an engineering-based risk assessment to help characterize risk to critical HM&E/ICS components. These assessments can help identify:

- The potential access points into the HM&E/ICS environment
- The kinds of malicious activity that can be detected
- The critical components and key failure modes that an adversary could try to exploit
- The range of tools available to system users and maintainers to detect potential compromise

These risk assessments are also useful for focusing and scoping laboratory and on-ship testing. Optimally, the output of such an assessment is a detailed, formal report that describes the potential attack surface and risks, as well as the mitigation measures a system owner might employ to lower risk to critical systems.

3. Demonstrations in Controlled, Laboratory Environments

For ground engineering assessments and the validation of potential, high-risk attack vectors against an HM&E/ICS, we recommend the development of HM&E/ICS-specific tools and their application in controlled, laboratory environments. For example, OPTEVFOR is already developing a non-internet protocol (non-IP) cybersecurity suite focused on HM&E/ICS to support future operational testing.

Because of the potential for damage from active testing (e.g. transmitting commands/signals to HM&E/ICS networks), IDA recommends first applying these tools in controlled, laboratory environments to minimize risk against deployed Navy platforms. In addition, successful testing with these tools in laboratory environments may increase stakeholder confidence in the safe and effective application of these tools to shipboard systems.

While it might not be feasible to verify, validate, and accredit laboratory-based demonstrations for every program of record on DOT&E oversight, it may be possible to select types of HM&E/ICS implementations that are common across Navy platforms as potential subjects of laboratory testing.

4. On-ship Operational Testing to Determine Accessibility of HM&E/ICS Components and Demonstrate High-Confidence Attack Vectors

Regardless of whether a system or platform is the subject of a laboratory-based test event, all programs on DOT&E oversight should probe how accessible HM&E/ICS components are from starting postures elsewhere on a system's computing network. At a minimum, operational testing should be able to provide information on:

- The presence of appropriate access controls between HM&E/ICS systems and the rest of the ship/platform
- Whether shipboard operators are trained and equipped to identify cyber compromise on HM&E/ICS networks
- Whether support activities (e.g. Naval Surface Warfare Centers) have response procedures to support triage of critical HM&E/ICS components

Additionally, for systems that have undergone controlled, laboratory-based testing, testers can conduct focused demonstrations against specific elements of an HM&E/ICS aboard ship, with the technical support of system subject matter experts.

C. Recommendations

We recommend that DOT&E consider the following immediate and long-term courses of action to support the adequate assessment of these critical shipboard systems:

1. Immediate

- Require the consistent conduct of engineering-based risk assessments (and delivery of formal reports) as part of the cyber assessment for Navy platforms.
- Require that all on-ship operational tests assess interface between HM&E/ICS systems and the rest of a ship's computing environment.
- Continue to encourage OPTEVFOR's development of active, non-IP, HM&E/ICS-specific test tools and the use of passive collection methods on HM&E/ICS systems.
- After HM&E/ICS tools and tactics have been proved out in laboratory environments, advocate for their inclusion in select operational cyber assessments.

2. Long-Term

- Advocate for the funding, development, and use of land-based test sites for families of HM&E/ICS systems (e.g. power distribution, steering control).
- Encourage system owners to conduct passive data collection on-ship to improve their ability to defend these critical components and support land-based test sites and engineering-based risk assessments.

Challenges and Recommendations: Operational Cyber Testing of Hull, Mechanical, and Electrical (HM&E) / Industrial Control Systems (ICS)

Mark R. Herrera, Task Lead

15 February 2022

Institute for Defense Analyses
730 East Glebe Road ● Alexandria, Virginia 22305

Background

Provide background on the current state and challenges of testing **Hull, Mechanical, and Electrical (HM&E) / Industrial Control Systems (ICS)** on Navy platforms.

Purpose

Provide recommendations on how DOT&E can advocate for near-term inclusion of HM&E/ICS in future cyber assessments

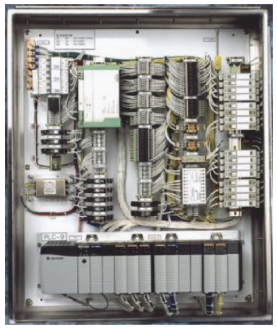
Background – What is an ICS?

