



UNIVERSITY OF
BIRMINGHAM

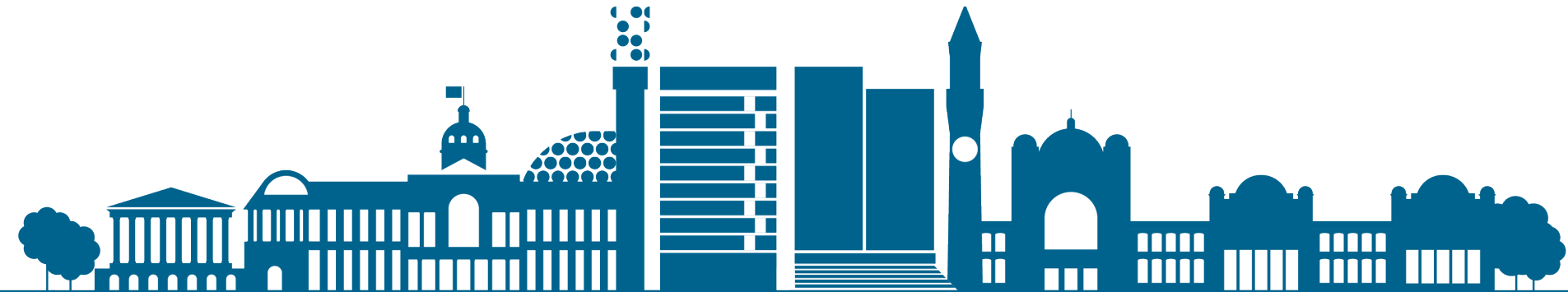
RITICS

Threats to Industrial Control Systems: Lessons Learnt from Rail

Richard James Thomas

Security and Privacy Group

R.J.Thomas@cs.bham.ac.uk



Outline

- ❑ Defining an Industrial Control System and Attack Vectors
- ❑ Current state of Power Grids
- ❑ The Future of Power – Smart Grids
- ❑ Research at Birmingham – SCEPTICS Project
 - Lessons Learnt from Rail
 - Shift to Power - applying these methodologies to Smart Grids
- ❑ What can the Industry do?



First...





[DATA CENTRE](#) [SOFTWARE](#) [SECURITY](#) [TRANSFORMATION](#) [DEVOPS](#) [BUSINESS](#) [PERSONAL TECH](#) [SCIENCE](#) [EMERGENT TECH](#) [BOOTNOTES](#)



[Security](#) 14

Homebrew crypto SNAFU on electrical grid sees GE rush patches

Boffins turned up hard-coded password in ancient controllers

27 Apr 2017 at 01:59, Richard Chirgwin

Updated General Electric is pushing patches for protection relay bugs that, if exploited, could open up transmission systems to a grid-scale attack.

The company hasn't published much by way of detail, but spoke to Reuters after this Black Hat [abstract](#) was published (the talk will be delivered to the July conference in Las Vegas).

The three New York University researchers say they cracked the homebrew encryption in the ancient GE Multilin systems. The abstract is light on detail, but it appears the researchers found a hardcoded password: "we completely broke the home brew encryption algorithm used by these protection and management devices to authenticate users and allow privileged operations. Knowledge of the passcode enables an attacker to completely pwn the device and disconnect sectors of the power grid at will, locking operators out to prolong the attack".

GE [told Reuters](#) the bug is in units dating from the 1990s (a time when, *The Register* notes, "homebrew" encryption was the norm, rather than known bad practice).

GE's Annette Busateri told Reuters the company is notifying customers and rolling out upgrades for the bug. There's a patch available for five out of the six affected products, she said, with the sixth to land soon.

The protection relays are used to cut off parts of the grid to protect against dangerous conditions.

A remote exploit would demand that the relays are connected to the Internet, with inadequate protection against access.

The researchers, Anastasis Keliris and Charalambos Konstantinou of New York University and Mihalios Maniatakos of NYU in Dubai, say they'll show off an exploit on a feeder management relay – but don't specify that they'll be demonstrating a remote attack.

The Register has contacted GE for comment. ®



Who's afraid of the big, bad botnet?

