

Cyber Security Risk



John Pirie

HM Principal Specialist Inspector,
Team Leader – EC&I – Energy Division

Safety 30 Conference – June 2018

TLP Green

Crown © Jan 2018

Outline

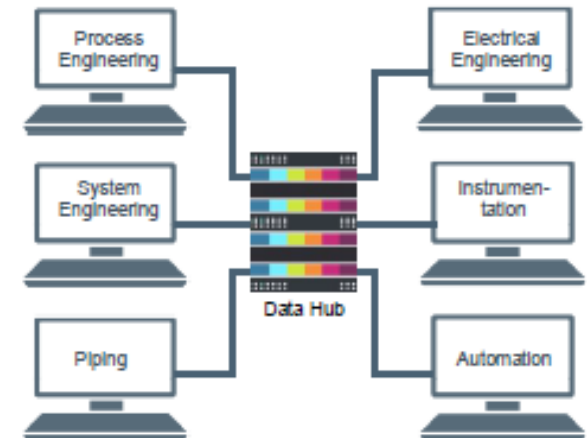
- Why Cyber Security is an issue
- What are the risks
- Trends / Threats
- Scenario
- Guidance / Standards / Regulations
- Key Messages

Why Cyber Security is an Issue

Why cybersecurity is an issue - Technology



- Increased use of programmable systems
- Convergence of technologies used for industrial automation control systems (IACS) and IT systems – OS, network protocols etc.
- Not just plant control systems –also power management, utilities, phones (VoIP) etc.
- Also management systems – e-Permits, e-Procedures...
- Increased connectivity between industrial control systems and business systems and 'the cloud' (internet, remote access, cloud services)
- **Much greater potential attack space**



Why cybersecurity is an issue - Design



- Traditional design concepts were based upon independent layers of protection, i.e. the likelihood of all the protection layers failing at the same time is very low.
- Risk assessments didn't consider multiple failings or malicious intent as credible.
- Our experience shows that accidents are more often due to (non-intentional) common cause or systemic failure (such as, inadequate functional safety management, competence leading to human error)
- Cyber attack (intentional or otherwise) is another potential common cause failure.

Why cybersecurity is an issue

But you're OK – You have a Firewall



What are the risks?

What are the risks?

- Safety / Environmental – increased risk of accident
- Mal-operation or loss of a control system leading to an unsafe state-an initiating event
- Mal-operation or loss of a safety system such that it does not operate - protection layers fail
- Loss of other utilities – power, comms etc. (for incident response)
- **All can occur at the same time ➡ common cause failure**

What are the risks?

- Business –Loss of data, intellectual property –for business to manage (GDPR applies to certain sensitive data) –not regulated by HSE
- Critical national infrastructure (CNI) –e.g. loss of power, utilities –to be regulated under new NIS directive from May 2018. (HSE will regulate energy sector under agency agreement to BEIS)

Do you know what systems are vulnerable?

Do you know the extent of those vulnerabilities?

What are the risks?

Typical Systems:

- Process Control Systems
- Fire and Gas Systems
- Power Systems
- Stability Systems – MODU
- Jacking Systems
- Dynamics position Systems
 - FPSO / Dive vessels / Drilling Rigs
- Well Control
- Cyber Drilling Rigs
-etc.



