CNI and Cyber Security

Chris Hankin, Imperial College London and Director of RITICS

January 2019

Overview

RITICS

- IACS
- Cyber Assessments
- Intrusion Detection
- RITICS 1&2

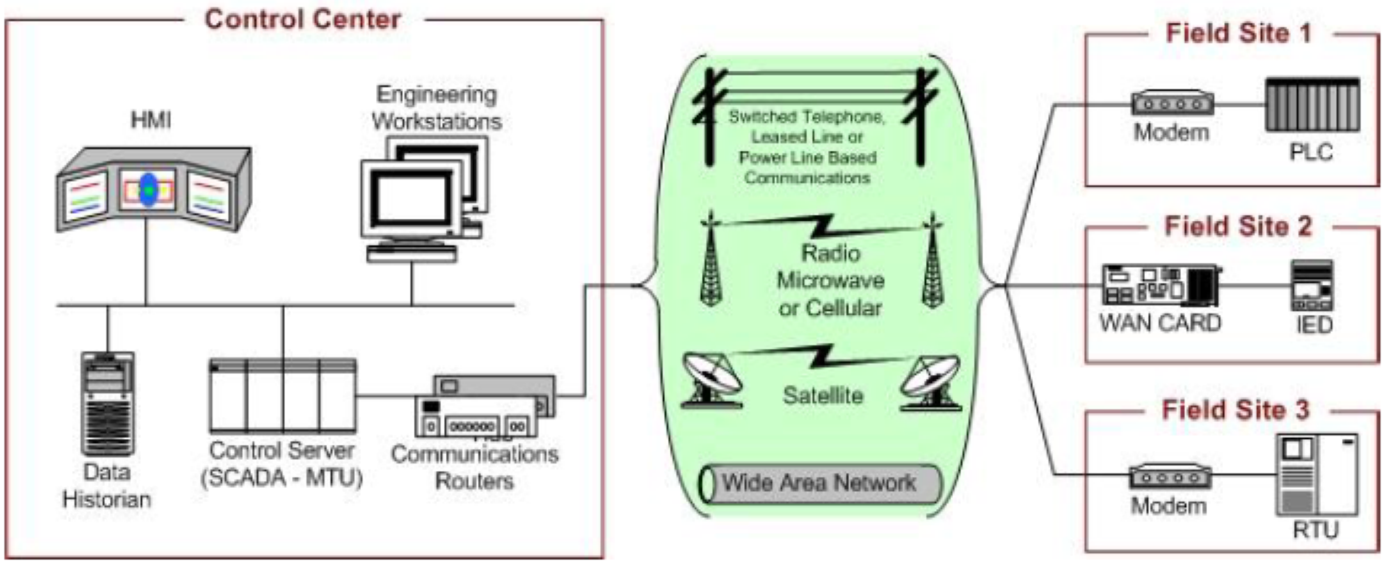


Figure 2-2. SCADA System General Layout

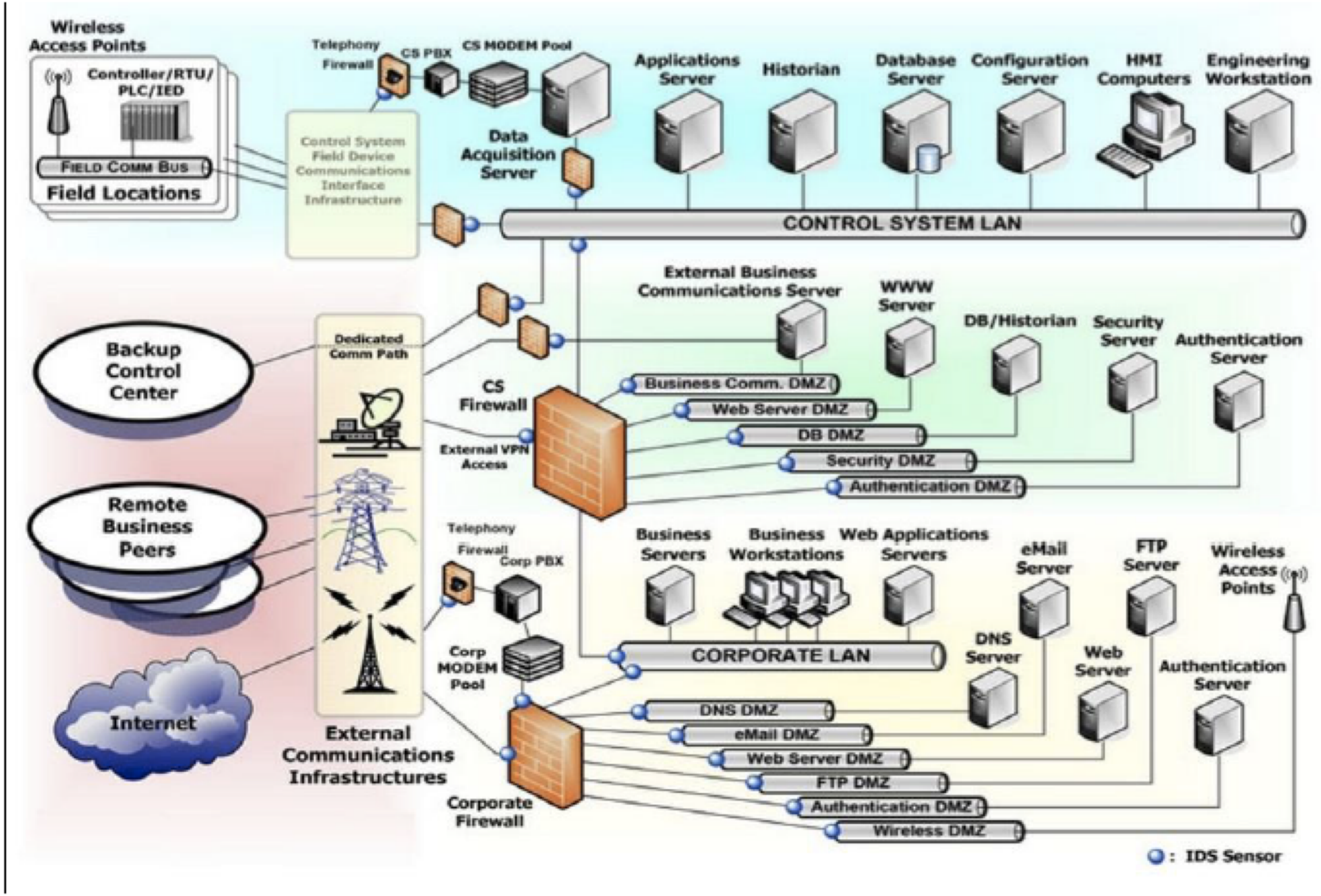
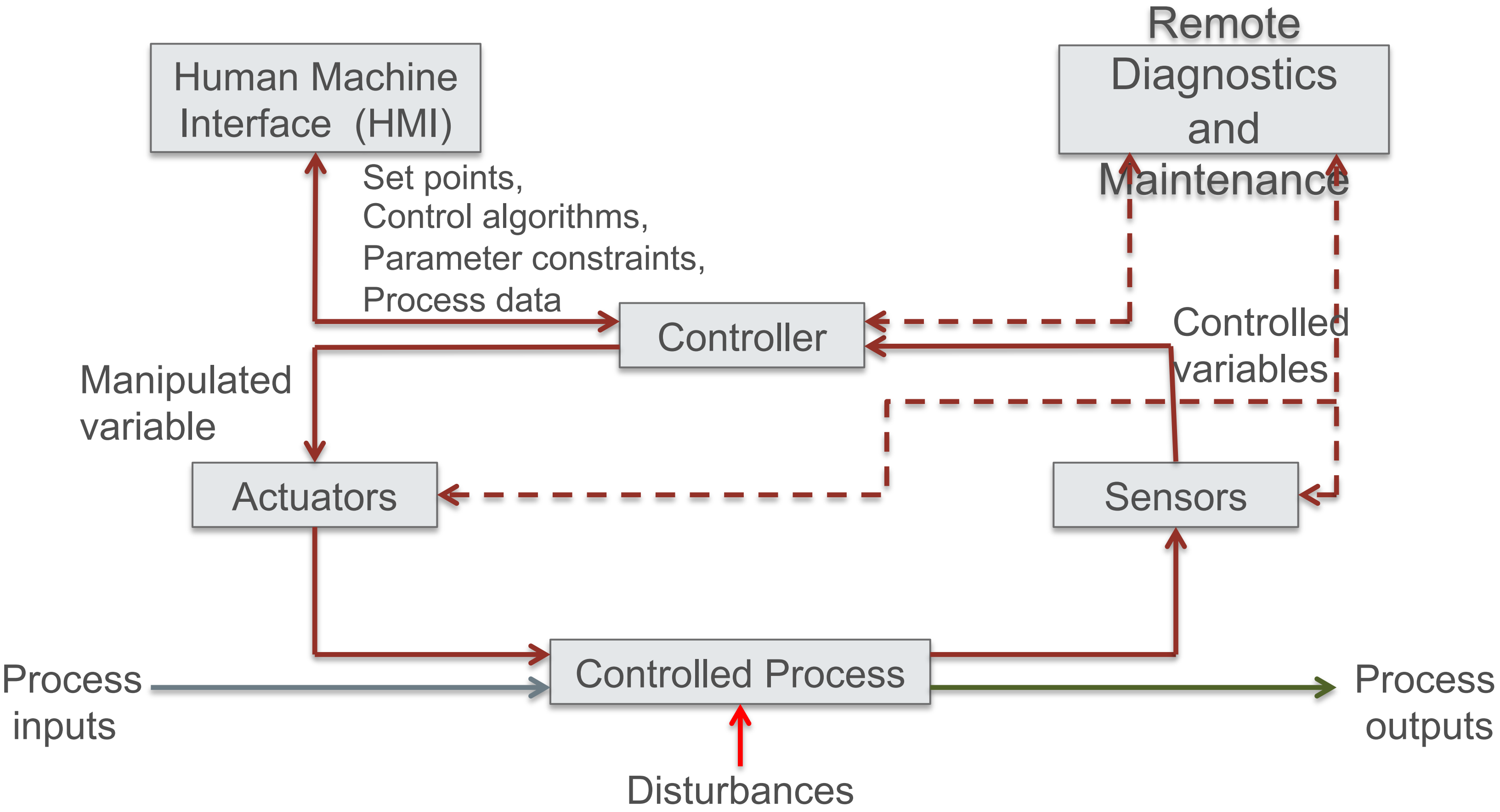


