11TH INTERNATIONAL CONFERENCE
ON CRITICAL INFORMATION
INFRASTRUCTURES
SECURITY

10-12 October 2016
UIC HQ Paris

CRITIS
2016

Railway System Failure Scenario Analysis

William G. Temple[a], Yuan Li[a], Bao Anh N. Tran[a],
Yan Liu[a], and Binbin Chen[a]

[a] *Advanced Digital Sciences Center, Illinois at Singapore*

ADSC

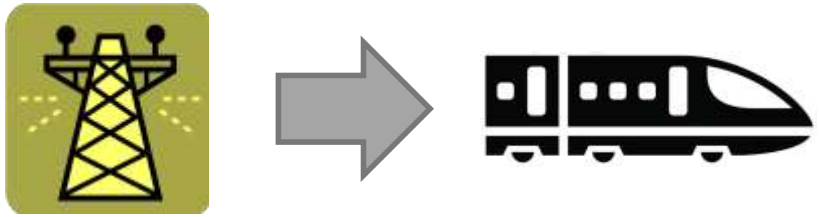
My Talk in One Slide

Railway System

- Timely and important cyber security challenges

Failure Scenario

- Bringing a practice from the energy sector to railway



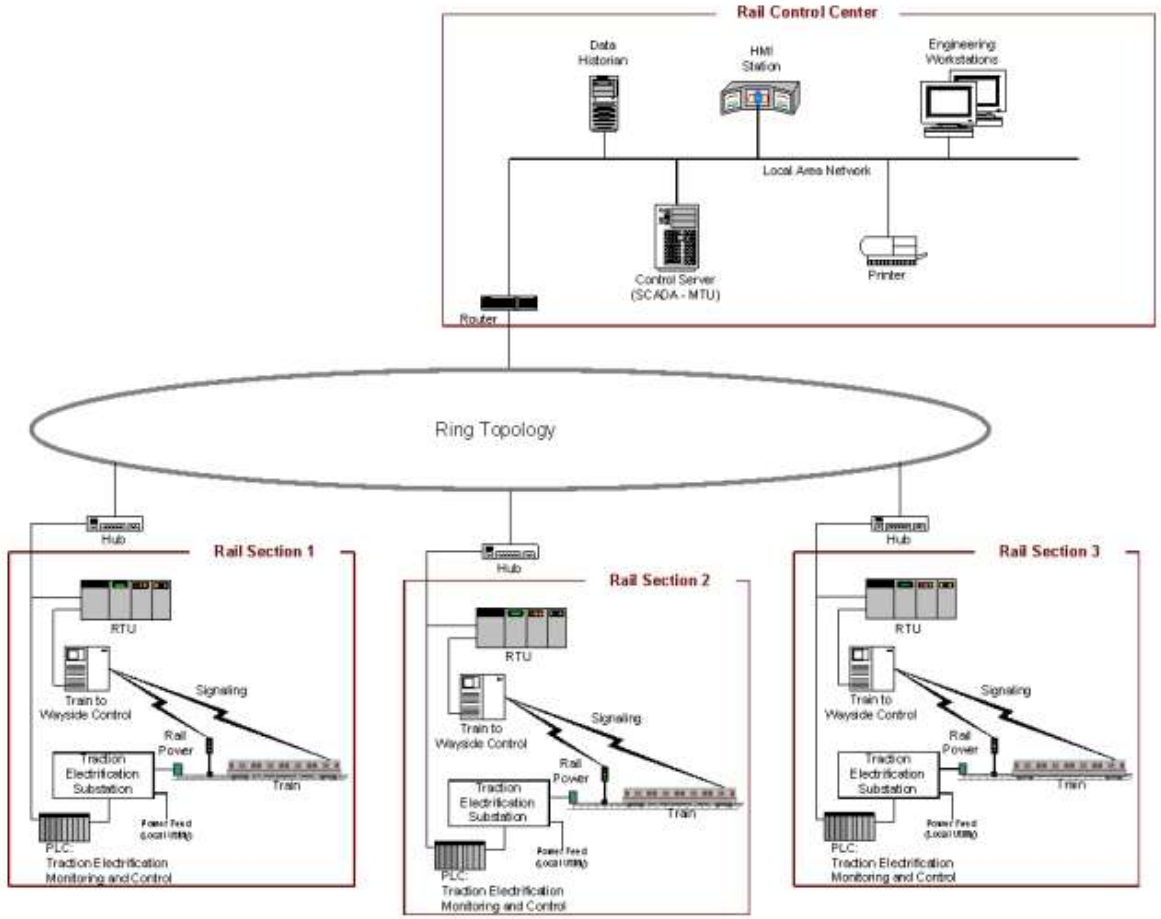
Analysis

- A case study with a failure scenario modelling tool

Railway as Critical Infrastructure

- **Vital role in transportation**
  - Passengers
  - Freight
- **Safety critical**
- **Reliant on automation & ICS**

