# Rethinking Cyber Security in the Smart Manufacturing

# Environment

Matthew E. Luallen

Lead Research Scientist Information Trust Institute, University of Illinois – Urbana

Vice-President of Coordinated Vulnerability Awareness, CyManII

/imagine: securing in small bytes

## Agenda (underlying theme)

- Understanding how cyber risks are impeding the implementation of analytics and AI initiatives
- Discussing how the interface of IT and OT systems are greatly increasing the attack surface area
- Analyzing the risks and consequences of a breach
- Where to start building cyber resilience in the smart factory

Awareness with a formalized approach to cybersecurity and the selection of smart factory and connected worker improvements

## **ICS Advisory Project**

			S ADVISORIES: ICS Asset	t Type Metrics				
		1 Vendor	- Product	• Asset Type	e	- Select da	ate range	•
		Arlvisonv	Percentage by Vendor	Advisory Percentage by Prode	uct	ICS Asset Type Per	centage by Advi	sory
	ICS Asset Type	Count Per CISA ICS Advisory 🔻	• Siemens					Control System ( DCS, SCADA, BMS) Field Controller/ RTU/PLC/IED/IoT
1.	Control System (DCS, SCADA, BMS)	543	Schneider Electric     Rockwell     Automation	9.1% D	Multiple Products DIAEnergie VDesigner	21.		Engineering Workstation Operation System ( MES, PLM, EMS, N
2.	Field Controller/RTU/PLC/IED/IoT Edge	543	<ul> <li>Mitsubishi Electric</li> <li>Moxa</li> <li>GE</li> </ul>	42.4% 6.1% 0 D	IMPLICITY DASDEC Sutomation Worx Software Suite	7.9%		Switch/Wireless Access Point/Rout Actuator/Converter/ Sensors/IoT/Meas
3.	Engineering Workstation	314	<ul> <li>ABB</li> <li>Hitachi Energy</li> <li>Philips</li> <li>Delta Electronics</li> </ul>	6.1% A	vehMI	12.3%		Human-Machine Interface (HMI) Physical Access C Data Historian
4.	Operation System (MES, PLM, EMS, NMS, CMMS, EPM, RS, MS) Engineering Workstation	312	Deta Lectronics     Honeywell     others	0. 70 6 104	Drawings SDK thers	12.4%		Operating System Input/Output Serv Safety Instrument Data Diode Serial Firewall
5.	Switch/Wireless Access Point/Router/Gateway/Firewall/Remote Access/Process Communication Unit	281	c	ount Per CISA ICS Advisory 🔹	Release Date	<ul> <li>CISA ICS Advisory</li> </ul>	Vendor	Product
6.	Actuator/Converter/Sensors/IoT/Measurement/Power Supply	200	dge	543 1. 543 314	Jul 20, 2023	Schneider Electric EcoStruxure Products, Modicon PLCs, and Programmable Automation Controllers		EcoStruxure Products, Modicon PLCs, and Programmable Automation Controllers
-			NMS, CMMS, EPM, RS,	312 2.	Jul 18, 2023 Jul 18, 2023	WellinTech KingHistorian GeoVision GV-ADR2701	WellinTech	KingHistorian GV-ADR2701
7.	Human-Machine Interface (HMI)	115	note Access/Process	281 4.	Jul 18, 2023	Keysight N6845A Geolocation Server	Keysight Technologies	N6854A Geolocation Server
8.	Physical Access Control System/CCTV	99	easurement/Power	200 5.	Jul 18, 2023	GE Cimplicity	GE Digital	CIMPLICITY
		2000		6.	Jul 18, 2023	Weintek Weincloud	Weintek	Weincloud
9.	Data Historian	56	TV	99 56	Jul 18, 2023 Jul 18, 2023	Iagona ScrutisWeb Rockwell Automation Kinetix 5700 DC Bus Power	Iagona Rockwell Automation	ScrutisWeb Kinetix 5700
10.	Operating System/RTOS	38		38 o 1 - 15 / 15 < >		Supply Series A		Everyon BKS LY and 100/2529 < >
		1 - 15 / 15 < >	roject on Twitter @AdvisoryIcs	© 2023 ICS Advisory Project	Send question or comm	ents about the ICS Advisory Proj Priva		yproj@icsadvisoryproject.com ker Studio   []

https://www.icsadvisoryproject.com/ics-advisory-dashboards/ics-asset-id-pm-levels