Industrial control system (ICS) is a general term that encompasses several types of control systems, including:

- Architectures
  - Supervisory Control and Data Acquisition (SCADA)
  - Distributed Control Systems (DCS)
- Field Components
  - Programmable Logic Controllers (PLC)
  - Remote Terminal Units (RTUs)

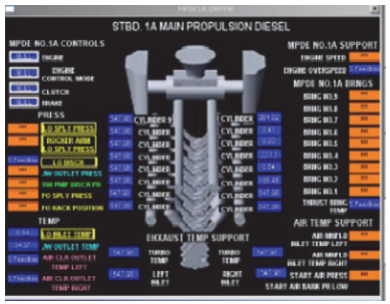
… often found in the industrial sectors and critical infrastructures.
(NIST 800-82)

PLC
HMI: Human Machine Interface



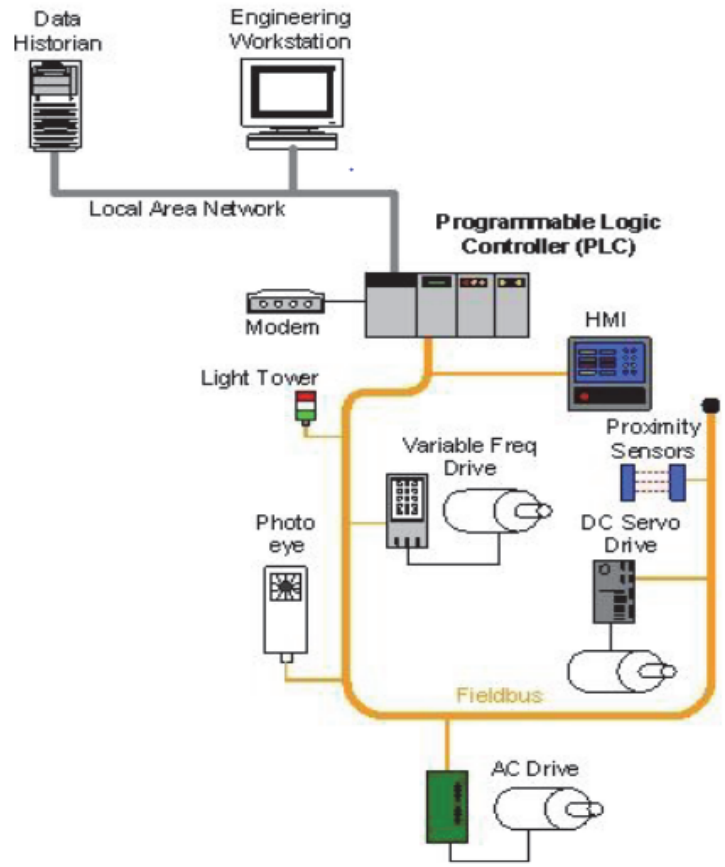
RTU

HMI
Station



Physical
Process

ICS components allow computer networks to monitor, interact, and control *physical processes*.

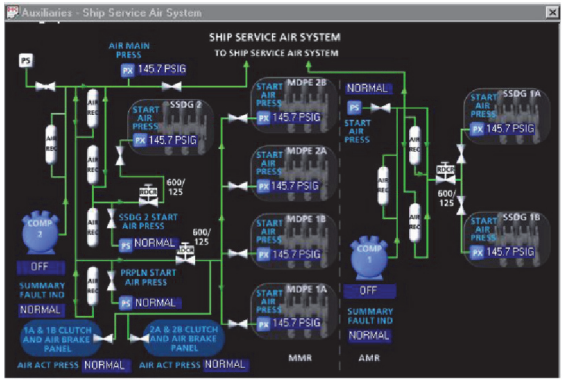


If there's a valve connected to a computer, there's likely a PLC acting as the interface between the computer and the physical world.