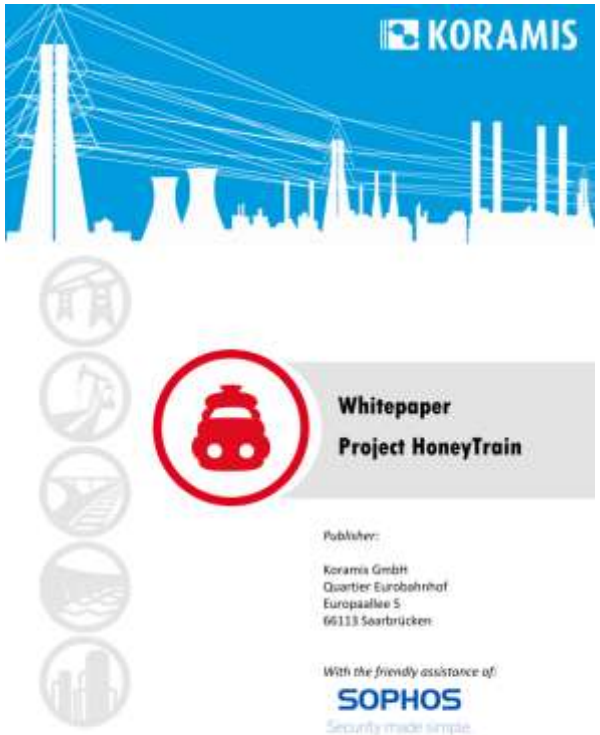
GoA 1	• Manual operation (driver)
GoA 2	• Semi-automatic (i.e., stop/start)
GoA 3	• Driverless (attendant operates doors)
GoA 4	• Unattended



Source: NIST SP 800-82

Threats in the Rail Industry (I)

September 2015



https://www.sophos-events.com/honeytrain/index.cfm?src=soc

Over 2.7M attacks detected over 6 weeks

Country of origin (last resolvable IP address)

Threats in the Rail Industry (II)

SECURITYWEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

Malware & Threats | Cybercrime | Mobile & Wireless | Risk & Compliance | Security Architecture

Trains Vulnerable to Hacker Attacks: Researchers

By Eduard Kovacs on December 29, 2015

A team of researchers has analyzed modern railway systems and it would not be difficult for a motivated attacker to pull off a

Technology

UK rail network hit by multiple cyber attacks last year

Hackers could have disrupted train lines and even caused trains to derail, researchers said. CREDIT: PA

By Cara McGoogan and Lydia Willgress

12 JULY 2016 • 5:15PM

The UK railway network was the victim of at least four major cyber attacks in the last 12 months, according to a private security company that works with the network.

Login | Subscribe

South China Morning Post
CHINA
FRI Jul 18, 2014 Updated: 7:34pm

News | Business | Comment | Lifestyl

Home › News › China

NEWS • CHINA • TRANSPORT

Passenger Wi-fi freezes third Shenzhen Metro train in a week

Shenzhen Metro under fire about security of its wireless control system amid breakdowns

He Huifeng
huifeng.he@scmp.com

PUBLISHED : Friday, 09 November, 2012, 12:00am

InformationWeek CONNECTING THE BUSINESS TECHNOLOGY COMMUNITY

Home | News & Commentary | Authors | Slideshows | Video | Reports | White Papers | Events | Interop

STRATEGIC CIO | SOFTWARE | SECURITY | CLOUD | MOBILE | BIG DATA | INFRASTRUCTURE | GOVERNMENT | HEALTHCARE | SMART CITIES

NEWS

Computer Virus Brings Down Train Signals

The virus infected the computer system at CSX's headquarters, shutting down signaling, dispatching, and other systems for trains throughout the East.