## Infrastructure Attacks (IT / OT interconnection)

- Customized malware with persistence in routers
- BlackTech actors use Living off the Land (LotL) TTPs to blend in with normal operating system and network activities, allowing them to evade detection by endpoint detection and response (EDR) products.
- Network defenders should monitor network devices for unauthorized downloads of bootloaders and firmware images and reboots. Network defenders should also monitor for unusual traffic destined to the router, including SSH
- People's Republic of China-Linked Cyber Actors Hide in Router Firmware
- September 27, 2023 : Alert: AA23-270A

https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-270a



demonstrated capabilities in modifying router firmware without detection and exploiting routers

### Attacks with Machine Learning

- Inclusion of Dall E 3 with GPT-4
  - Associating models together with generative AI
  - Analyze text, objects and the setting
- What other inputs can and will add to Generative Al abilities



Describe, are there any passwords on the slide?

Yes, the image contains multiple instances of usernames and their associated passwords listed under various operating systems and applications, such as:
 Kali 2 Linux: username "root" with a corresponding password
 Windows Server 2008: username "Administrator" with a corresponding password "P@sswOrd"
 Windows 10: username and a corresponding password are mentioned
 Ubuntu: username "root" with a corresponding password
 Windows Server 2022: username "Administrator" with a corresponding password
 Windows Server 2022: username "Administrator" with a corresponding password

# **Researching Attacks on Machine Learning**

- MITRE Caldera Automated Adversary Emulation Platform
  - Arsenal Plugin
- Discover ML specific services Torchserve
- Discover GPUs on a system
- Stage a local image for classification
- Install ML-related tools (on C2-server or victim system): Python, <u>Microsoft Counterfit</u>, Tensorflow-CPU, Tensorflow-GPU
- Gain API access to a served model (Torchserve)
- Build a custom Microsoft Counterfit target and stage an attack

25 mitre.org/news-insights/news-release/microsoft-and-mitre-create-tool-help-security-teams-prepare-attacks

G 🛧 😥 🛛 🔵

Home 
Mews & Insights
Microsoft and MITRE Create Tool to Help Security Teams Prepare for Attacks on Machine Learning Systems

Microsoft and MITRE Create Tool to Help Security Teams Prepare for Attacks on Machine Learning Systems



ARTIFICIAL INTELLIGENCE

CYBERSECURITY

New Arsenal plug-in brings together Microsoft Counterfit, MITRE CALDERA<sup>™</sup>, and MITRE ATLAS<sup>™</sup> to help cybersecurity practitioners better understand threats to machine learning systems. (*Above, MITRE's Christina Liaghati and Tabitha Colter test Arsenal in* 

### **Recent Harvard Business School Paper**

- Study conducted with Boston Consulting Group, a global management consulting firm, we examine the performance implications of AI on realistic, complex, and knowledge-intensive tasks.
- Centaurs (delegation) and Cyborgs (complete integration)
- 758 Consultants
  - 12.2% more tasks, 25.1% faster, 40% higher quality
- Tasks outside the frontier
  - 19% error rate using AI vs not using it
  - Do not just implement AI for the sake of implementing AI

https://papers.ssrn.com/sol3/papers.cfm?abstract\_id=4573321

#### Working Paper 24-013

Navigating the Jagged Technological Frontier: Field Experimental Evidence of the Effects of AI on Knowledge Worker Productivity and Quality