HMI: Human Machine Interface
AC: Alternating Current
DC: Direct Current

In the shipboard context, these components are typically part of **Hull, Mechanical, and Electrical (HM&E) Systems.**

- Electrical power and distribution
- Steering propulsion
- Damage control
- Heating, ventilation, and air conditioning
- Auxiliaries (e.g. degaussing)

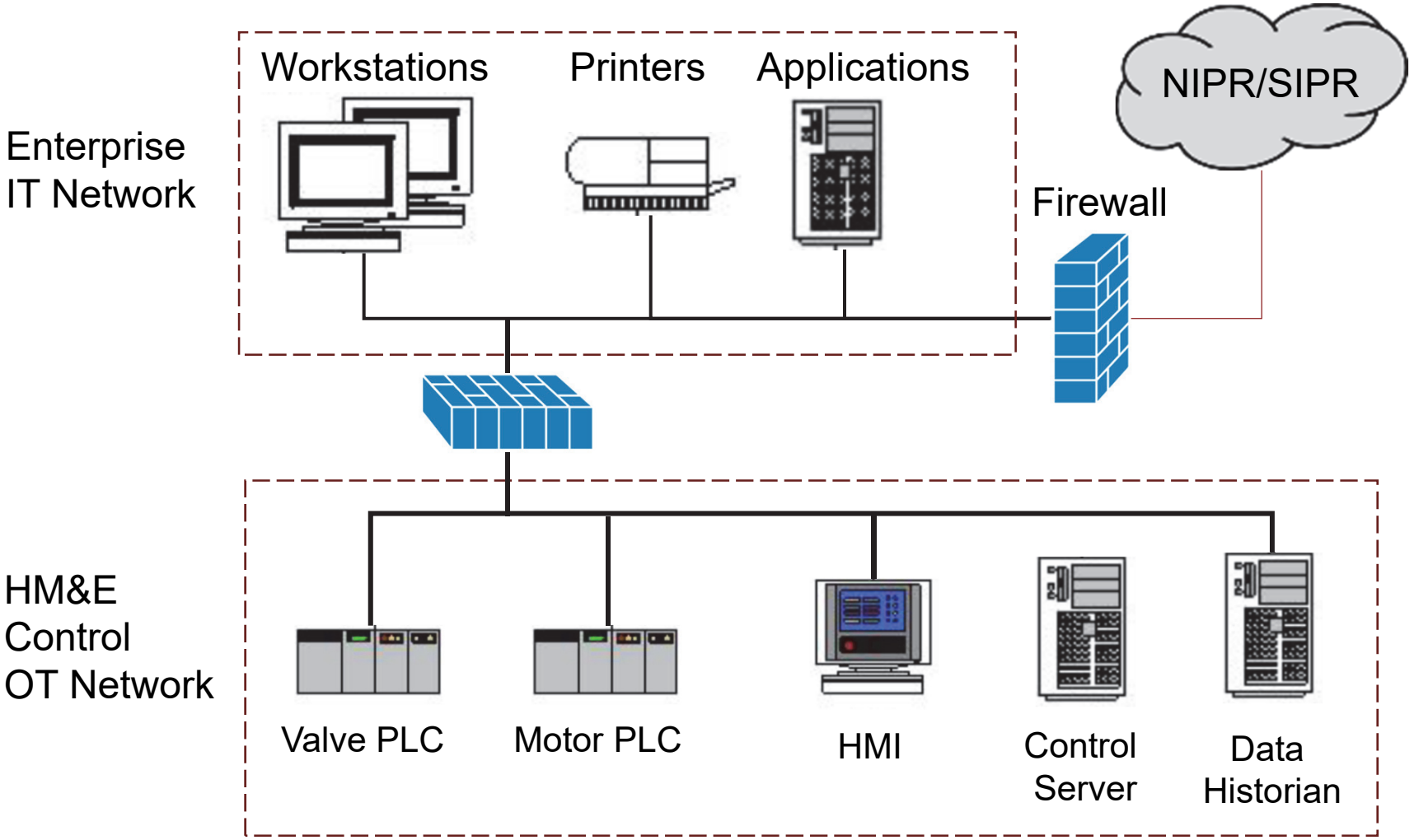


For the purposes of this briefing, we'll use the terms HM&E and ICS as interchangeable catchalls