The dangers, and how to guard against them

ARBOR

TUESDAY, 13 JUNE AT 11 AM BST

SIGN UP NOW

LIVE

Most read



Ta-ta, security: Bungling Tata devs leaked banks' code on public GitHub repo, says IT bloke



Virgin Media resolves flaw in config backup for Super Hub routers



IBM warns itself of possible outages in lab shift screw-up



Situation normal, blurs T-Mobile, while network continues to crap itself



Mac ransomware author is giving away malicious code to script kiddies



[sign in](#) [become a supporter](#) [subscribe](#) 

[UK](#) [election](#) [world](#) [sport](#) [football](#) [opinion](#) [culture](#) [business](#) [lifestyle](#) [fashion](#) [environment](#) [tech](#) [travel](#) [browse all sections](#)

[home](#) > [business](#) [economics](#) [banking](#) [retail](#) [markets](#) [eurozone](#)

National Grid

Blackouts? What blackouts? How National Grid keeps the lights on

A visit to the chief control centre in Berkshire reveals how solar and wind are keeping blackouts at bay ... for now



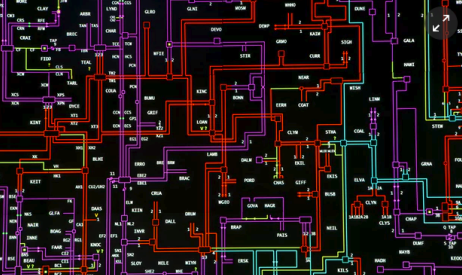
< 167 240



Adam Vaughan

@adamvaughan_uk

Monday 6 February 2017 13:12 GMT



The National Grid control centre's transmission system. Photograph: National Grid

Advertisement

Despite [claims](#) that Britain is on the brink of blackouts and amid forecasts of a looming cold snap, all is calm inside the room where a score of engineers and analysts work to ensure the lights stay on.

Below a huge, illuminated map of the UK's electricity network and myriad displays, a gentle hubbub of conversation washes over the desks of the control centre in Berkshire, the chief site of three run by [National Grid](#).

"It should look like a swan paddling across the pond," says Nick Easton, one of the grid's power system managers who sit at the back of the windowless room with six screens of their own, overseeing three teams around the clock in eight- and 12-hour shifts.



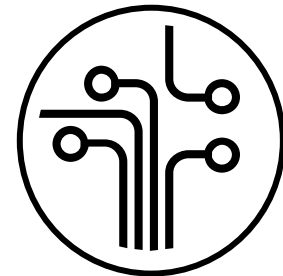
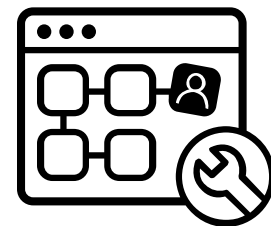
Generic ICS Environments

- ❑ Formed of HMI, PLCs, Actuators...
 - CIA Triad gets inverted
- ❑ Some Siemens S7 devices known for Man-in-the-Middle (MitM) attacks
- ❑ Sometimes connected to the Internet
 - Critical for widespread operations e.g. Oil Fields
- ❑ Formed of legacy and modern equipment
 - That 'one device' that no-one knows what it does
- ❑ How can you attack these systems?



Current State of Power Grids

- ❑ Generation, Transmission and Distribution
- ❑ Very straightforward architecture
- ❑ Driven by manual and automatic processes
 - Switching in the event of local power outage
 - Maintaining the Sync Phase
 - Reacting to demand
- ❑ Networks isolated and typically dedicated
- ❑ Closely monitored and governed by Standards Bodies and CPNI (now NCSC, a part of GCHQ)