Figure 5-5. CSSP Recommended Defense-In-Depth Architecture

Generic ICS Architecture



Convergence of OT and IT …

… but with major differences:

- Time critical versus high throughput
- Continuous operation
- Increased importance of edge clients
- Complex interactions with physical processes
- Resource constraints
- Legacy issues: 15-20+ years of operation
- Access to components can be difficult

Emerging Topics in ICS Security

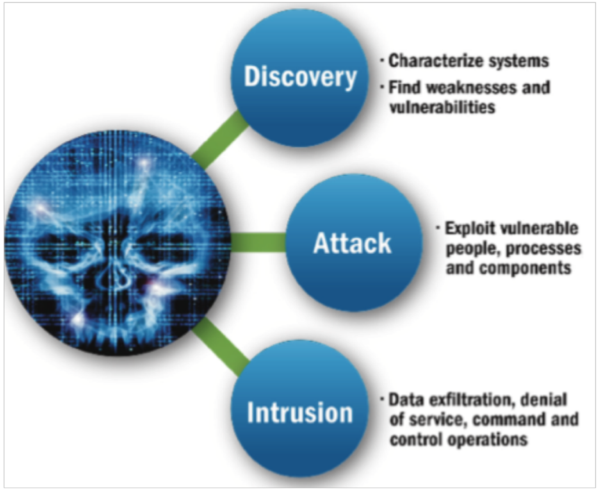
- Bring Your Own Device (BYOD)
- Virtual Machine Technologies
- Security Monitoring in an ICS environment
- ICS Intrusion Detection and Prevention Systems
- Security Information and Event Management (SIEM) technologies
- ICS Supply Chain Management
- Managed Services and Outsourcing
- Leveraging Cloud Services in ICS

Basis for ICS Security Controls

- Identification and Characterization of Risk
- Criticality-Based Asset Inventory
- Understanding Company Risk Appetite
- Implementation of Tailored Security Controls
- Using Communications Monitoring
- Physical Security Controls
- ICS Network Architecture
- Network Security Architecture

ICS Attack Methods

- Exploiting Weak Authentication
- Network Scanning/Probing
- Removable Media
- Brute Force Intrusion
- Abuse of Access Authority
- Spear Phishing
- SQL Injection