HM&E: Hull, Mechanical and Electrical

ICS: Industrial Control System

Networks are traditionally separated into **Information Technology (IT)** and **Operational Technology (OT)**



HM&E: Hull, Mechanical and Electrical
NIPR: Non-classified Internet Protocol Router
SIPR: Secret Internet Protocol Router
HMI: Human-Machine Interface
PLC: Programmable Logic Controller

What's the current state of ICS testing in the Navy OT&E community?

DOT&E guidance states that "test agencies must continue to use all available tools and resources to assess these [ICS] systems."

--DOT&E Memorandum. Cybersecurity Operational Test and Evaluation Priorities and Improvements. 27JUL2016

Additionally, DOT&E has also invested in the development of safe test and evaluation techniques for ICS.

--DOT&E Memorandum. Cybersecurity Operational Test and Evaluation Priorities and Improvements. 27JUL2016

However, to date, no Navy platform on DOT&E oversight has included on-ship testing of ICS as part of cyber operational testing.

ICS: Industrial Control Systems OT&E: Operational Test and Evaluation

What has hampered testing of ICS networks of systems on DOT&E oversight?

In the past, system owners and test teams have resisted the inclusion of ICS systems as part of cyber operational testing for a number of reasons.*

- ICS protocols have traditionally been serial/non-IP and are outside of the current expertise and toolsets of operational test teams.

- Concerns that ICS testing can cause unforeseen disruption or damage to critical systems.
  - DOT&E guidance has expressed the necessity for caution in testing ICS components due to the risk of damage.

  - Testing of ICS systems in private industry has demonstrated that these kinds of systems can be too sensitive for common red-team tools like active scanning.

ICS: Industrial Control Systems IP: Internet Protocol

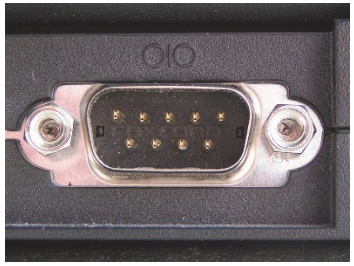
* For example, see IDA Memorandum: Littoral Combat Ship Surface Warfare Package Increment 3 CVPA Trip Report. 10FEB2022

ICS implementations depend less and less on legacy serial/non-IP protocols.

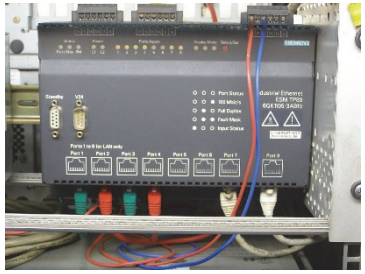
- The distinction between the IT networks and OT networks is vanishing as legacy serial interfaces get replaced by enterprise-like TCP/IP hardware.*

- Modern ICS protocols run as layers on TCP/IP networks—allowing network owners to use the same kind of infrastructure.

Serial



Industrial Ethernet



- BUT: Even if an ICS uses the types of networks that red teams are familiar with, there is still risk due to the potential of damage to the underlying system.

- AND: An assessment should involve more than just finding vulnerabilities.

ICS: Industrial Control Systems IT: Information Technology OT: Operational Technology
TCP/IP: Transmission Control Protocol/Internet Protocol

* M. Keene. https://www.sans.org/blog/the-risks-of-an-it-versus-ot-paradigm/

Actively testing ICS components is still a higher risk activity than traditional IT cyber testing

- A failure in a critical safety system or physical process can lead to costly downtime or even unsafe conditions.

- Even scanning tools that vendors claim are "ICS specific" or "use native ICS protocols" can lead to unforeseen circumstances/situations.
  - Often, the challenge in testing ICS is not the lack of a tool (though having one helps): Creating reproducible, safe effects on an ICS typically requires a detailed understanding of the physical process the ICS is managing.