NEW YORK (AP) — A computer virus was blamed for bringing down train signaling systems throughout the East on Wednesday

IN HOMELAND SECURITY

News & Analysis of Critical Issues in Terrorism & Homeland Defense

Home | About the Blog | Categories | Contributors | Partnerships | Newsletter | Blogroll

Teen Hacker in Poland Plays Trains and Derails City Tram System

February 12, 2008

Analyzing Cyber Risk

- **Multiple systems**: train communications, traction power, control network, etc.
  - Each can have vulnerabilities
  - Different impacts on the system

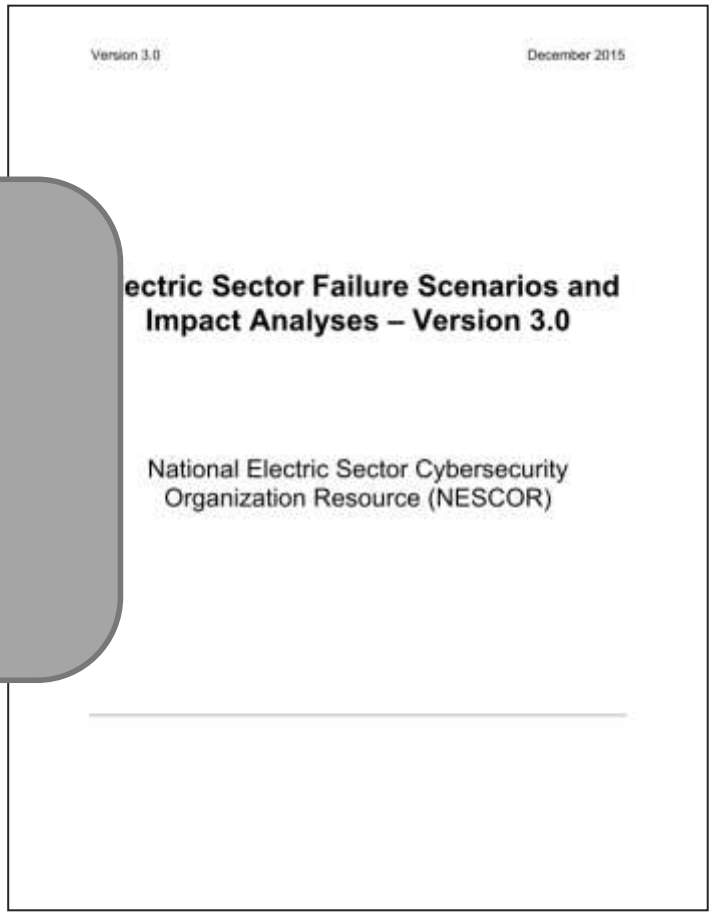
- **A structured process** is necessary to document and analyze risks, and to prioritize hardening efforts

Failure Scenario Analysis

- **Inspired by NESCOR**
  - *"A cyber security failure scenario is a realistic event in which the failure to maintain confidentiality, integrity, and/or availability of sect on the generation*
- **What is a failur**
  - **Classified by (su**
  - **Plain text descri**
  - **Relevant vulnerabilities**
  - **Impact**
  - **Potential Mitigations**

Use Cases:

Training staff
Interacting with vendors
Risk assessment & testing


Version 3.0 December 2015

ectric Sector Failure Scenarios and Impact Analyses – Version 3.0

National Electric Sector Cybersecurity Organization Resource (NESCOR)

EPRI ELECTRIC POWER RESEARCH INSTITUTE

U.S. DEPARTMENT OF ENERGY

Adapting NESCOR Scenarios for Railway

- **Description and impact – sector specific**
  - Need railway expertise, interaction with industry
- **Common vulnerabilities and mitigations – easy to translate**
  - Feature introduced by NESCOR team in more recent iterations
- **Do specific scenarios or broad classes of failures translate?**
  - 62 out of 123 NESCOR scenarios (52%) found to be translatable with minor adjustment
    - **Message** [34%] (e.g., spoofing, false data injection)
    - **Malware** [19%]
    - **Configuration** [14%] (e.g., maliciously changing system setting)
    - **Denial of Service** [9%]
    - **Process** [4%] (e.g., supply chain threats)

Analyzing Scenarios – CyberSAGE Tool

CRITIS 2016

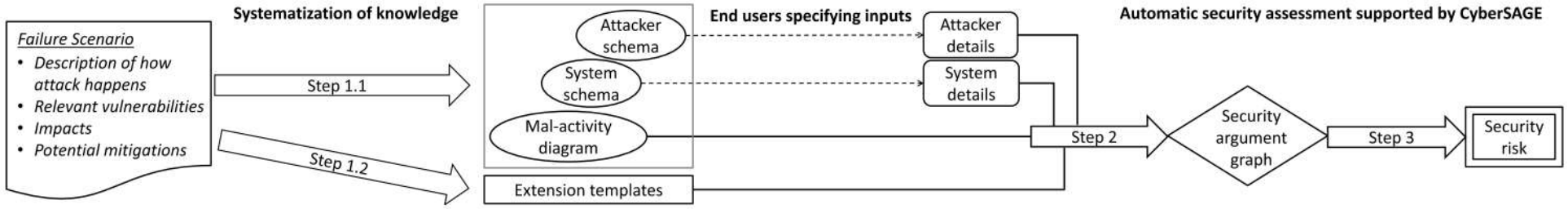
- **Security assessment tool**
  - Workflow-based process availability analysis
  - Failure scenario probability analysis
- Incorporates system model, attacker model