NCCIC

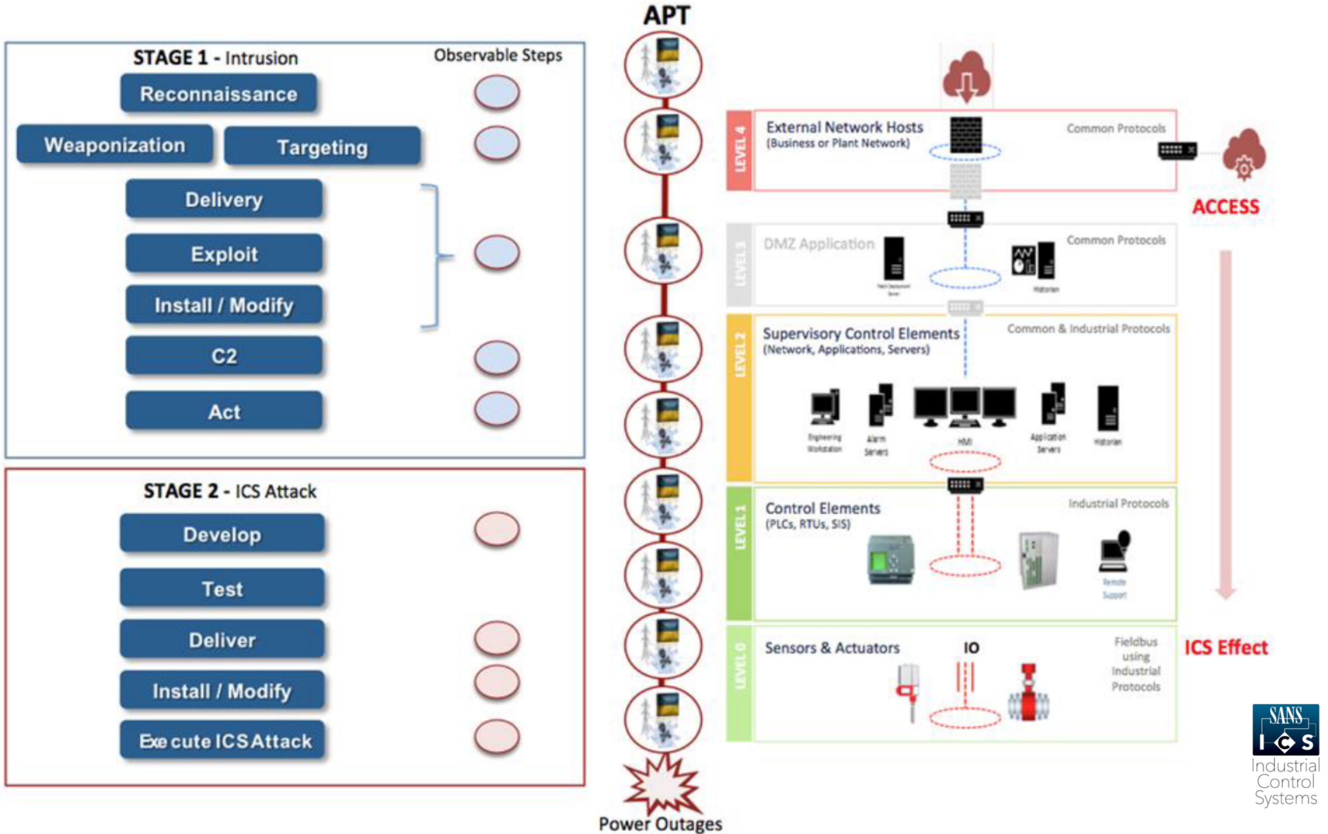
RITICS

FY 2017 Most Prevalent Weaknesses

Area of Weakness	Rank	Risk
Boundary Protection	1	• Undetected unauthorized activity in critical systems • Weaker boundaries between ICS and enterprise networks
Identification and Authentication (Organizational Users)	2	• Lack of accountability and traceability for user actions if an account is compromised • Increased difficulty in securing accounts as personnel leave the organization, especially sensitive for users with administrator access
Allocation of Resources	3	• No backup or alternate personnel to fill position if primary is unable to work • Loss of critical knowledge of control systems
Physical Access Control	4	• Unauthorized physical access to field equipment and locations provides increased opportunity to: ○ Maliciously modify, delete, or copy device programs and firmware ○ Access the ICS network ○ Steal or vandalize cyber assets ○ Add rogue devices to capture and retransmit network traffic
Account Management	5	• Compromised unsecured password communications • Password compromise could allow trusted unauthorized access to systems
Least Functionality	6	• Increased vectors for malicious party access to critical systems • Rogue internal access established

U.S. Department of Homeland Security NCCIC

Ukrainian 2015 Power Outage (SANS Institute)



RITICS

Completion of Stage 1 of the ICS Cyber Kill Chain:

Identify and gain access to a system able to communicate with target SIS.

Stage 2 Develop:

Identify target SIS type and develop TRISIS with replacement logic and loader

Stage 2 Test:

Ensure TRISIS works as intended, likely off network in the adversary environment

Stage 2 Deliver:

Transfer TRISIS to the SIS which contains the 'loader' module for the new logic and support binaries that provide the new logic

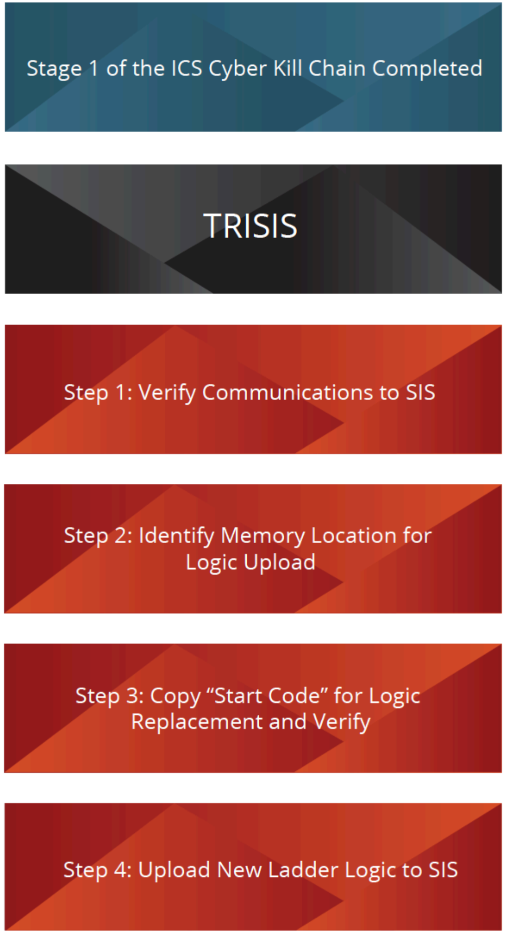
Stage 2 Install/Modify:

Upon running the TRISIS executable, disguised as Triconex software for analyzing SIS logs, the malicious software utilizes the embedded binary files to identify the appropriate location in memory on the controller for logic replacement and uploads the 'initializing code' (4-byte sequence)