- Ultimately, finding vulnerabilities/exposures in an ICS system (e.g. using ICS test tools) is only one part of a holistic approach to evaluating a system.

It's not enough to test if an adversary can get in.

What happens *when* they do get in, and *how do systems and users respond*?

ICS: Industrial Control Systems IT: Information Technology

Proposal: An integrated (developmental + operational) assessment of ICS systems, using data from operational testing and other sources.

We propose an integrated approach to assessing cyber posture of ICS systems, using data from operational testing and other sources

- Use *passive* techniques to collect **on-ship data** as part of program office enumeration activities.
- Require **engineering risk assessments** that characterize the risk to ICS systems.
- Advocate for general "demonstrations" of HM&E systems in **controlled laboratory environments** to ensure that these risk assessments are grounded in reality.
- Dedicate **operational testing** events to probe the interface between traditional shipboard IT systems and ICS components, and potentially targeted, vetted actions against an ICS system.

ICS: Industrial Control Systems IT: Information Technology OT: Operational Technology

Passive techniques to increase visibility and asset identification on ship

In order for system defenders to protect an ICS, they need to know what is in their environment!

- Not just *as designed* but also *as deployed.*

The test and evaluation community could encourage program offices to identify assets in their ICS networks using non-disruptive techniques:

Review of configuration files	Physical Inspection	Passive Collection/Traffic Sniffing
• Router/hardware • Verify access controls	• Important for non-networked components	• Use framework of existing defensive appliances (e.g. SPAN ports)

Environment enumeration is useful for an assessment and necessary for cyber defense!

ICS: Industrial Control Systems SPAN: Switch Port Analyzer

Engineering-Based Risk Assessments to describe the potential effects of ICS compromise

The combined test and evaluation community (DT/OT/program office) along with contractor subject matter experts could develop engineering risks assessments of these ICS subsystems:

- Identify potential access points into the ICS environment from the platform.
- Identify the kinds of malicious activity the system can actually detect.
  - How would these data overlay with known threat actors?
- Identify critical components and key failure modes that an adversary could potentially try to cause.
- Develop potential attack paths that could cause those failure modes.
- Determine what tools are available to system users and maintainers to postulate potential compromise.

Consider leveraging one of the existing frameworks to scope these questions: e.g. MITRE ATT&CK Framework for ICS.

ICS: Industrial Control Systems IT: Information Technology OT: Operational Technology

Example: What do known threats do, and can the system detect that kind of behavior?

The MITRE ATT&CK Framework for ICS is useful in characterizing the tools and techniques of world ICS threats.

Source: https://www.dragos.com/mitre-attack-for-ics/

ICS: Industrial Control Systems

Advocate demonstrations in a controlled, laboratory environment

- To ground the engineering analyses in reality, DOT&E could work with program offices and DTE&A to stand up demonstration events for the kinds of attacks developed in the engineering analysis.

- One demonstration could cover multiple programs of record, since there may be commonalities between the implementations of their ICS solutions.

- Working closely with system owners and process engineers, develop and deploy ICS attacks to prove out attack threads in the engineering risk assessment.

- It might not be feasible to verify, validate, and accredit a lab based event for each program of record.
  - But it is also likely not feasible to conduct this level of testing for every program on ship, due to safety constraints and the intensive nature required to develop controlled ICS attacks.

