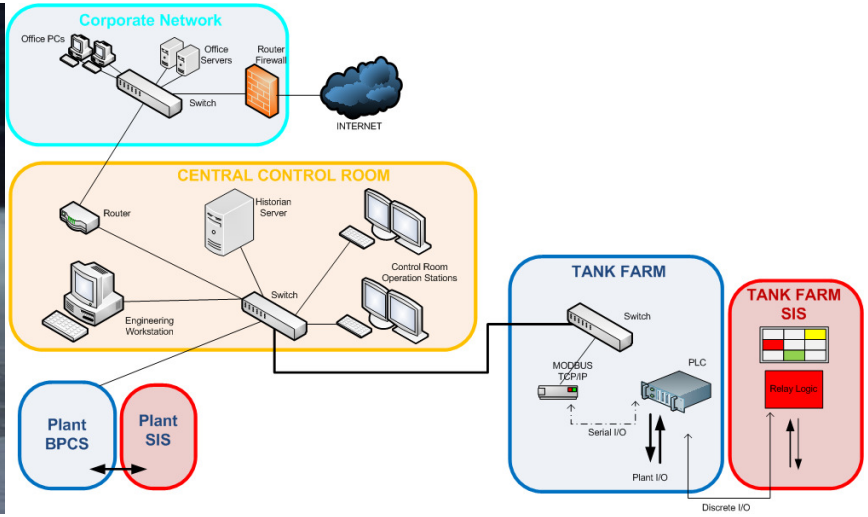
COMAH

The Competent Authority

Cyber Security MAH Example



Nic Butcher MIChemE CEng

HM Specialist EC&I Inspector

Health & Safety Executive

HSE Environment Agency SEPA ONR Office for Nuclear Regulation Cyfoeth Naturiol Cymru Natural Resources Wales

Introduction

COMAH

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.

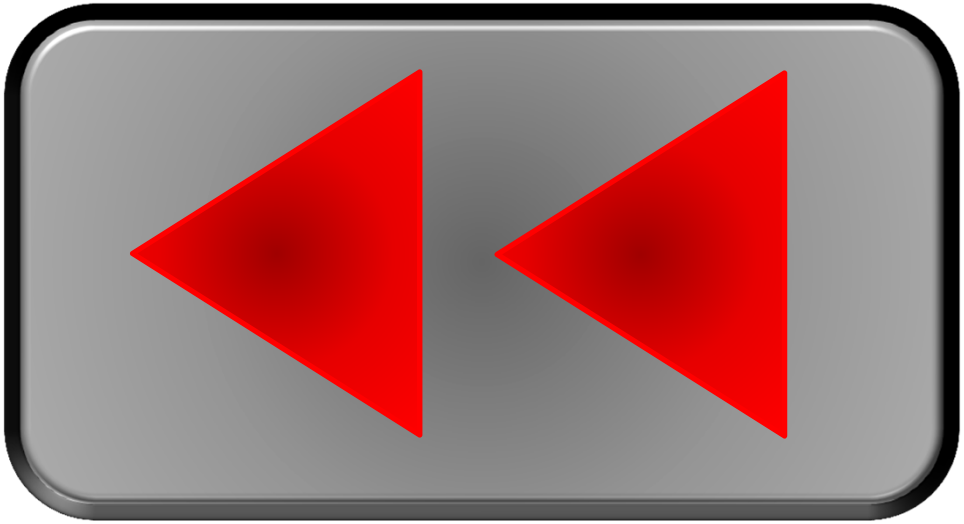
The cloud ignited shortly after causing a massive explosion.

Two people on a boat in the estuary were killed as well as a third person found on the footpath next to the site, along with their dog.

