ENSCO

Cyber Attacks Made Simple

2023 Emergency Management Roundtable
Pittsburg, PA

Jeffrey Baca & Erin Plemons

CCIP
Center for Critical Infrastructure Protection

Introduction

Jeffrey Baca

- Air Force Veteran
- 7-Years Federal Government
- Background in network defense, insider threat, policy, and strategy

Erin Plemons

- Navy Veteran
- Background in penetration testing, blue-teaming, and cyber instruction
- Adjunct Professor at NYU

Center for Critical Infrastructure Protection (CCIP)

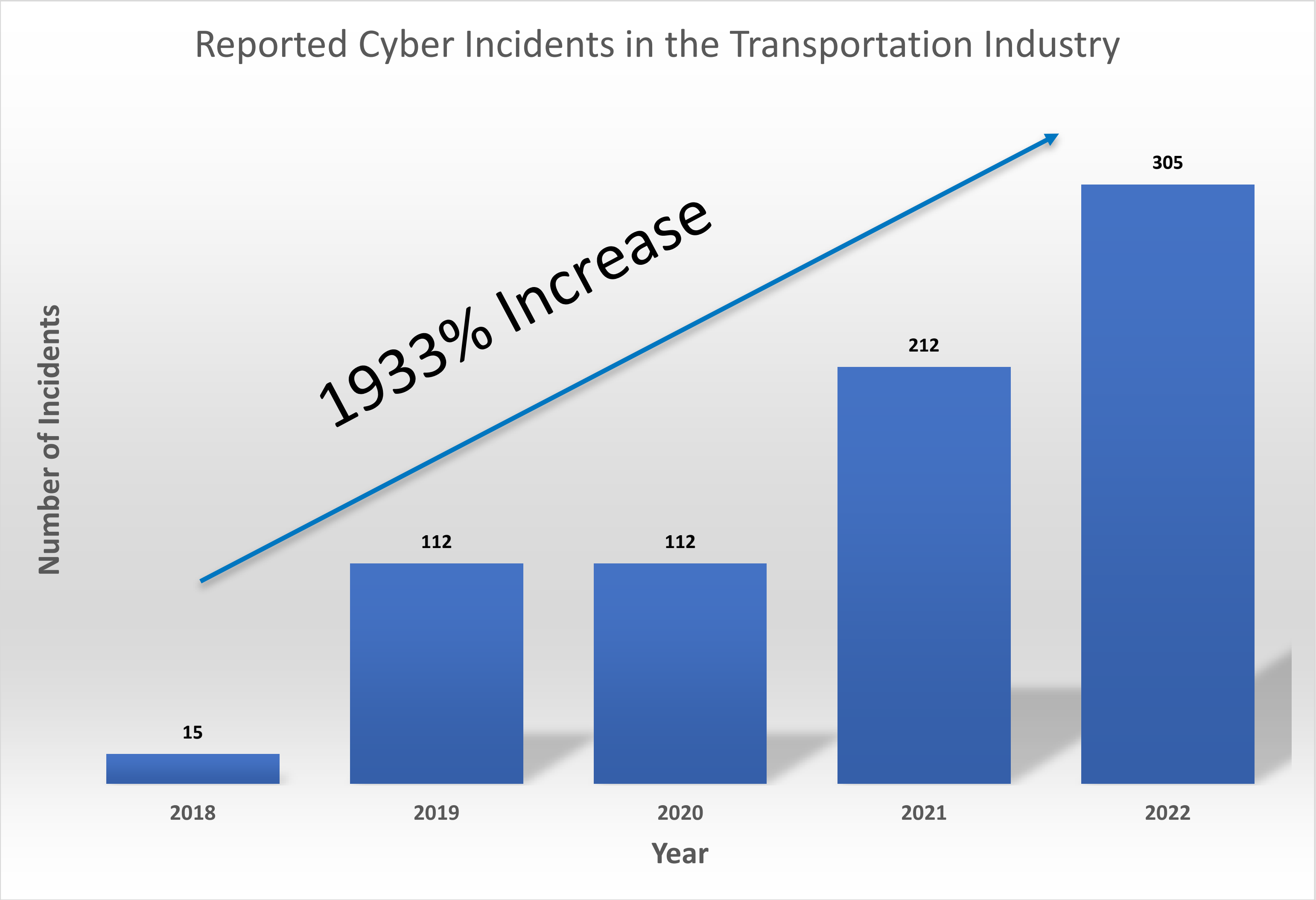
ENSCO created the Center for Critical Infrastructure Protection (CCIP) located at the Transportation Technology Center (TTC) located in Pueblo, CO. The CCIP's goal is to support critical infrastructure organizations with cyber demands and government protection mandates.

The CCIP focused on the following four areas: Training, Assessment, Testing, and Protection. The CCIP's success is built on ENSCO's 30+ year experience in cyber and physical security.

Cyber Attacks in Transportation

Cyber attacks in rail and other transportation modes have significantly increased over time.

Increased cyber vigilance is required to understand the threat, sustain operations, and ensure the safety, security, and resilience of our US National Interests.