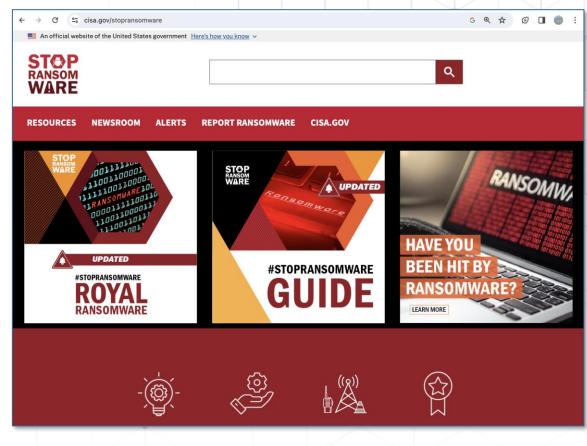
Fabrizio Dell'Acqua Edward McFowland III Ethan Mollick Hila Lifshitz-Assaf Katherine C. Kellogg Saran Rajendran Lisa Krayer François Candelon Karim R. Lakhani



Harvard Business School

### **Impacts of a Breach**

- Awareness of the breach
  - Outside notification
  - Internal detection
  - Late cycle awareness (quality)
- Manufacturing system down
- Part/material/mixture quality
- Workforce moral
- Supply chain



https://www.cisa.gov/stopransomware

### Towards Common Weakness Enumeration in Industrial Control Systems

- August 2023 IEEE Security & Privacy Paper
- Connecting MITRE CWEs with ISA 62443 in support of addressing categories of weaknesses formally
- Connected use cases
  - Equipment and Software Manufacturer and Their Associated Integrators
  - Workforce Development
  - Organizational Risks and Maturity