CyberSAGE

- Available at www.cybersagetool.com

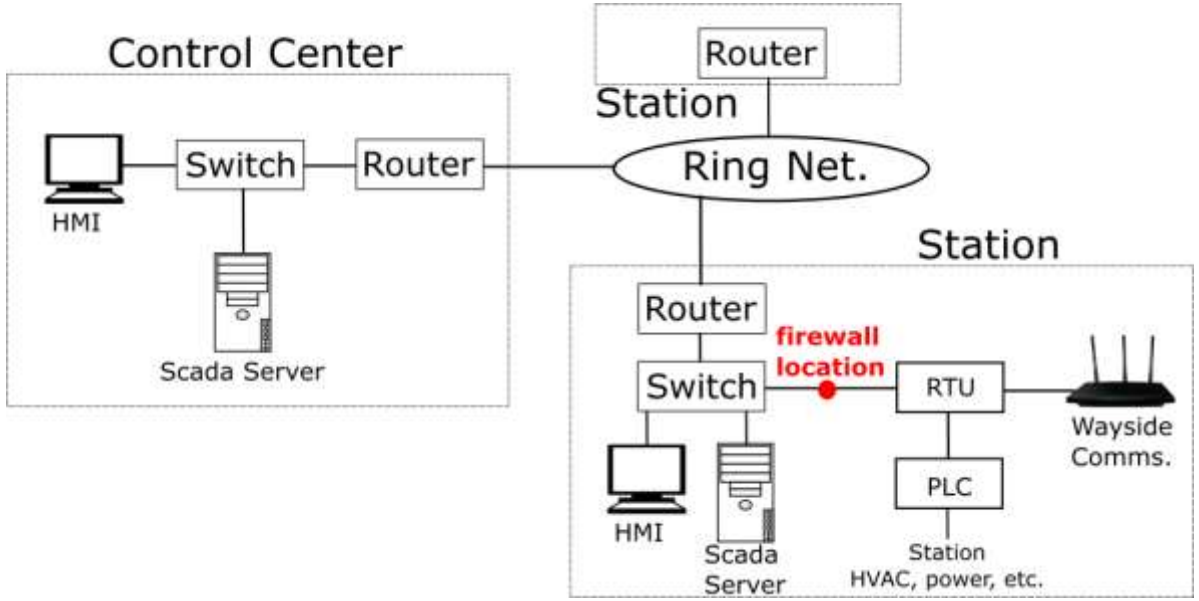
Relevant Publications

- Sumeet Jauhar et al., "Model-Based Cybersecurity Assessment with NESCOR Smart Grid Failure Scenarios," IEEE PRDC 2015.
- Nils Ole Tippenhauer et al., "Automatic Generation of Security Argument Graphs," IEEE PRDC 2014.
- An Hoa Vu et al., "CyberSAGE: A Tool for Automatic Security Assessment of Cyber-Physical Systems," QEST 2014.
- Binbin Chen et al., "Go with the Flow: Toward Workflow-Oriented Security Assessment," NSPW 2013.



Case Study: Railway SCADA

- **System**
  - Based on NIST SP 800-82
- **Attacker models**
  - Insider
  - Contractor
  - Nation State
- **Questions**
  - Which attacker poses the greatest threat?
  - What is the impact of adding a firewall?



Railway SCADA: Modelling the Scenario

3.1 Compromised HMI sends malicious commands to devices

A human-machine interface is infected with malware, either through a USB flash drive, or through the network. This malware can send unauthorized commands to devices in the station or at the trackside to disrupt railway operations.