Data reported by Verizon in yearly Data Breach Incident Report (DBIR)

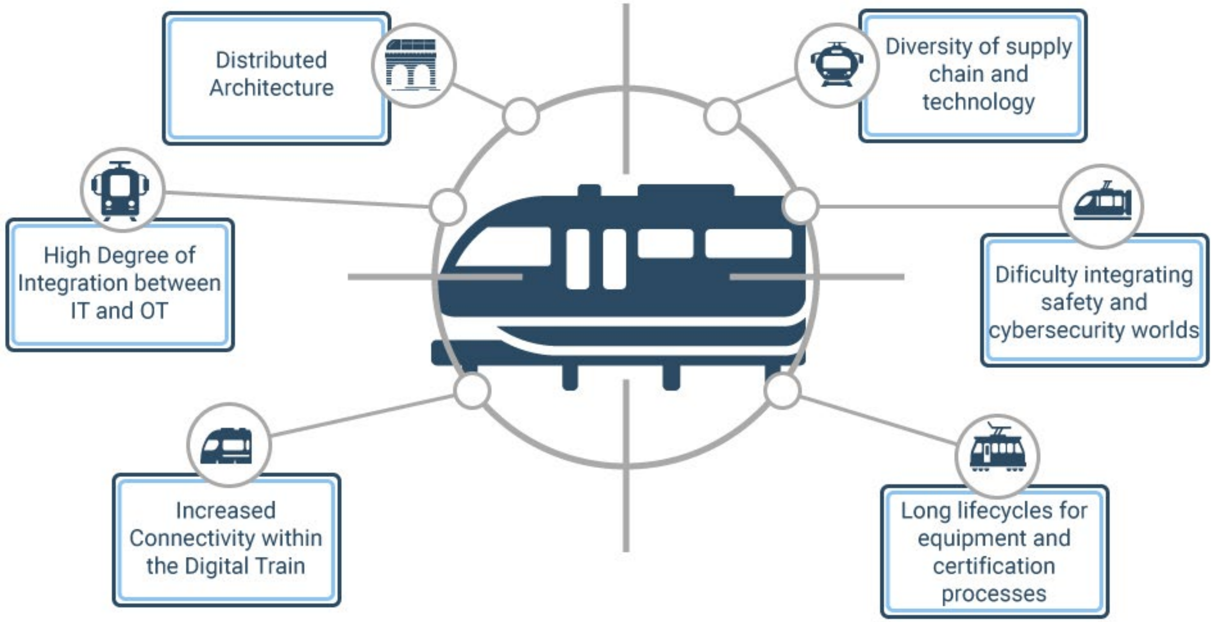
Cyber Risk

RISK = THREAT x VULNERABILITY x CONSEQUENCE

Enterprise Systems
Safety
Fire / Life
Operational Control

Potentially susceptible to

Electromagnetic interference
Jamming & Spoofing
Message modification
Denial of Service (DoS)
Assumption of control or denial of control
False data injects
Unauthorized access & intrusions
Data exfiltration
Malware & Ransomware
Supply chain risks
Physical damage or destruction


Distributed Architecture

Diversity of supply chain and technology

High Degree of Integration between IT and OT

Dificulty integrating safety and cybersecurity worlds

Increased Connectivity within the Digital Train

Long lifecycles for equipment and certification processes

Source: Securing the Railway Infrastructure - Infographic - Cyber Startup Observatory

Password Cracking

“Password cracking” is the process of guessing passwords to attempt to gain access to an account.

Password cracking utilities are openly available, easy to use, and billions of known passwords.

“Keyboard walks” are often used to create acceptable passwords but are known and often recognized by password cracking utilities.

8.4 billion passwords currently available in the most common password cracking list.

Characters	Numbers	Lowercase Letters	Uppercase and Lowercase Letters	Numbers, Lowercase, Uppercase Letters	Numbers, Upper, Lower, Letters, Symbols
6	Instantly	Instantly	Instantly	1-Second	5-Seconds
8	Instantly	5-Seconds	22-Minutes	1-Hour	8-Hours
10	Instantly	58 Minutes	1-Month	7-Months	5-Years
12	25-Seconds	3-Weeks	300-Years	2K-Years	34K-Years
15	6-Hours	1K-Years	43M-Years	600M-Years	15B-Years

Social Engineering

“Social engineering” is the tactic used by threat actors to attempt to trick users into permitting access to a system or sensitive information.

The price tag of the average social engineering related breach is $4.1M (IBM 2022 Cost if a Data Breach Report).

82% of data breaches involve the “human element” (2022 Data Breach Investigations Report).

90% of cyber attacks are targeting your employees instead of your technology (2022 State of Cybersecurity Trends Report).

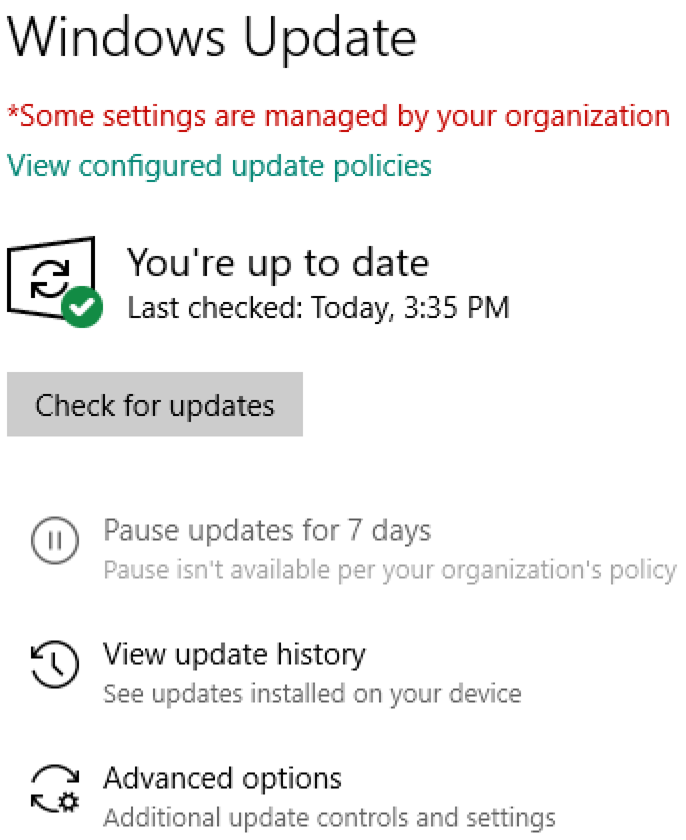
Out-Dated Software

“Out-dated software” refers to applications and operating systems that are missing security patches and updates.