	-		
SPOTLIGHT			
Tours	and Common	Weakness En	
IOWa	ira Common	weakness En	umerations
in In	deservial Court	I Customer	
in in	dustrial Cont	rol Systems	
		ampaign and Cyber Manufacturing Inno	
		l Cyber Manufacturing Innovation Institu Cyber Manufacturing Innovation Institut	
Matt Bishop	University of California, Davis and C	ber Manufacturing Innovation Institute	
		ber Manufacturing Innovation Institute	unting lastitute
matthew Lua	inen   University of Illinois at Urbana-Cl	ampaign and Cyber Manufacturing Inno	vation institute
	The storyline of MITRE's com	mon weakness enumeration frames	work illustrates how the security
		nity can collaborate/cooperate with	
	infrastructure.	ps of technical knowledge to improv	e security and resilience of critical
		on a particular objective called for in	that apply more generally: classes,
	· · · · · · · · · · · · ·		
at	Station of the	the congressional language. One sub- group was tasked with identifying	categories. The hope is that design- ers and vendors of ICS hardware,
		the congressional language. One sub- group was tasked with identifying new classes of security vulnerabilities	categories. The hope is that design- ers and vendors of ICS hardware, software, and middleware will use
		the congressional language. One sub- group was tasked with identifying new classes of security vulnerabilities that are likely to arise in industrial	categories. The hope is that design- ers and vendors of ICS hardware, software, and middleware will use these identifications to provide bet-
art)		the congressional language. One sub- group was tasked with identifying new classes of security vulnerabilities that are likely to arise in industrial control systems (ICS). This group was known as the <i>Technical Project</i>	categories. The hope is that design- ers and vendors of ICS hardware, software, and middleware will use these identifications to provide bet- ter defense in their designs, and that asset owners will use them to develop
ALL A		the congressional language. One sub- group was tasked with identifying new classes of security vulnerabilities that are likely to arise in industrial control systems (ICS). This group was known as the Technical Project Team for New Classes of Security Vul-	categories. The hope is that design- ers and vendors of ICS hardware, software, and middleware will use these identifications to provide bet- ter defense in their designs, and that asset owners will use them to develop more care and defense in the con-
		the congressional language. One sub- group was tasked with identifying new classes of security vulnerabilities that are likely to arise in industrial control systems (ICS). This group was known as the <i>Technical Project</i>	categories. The hope is that design- ers and vendors of ICS hardware, software, and middleware will use these identifications to provide bet- ter defense in their designs, and that asset owners will use them to develop
		the congressional language. One sub- group was tasked with identifying new classes of security vulnerabilities that are likely to arise in industrial control systems (ICS). This group was known as the <i>Technical Project Team for New Classes of Security Vul-</i> nerabilities for ICS (TPT-NCSV). Introduction	categories. The hope is that design- ers and vendors of ICS hardware, software, and middleware will use these identifications to provide bet- ter defense in their designs, and that asset owners will use them to develop more care and defense in the con- figurations and operations of what the vendors provide. Furthermore, a framework enables the identifica-
Y		the congressional language. One sub- group was tasked with identifying new dasses of security vulnerabilities that are likely to arise in industrial control systems (ICS). This group was known as the Tedminal Project Team for New Classes of Security Vul- nerabilities for ICS (TPT-NCSV). Introduction The DoE TPT-NCSV leadership rec-	categories. The hope is that design- ers and vendors of ICS hardware, software, and middleware will use these identifications to provide bet- ter defense in their designs, and that asset owners will use them to develop more care and defense in the con- figurations and operations of what the vendors provide. Furthermore, a framework enables the identifica- tion and association of new vulner-
	The U.S. Congress 2020 Nation	the congressional language. One sub- group was tasked with identifying new dasses of security vulnerabilities that are likely to arise in industrial control systems (ICS). This group was known as the <i>Technial Projec- Tam for New Classe of Security Vul- nerabilities for ICS</i> (TPTENCSV). Introduction The DoE TPTENCSV leadership rec- ognized the vulne of existing systems of	categories. The hope is that design- ers and vendors of ICS hardware, software, and middleware will use these identifications to provide bet- ter defense in their designs, and that asset owners will use them to develop more care and defense in the con- figurations and operations of what the vendors provide. Furthermore, a framework enables the identifica-
	Defense Authorization Act con	the congressional language. One sub- group was tasked with identifying new classes of security vulnerabilities that are likely to arise in industrial control systems (ICS). This group was known as the Technical Projec- Tam for New Classe of Security Vul- nerabilities for ICS (TPT-NCSV). Introduction The DoE TPT-NCSV leadership rec- ognized the value of existing systems of la knowledge about cybersecurity in T systems [such as MITRE's common	categories. The hope is that design- ers and vendors of ICS hardware, software, and middleware will use these identifications to provide bet- ter defense in their designs, and that asset owners will use them to develop more care and defense in the con- figurations and operations of what the vendors provide. Furthermore, a framework enables the identifica- tion and association class; this enables data analysis of vulnerability cocurrences, which informs priori-
