# ICS Security Risk: The Wider Context

**Michael Stubbings**

NEPIC: 22nd March 2018

SYSTEMS AND ENGINEERING TECHNOLOGY

FRAZER-NASH CONSULTANCY

# Introduction

- The Topic
  - ICS security for purposes apart from COMAH and NIS regulation
  - A single view of ICS security risk – and where it fits with corporate risk
- The Speaker
  - HMG background in cyber security policy and practice
  - Working in civil nuclear, rail control system security

# Risk and its context

- Threat is real
  - State versus non-state
  - Intention - if they don’t have the intention now, they might before your next technology refresh
  - Capability – if the threat doesn’t have the capability, it can be bought on the criminal market
- Risk and Regulation: COMAH, NIS and HSE
  - NIS is a positive development for the practice of control systems security and for the security of critical national infrastructure (CNI) in particular
  - Role of HSE and other Competent Authorities is also a positive development for CNI and the UK in general
- Remainder of presentation: broader, complementary aspects of risk

# Components of risk

- Terminology can – quite legitimately - vary
- Risk: A threat exploiting a vulnerability to produce an unwanted business impact
- Threat: Environmental (e.g. weather, power supply failure) or personal (e.g. malware writer, malicious or inattentive user)
- Vulnerability: A weakness in an organisation’s assets (e.g. poorly configured software) or systems (e.g. user training or visitor control)
- Business impact: If it would need Board attention, the risk should be on the corporate risk register

# Key risk starting points

- Threats: Know your threats and keep your knowledge up to date. Public and HMG sources of information are available including HMG/industry forums.
- Vulnerabilities: Know your assets, including hardware and software versions, network topologies, business or process-critical data and operational procedures, supply chain. Knowledge of legacy assets frequently a problem. Keep up to date with known technical vulnerabilities.
- Impacts: Ensure corporate risk register (business-critical risks) and potential ICS security significant risk impacts stay in step

# Types of risk assessment

- Lots of methods available, some proprietary, some freely available, some published as standards, some backed by software tools

- General principles pretty constant:
  - Identify and value your assets;
  - Identify the vulnerabilities in your assets;
  - Identify your threats;
  - Identify the outcomes of threats acting on vulnerabilities;
  - Identify the extent to which your existing security controls will manage the risks – include the safety controls in this;

- Note the overlap with safety hazard assessment – capitalise on this by aligning cyber security and safety assessment processes

# A complementary risk approach

- Top down: starting from the corporate risk register
  - What are the corporate priority risks?
  - What are the threat-vulnerability-impact scenarios which would allow them to be realised?
- Two approaches can validate each other, and help ensure that business-critical risks are identified
- Helps align cyber security risks with business priorities

# Risk tolerance

- Once you know your risks, what to do with them?
  - Accept;
  - Avoid;
  - Mitigate;
  - Transfer

- For this you need a concept of risk tolerance.  As noted, ALARP may not be appropriate (i.e. cost-effective within legal constraints)
  - The ALARP ‘carrot’ diagram may still be a useful model, but;
  - Where do you draw the toleration zone boundaries (i.e. where do we need to invest in our security procedures)? – may be affected by practicalities
  - This is a business decision with technical consequences rather than the other way around

# Selection of security controls

- If you’re not sure of the state of your Operational Technology assets, start with a well-attested checklist, e.g. NCSC or SANS (‘critical controls’), don’t wait until after detailed asset discovery and risk assessment exercises

- Otherwise: select your control objective (transfer, avoid, accept, mitigate) according to your business risk tolerance, to do one of the following:
  - Prevent/deter an attack (stop or impede an attacker in the first place);
  - Detect an attack taking place (for immediate action);
  - React/recover (during or after an attack to limit its impact)

# Cyber security assurance

- How do you know your security controls are sufficiently effective?
  - Penetration testing;
  - Design reviews;
  - Modelling (mathematical);
  - Modelling (test rigs);
  - Functional testing;
  - Observation;
  - Exercises;

- Selection of nature and frequency of assurance?

- Who needs to know?

# Project life cycle (new systems/significant upgrades)

- Incorporate cyber security risk assessment and control selection into the requirements capture and design processes as the same requirements or controls might have dual use – safety and non-safety;
- Align safety and security processes, including governance (e.g. review and sign-off) to allow this to happen
- Allow for iterative assessments as designs mature;
- Incorporate cyber security into the safety case process – safety cases must allow for deliberate attack;
- Ensure you maintain a security case which includes non-safety controls

# Legacy systems

- Risk tolerance may have to be different for legacy systems;
- Determining asset state and configuration may be difficult – e.g. identifying software provenance and current state for old assets;
- Precise effect of system changes may be difficult to forecast;
- Older, proprietary hardware and software assets may not be amenable to monitoring or testing;
- Detailed technical knowledge may be narrowly distributed (i.e. in a very few – possibly older – heads);
- Resilience of legacy systems may not be fully known.
- On the other hand: in general terms, older more proprietary projects have a lower level of vulnerability to attack

# Summary

- Cyber security threats to control systems are real
- Tools and techniques to deal with them are available
- Support is available, including government and public domain support
- Legacy and new systems are likely to need different approaches
- Safety and cyber security are complementary and must be aligned
- Control system risks are business risks

# Contact details

Martin Concannon

m.concannon@fnc.co.uk

01925 404062

07793 528249

Michael Stubbings

m.stubbings@fnc.co.uk

0117 9226242

07753 311243