For most organizations, it takes at least 215 days to patch vulnerabilities (Security Navigator 2023 Report)

40% of businesses do not have a formal patching process (Project Quant).

82% of successful cyber attacks use known vulnerabilities for which a patch is available (Dark Wolf's Incident Response Insights Report 2022)



Windows Update

*Some settings are managed by your organization

View configured update policies

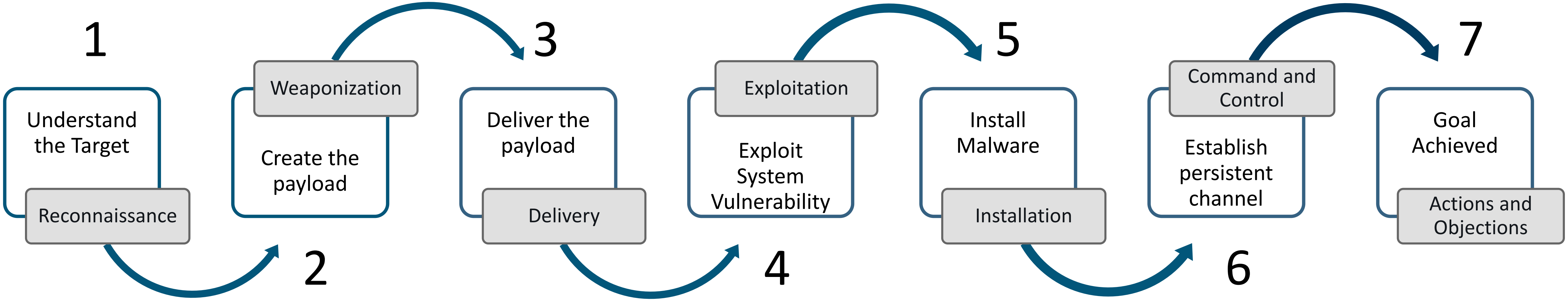
You're up to date
Last checked: Today, 3:35 PM

Pause updates for 7 days
Pause isn't available per your organization's policy

View update history
See updates installed on your device

Advanced options
Additional update controls and settings

Cyber Attack Process



1

Understand the Target

Reconnaissance

2

Weaponization

Create the payload

3

Deliver the payload

Delivery

4

Exploitation

Exploit System Vulnerability

5

Install Malware

Installation

6

Command and Control

Establish persistent channel

7

Goal Achieved

Actions and Objections

Common Vulnerabilities

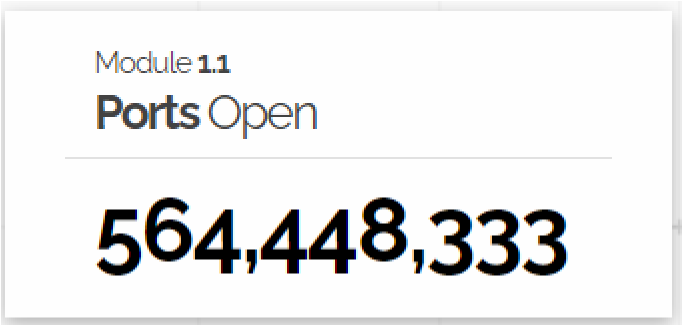
Default usernames and passwords

Lack of vendor support

Unpatched, outdated software, protocols and Services

Reduced awareness (safety focused vs security focused)

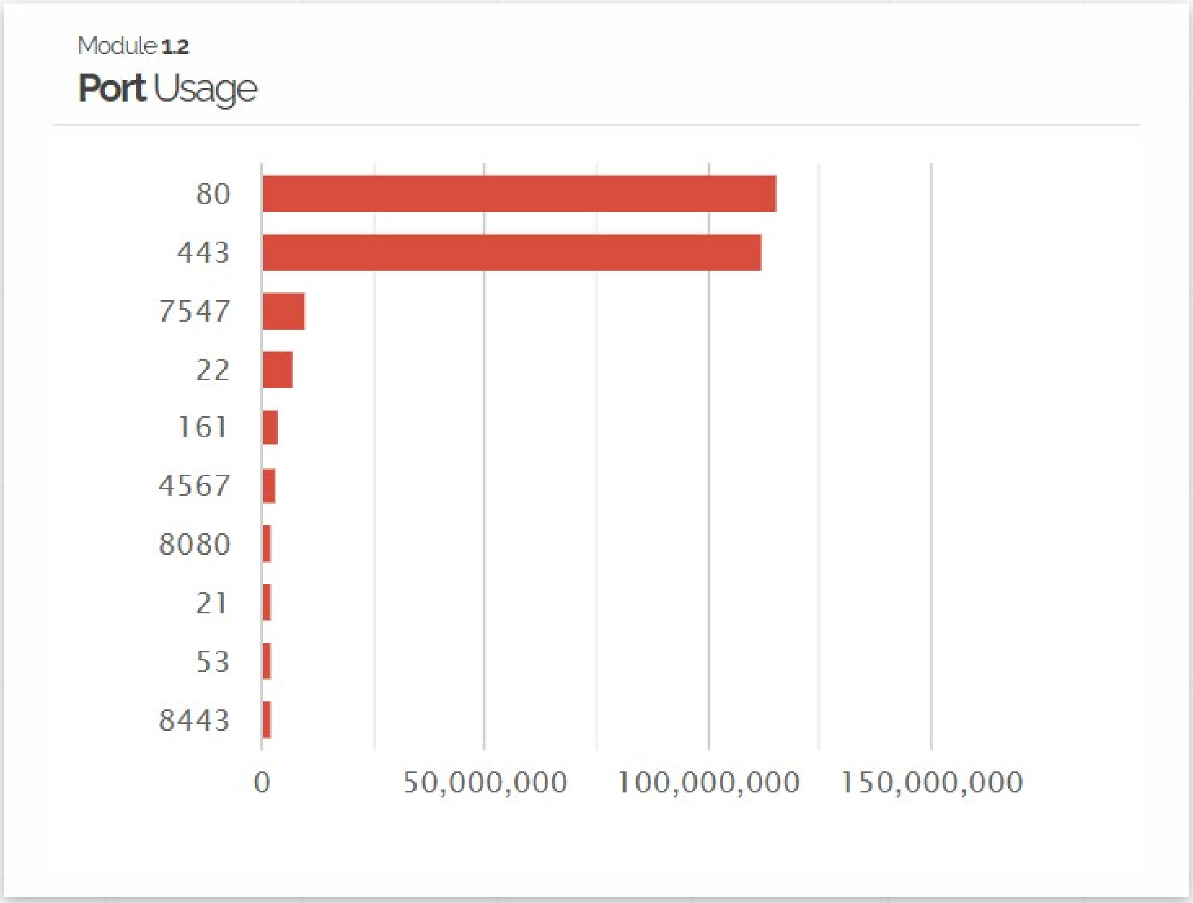
Operational and availability needs supersede security needs