Now to the 21st Century – Smart Grids

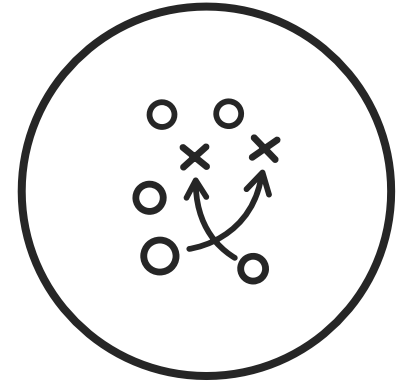
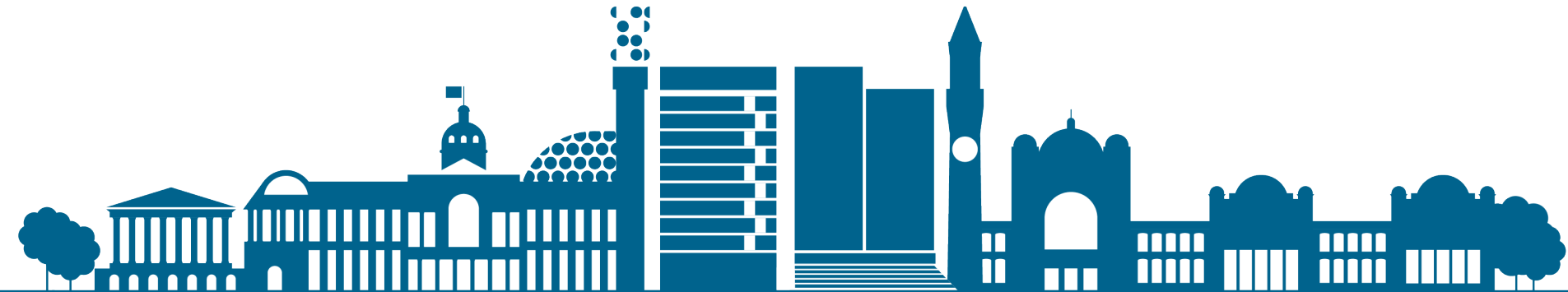
- Suddenly, everything is interconnected
- Greater visibility of the network for the DSOs and Grid Operators
- However...
 - Large Privacy Issues for customers
 - Very few ‘accredited’ devices for use in Smart Grids
 - Through interconnectivity comes a greater exposure
 - Through greater exposure comes an attack surface
- EU NIS/GDPR Directives
 - Great concern across the industry
 - Step change in how we think securely



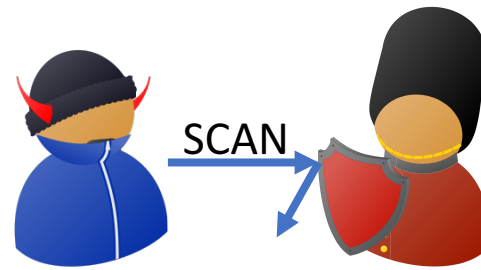
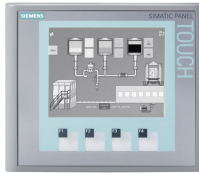


Example Attack

*Courtesy of SPARKS EU-FP7 Project
(Queens University, Belfast and AIT)*

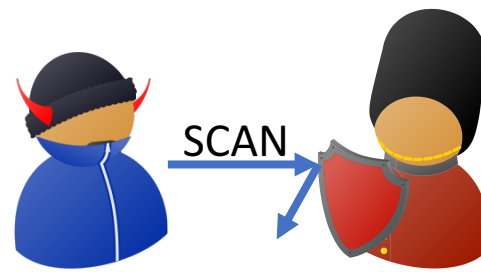
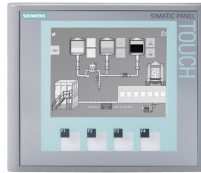