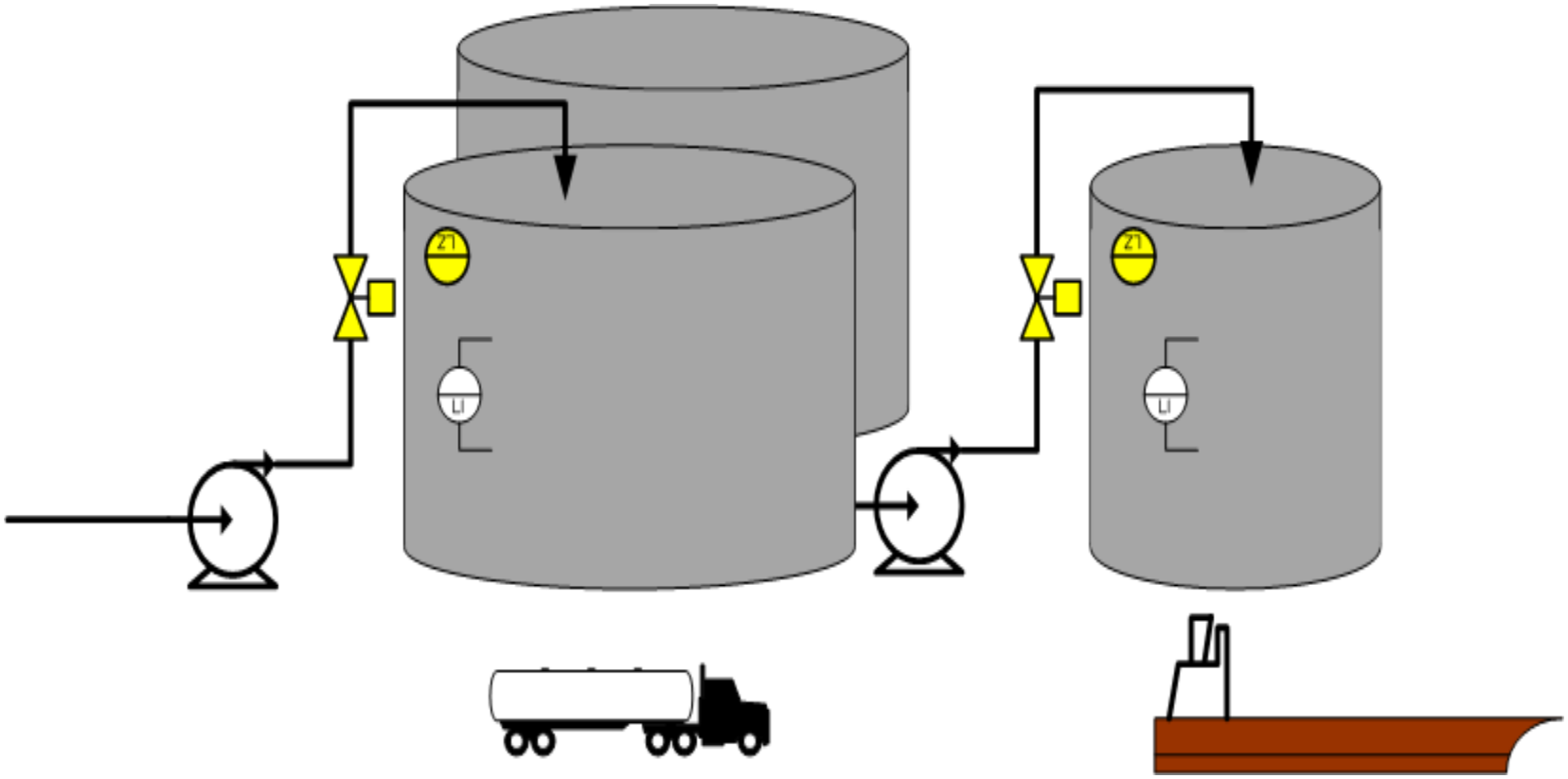
There was substantial blast damage to the residential area and some injuries.

HSE Environment Agency SEPA Cyfoeth Naturiol Cymru Natural Resources Wales ONR Office for Nuclear Regulation