Module 1.1

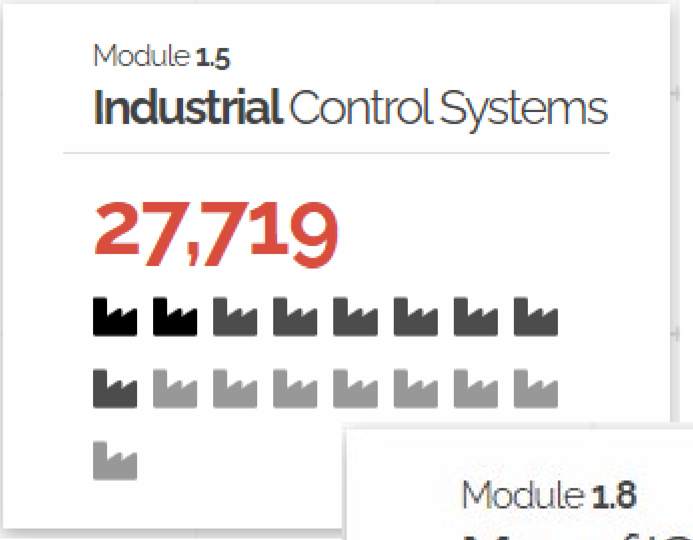
Ports Open

564,448,333



Module 1.2

Port Usage



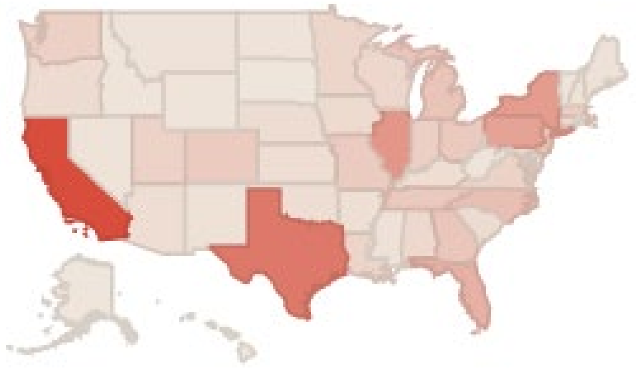
Module 1.5

Industrial Control Systems

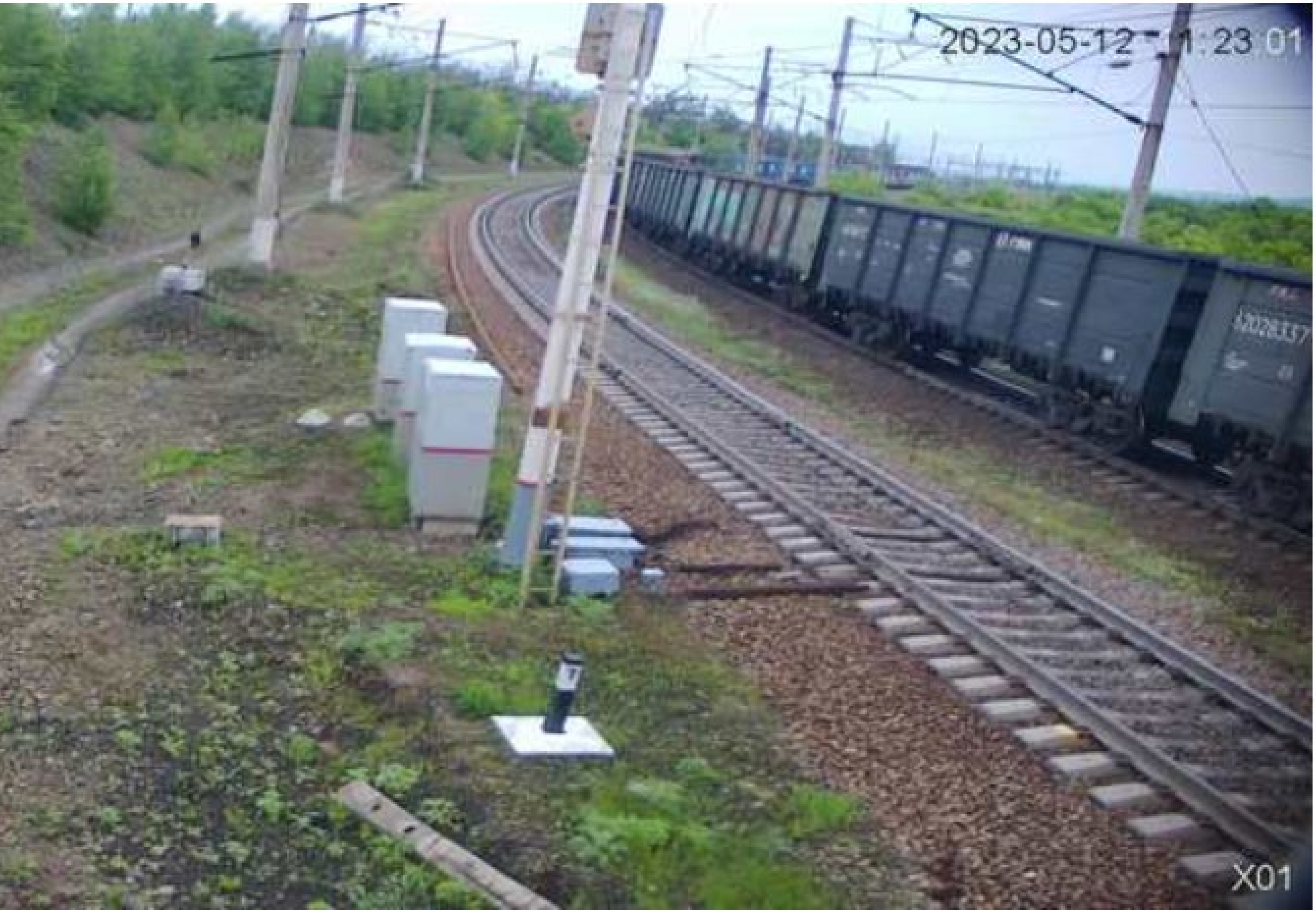
27,719

Module 1.8

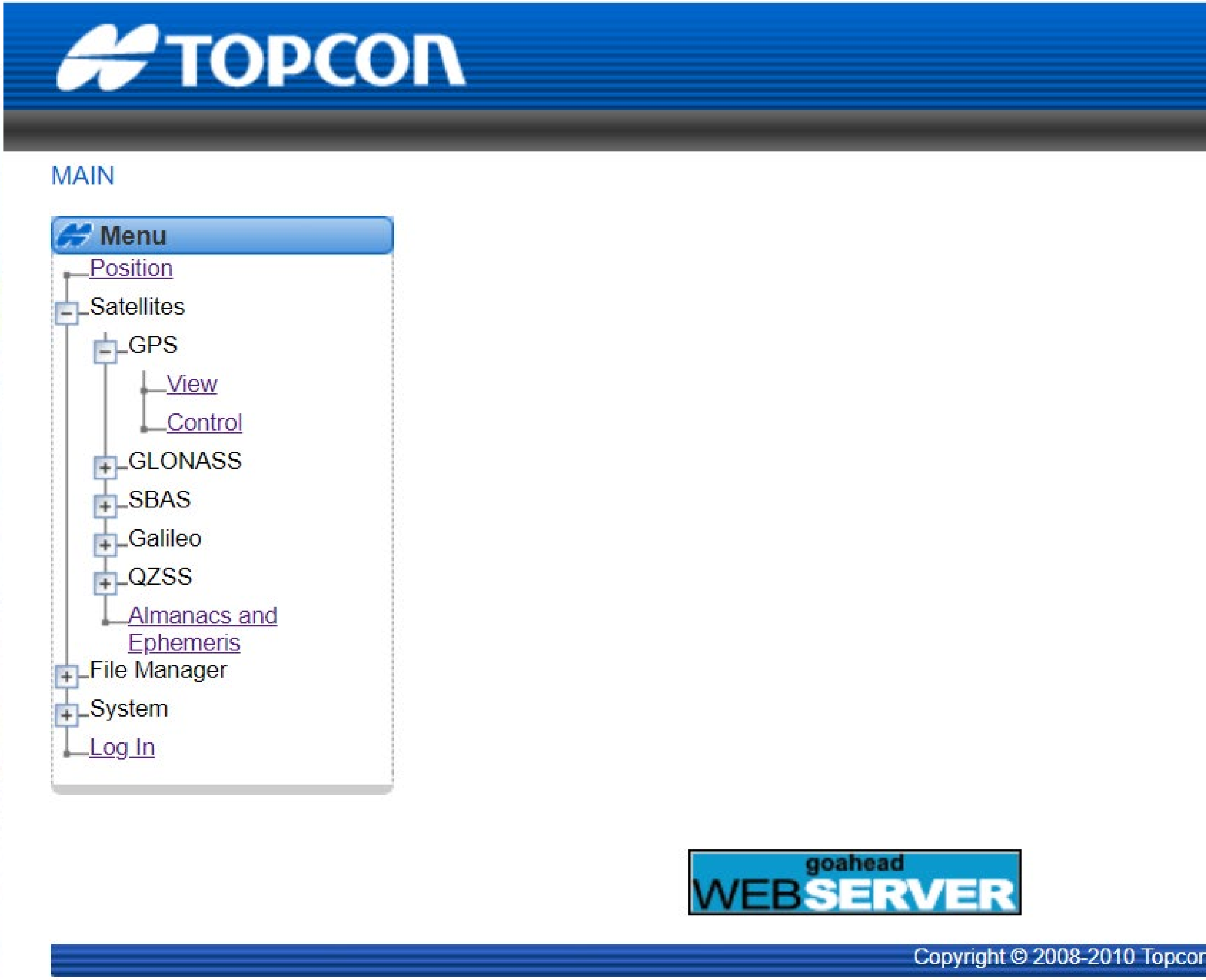
Map of ICS



Vulnerable Devices in Transportation

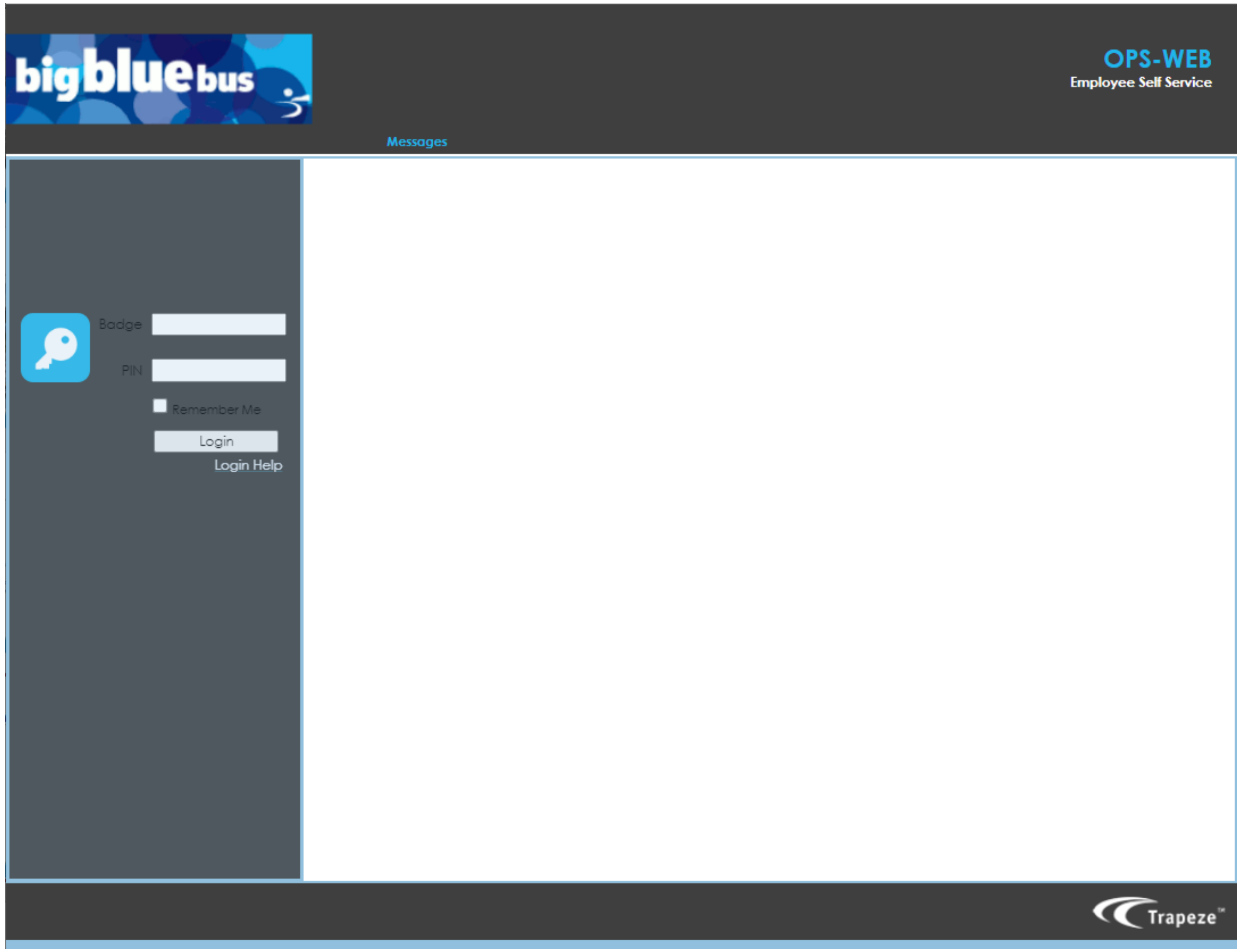


