Defining Effective Solutions to **Assure the 'Industrial IOT' for** NIS Directive Compliance

Dr Richard J. Thomas (r.j.thomas@cs.bham.ac.uk)
Birmingham Centre for Cyber Security and Privacy
UKRRIN Centre of Excellence in Digital Systems

RITICS at Birmingham

- Collaboration between Computer Security and the UK Rail Research and Innovation Network (UKRRIN) Centre for Excellence in Digital Systems:
  - Tom Chothia
  - John Easton
  - Richard Thomas

- Previous Work (SCEPTICS):
  - Security assurance of parts of the ERTMS standards
  - Formal verification of safety-critical protocols used in ERTMS from a security perspective
  - Cryptanalysis of ERTMS MAC schemes
  - Defining a post-quantum key management solution for ERTMS
  - Developed a modelling tool for asset owners to carry out hazard/threat analysis

The EU NIS Directive

- Requires a “culture of security across sectors”
  - Asset owners have to consider the security of their own infrastructures *and* their supply chain
- An inherent skills gap exists between cybersecurity and engineering
  - In some sectors, asset owners relied on assurances provided by their suppliers - it is now *their* responsibility to assure the security of their systems
- Presents a financial *and* legislative impetus for compliance and reporting incidents with regular inspections

The EU NIS Directive

- Requires a “culture of security across sectors”
  - Asset ow… …*and* their supply chain
- An inherent s…
  - In some s… …uppliers - it is nov…
- Presents a fi… …cidents with regular inspe…

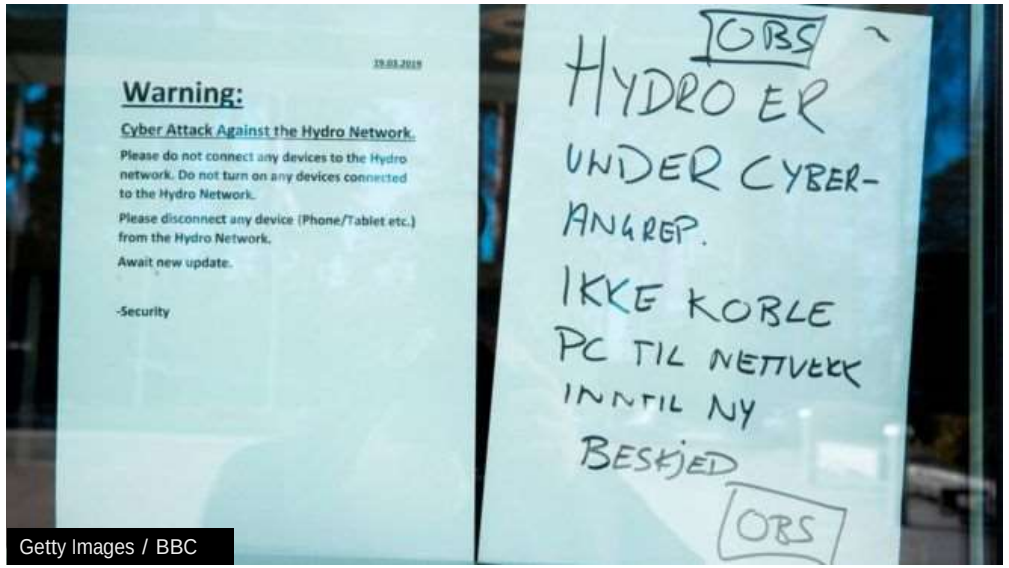
The Changing Nature of Industry - A problem for Asset Owners

- Systems are no longer bespoke
  - Step-change to Commercial-off-the-Shelf (COTS) solutions
  - Mass proliferation of digital systems over electro-mechanical
  - “We need the data, we need automation”
- With new architectures and systems come new threats and attack vectors
  - The attack surface has changed
  - Attacks against specific components in one factory may now work in scale
- Asset owners *must* be confident in the security in the systems they procure
- “My email is in the cloud. Why isn’t my production plant?”

Interlude: Norsk Hydro

- Malware/Ransomware affecting production systems
  - LockerGoga variant
- Brought one division ‘to a standstill’
- Return to manual processes
  - Response was fast and visible

- Whilst IT-focused, it *significantly* affected the OT side of the business.



Getty Images / BBC


Norsk Hydro

How are we contributing?