	Defense Authorization Act con tains a Section 5726 entitled "Secu	the congressional language. One sub- group was tasked with identifying new dasses of security valuenabilities that are likely to arise in industrial control systems (ICS). This group was known as the <i>Technical Project Tam for New Classes of Security Val-</i> nerabilities for ICS (TPT-NCSV). Introduction The DoE TPT-NCSV leadership rec- ognized the value of existing systems of knowledge about cybersecurity in IT - systems [such as MITRE's common weakness enumeration (CWE) <sup>1</sup> ].	categories. The hope is that design- ers and vendors of ICS hardware, software, and middleware will use these identifications to provide bet- ter defense in their designs, and that asset owners will use them to develop more care and defense in the con- figurations and operations of what the vendors provide. Furthermore, a framework enables the identifica- tion and association of new valuer- abilities within a common class; this enables data analysis of valuerability occurrences, which informs priori- tization of mitigation investments.
	Defense Authorization Act con	the congressional language. One sub- group was tasked with identifying new classes of security vulnerabilities that are likely to arise in industrial control systems (ICS). This group was known as the Tachnial Project Tam for New Classe of Security Vul- nerabilities for ICS (TPT-NCSV). Introduction The DoE TPT-NCSV leadership rec- ognized the value of existing systems (of knowledge about cybersecurity in IT systems [such as MITRE's common weakness enumeration (CWE <sup>13</sup> ), and approxide their mission so as to	categories. The hope is that design- ers and vendors of ICS hardware, software, and middleware will use these identifications to provide bet- ter defense in their designs, and that asset owners will use them to develop more care and defense in the con- figurations and operations of what the vendors provide. Furthermore, a framework enables the identifica- tion and association class; this enables data analysis of vulnerability cocurrences, which informs priori-
Y	Defense Authorization Act con tains a Section 5726 entitled "Secu ing Energy Infrastructure" that direc the Department of Energy (DoE) 1 establish a working group responsib	the congressional language. One sub- group was tasked with identifying new classes of security vulnerabilities that are likely to arise in industrial control systems (ICS). This group was known as the Tachnical Project Tam for New Classe of Security Vul- nerabilities for ICS (TPT-NCSV). Introduction The DoE TPT-NCSV leadership rec- opsing the value of existing systems (of knowledge about cybersecurity in IT systems (such as MITRE's common weakness enumeration (CWEF) <sup>1</sup> ), and approached their mission so as to emulate and potentially integrate with those systems, particularly with trends	categories. The hope is that design- ers and vendors of ICS hardware, software, and middleware will use these identifications to provide he- ter defense in their designs, and that asset owners will use them to develop more care and defense in the con- figurations and operations of what the vendors provide. Furthermore, a framework enables the identifica- tion and association of new vulner- abilities within a common class; this enables data analysis of vulnerability occurrences, which informs priori- tization of mitigation investments. Importantly, TPT-NCSV leadenship viewed cybersecurity management
	Defense Authorization Act cor tains a Section 5726 entitled "Secu ing Energy Infrastructure" that direc the Department of Energy (DoE) t establish a working group responsib for evaluating elements of securit	the congressional language. One sub- group was tasked with identifying new dasses of security valneabilities that are likely to arise in industrial control systems (ICS). This group was known as the <i>Technial Projec- Tam for New Classe of Security Val- neabilities for ICS</i> (TPT-NCSV). Introduction The DoE TPT-NCSV leadership rec- ognized the value of existing systems of knowledge about cybersecurity in T - systems [such as MITRE's common weakness enumeration (CWEF)], and approached their mission so as to enualize and potentially integrate with the those systems, particularly with trends of IT/operational technology (IT/	categories. The hope is that design- ers and vendors of ICS hardware, software, and middleware will use these identifications to provide bet- ter defense in their designs, and that asset owners will use them to develop more care and defense in the con- figurations and operations of what the vendors provide. Furthermore, a framework enables the identifica- tion and association of new valuer- abilities within a common class; this enables data analysis of vulnerability. Importantly, TPT-NCSV leadership viewed cybersecurity management and procurement processes a poten- tial sources of vulnerabilities, not just