Step 1: Reconnaissance

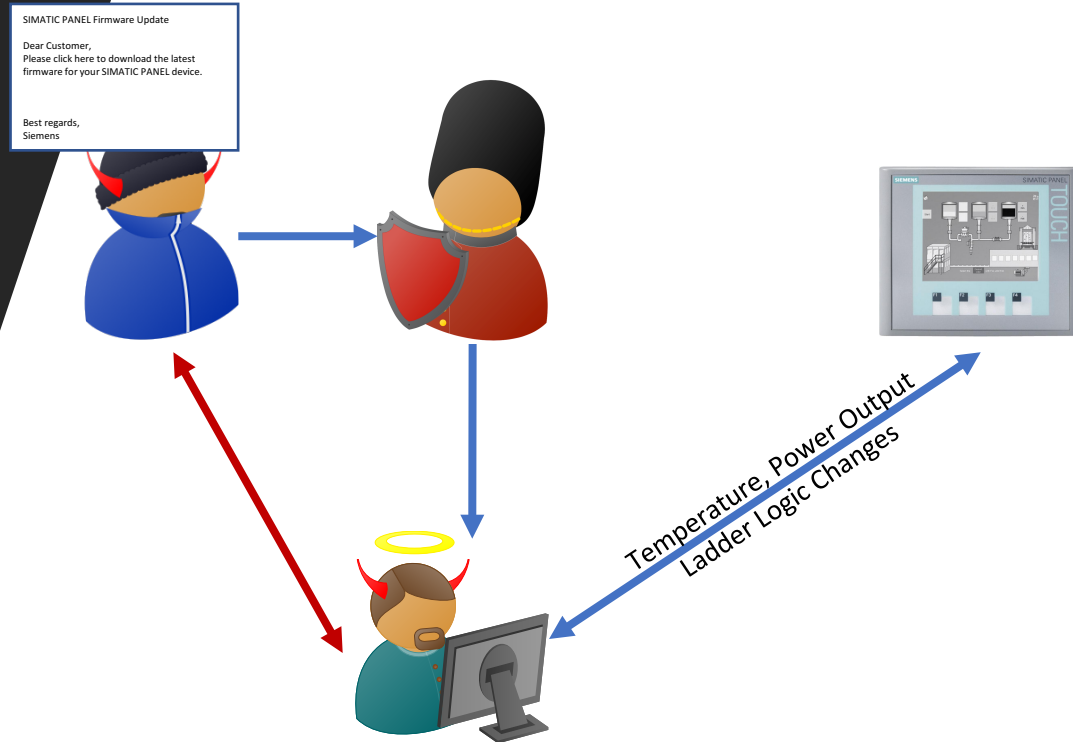


- Attacker attempts to identify entry points into the network
- ICS components are not publicly accessible on the Internet
- However, the IT and OT networks may be interconnected

Step 2: Preparation

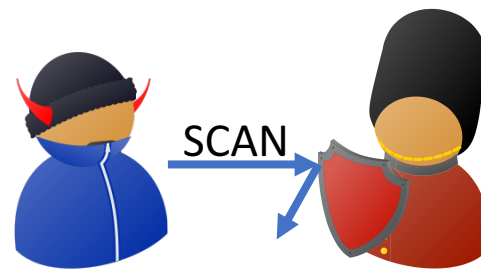
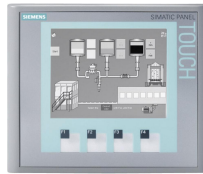
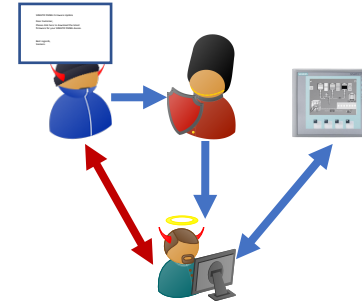
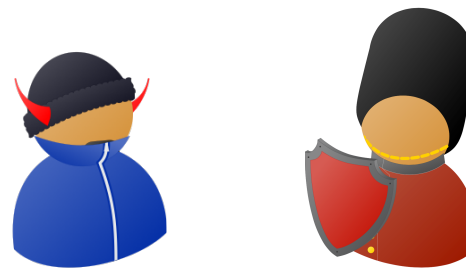
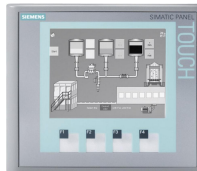
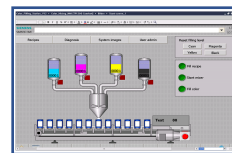


- Attacker attempts to identify entry points into the network
- ICS components are not publicly accessible on the Internet
- However, the IT and OT networks may be interconnected
- Attacker carries out a spearphishing campaign to install RAT tool on IT Network