- Effective Solutions for the NIS Directive Project
  - WP1: Guidance to industry on secure specifications for devices
    - Looking at existing vulnerabilities – how did they enter the supply chain (e.g. via standards/coding error)
    - Identifying good strategies to secure these devices before/post-procurement, and pre-deployment
  - WP2: Threat and Asset Identification in Operational Systems
    - What automated tools can asset owners use to analyse their infrastructure and detect possible issues?
  - WP3: Guidance on in-depth testing
    - Carrying out manual analysis of devices and identifying strategies for the ‘keen’ asset owner to do their own analysis
- Making it easier for ICS owners to understand and detect weaknesses
  - Reduces the challenge in maintaining/working to NIS compliance
  - Does their equipment do what it says it does – nothing more, nothing less

Progress to Date

- Surveying existing vulnerabilities in commonly-deployed ICS devices
  - Unauthenticated traffic, coding errors for web services, improper validation of Ethernet frames leading to reboots
- Assessing the wider security of open standards used by industrial devices
  - If the standard has a ‘smoking gun’, your devices will
- Developing a rail-specific demonstrator using PLCs and HMIs from various vendors
  - Simulating existing attacks and looking for new vectors
- Engaging with Industrial Partners to look at the ‘real world’ of deployed systems
  - Fuzzing and observing ‘real’ traffic in a *safe* environment

Progress to Date

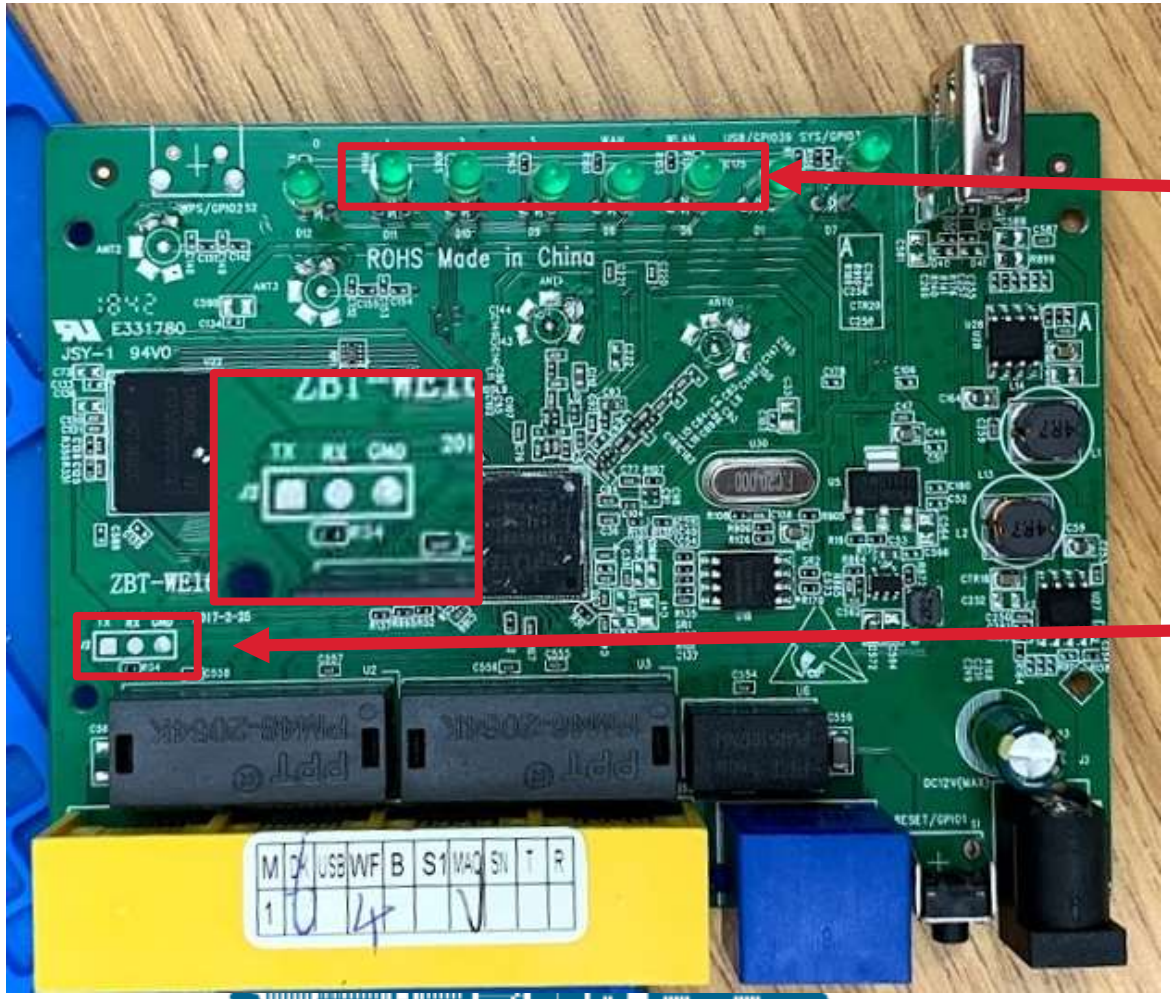
- Surveying existing vulnerabilities in commonly-deployed ICS devices
  - net
- A
- D
- E

Hardware Analysis:
Why are we starting with Firmware?