Stage 2 Execute ICS Attack:

TRISIS verifies the success of the previous step and then uploads new ladder logic to SIS

Figure 4: TRISIS Attack Flow



Triton/Trisis

Source: Trisis Malware, Dragos

HSE Guidance for Safety Inspectors

- Protect, detect and respond
- Defence in Depth
  - Organisational Countermeasures: Governance, Risk and Asset Management, etc…
  - Protective Countermeasures: Access control, Data security, etc…
  - Detect and Respond Countermeasures: Security Monitoring, Incident Response

Cyber Security Management Sytem

- A: Managing Security Risk
- B: Protecting Against Cyber Attack
- C: Detecting Cyber Security Events
- D: Minimising the Impact of Cyber Security Incidents

Threat Scenarios

Threat Scenario	Technical Countermeasure
Unauthorised physical / logical access to IACS assets by un-authorised employee	B2 Identity and Access Control ○ Physical and logical access controls to limit access to minimum B3 Data Security ○ Encryption for recorded user / device credentials / certificates to prevent unauthorised use B4 System Security ○ IACS Network Architecture, Segregation and Access to prevent access from other networks, e.g. corporate C1 Security Monitoring ○ Security data capture and distribution to allow monitoring and detection of unauthorised actions

NIDS – Anomaly Detection (Cheng, Li and Chana)

RITICS

Package Level Detection by *Bloom Filter*

- Construct a *signature database* by observing regular communication patterns.
- Incorporate the signature database into the *bloom filter detector.*
- *Detect* anomalous data packages *at package-content level.*

Time-series Level Detection by *Long Short Term Memory (LSTM)*

- Address *temporal dependence* between consecutive packages
- *Learn the most likely* package signatures from seen packages by *LSTM*.
- *Further classification* of packages *at time-series level.*

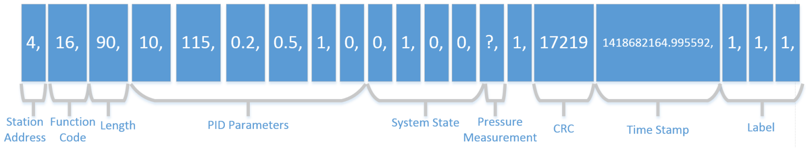
Evaluation by Public ICS Database and Comparison

- Apply to a public *ICS dataset* created from a SCADA system for a gas pipeline.
- Significantly outperform other existing approach and produce *state-of-the-art* results.

Public ICS Dataset by Mississippi State SCADA Lab

Mississippi ICS Attack Dataset

ARFF Data Format



Seven Types of Attacks

Type of Attacks	Abbreviation
Normal	Normal(0)
Naïve Malicious Response Injection	NMRI(1)
Complex Malicious Response Injection	CMRI(2)
Malicious State Command Injection	MSCI(3)
Malicious Parameter Command Injection	MPCI(4)
Malicious Function Code Injection	MFCI(5)
Denial of Service	DOS(6)
Reconnaissance	Recon(7)

Feature	Type
address	Network
function	Command Payload
length	Network
setpoint	Command Payload
gain	Command Payload
reset rate	Command Payload
deadband	Command Payload
cycle time	Command Payload
rate	Command Payload
system mode	Command Payload
control scheme	Command Payload
pump	Command Payload
solenoid	Command Payload
pressure measurement	Response Payload
crc rate	Network
command response	Network
time	Network
binary attack	Label
categorized attack	Label
specific attack	Label

Experiments – Comparison

RITICS

Comparison with Other Anomaly Detection Methods

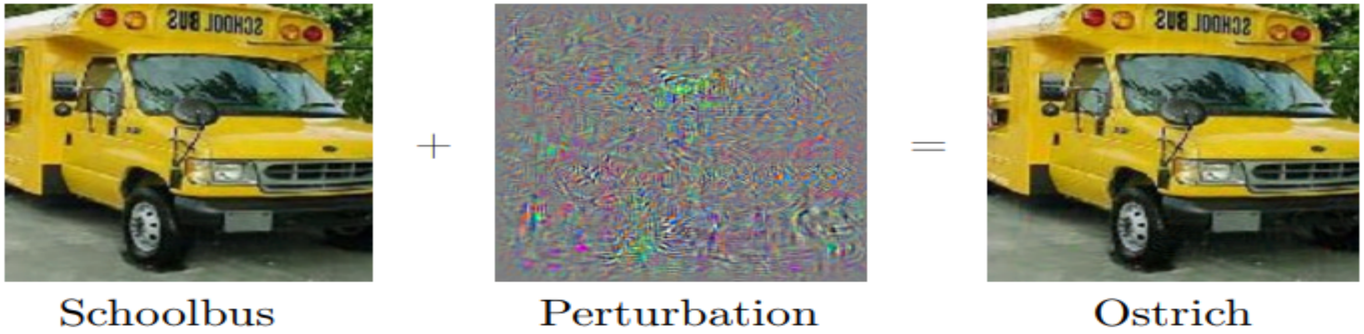
- Evaluation metrics – *Precision, Recall, Accuracy and F-score.*
- Compare with other anomaly detection methods.
- Detected ratio (recall) for seven types of attacks.