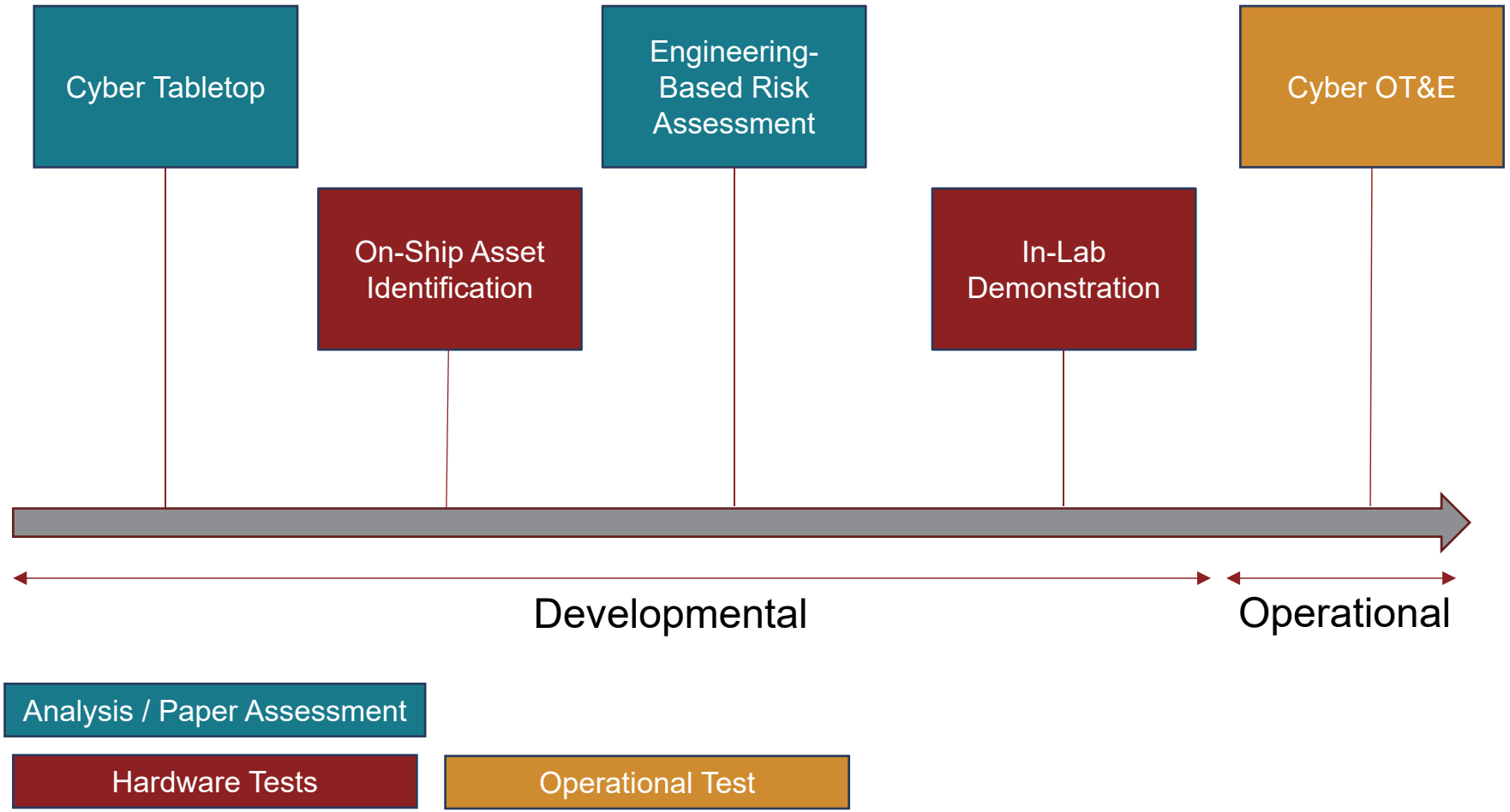
ICS: Industrial Control Systems DTE&A: Developmental Test, Evaluation, and Assessments

Operational tests to determine accessibility of ICS components

- Regardless of whether a system conducts a laboratory-based test event, all programs should include probing how accessible ICS components are from traditional IT systems.
  - Are ICS networks adequately separated from the rest of the ship?
  - What parts of the ICS are routable from the non-ICS enclave?
  - Are there appropriate access controls in place to prevent intrusion?
  - Are shipboard operators trained and equipped to identify cyber compromise on ICS networks, and do they have an appropriate incident response plan?
  - If the ship outsources this work to a support activity (e.g. Navy Surface Warfare Center), what are that entities response procedures?
- The answers to these questions can directly translate into recommendations to increase the robustness of HM&E systems.
- OPTEVFOR has also sponsored NSWC-Philadelphia to develop ICS specific test tools to support their assessments.
  - After their application and testing in a controlled lab environment, these tools could potentially be used on ship against high interest components, with the *technical support of system subject matter experts.*