Vulnerabilities

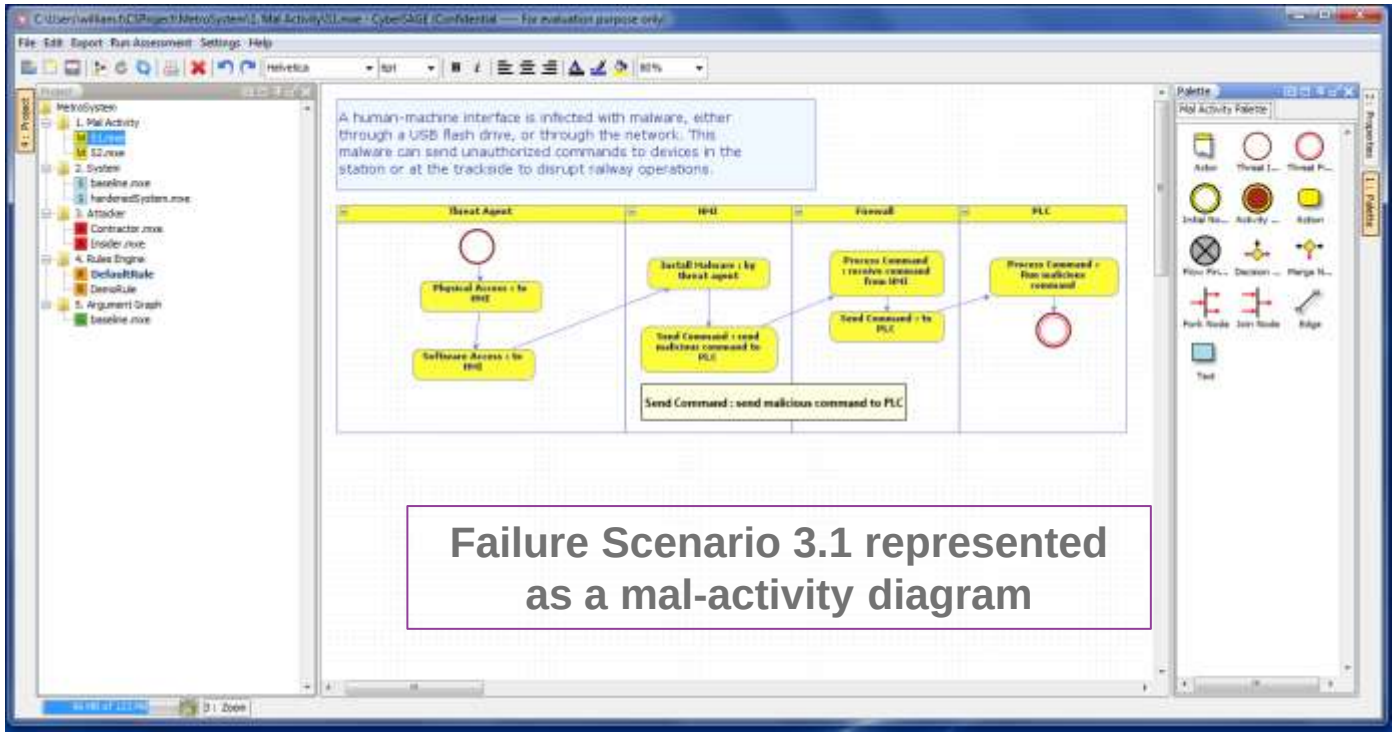
- *system permits installation of malware* in the HMI
- *system permits potentially harmful command sequences* enabling the compromised device to affect operations

Impact

- Settings are changed, degrading system performance
- Devices are remotely shut down, affecting train service