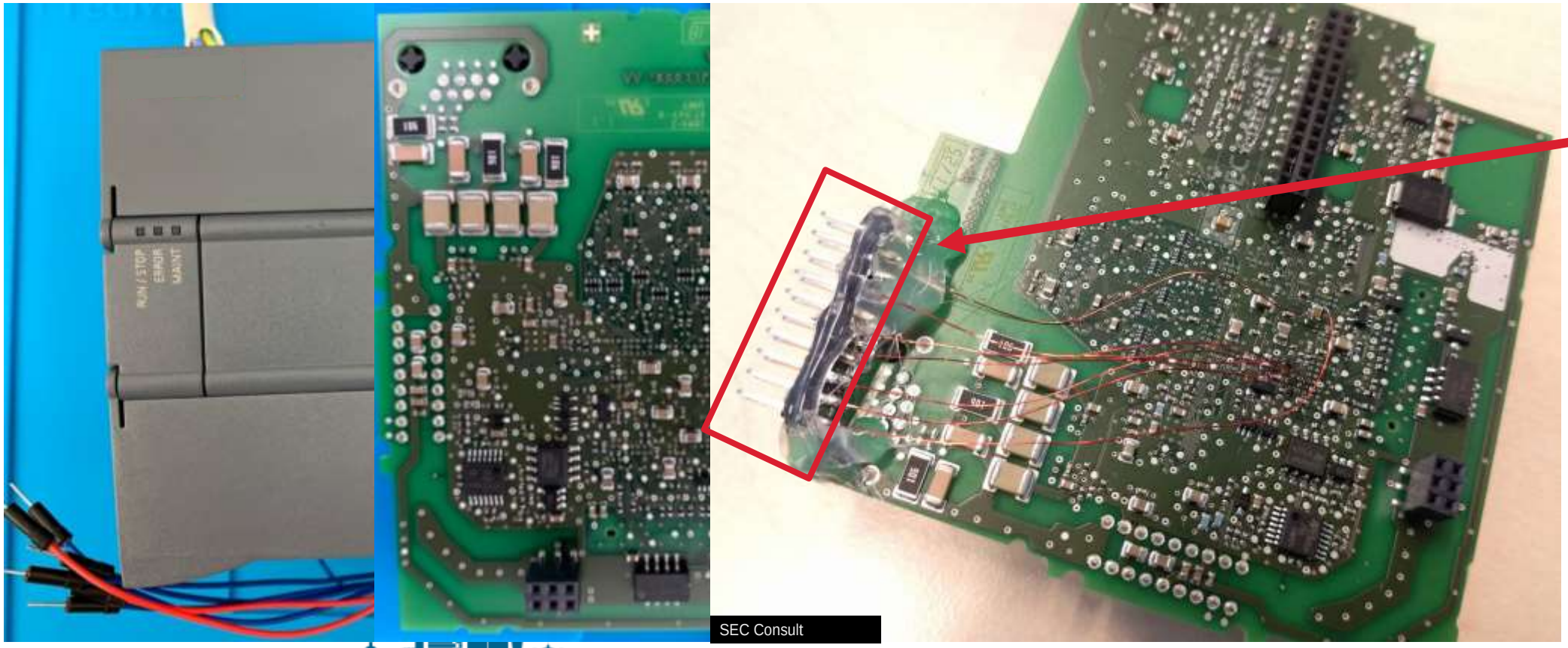
- Lots of common vulnerabilities in devices are discovered through firmware analysis
  - Most analyses have focused on commodity hardware, e.g. routers and switches
- Firmware Analysis has led to the discovery of major recent attacks
  - e.g. IP Webcams, IoT devices, Joel's Backdoor
- Device firmware images provide a ground truth about the security of a device
  - It demonstrates the vendor's intent and competency.

- Asset owners aren't expected to carry out this analysis
  - Can we distil a useful and easy process for them to assure the security of their supply chain based on what we're doing?