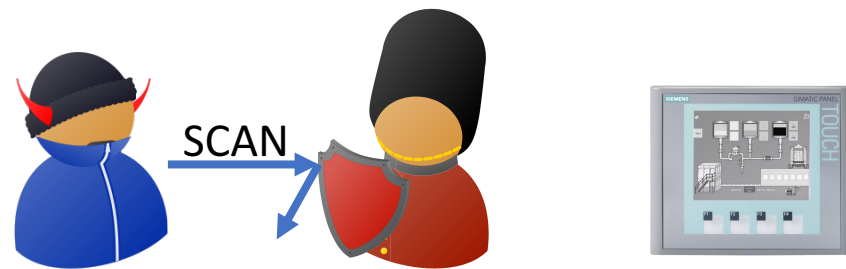
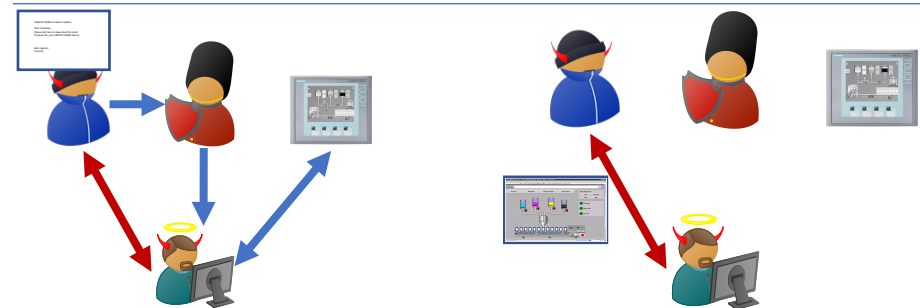
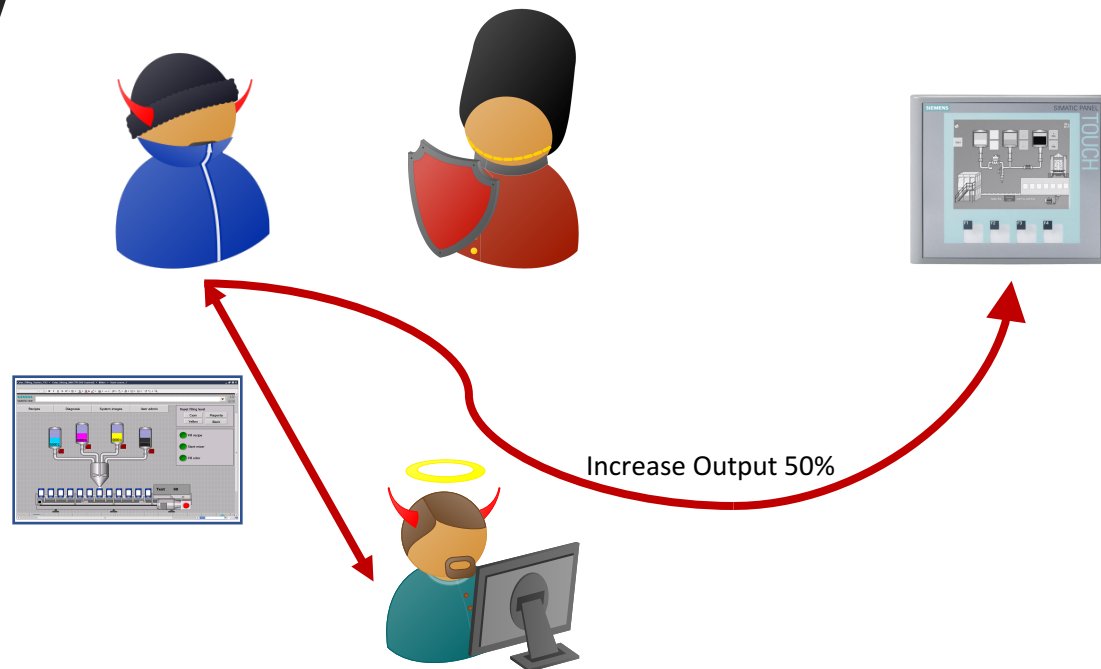
Step 3: Observation

- Attacker attempts to identify entry points into the network
- ICS components are not publicly accessible on the Internet
- However, the IT and OT networks may be interconnected
- Attacker carries out a spearphishing campaign to install RAT tool on IT Network
- Attacker now has access to the internal ICS Network