Trends / Threats

Threat Summary



States

Criminals

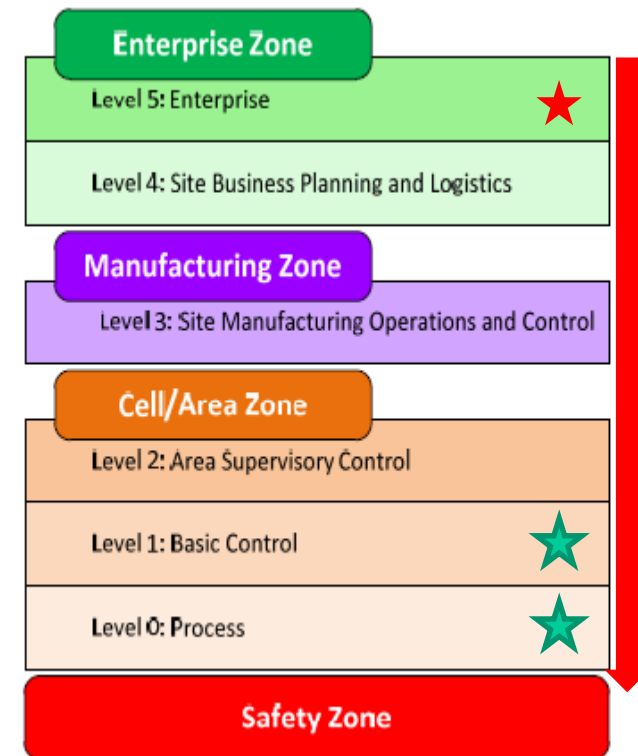
Hacktivists

Terrorists

Trends / Threats

Evolving Threat Landscape – High End Attacks

- Changing appetite of nation states for destructive attacks - e.g. Saudi Aramco, TV5, Sony.
- Capability developed specifically to target complex and cyber-physical software components e.g. Stuxnet, Bangladeshi Swift incident, Ukrainian Power Grid incidents.
- Trend towards exploitation of devices deeper in the Purdue Model.
- “Industroyer/CrashOverride” Protection Relay Denial of Service malware.
 - Functionality to enumerate and control industrial systems.
 - Evidence that the threat actors understood the target environment.



Trends/Threats

- Availability of hacking hardware and software 'toolkits' and coordination – reduced entry level
- Social engineering techniques / Spear phishing
- Average time to detect intrusion into your corporate network is months. (175 days in Europe)

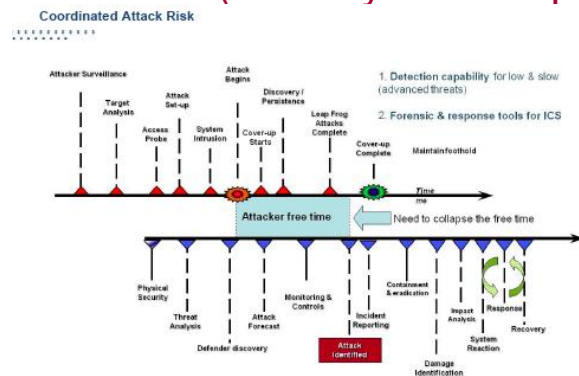


Figure 3: Typical attack time cycle



Ransomware attack hits Chernobyl, Cadbury, Maersk

RADIATION monitoring systems at the Chernobyl nuclear plant were put out of action by a ransomware attack which began in Ukraine on 27 June and hit companies around the world.

Chernobyl workers had to manually monitor radiation after the cyberattack knocked out the operation's Windows-based systems.

The attack, a modified form of existing *Petya* ransomware, dubbed by some security firms as *NotPetya* or *Nyetya* to distinguish it, was first reported in Ukraine. It spread around Russia, Europe and Australia affecting firms including Rosneft, Merck, Reckitt Benckiser and Beiersdorf.

Victims were told they must pay US\$300 in Bitcoin to recover their encrypted files.

The Maersk Group said IT systems went down across its business units including its oil and drilling activities, though they were "not operationally affected," while local news in Australia reported that computers at a Cadbury factory in Hobart owned by Mondelez were displaying messages demanding payments to release files.

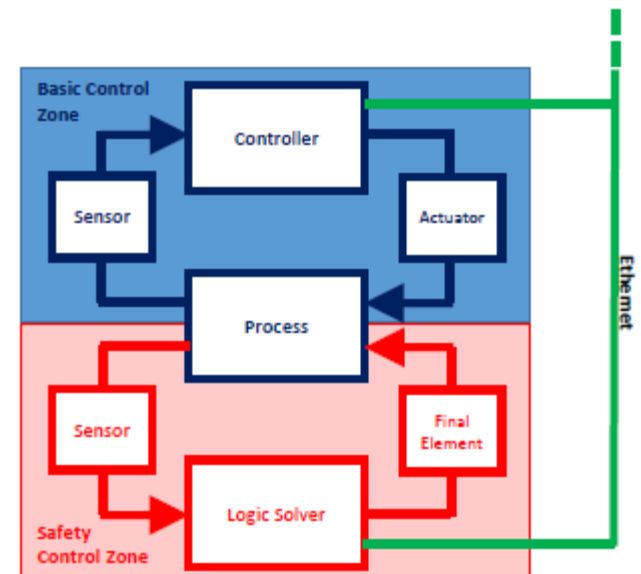
There is no clear indication of who was behind the latest attack.