Live screen capture from security cameras without authentication



Web page for GPS and positioning without authentication

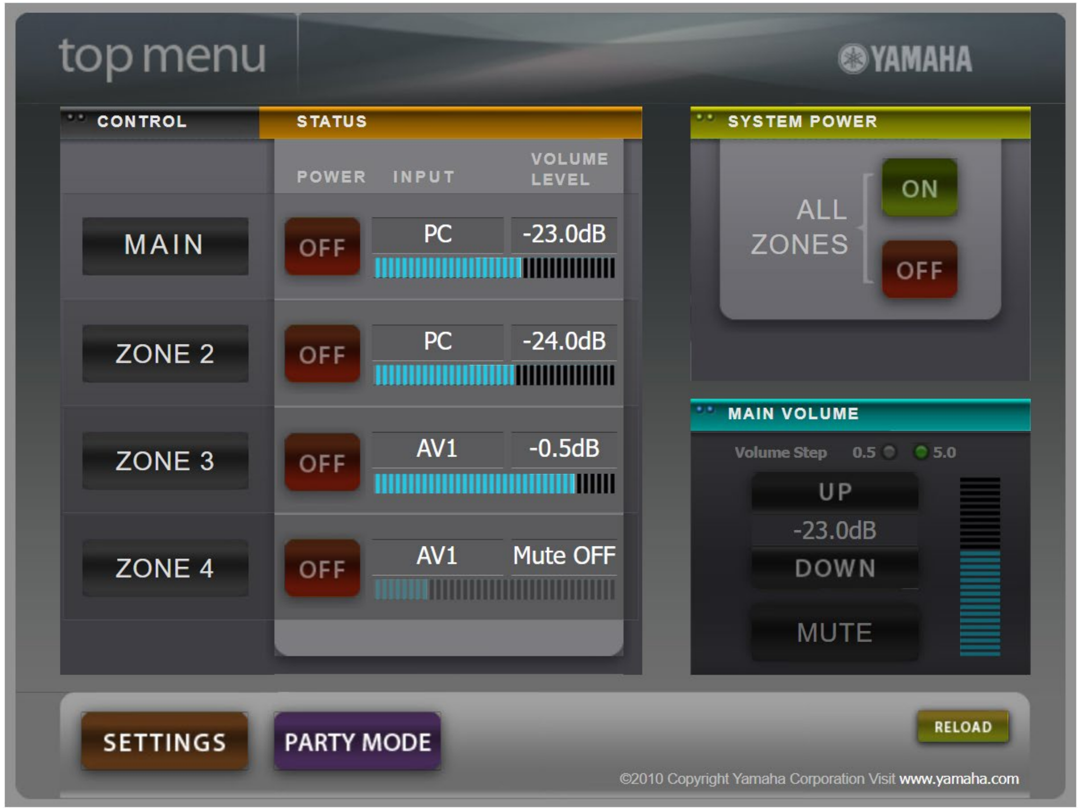
Vulnerable Devices in Transportation



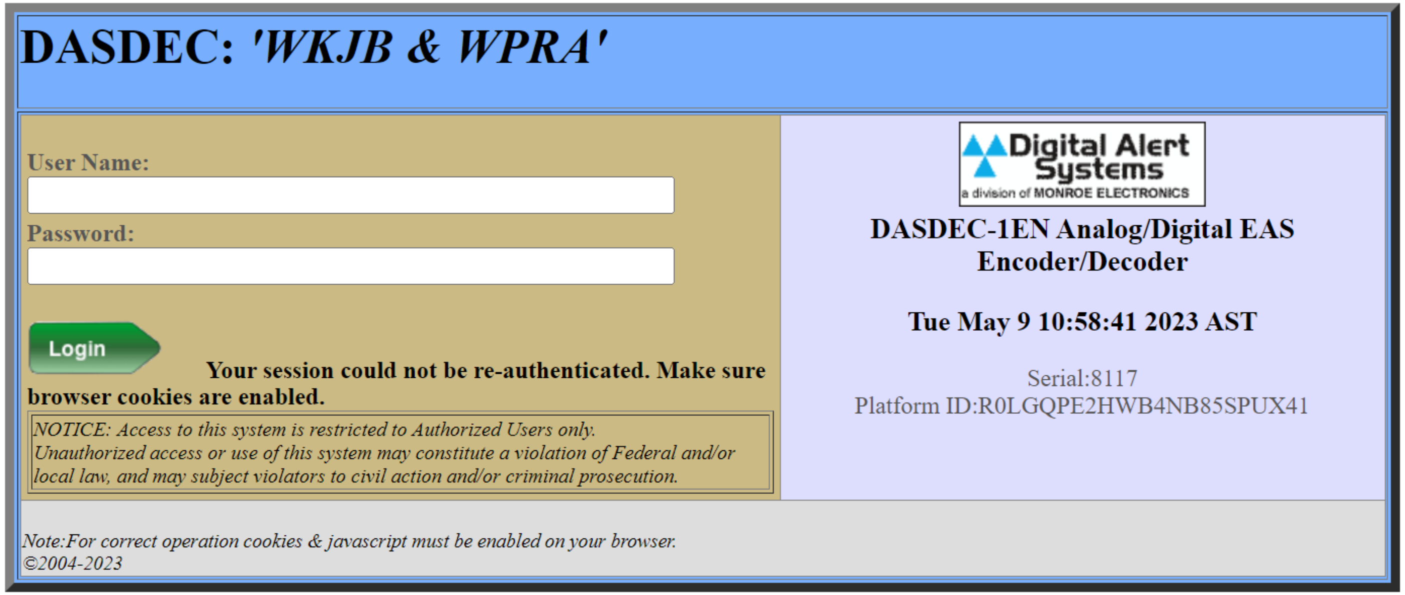
Web page for employees with:

- Internet-exposed log-in page
- Insufficient authentication requirements
- Clear-text protocols
- Exploitable vulnerabilities (CVE-2014-4078)