Step 4: Attack Deployment

- Attacker attempts to identify entry points into the network
- ICS components are not publicly accessible on the Internet
- However, the IT and OT networks may be interconnected
- Attacker carries out a spearphishing campaign to install RAT tool on IT Network
- Attacker now has access to the internal ICS Network
- Arbitrary messages may then be sent to the ICS system



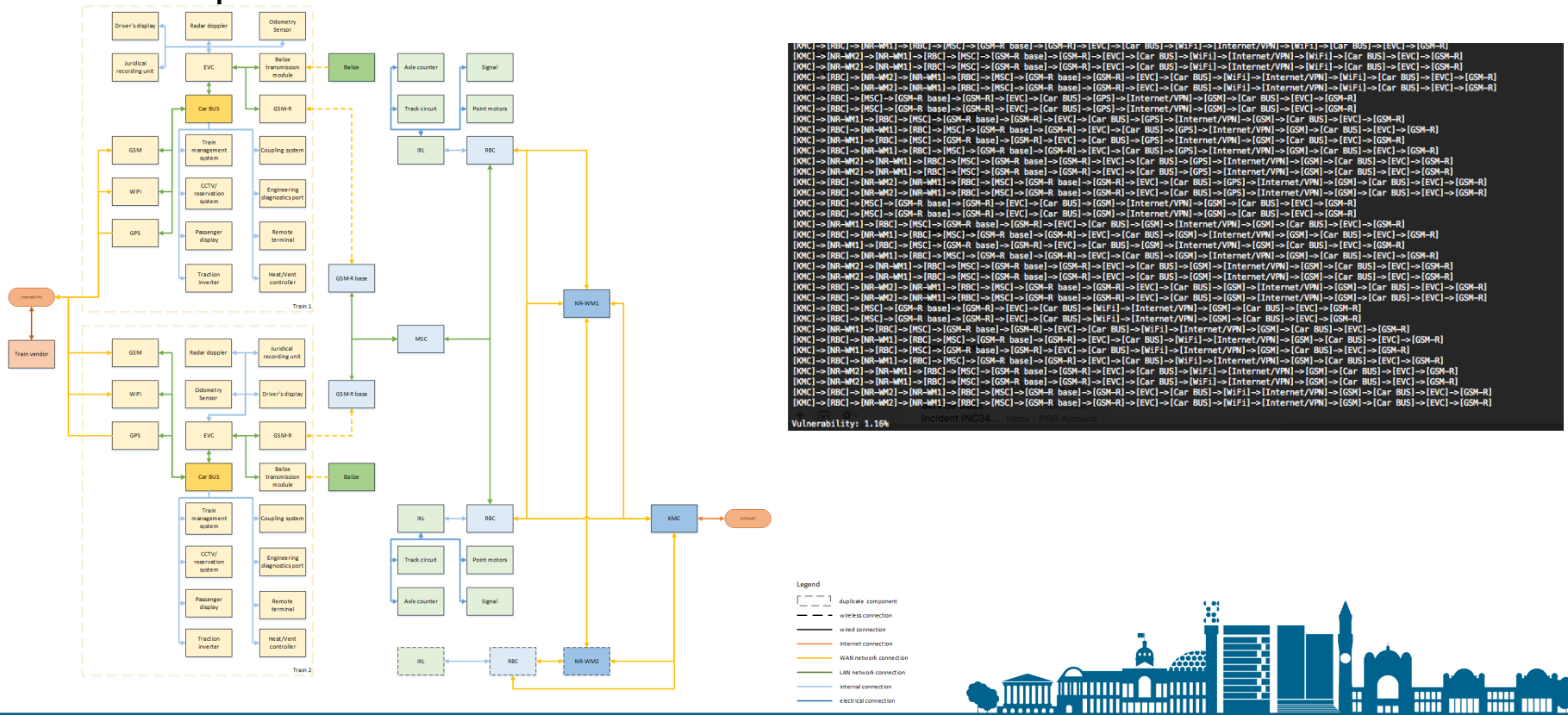
Lessons Learnt from Rail

- ❑ European Rail Traffic Management System (ERTMS)
 - Uses a 20+ year old communications standard (GSM-R)
 - ❑ Cryptography broken in less than 9 seconds (2015)
 - Trains authenticate to a signalling centre and use Message Authentication Codes (MACs) to prove integrity of messages
 - ❑ Uses custom built algorithm, which has been broken (2017)
 - Mix of legacy and new equipment
 - ❑ Track Circuit Detection systems
 - ❑ Signalling Interlocking
- ❑ Creating a methodology founded in Security that an engineer can apply to identify critical systems and exposure