ICS: Industrial Control Systems
HM&E: Hull, Mechanical, and Electrical
IT: Information Technology
OT: Operational Technology
OPTEVOR: Operational Test and Evaluation Force

These combined activities provide an integrated, executable timeline to assess ICS components



IDA Recommendations that DOT&E consider the following courses of action

Immediate

- Require the consistent conduct of Engineering Risk Assessments (and delivery of formal reports) as part of the cyber assessment for Navy platforms.
- Require that all on-ship operational tests assess interface between HM&E systems and the rest of a ship's computing environment.
- Continue to encourage OPTEVFOR's development of active, non-IP HM&E specific test tools and the use of passive collection methods on HM&E systems.
- After HM&E tools and tactics have been proved out in laboratory environments, advocate for their inclusion in select operational cyber assessments.

Long-Term

- Advocate for the funding, development, and use of land-based test sites for particular families of HM&E systems (e.g. power distribution, steering control).
- Encourage system owners to conduct passive data collection on-ship to improve their ability to defend these critical components and support land-based test sites and engineering risk assessments.

HM&E: Hull, Mechanical, and Electrical OPTEVFOR: Operational Test and Evaluation Force IP: Internet Protocol

Conclusions

- The challenges of testing ICS components continue to hamper the test community's ability to assess the cyber survivability of these subcomponents.

- An opportunity exists not only to leverage non-OT data for DOT&E assessments, but to encourage system owners to increase their visibility into their ICS systems.
  - "You can't defend what you don't know."

- Operational testing will still play an important part in determining how connected these ICS systems are to the rest of the ship, and whether system operators have the tools and procedures in place to identify and respond to cyber intrusion.

ICS: Industrial Control Systems

Backup

ICS Cyber Test Data Elements – Find Vulnerabilities and Exposures

How should the OTA and red team collect vulnerability and exposure data for each attack volume component?							
ICS Component							
Primary *Collection Method* Venue	Component of ICS to interrogate						
	Devices at the Interface of ICS				Operational and Control Units		Process/Field Units
Data to Obtain	**Edge Switches**	**Remote Access Server**	**Other DMZ Hosts**	**Data Historian Mirror**	**HMI**	**Data Historian**	**PLCs/RTUs**
Enumeration of Known (Hardware) Vulnerabilities	Deliberate Network Scanning			Deliberate Passive Network Sniffing / Configuration Review			Deliberate Dedicated ICS Tool + Passive Sniffing
Enumeration of Software Flaws/Data Flows	Deliberate Network Scanning			Deliberate Passive Network Sniffing / Configuration Review			Deliberate Dedicated ICS Tool + Passive Sniffing
Hardware and Software Configuration	Inferential Configuration Review			Deliberate Passive Network Sniffing / Configuration Review			Inferential Configuration Review

Analysis or Paper Assessment	Other Test Events
DT or IT Test Events	Operational Tests

OTA: Operational Test Agency
DMZ: Demilitarized Zone
HMI: Human-Machine Interface
PLC: Programmable Logic Controller

ICS: Industrial Control System
RTU: Remote Terminal Unit

ICS Cyber Test Data Elements – Characterize Potential Mission Effects

To what extent can mission effects be induced by attacks from each family, given an adversary's starting posture?			
Data Collected During Adversarial Cyber Attacks		**Cyber Attacker Seeking to Conduct Fire from Predetermined Starting Posture**	
Mission Effect Objectives	**Attack Family**	**Authenticated Access**	**Unauthenticated Access**
Exploit Initial Access on ICS to attack IT Network	*Confidentiality*	N/A	N/A
	Integrity	**Inferential**	**Inferential**
	Availability	N/A	N/A
Exfiltration Operational Process Information	***Confidentiality***	Deliberate (on-ship)	Deliberate (on-ship)
	Integrity	**N/A**	**N/A**
	Availability	**N/A**	**N/A**
Deny/Alter Operators View of Physical Process	*Confidentiality*	**N/A**	**N/A**
	Integrity	**Deliberate (on-ship)**	**Deliberate (on-ship)**
	Availability	**Deliberate (on-ship)**	**Deliberate (on-ship)**
Deny Availability of Physical Process (e.g. Shutdown Physical Process)	*Confidentiality*	**N/A**	**N/A**
	Integrity	**Deliberate (in-lab)**	**Deliberate (in-lab)**
	Availability	**Deliberate (in-lab)**	**Deliberate (in-lab)**
Intentionally Cause a Loss of Safety (e.g. Interfere with Safety Control System)	*Confidentiality*	N/A	N/A
	Integrity	**Inferential (by analysis)**	**Inferential (by analysis)**
	Availability	N/A	N/A