Vulnerable Devices in Transportation



Broadcast radio panel without authentication



DASDEC: *'WKJB & WPRA'*

User Name:

Password:

Login

Your session could not be re-authenticated. Make sure browser cookies are enabled.

NOTICE: Access to this system is restricted to Authorized Users only. Unauthorized access or use of this system may constitute a violation of Federal and/or local law, and may subject violators to civil action and/or criminal prosecution.

Digital Alert Systems
a division of MONROE ELECTRONICS

DASDEC-1EN Analog/Digital EAS Encoder/Decoder

Tue May 9 10:58:41 2023 AST

Serial:8117
Platform ID:R0LGQPE2HWB4NB85SPUX41

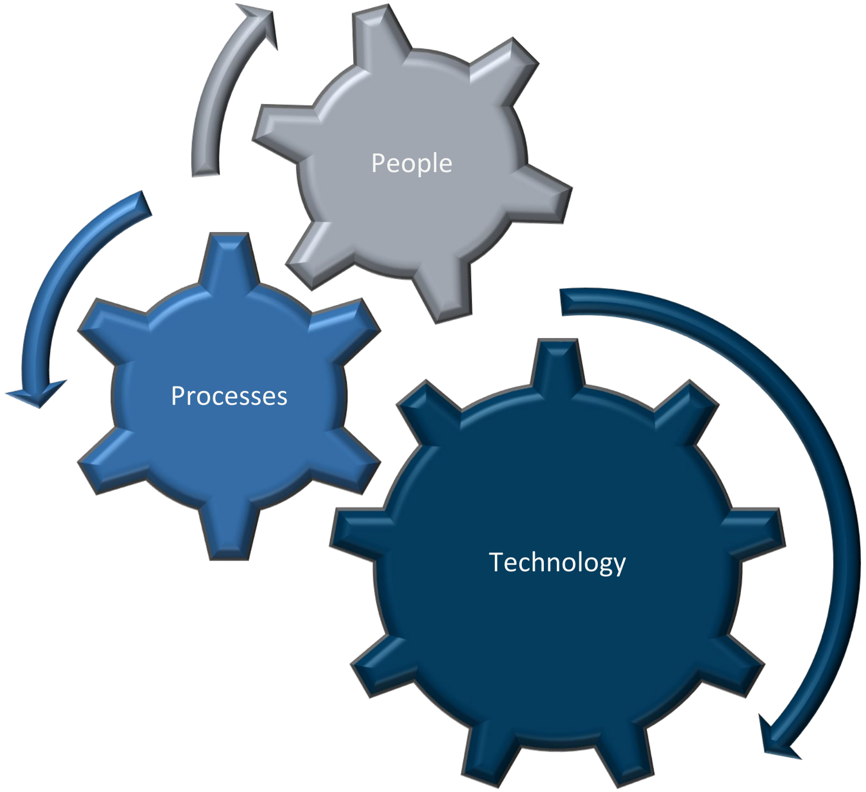
Note:For correct operation cookies & javascript must be enabled on your browser.
©2004-2023