Hardware Analysis: Finding Debug Functionality



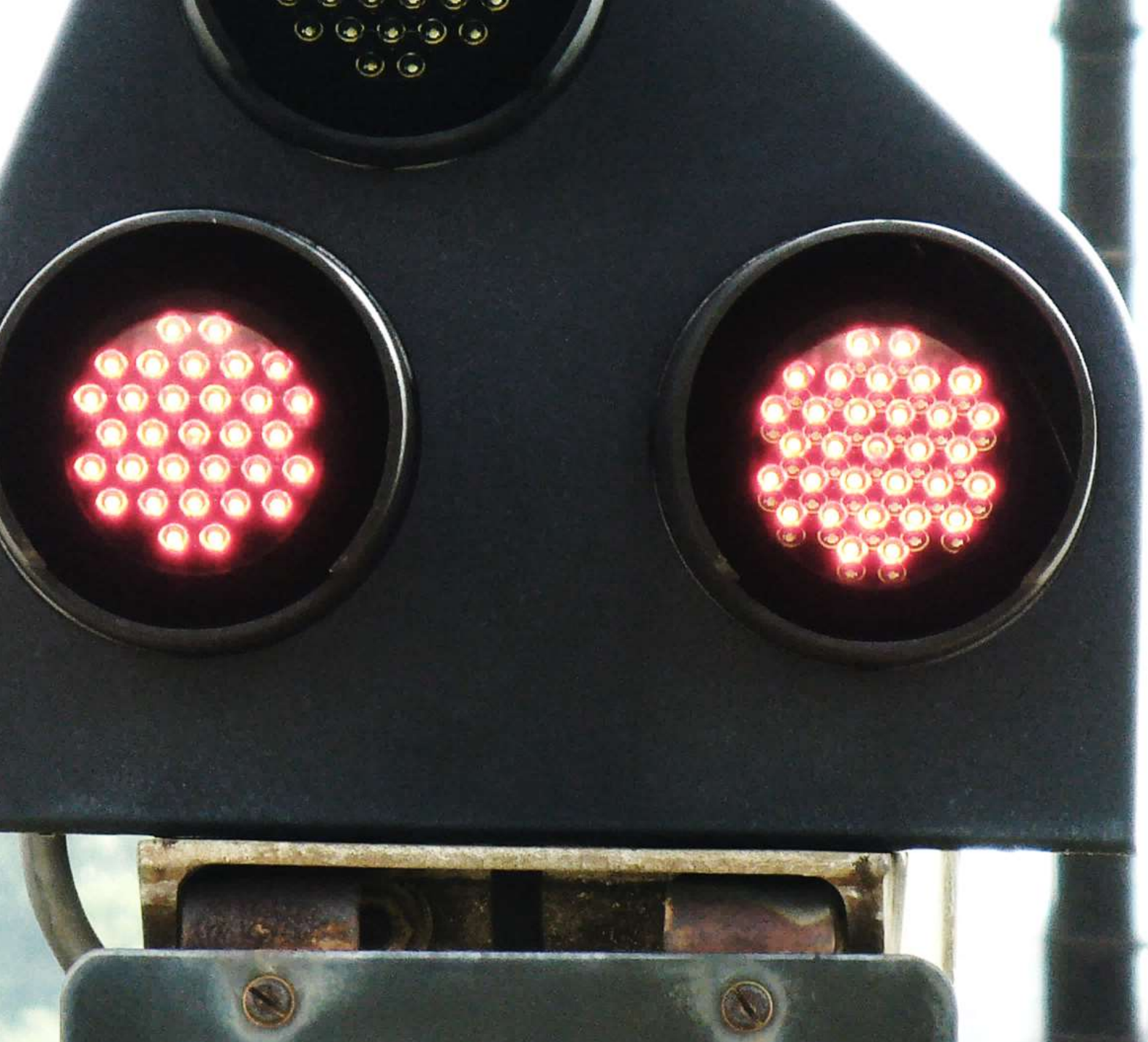
Hardware Analysis:
Finding Debug Functionality



Future Outlook

- What tooling currently available for asset owners to discover assets and carry out basic threat identification?
- What ‘interesting’ functionality exists on some of these devices which may be insecure from the outset?
- Developing guidance to industry and asset owners on what the supply chain *should* do to make sure devices are *secure by default* and how we can satisfy ourselves a device is secure
- Low-level analysis of devices – extracting firmware, and more ‘exotic’ attack vectors

- Move from the ‘general’ Industrial IoT to sector-specific through rail
  - Testing our solutions, and ‘fit’ for cross-industry guidance



Questions?

Defining Effective Solutions to **Assure the 'Industrial IOT' for** NIS Directive Compliance

Dr Richard J. Thomas (r.j.thomas@cs.bham.ac.uk)
Birmingham Centre for Cyber Security and Privacy
UKRRIN Centre of Excellence in Digital Systems