The Chemical Engineer (July / August 2017)

Trends/Threats - Triton/Trisis

When things go wrong – Petrochemical plant

- First documented example of an attack against a Safety Instrumented System.
- Engineering workstation was target of compromise.
- Malicious software masquerading as legitimate application.
- Appears to have been unsuccessful and the payload was not recovered.
- Attack framework allows the attacker to arbitrarily adjust safety loop parameters.



Scenario

Introduction

On 28 Feb 2020, a calm but cold and foggy evening, at approximately 11PM, a jetty tank at HackedChemCo overfilled and released significant quantities of flammable material.

The cloud drifted across the local estuary and towards a residential area where people later reported an unusual smell.

The cloud ignited shortly after causing a massive explosion.

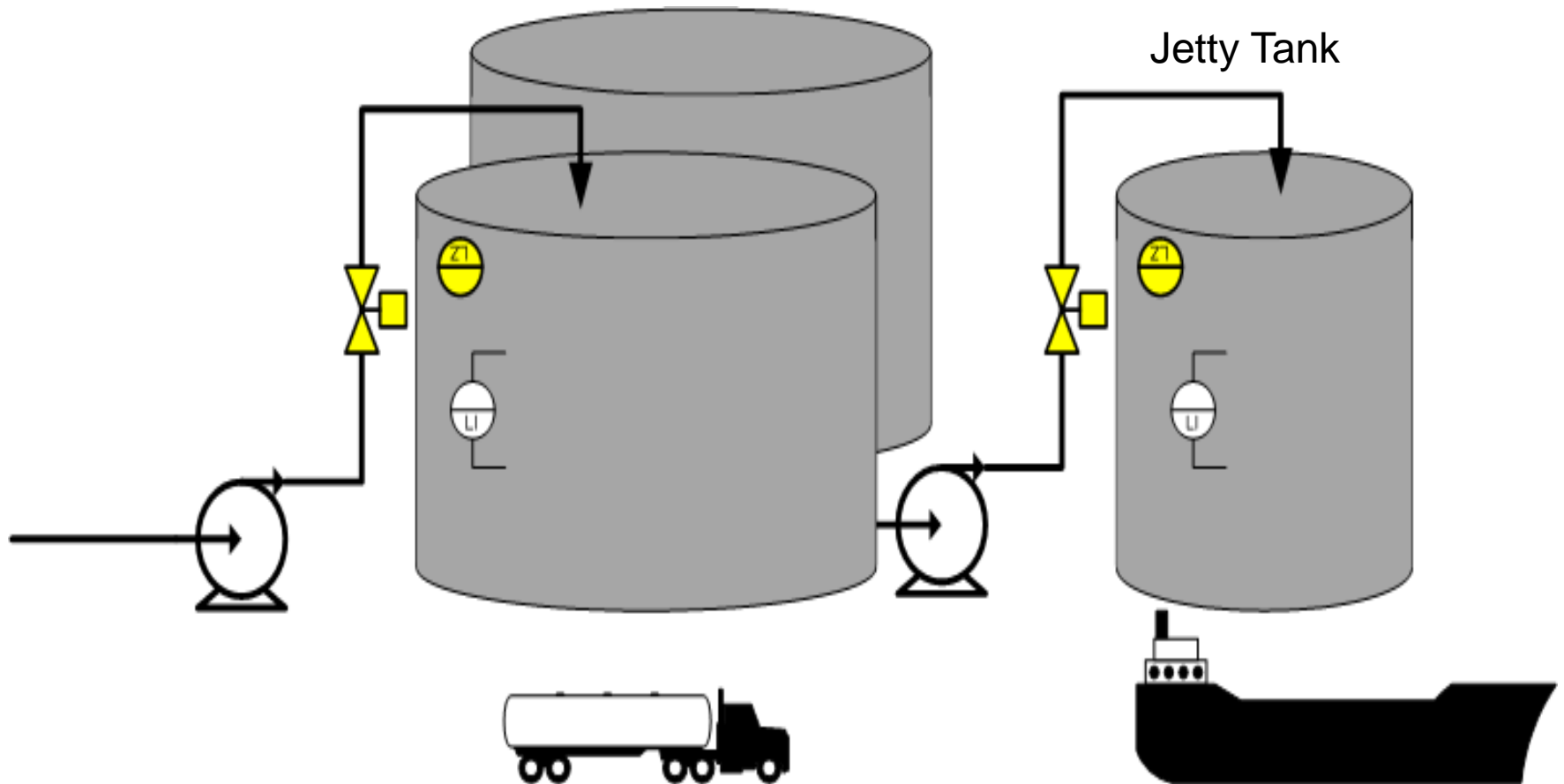
There was substantial blast damage to the residential area and some injuries.