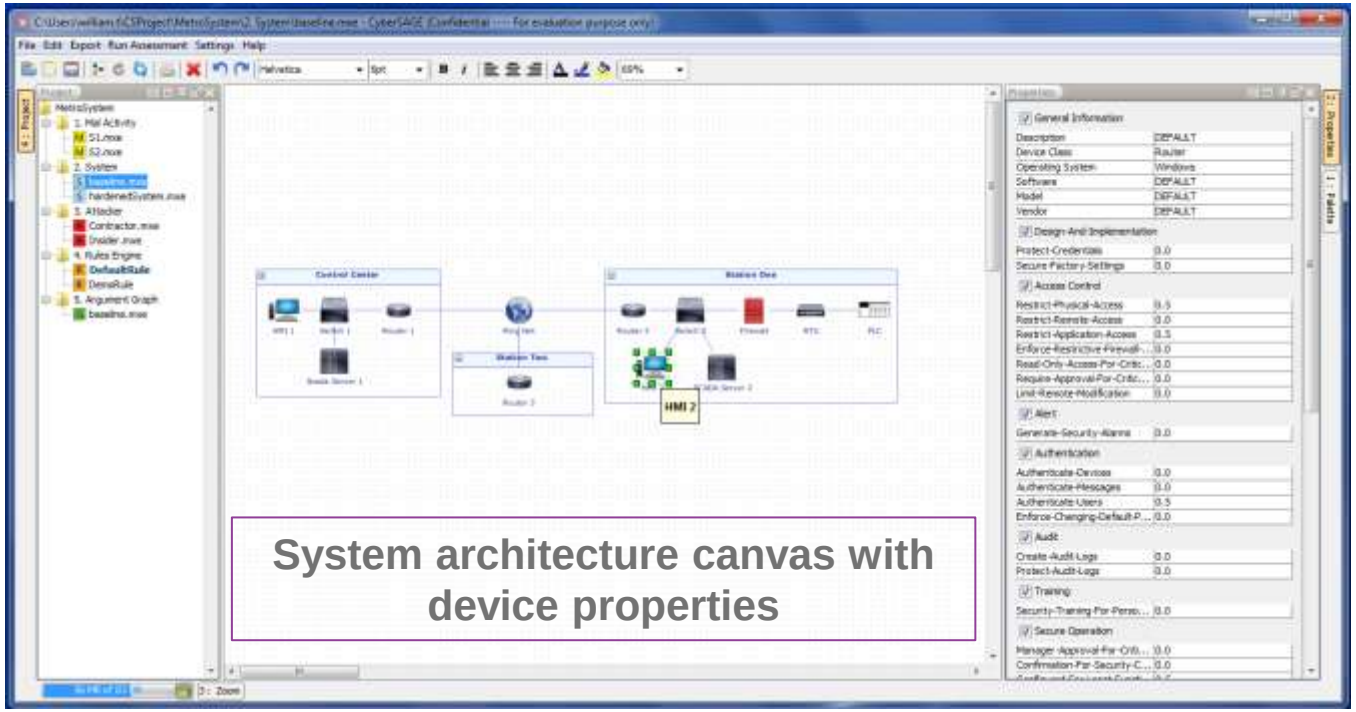
Mitigation

- *authenticate users* for all software changes
- *test after maintenance* for malware
- *create audit logs* of all changes to software
- *protect audit logs* from deletion
- *validate inputs* with the user for all control actions
- *authenticate messages* communicated in the SCADA network