Emergency broadcast radio with:

- Internet-exposed log-in page
- 12+ exploitable vulnerabilities
- Out-dated protocols
- Insufficient authentication requirements

Recommendations

1. Institute multi-factor authentication
2. Upgrade and update software to patch vulnerabilities
3. Prevent external access to internal devices
4. Increase user awareness through frequent, relevant training
5. Balance operational needs with cybersecurity needs by performing risk assessments



Contacts

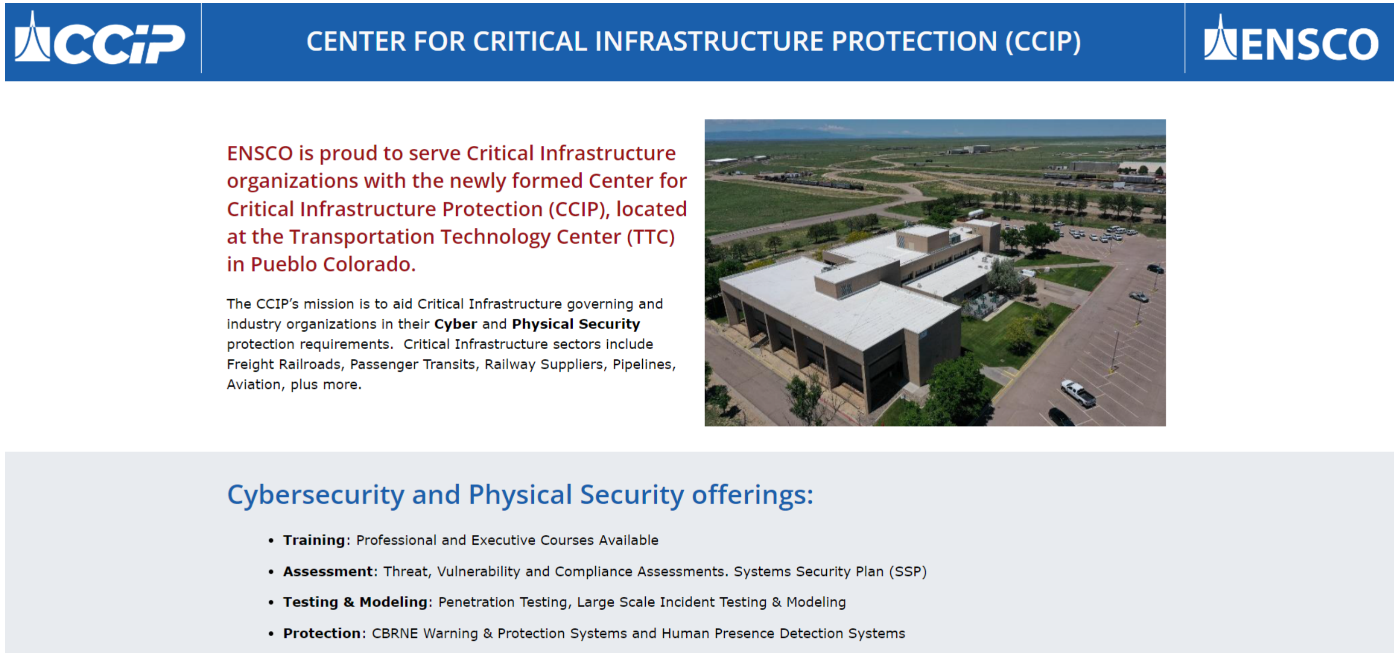
Jeffrey Baca

- baca.jeffrey@ensco.com

Erin Plemons

- plemons.erin@ensco.com

Visit the Center for Critical Infrastructure Protection (CCIP) today in Pueblo, CO or at https://ccip-ensco.com/



CENTER FOR CRITICAL INFRASTRUCTURE PROTECTION (CCIP)

ENSCO is proud to serve Critical Infrastructure organizations with the newly formed Center for Critical Infrastructure Protection (CCIP), located at the Transportation Technology Center (TTC) in Pueblo Colorado.

The CCIP's mission is to aid Critical Infrastructure governing and industry organizations in their **Cyber** and **Physical Security** protection requirements. Critical Infrastructure sectors include Freight Railroads, Passenger Transits, Railway Suppliers, Pipelines, Aviation, plus more.

Cybersecurity and Physical Security offerings:

- **Training**: Professional and Executive Courses Available
- **Assessment**: Threat, Vulnerability and Compliance Assessments. Systems Security Plan (SSP)
- **Testing & Modeling**: Penetration Testing, Large Scale Incident Testing & Modeling
- **Protection**: CBRNE Warning & Protection Systems and Human Presence Detection Systems