Process Overview

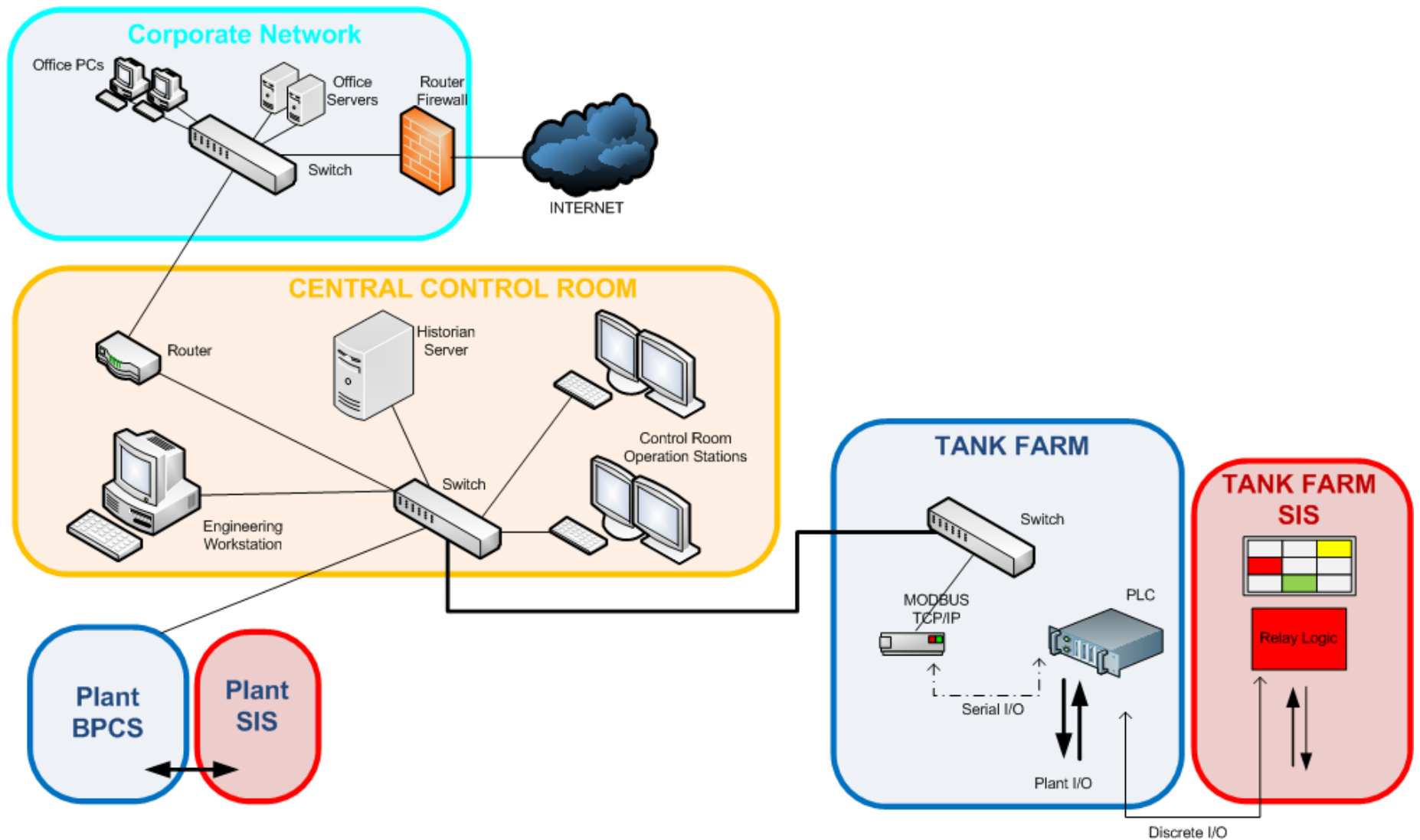


Storage Tanks

Jetty Tank



ICS Overview



Compromise the supply chain

The attacker uses a “watering hole” attack to compromise a SME supplier to the operator.



Send an email from the supply chain containing malware

The attacker crafts a “spear-phishing” email which is sent from the supplier’s systems. The email contains malware which gives the attacker command and control of the operator’s enterprise desktop.



Establish persistent access to the enterprise network



The attacker spreads laterally across the operator's corporate network, securing persistent access.



Exfiltrate network design documents, ICS docs, P&ID, maintenance schedules, passwords for key systems.