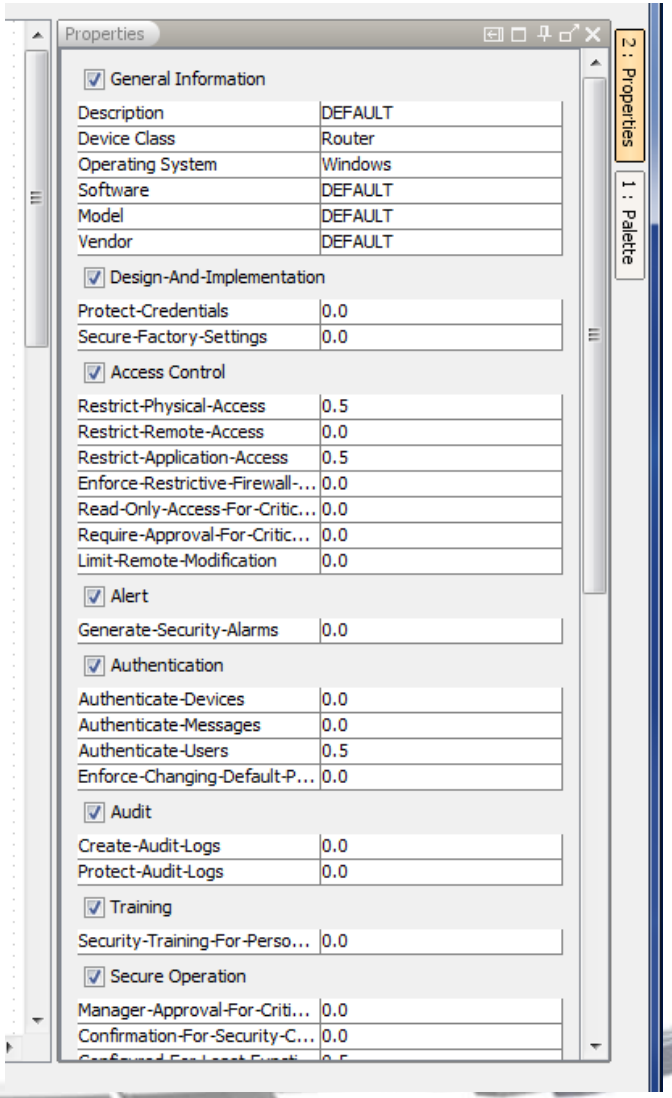


Failure Scenario 3.1 represented as a mal-activity diagram

Railway SCADA: Modelling the System



System architecture canvas with device properties



Properties take values over [0, 1], describe countermeasure effectiveness

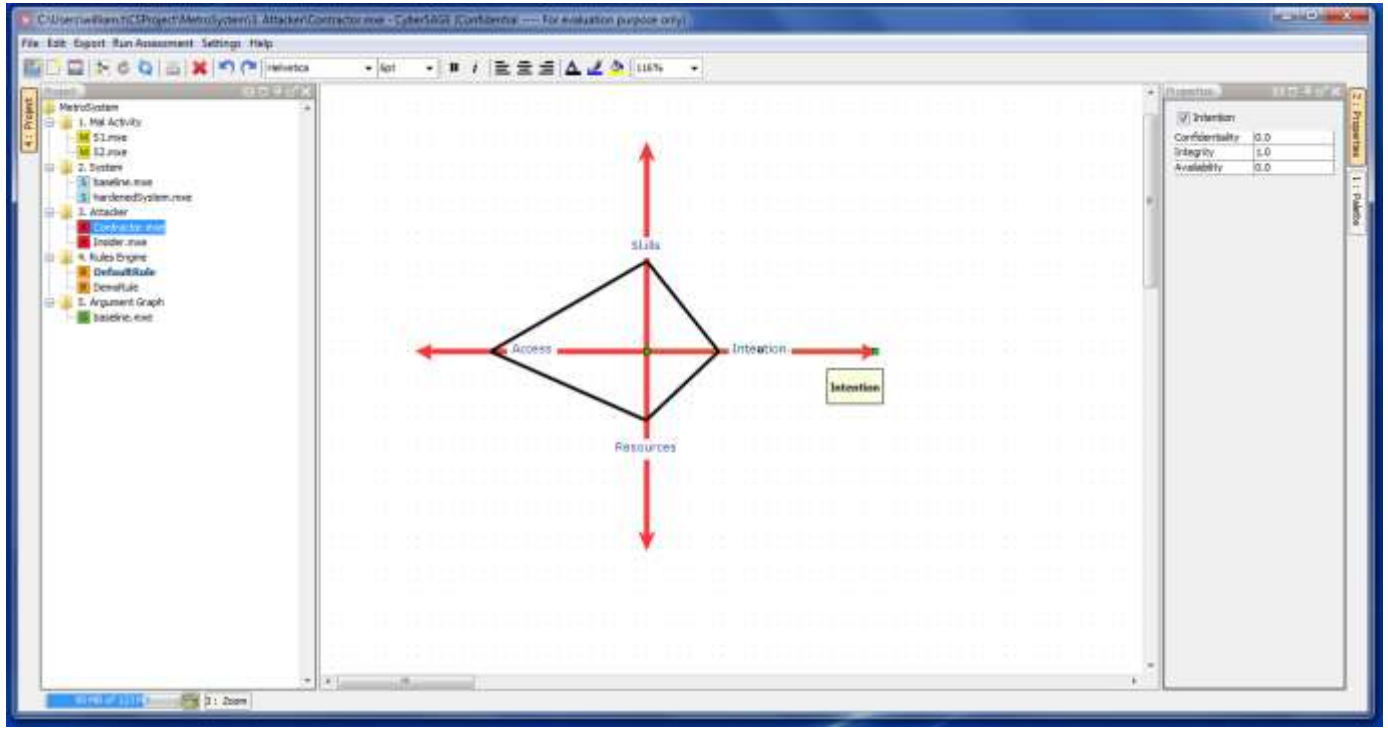
Railway SCADA: Modelling the Threats

- **User-defined**
  - Access, skills, resources, intention
  - Reusable across scenarios