Model	Precision	Recall	Accuracy	F-score
Our model	0.94	**0.78**	**0.92**	**0.85**
BF	**0.97**	0.59	0.87	0.73
BN	**0.97**	0.59	0.87	0.73
SVDD	0.95	0.21	0.76	0.34
IF	0.51	0.13	0.70	0.20
GMM	0.79	0.44	0.45	0.59
PCA-SVD	0.65	0.28	0.17	0.27

Attack Type	Model	Detected Ratio
NMRI	Our model	**0.88**
	BF	0.77
	BN	0.77
	SVDD	0.01
	IF	0.13
	GMM	0.31
	PCA-SVD	0.45
CMRI	Our model	**0.67**
	BF	0.53
	BN	0.53
	SVDD	0.02
	IF	0.08
	GMM	0.33
	PCA-SVD	0.19
MSCI	Our model	0.62
	BF	0.18
	BN	0.53
	SVDD	0.19
	IF	0.46
	GMM	**0.66**
	PCA-SVD	0.62
MPCI	Our model	**0.80**
	BF	0.49
	BN	0.34
	SVDD	0.26
	IF	0.08
	GMM	0.64
	PCA-SVD	0.66
MFCI	Our model	**1.00**
	BF	**1.00**
	BN	**1.00**
	SVDD	**1.00**
	IF	0.00
	GMM	0.32
	PCA-SVD	0.54
DOS	Our model	**0.94**
	BF	0.93
	BN	0.93
	SVDD	0.40
	IF	0.12
	GMM	0.15
	PCA-SVD	0.58
Recon.	Our model	**1.00**
	BF	**1.00**
	BN	**1.00**
	SVDD	**1.00**
	IF	0.12
	GMM	0.72
	PCA-SVD	0.54

Evasion Attacks

Originally discovered by researchers when trying to better interpret neural networks.



Szegedy, Christian, et al. "Intriguing properties of neural networks." (2013).

Stealthy Attacks (Cheng, Li and Chana)

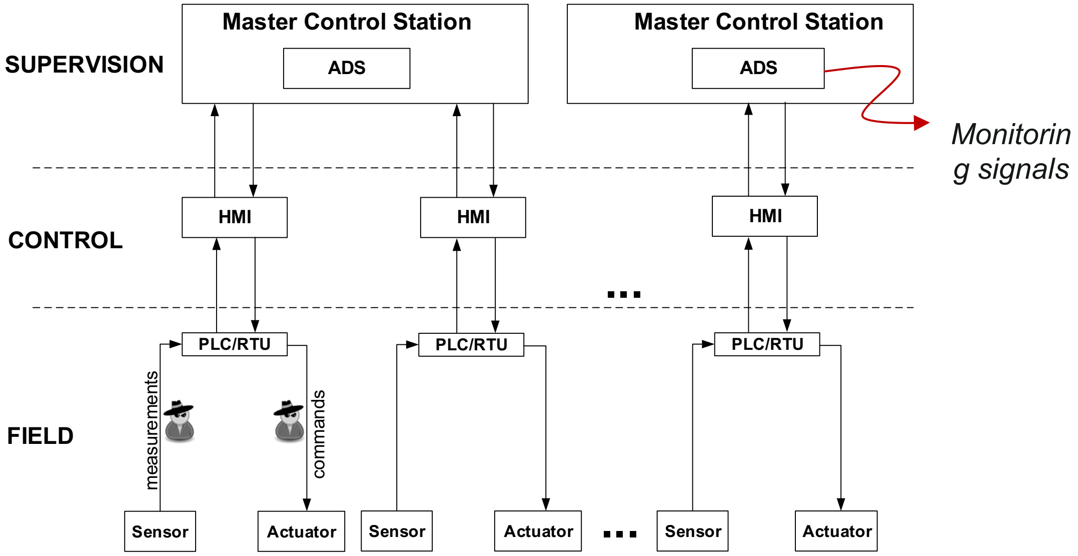
Objectives

- A framework for conducting stealthy attacks with minimal knowledge of the target ICS
- Better understanding of the limitations of current detection mechanisms, and the real threat posed by stealthy attacks to ICS.

Main Contributions

- Demonstrated attacks can be automatically achieved by intercepting the sensor/control signals for a period of time using a particularly designed real-time learning method.
- Used adversarial training technique – Wasserstein GAN to generate false data that can successfully bypass the IDS and still deliver specific attack goals.
- Two real-world datasets are used to validate the effectiveness of our framework.
  - A gas pipeline SCADA system.
  - Secure Water treatment testbed from iTrust@SUTD.

Stealthy Attacks against ICS



- Intercept the expected behaviours of the system via compromised channels.
- *Injected malicious sensor reading* at each time step to achieve certain attack goals.
- Attackers attempt to hide their manipulation; *remain undetected by ADS.*

GAS Pipeline Case Study

RITICS

Mississippi Dataset of a gas pipeline SCADA

- Controls the air pressure in a pipeline; contains a PLC, a sensor and several actuators.
- Pressure measurements at every 2s, 68,803 time series signals are collected.