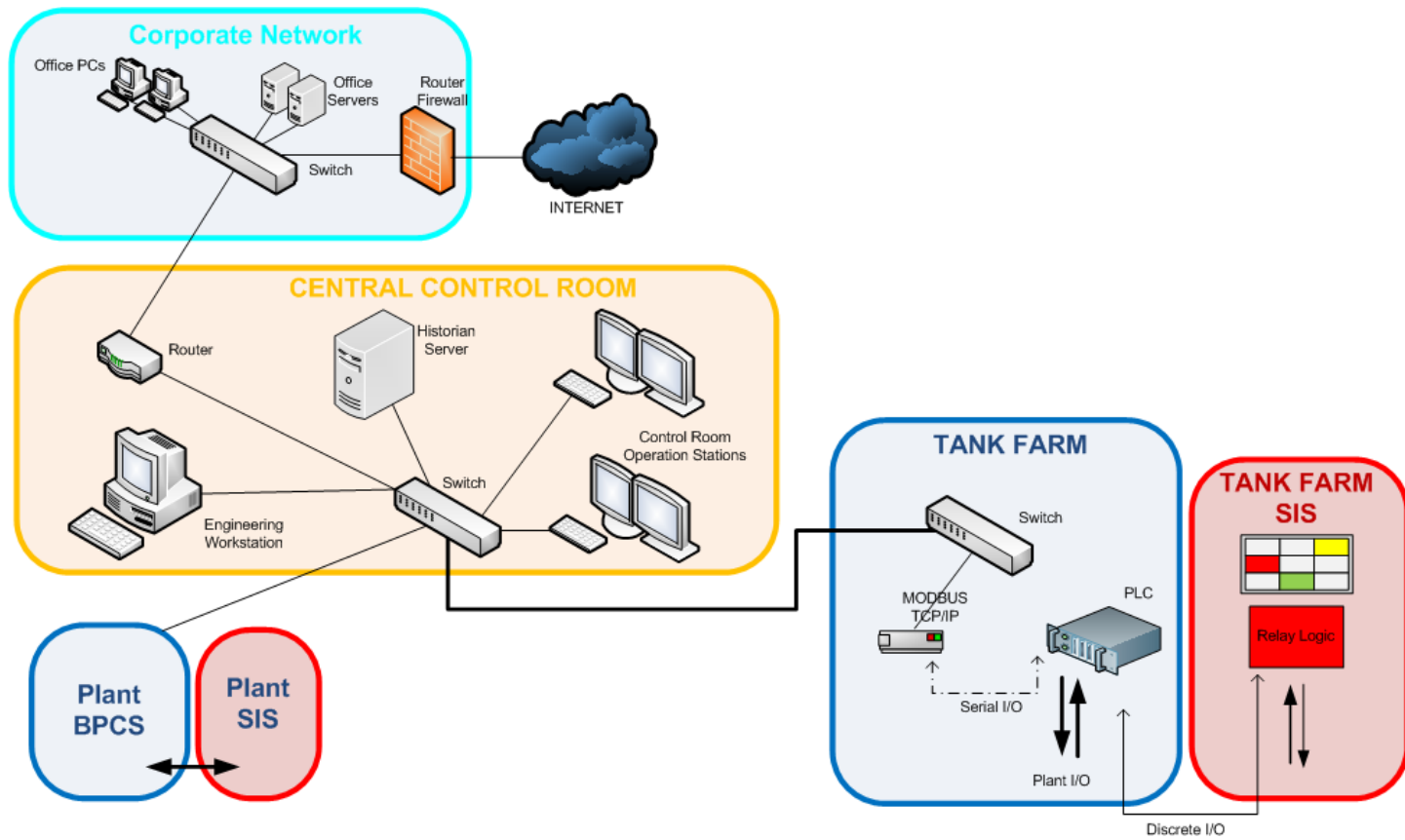


The attacker accumulates the technical information they need in order to attack the system.



Move laterally to the ICS

The attacker obtains the credentials and has the knowledge of the network to penetrate deeper into the control system.



Attack ICS

The attacker intercepts and modifies MODBUS over TCP/IP communications between the tank farm PLC and DCS. The SIS is overridden, and material covertly pumped to overfill the jetty tank.

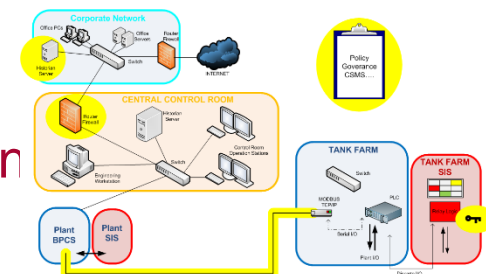


The actual story

What really happened...

The Operator had:

- a cyber security management system (CSMS) and a cyber security policy (CSP)
- stipulated Cyber Essentials as a minimum requirement
- Provided Staff awareness training
- As built Network diagram split into relevant zones and connected by conduits.
- an Asset Register of all IACS assets
- carried out a Risk Assessment
- identified and implemented countermeasures arising from the Risk Assessment



Guidance / Standards / Regulations

Applicable Industry Guidance

- Lots of good guidance available, but it can be overwhelming, and it's not all limited to safety and environmental risks.

- ISA-TR84.00.09-2013-Security Countermeasures Related to Safety Instrumented Systems (SIS).
 - National Cyber Security Centre –Security for Industrial Control Systems

- www.ncsc.gov.uk/guidance/security-industrial-control-systems

- NIST Publication 800-82 –Guide to Industrial Control Systems (ICS) Security

- nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

- 10 steps to Cyber security

- <https://www.ncsc.gov.uk/guidance/10-steps-cyber-security>



HSE Operational guidance (OG)

Cyber Security for Industrial Automation and Control Systems (IACS)

Open Government status
Open

Target audience

Chemical Explosives and Microbiological Hazards Division (CEMHD) and Energy Division, Electrical Control and Instrumentation (EC&I) Specialist Inspectors