	Defense Authorization Act cor tains a Section 5726 entitled "Secu- ing Energy Infrastructure" that direc the Department of Energy (DoE) t establish a working group responsis for evaluating elements of securit program elements, and development	the congressional language. One sub- group was tasked with identifying new dasses of security vulnerabilities that are likely to arise in industrial control systems (ICS). This group was known as the <i>Technical Project Team for New Classes of Security Vul- nerabilities for ICS (TPT-NCSV)</i> . Introduction The DoE TPT-NCSV leadership rec- ognized the value of existing systems of knowledge about cybersecurity in IT - systems [such as MITRE's common weakness enumeration (CWE) <sup>17</sup> ), and approached their mission so as to e-mulate and potentially integrate with those systems, particularly with trends of IT/operational technology (IT/ OT) covergence underway.	categories. The hope is that design- ers and vendors of ICS hardware, software, and middleware will use these identifications to provide bet- ter defense in their designs, and that asset owners will use them to develop more care and defense in the con- figurations and operations of what the vendors provide. Furthermore, a framework enables the identifica- tion and association of new vulner- abilities within a common class; this enables data analysis of vulnerability occurrences, which informs priori- tization of mitigation investments. Importantly, TPT-NCSV leadership viewed cybersecurity management and procurement processes as poten- tial sources of vulnerabilities, not just
e e e e e e e e e e e e e e e e e e e	Defense Authorization Act cor tains a Section 5726 entitled "Secu- ing Energy Infrastructure" that direc the Department of Energy (DoE) t establish a working group responsab for evaluating elements and developmen of national strategy. The DoE forme a voluntary group of public and pr	the congressional language. One sub- group was tasked with identifying new dasse of security valuenbilities that are likely to arise in industrial control systems (ICS). This group was known as the <i>Technical Project Tam for New Classe of Security Val-</i> nerabilities for ICS (TPT-NCSV). Introduction The DoE TPT-NCSV leadership rec- oprized the value of existing systems of knowledge about cybersecurity in IT - systems [such as MITRE's common weakness enumeration (CWE) <sup>17</sup> ], and approached their mission so as to emulate and potentially integrate with the those systems, particularly with treds of IT/operational technology (IT/ OT) convergence underway: They adopted the fundamental idea of highlighting areas and activi-	categories. The hope is that design- ers and vendors of ICS hardware, software, and middleware will use these identifications to provide bet- ter defense in their designs, and that asset owners will use them to develop more care and defense in the con- figurations and operations of what the vendors provide. Furthermore, a framework enables the identifica- tion and association of new valuer- abilities within a common class; this enables data analysis of vulnerability occurrences, which informs priori- tization of mitigation investments. Importantly, TPT-NCSV leadership viewed cybrescurity management and procurement processes a poten- tial sources of vulnerability, not just the technology itself in isolation. The TPT-NCSV committee drew its membership from govern-
	Defense Authorization Act cor tains a Section 5726 entitled "Secu ing Energy Infrastructure" that direc the Department of Energy (DoE) istabilia avoing group responsib for evaluating elements, and developme of national strategy. The DoE forme a voluntary group of public and pr vate secore teaders called the Scouri	the congressional language. One sub- group was tasked with identifying new classes of security vulnerabilities that are likely to arise in industrial control systems (ICS). This group was known as the Tachnial Projec- Tam for New Classe of Security Vul- nenibilities for ICS (TPT-NCSV). Introduction The DoE TPT-NCSV leadenship rec- ognized the value of existing systems of la knowledge about cybersecurity in IT systems [such as MITRE's common weakness enumeration (CWEF)], and approached their missions on as to emulate and potentially integrate with those systems particularly with trends of IT/operational technology (TI/ OT) corresponce underway. They adopted the fundamental idea of highlighting areas and activ- ties within ICS that potentially allow	categories. The hope is that design- ers and vendors of ICS hardware, software, and middleware will use these identifications to provide bet- ter defense in their designs, and that asset owners will use them to develop more care and defense in the con- figurations and operations of what the vendors provide. Furthermore, a framework enables the identifica- tion and association of new vulner- abilities within a common class; this enables data analysis of vulnerability cocurrences, which informs priori- tization of mitigation investments. Importantly, TPT-NCSV leadership viewed cybersecurity management tal sources of vulnerabilities, not just the technology itself in isolation. The TPT-NCSV committee drew its membership from govern- ment organizations, owner/opera-