Features	Description
Setpoint	The pressure set point
Gain	PID gain
Reset rate	PID reset rate
Deadband	PID dead band
Cycle time	PID cycle time
Rate	PID rate
System mode	Automatic(2), manual (1) or off (0)
Control scheme	Pump (0) or valve (1)
Pump	Open(1) or off (0) – for manual mode
Valve	Open(1) or off (0) – for manual mode
Pressure measurement	Pressure measurement

Experiment Setup

- Baseline Anomaly Detector uses LSTM model.
- Four Attack Scenarios: being 4 or 8 units smaller than real values; different compromised channels

		Attack Goal	
		$\tilde{y}_g^{(t)} = max(y_g^{(t)} - 4, 0)$	$\tilde{y}_g^{(t)} = max(y_g^{(t)} - 8, 0)$
Attacker's Abilities	PLC-Sensor channel Compromised	Attack Scenario 1	Attack Scenario 2
	All channels Compromised	Attack Scenario 3	Attack Scenario 4

GAS Pipeline Case Study

RITICS

Results and Evaluation

- Generated malicious measurements successfully capture the trend of the real trace.

- Generated malicious measurements mostly can bypass the anomaly detector
  - Most malicious values have similar or less residual error than the true values.
  - Outliers are caused by HMI human input at manual mode.

- Ratio of attack goal achieved the detection ratio of malicious measurements
  - Ignored the outliers (residual error > 0.05)
  - Less detection ratio for attack scenario 3 and 4.
  - Only compromising PLC-sensor channel still generates high-quality attacks.

Attack Scenario	Ratio of goal achieved	Detected ratio	
		by residual error	by CUSUM
1	88.1%	2.6%	0.2%
2	86.0%	2.4%	0.1%
3	85.9%	1.1%	0.01%
4	90.5%	1.2%	0.01%

Water Treatment System Case Study

Experiment Setup

- A water treatment plant (SWaT from iTrust@SUTD) maintains the water quality within acceptable limits.
- 51 sensors extracted every second, in total 496,800 signals for normal operation are collected.

Features	Description
AIT201	Measures NaCl level
AIT202	Measures HCl level
AIT203	Measures NaOCl level
FIT201	Flow transmitter for dosing pumps
P101	Raw water tank pump state
MV201	Motorized vale state
P201	NaCl dosing pump state
P203	HCl dosing pump state
P205	NaOCl dosing pump state

- Focus on generating malicious HCl and NaOCl measurements, still within normal range.

$$\tilde{y}_{g_1}^{(t)} \geq \min(y_{g_1}^{(t)} + 0.1, 1) \qquad \tilde{y}_{g_2}^{(t)} \leq \max(\tilde{y}_{g_2}^{(t)} - 0.1, 0)$$

Simulation and Evaluation

- A successful attack -- either the HCl (>0.99) or the NaOCl (<0.01) dosing pump is turned on unexpectedly by the injected malicious measurements + bypassed the detector.

Compromised Channels	Successful Ratio	
	by residual error	by CUSUM
Only PLC-AIT202, PLC-AIT203	90.1%	93.8%
all channels	92.4%	94.6%

Research Institute in Trustworthy Industrial Control Systems

RITICS

EPSRC Engineering and Physical Sciences Research Council

CPNI Centre for the Protection of National Infrastructure

Queen's University Belfast

Scottish and Southern Energy Power Distribution

THALES

Statnett

CAPRICA: Converged approach towards resilient industrial control systems and cyber assurance

LANCASTER UNIVERSITY

AIRBUS

Raytheon

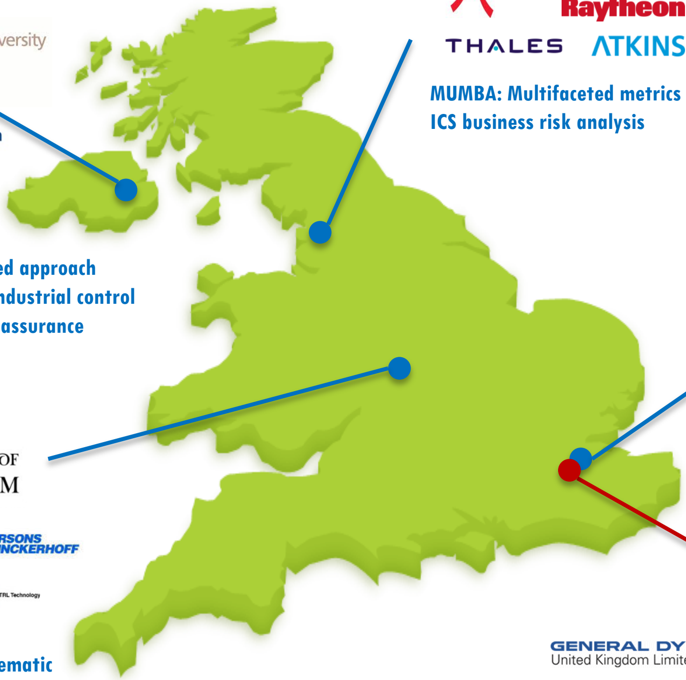
THALES ATKINS

MUMBA: Multifaceted metrics for ICS business risk analysis

£2.4M programme, 5 coordinated projects.