Contents

Cyber Security for Industrial Automation and Control Systems (IACS)	1
Open Government status	1
Target audience	1
Summary	2
Introduction	2
Action	4
Background	4
Organisation	4
Targeting	4
Timing	4
Resources	4
Recording & Reporting	4
Health & Safety	4
Diversity	4
Further References	5
Relevant Regulations	5
Recognised Good Practice	5
Other Relevant Standards	5
Contacts	5
Appendix 1: Process for the Management of Cyber Security on IACS	6
Note 1 – Security Threat	7
Note 2 – Cyber Security Management System (CSMS)	7
Note 3 – Defining the IACS	10
Note 4 – Risk Assessment	12
Note 5 – Define and Implement Countermeasures	13
Note 6 – Safety Instrumented Systems (SIS)	15

- Published on HSE website Mar 2017.
<http://www.hse.gov.uk/foi/internalops/og/og-0086.pdf>
- Why was this needed
 - Provides a regulatory and technical framework which did not exist.
 - It provides for proportionate risk reduction and one means to demonstrate ALARP which other guidance does not cover.
 - For MH regulated industries.
 - Consistent with wider available guidance.

PSA Recommended Guidelines

- Published on PSA website
 - Also provides a regulatory and technical framework.
 - A basis for regulate against for H&S risks
 - Provides a baseline for Information Security Requirements in Industrial Control Systems
 - Consistent with wider available standards, such as IEC 62443.

104 – Norwegian Oil
and Gas recommended
guidelines on
information security
baseline requirements
for process control,
safety and support ICT
systems

Applicable Standards

- Functional safety. IEC 61511 Ed 2 has specific requirements for cybersecurity threats. This is the benchmark Standard HSE uses for safety instrumented systems.
- Security standards are developing
- IEC 62443. Note this is not limited to functional safety.
 - Part 1: Framework and threat-risk analysis
 - Part 2: Security assurance
 - Part 3: Security requirements
 - Part 4 Relevant to system integrators.

NIS Directive



EU Network & Information Systems Directive (NIS)

Became UK Law in May 2018

- Top Level Objectives:
 - A. Managing Security Risk
 - B. Protecting against Cyber Attack
 - C. Detecting Cyber Security Events
 - D. Minimizing the Impact of Cyber Security Incidents

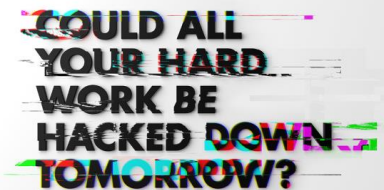
Applicable to Operators of Essential Services

A screenshot of the National Cyber Security Centre (NCSC) website. The page is titled 'The NIS Guidance Collection' and is part of the 'Guidance' section. It features a search bar at the top right and a navigation menu with links to 'Guidance', 'Threats', 'Incident Management', 'Marketplace', 'Education & Research', 'Insight', 'Press & Media', and 'Topics'. The main content area includes a version box for 'VERSION 1.0 (30 APRIL 2018)', an introduction to the NIS Directive, and a list of guidance documents. On the right side, there are sections for 'Subscribe to guidance updates' with a 'Guidance RSS Feed' link, 'More like this' with links to 'What is a WARP', 'HMIG IA Maturity Model', 'Independent Review', 'IA Maturity Model - Self Assessment and Supported Self Assessment', 'Systems administration architectures', and 'Internet edge device security'. At the bottom right, there is a 'Most Popular' section with a list of popular guidance documents.

Key Messages

Key messages

Cyber security is most **effective** when integrated well with risk management. Businesses can refer to a wide range of good cyber security guidance and adopt one or more of the available schemes to achieve a recognised level; **ultimately** the aim is to make it hard for attacks to be successful and be ready to respond to cyber security incidents. **NCSC**

A graphic with a grey background and a black border. It contains the text 'COULD ALL YOUR HARD WORK BE HACKED DOWN TOMORROW?' in a bold, black, sans-serif font. The text is surrounded by colorful, pixelated lines in red, green, blue, and yellow, giving it a digital or cyber-themed appearance.

Key messages

“A combination of factors is dramatically reshaping OT security. More Internet connected industrial automation devices and the convergence of OT and IT infrastructures, in addition to a shortage of security skills, means that accurate evaluation and mitigation of security risks is increasingly challenging.” Robert Westervelt

Thank You