	Defense Authorization Act cor tains a Section 5726 entitled "Secu- ing Energy Infrastructure" that direc the Department of Energy (DoE) establish a working group responsib for evaluating elements, and developme of national strategy. The DoE forme a voluntary group of public and pr vate sector leaders called the Sociir Energy Infrastructure Taik Force (SI	the congressional language. One sub- group was tasked with identifying new dasse of security valueabilities that are likely to arise in industrial control systems (ICS). This group was known as the <i>Tachnial Project</i> <i>Tame for New Classe of Security Val- nenibilities for ICS</i> (TPT-NCSV). <b>Introduction</b> The DoE TPT-NCSV leadership rec- ognized the value of existing systems of la knowledge about cybersecurity in T systems [such as MITRE's common weakness enumeration (CWE) <sup>1</sup> ], and approached their mission so as to e- mulate and potentially integrate with the those systems, particularly with trends of TT/operational technology (TT/ OT) convergence underway. They adopted the fundamental idea of highlighting areas and activi- ties within ICS that potentially laigues	categories. The hope is that design- ers and vendors of ICS hardware, software, and middleware will use these identifications to provide bet- ter defense in their designs, and that asset owners will use them to develop more care and defense in the con- figurations and operations of what the vendors provide. Furthermore, a framework enables the identifica- tion and association of new valuer- abilities within a common class; this enables data analysis of vulnerability cocurrences, which informs priori- tization of mitigation investments. Importantly, TPT-NCSV leadership wiewed cybersecurity management and procurement processes a poten- ial sources of vulnerabilities, not just the technology itself in isolation. The TPT-NCSV committee drew its membership from govern- ment organizations, owner/opera- tors of power systems, industry
	Defense Authorization Act cor tains a Section 5726 entitled "Secu ing Energy Infrastructure" that direc the Department of Energy (DoE) istabilia avoing group responsib for evaluating elements, and developme of national strategy. The DoE forme a voluntary group of public and pr vate secore teaders called the Scouri	the congressional language. One sub- group was tasked with identifying new dasses of security valneabilities that are likely to arise in industrial control systems (ICS). This group was known as the <i>Technial Projec- Tame for New Classe of Security Val- neabilities for ICS</i> (TPT-NCSV). Introduction The DoE TPT-NCSV leadership rec- ognized the value of existing systems of la knowledge about cybersecurity in T - systems [such as MITRE's common weakness enumeration (CWEF)], and approached their mission so as to on emulate and potentially integrate with the those systems, particularly with trends of IT/operational technology (IT/ CVT) convergence underway. They adopted the fundamental is dea of highlighting areas and acti- ties within ICS duat potentially allow for high-consequence valuneabilities. The focus is not on particular value- abilities (e.g., unused web-servers	categories. The hope is that design- ers and vendors of ICS hardware, software, and middleware will use these identifications to provide bet- ter defense in their designs, and that asset owners will use them to develop more care and defense in the con- figurations and operations of what the vendors provide. Furthermore, a framework enables the identifica- tion and association of new valuer- abilities within a common class; this enables data analysis of vulnerability cocurrences, which informs priori- tization of mitigation investments. Importantly, TPT-NCSV leadership viewed cybersecurity management and procurement processes a poten- tial sources of vulnerabilities, not just the technology itself in isolation. The TPT-NCSV committee drew its membership from govern- ment organizations, owner/opera- tors of power systems, industry and manufacturers, academic insti-
	Defense Authorization Act cor tains a Section 5726 entitled "Secu- ing Energy Infrastructure" that direc the Department of Energy (DoE) establish a working group responsib for evaluating elements, and developme of national strategy. The DoE forme a voluntary group of public and pr vate sector leaders called the Sociir Energy Infrastructure Taik Force (SI	the congressional language. One sub- group was tasked with identifying new classes of security vulnerabilities that are likely to arise in industrial control systems (ICS). This group was known as the <i>Technical Project Tam for New Classe of Security Vul- nerabilities for ICS</i> (TPT-NCSV). Introduction The DoE TPT-NCSV leadership rec- ognized the value of existing systems of knowledge about cybersecurity in IT systems [sech as MITRE's common weakness enumeration (CWE <sup>31</sup> )], and approached their mission so as to emulae and potentially integrate with those systems, particularly with trends of IT/operational technology (TI/ OT) corregrence underway. They adopted the fundamential idea of highlighting meas and activ- ties within ICS that potentially allow for high-consequence vulnerabilitas.	categories. The hope is that design- ers and vendors of ICS hardware, software, and middleware will use these identifications to provide bet- ter defense in their designs, and that asset owners will use them to develop more care and defense in the con- figurations and operations of what the vendors provide. Furthermore, a framework enables the identifica- tion and association of new vulner- abilities within a common class, this enables data analysis of vulnerability cocurrences, which informs priori- tization of mitigation investments. Importantly, TPT-NCSV leadership viewed cybersecurity management and procurement processes as poten- tial sources of vulnerabilities, not just the technology itself in isolation. The TPT-NCSV committee draw its membership from govern- ment organizations, owner/opera- tors of power systems, industry