CEC: Cooperative Engagement Capability
BIT: Built-In Test

ICS Cyber Test Data Elements – Defensive Actions

How do ICS defenders and operators deal with cyber effects and subsequent mission effects?						
Data Collected During Defensive Actions (Potentially in laboratory setting due to safety constraints)			**Defensive Capabilities**			
			Inherited Defenses (Host Platform)		**Inherent Defenses (ICS)**	
			Cyber (CSSP)	*Non-cyber* (Fire Control Operator)	*Cyber*	*Non-cyber* (Maintainer)
Detections	*Authenticated Access*	*Native Tool*	Inferential Based on observations from platform/host CVPA and AA		No Role	Opportunistic
		Foreign Tool				Opportunistic
	Unauthenticated Access	*Native Tool*				Deliberate
		Foreign Tool				Deliberate
Responses	*Treat*		Inferential Based on observations from platform/host CVPA and AA		No Role	Deliberate
	Tolerate					Deliberate
	Terminate					Opportunistic
	Transfer					No Role
Recovery Actions	*Reboot ICS*		No Role		No Role	Deliberate
	Revert to Known Good State					Opportunistic
	Other Actions				Inferential	Inferential

AA: Adversarial Assessment
CEC: Cooperative Engagement Capability
CSSP: Cybersecurity Service Provider
CVPA: Cooperative Vulnerability and Penetration Assessment

REPORT DOCUMENTATION PAGE

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED	
03-2022	Final	START DATE	END DATE Mar 2022

4. TITLE AND SUBTITLE
Challenges and Recommendations: Operational Cyber Testing of Hull, Mechanical, and Electrical (HM&E) / Industrial Control Systems (ICS)

5a. CONTRACT NUMBER	5b. GRANT NUMBER	5c. PROGRAM ELEMENT NUMBER
HQ0034-19-D-0001		
5d. PROJECT NUMBER	**5e. TASK NUMBER**	**5f. WORK UNIT NUMBER**
BD-09-2299	229993	

6. AUTHOR(S)
Herrera, Mark, R.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Institute for Defense Analyses 730 East Glebe Road Alexandria, Virginia 22305	D-32986 H 2022-000064

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)	11. SPONSOR/MONITOR'S REPORT NUMBER
Director, Operational Test and Evaluation 1700 Defense Pentagon Room 1D548 Washington, DC 20301-1700	DOT&E	

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for Public Release. Distribution Unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
This test and evaluation concept proposes IDA's general evaluation approach for assessing the cybersecurity posture of Hull, Mechanical, and Electrical (HM&E) systems aboard US Navy platforms. HM&E systems, also described as Industrial Control Systems (ICS), allow operators and maintainers to control critical ship functions. This test concept outlines an integrated methodology using passive data collection techniques, engineering-based risk assessments, laboratory-based demonstrations, and focused on-ship operational testing to help DOT&E assess these critically important but so-far unassessed systems.

15. SUBJECT TERMS
Industrial Control Systems; Navy Ships; cybersecurity; Operational Test and Evaluation

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES
a. REPORT	b. ABSTRACT	c. THIS PAGE	SAR	35
Unclassified	Unclassified	Unclassified		

19a. NAME OF RESPONSIBLE PERSON	19b. PHONE NUMBER
Mark Herrera	703-578-2762