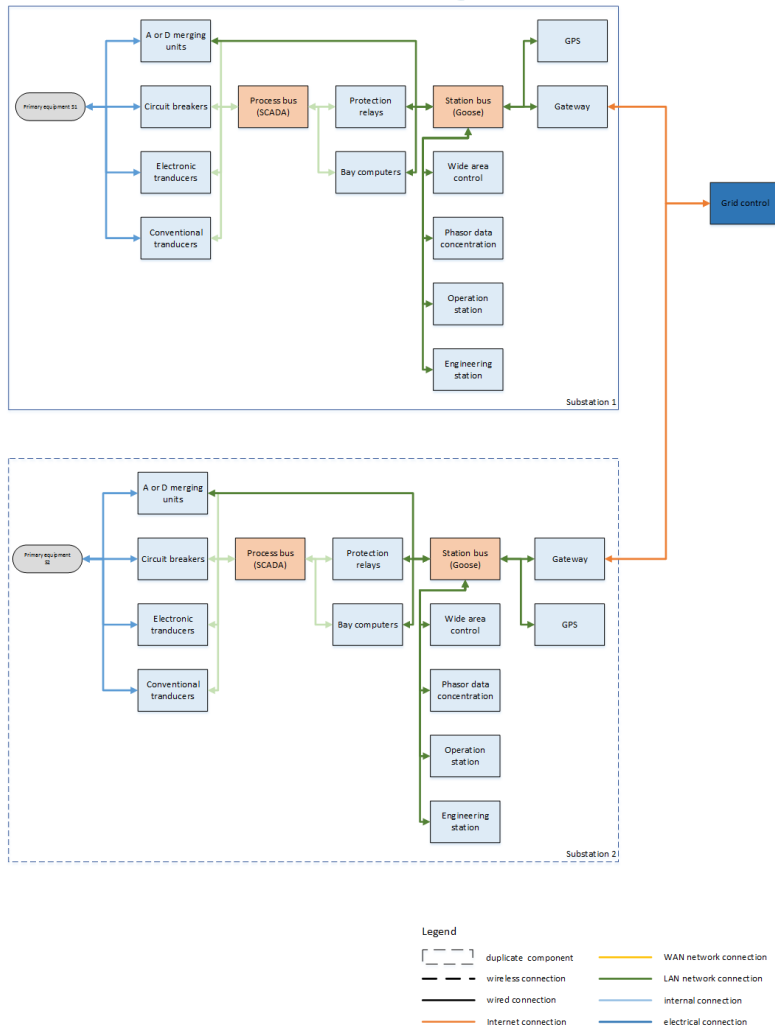


A Systematic Methodology to Identify Threats to Industrial Control Systems (SCEPTICS)

- Taking system architectures and outputting risk and potential attack paths



Modelling Power

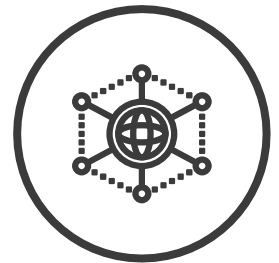


- Given some model, we can determine exposure and risk to attacks
- Challenges:
 - Not every grid is the same – generally some overlap
 - How accurate is the modelled architecture?
 - Required for NIS Compliance
 - How do you determine risk?
 - CVSS Scores



What can the Industry do?

- ❑ Introducing a Secure Supply Chain
- ❑ Audit of all devices – anything in use must have a purpose
- ❑ Intrusion Detection Systems – not a panacea
- ❑ Ensure Specifications and Standards are reviewed regularly and are in line with accepted standards
- ❑ Understand your architecture and what an attacker might be interested in – the rest will follow





UNIVERSITY OF
BIRMINGHAM

RITICS

Threats to Industrial Control Systems: Lessons Learnt from Rail

Richard James Thomas

Security and Privacy Group

R.J.Thomas@cs.bham.ac.uk