https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10194510

### **Cyber Informed Engineering Practioneer's Workshop**

- Leveraging generative Al to identify and prioritize weaknesses early for technology to start building resiliency early
  - Prioritization (High impact / consequence)
  - Segmentation
  - Systematic Monitoring

Cyber-Informed Engineering

PRACTITIONERS' WORKSHOP September 6, 2023

### Addressing Vulnerabilities Early: CIE for Research-Stage Technology



https://www.youtube.com/watch?v=TLdcc\_OI3-k

# **Sample Report Narrative (CIE Workshop)**

- Categorized by CWE, attack TTP, and mitigations
- ['CWE-20', 'CWE-306', 'CWE-89', 'CWE-200', 'CWE-119', 'CWE-78', 'CWE-434']
- A few pennies for our quick thoughts, 4.3

CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

**CWE Impact**: This CWE occurs when a program writes to or reads from a memory buffer beyond its boundaries, leading to buffer overflows or underflows. It can result in memory corruption, crashes, or the execution of arbitrary code.

MITRE ATT&CK TTPs: T1059 - Command and Scripting Interpreter, T1136 - Create Account, T1190 - Exploit Public-Facing Application

**Abstract and/or Technology Association**: CWE-119 can be associated with the abstract as it involves analyzing and redesigning the tooling used in the thermoforming process. If the tooling does not properly handle memory buffers, it can be vulnerable to buffer overflow or underflow attacks.

**SDA, CPP, SRDI, CEEQ Associations**: Implementing secure coding practices, such as bounds checking and input validation, can be part of a Secure Defensible Architecture (SDA). A Cyber Physical Passport (CPP) can store metadata related to memory buffer handling mechanisms used in the manufacturing process. Secure Research and Development Infrastructure (SRDI) can ensure that proper memory buffer handling techniques are integrated into the tooling design and development process. Cybersecurity, Energy, and Emissions Quantification (CEEQ) can consider the impact of CWE-119 on energy consumption and emissions associated with potential attacks.

Overall, the analysis of the provided CWEs in relation to the abstract and technology/system highlights several potential vulnerabilities and associated impacts. These vulnerabilities can be exploited using various MITRE ATT&CK TTPs, which an adversary may employ to compromise the security and integrity of the thermoforming manufacturing process.

To address these vulnerabilities and secure the efforts today and in the future, the following recommendations can be implemented:

- Implement strict input validation mechanisms to prevent CWE-20 (Improper Input Validation) vulnerabilities.
- Ensure proper authentication mechanisms are in place to prevent CWE-306 (Missing Authentication for Critical Function) vulnerabilities.
- Implement secure coding practices, such as input sanitization and parameterized queries, to prevent CWE-89 (SQL Injection) vulnerabilities.
- Implement access controls and encryption mechanisms to prevent CWE-200 (Information Exposure) vulnerabilities.
- Implement proper bounds checking and input validation to prevent CWE-119 (Improper Restriction of Operations within the Bounds of a Memory Buffer) vulnerabilities.
- Use secure coding practices, such as input sanitization and parameterized commands, to prevent CWE-78 (Improper Neutralization of Special Elements used in an OS Command) vulnerabilities.
- Implement strict file type validation and restrict execution permissions on uploaded files to prevent CWE-434 (Unrestricted Upload of File with Dangerous Type) vulnerabilities.

By addressing these vulnerabilities and following the recommendations, the researcher can enhance the security of the thermoforming manufacturing process, protect against potential attacks, and ensure the integrity and efficiency of the production system.

- Total Input Tokens Used: 3213
- Total Output Tokens Used: 8337

Total Cost: \$0.0430

# Thank you!



Matthew E. Luallen Lead Research Scientist Education Translation

University of Illinois Urbana-Champaign The Grainger College of Engineering Information Trust Institute mluallen@illinois.edu