Phase 1 (Directorship) awarded 01/01/14, Chris Hankin, Imperial College London.

Phase 2 awarded 01/10/14.



CITY UNIVERSITY LONDON

CEDRICS: Communicating and evaluating cyber risk and dependencies in ICS

ALSTOM Adelard

UNIVERSITY OF BIRMINGHAM

nationalgrid PARSONS BRINCKERHOFF

RSSB L3 TRL Technology

SCEPTICS: A systematic evaluation process for threats to ICS (incl. national grid and rail networks)

Imperial College London

GENERAL DYNAMICS United Kingdom Limited

ATKINS Symantec.

RITICS: Novel, effective and efficient interventions

Key Questions / Challenges

RITICS

Do we understand the harm threats pose to our ICS systems and business?

Can we confidently articulate these threats as business risk?

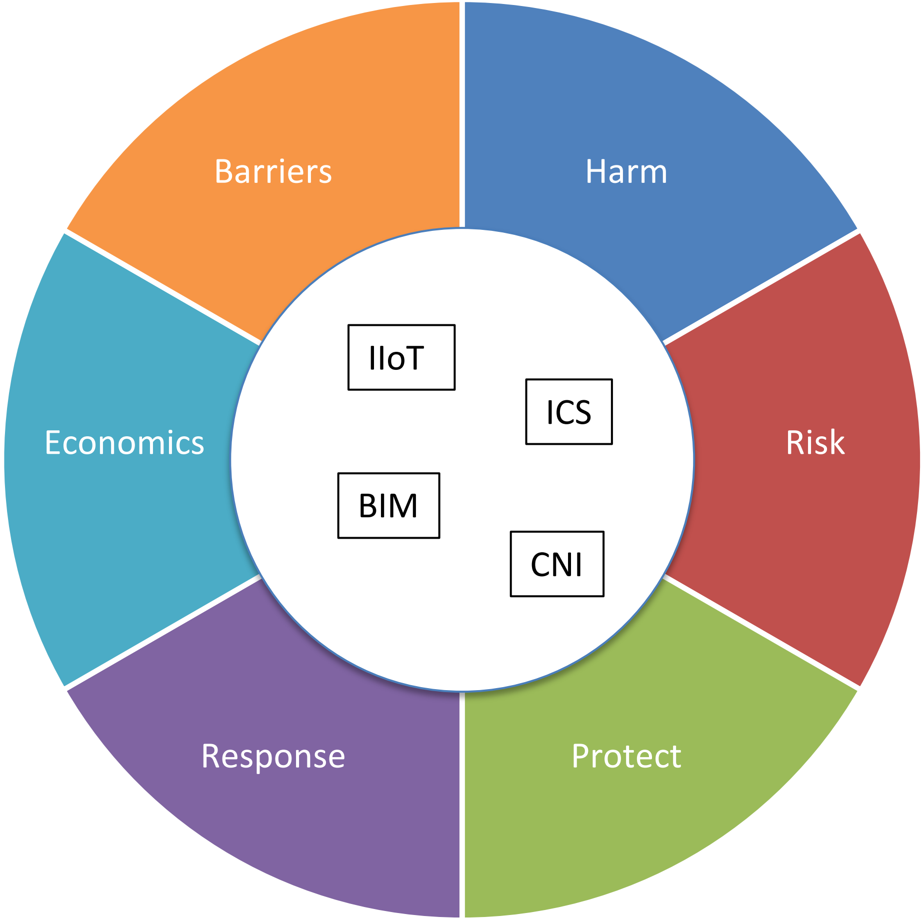
What could be novel effective and efficient interventions?

Impact

- Contribution to new Cyber Security Strategy for UK railways.
- Tools for building models of complex cyber physical systems.
- Testbeds.
- A serious game for studying security decisions.
- Secure implementation of gateway module compatible with IEC and IEEE standards.
- Contribution to European work on certification of ICS components.

Key Facts about RITICS

- Research Institute in Trustworthy Inter-connected Cyber-physical Systems
- 14 university partners
- 21 organisations involved in RITICS Council
- Links with NCSC Community of Interest in Industrial Control Systems
- Inter– and multi-disciplinary focus



RITICS ritics.org

EPSRC Engineering and Physical Sciences Research Council

National Cyber Security Centre

Projects

- NIS Directive – Baseline, Barriers, Impact
- Safety and Security
- Autonomous Systems
- Incident Response and Forensics
- Cyber Controls
- Interconnected Systems
- Supply Chain

RITICS

Thank you

ritics.org

c.hankin@imperial.ac.uk