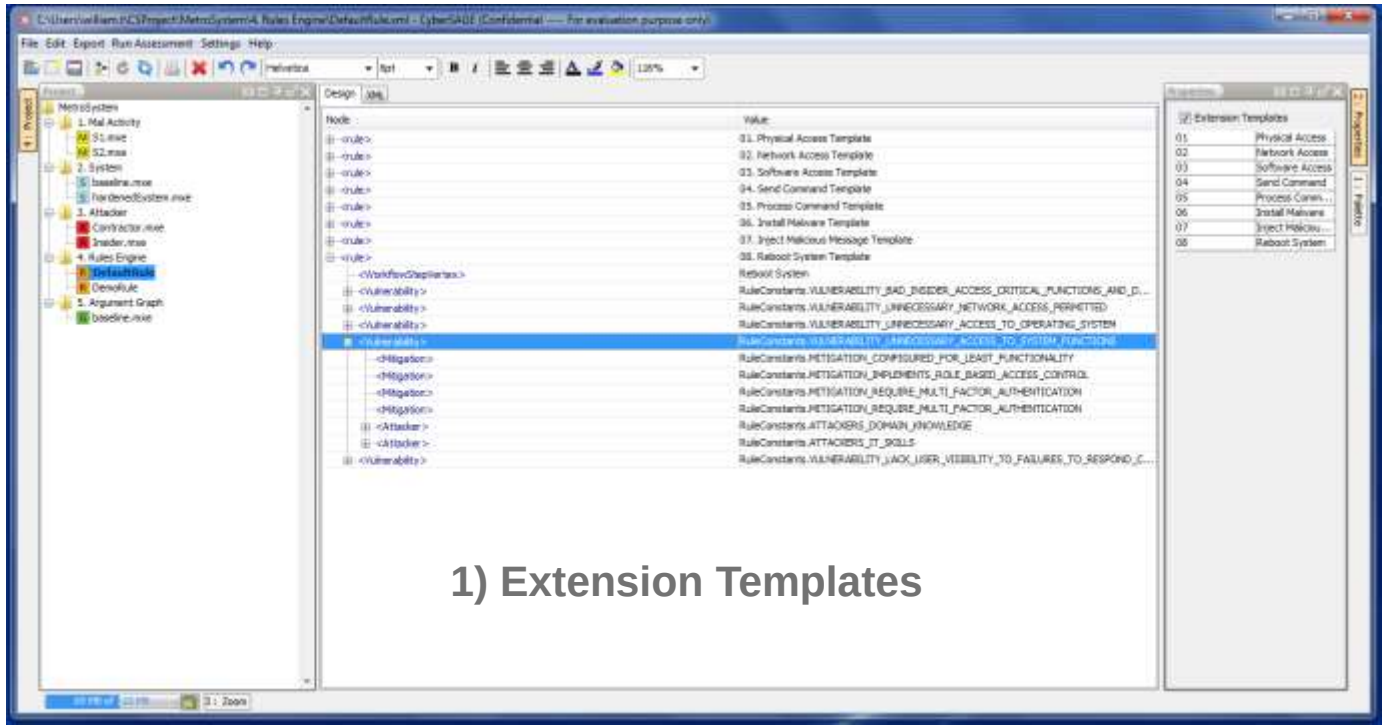
- **Selected attackers**

Attacker	IT Skill	Domain Knowledge	Physical Access	Logical Access
Insider	Medium	High	True	True
Contractor	Low	Low	True	False
Nation State	High	High	False	True

High, Medium, Low correspond to user-defined values over [0, 1]

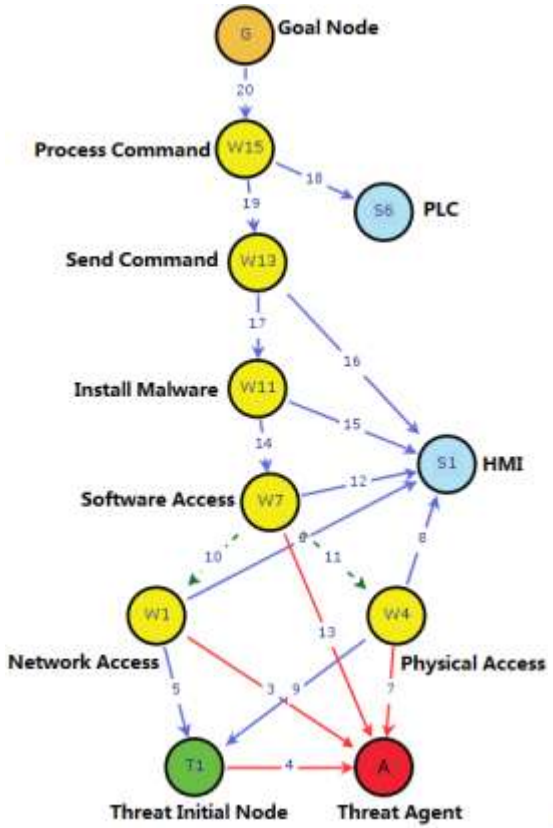


Railway SCADA: Generating Results



1) Extension Templates

2) Security Argument Graph
(defines AND, OR relationships)



3) Failure scenario probability

Attacker	Before Firewall	After Firewall	Improvement
Insider	0.0120	0.0095	~21%
Contractor	0.0050	0.0032	~35%
Nation State	0.0153	0.0129	~16%

Conclusion

- Establishing common failure scenarios can benefit the rail industry
  - The electric sector (NESCOR) scenarios are a valuable starting point
  - Challenges remain: diversity of railway systems, assessing impact

- Tool support helps organizations map scenarios to their infrastructure
  - Try CyberSAGE if you're interested!

Thank You!

William Temple
william.t@adsc.com.sg
www.secuts.net