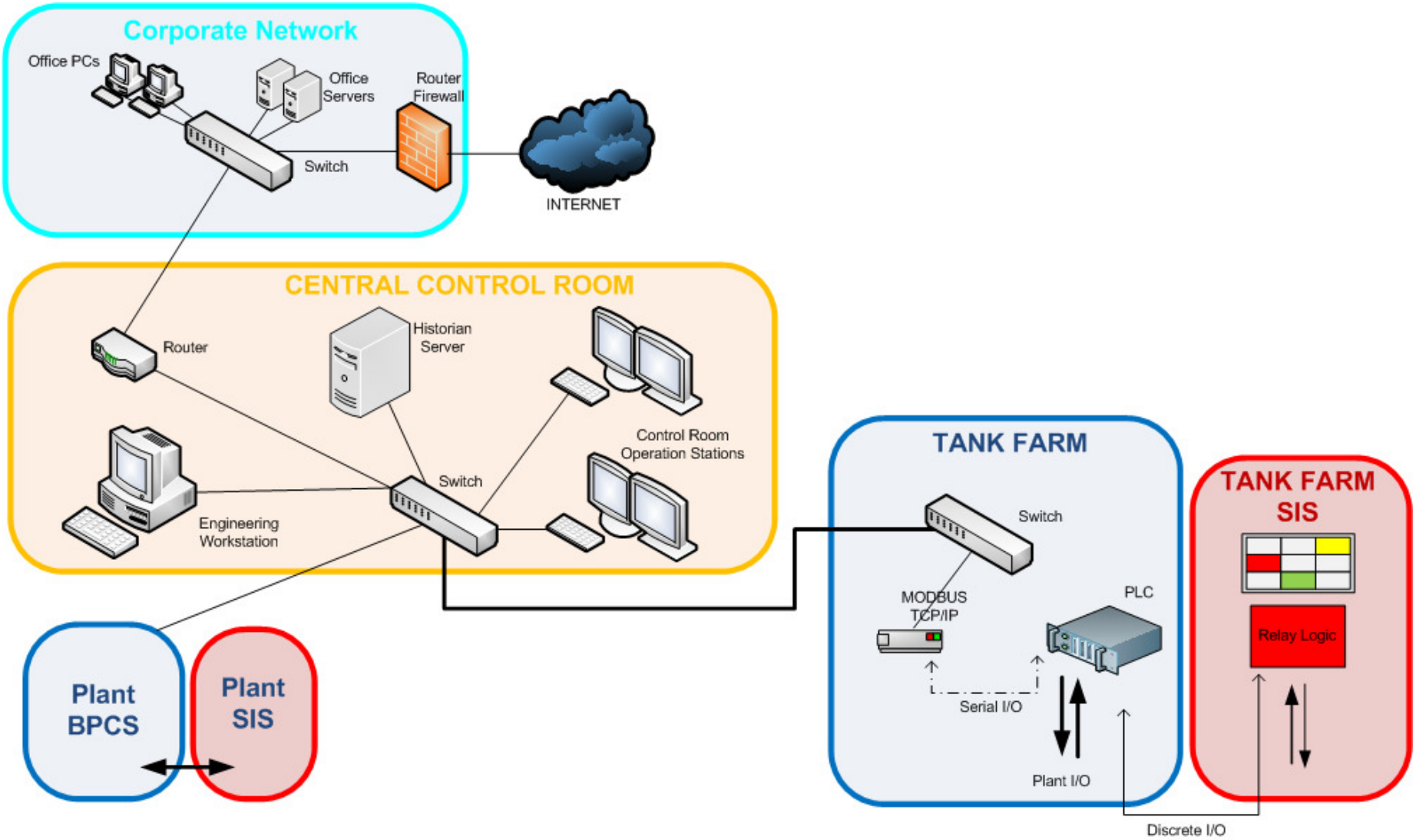
What happened?



Process Overview



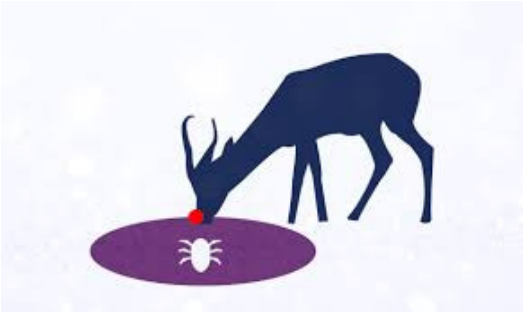
ICS Overview



1 Compromise the supply chain

COMAH

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



HSE Environment Agency SEPA Cyfoeth Naturiol Cymru Natural Resources Wales ONR Office for Nuclear Regulation

2 Send an email from the supply chain containing malware

COMAH

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 COMAH operator's enterprise desktop.

HSE Environment Agency SEPA Cyfoeth Naturiol Cymru Natural Resources Wales ONR Office for Nuclear Regulation

3 Establish persistent access to the enterprise network

COMAH

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

HSE Environment Agency SEPA Cyfoeth Naturiol Cymru Natural Resources Wales ONR Office for Nuclear Regulation

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

COMAH

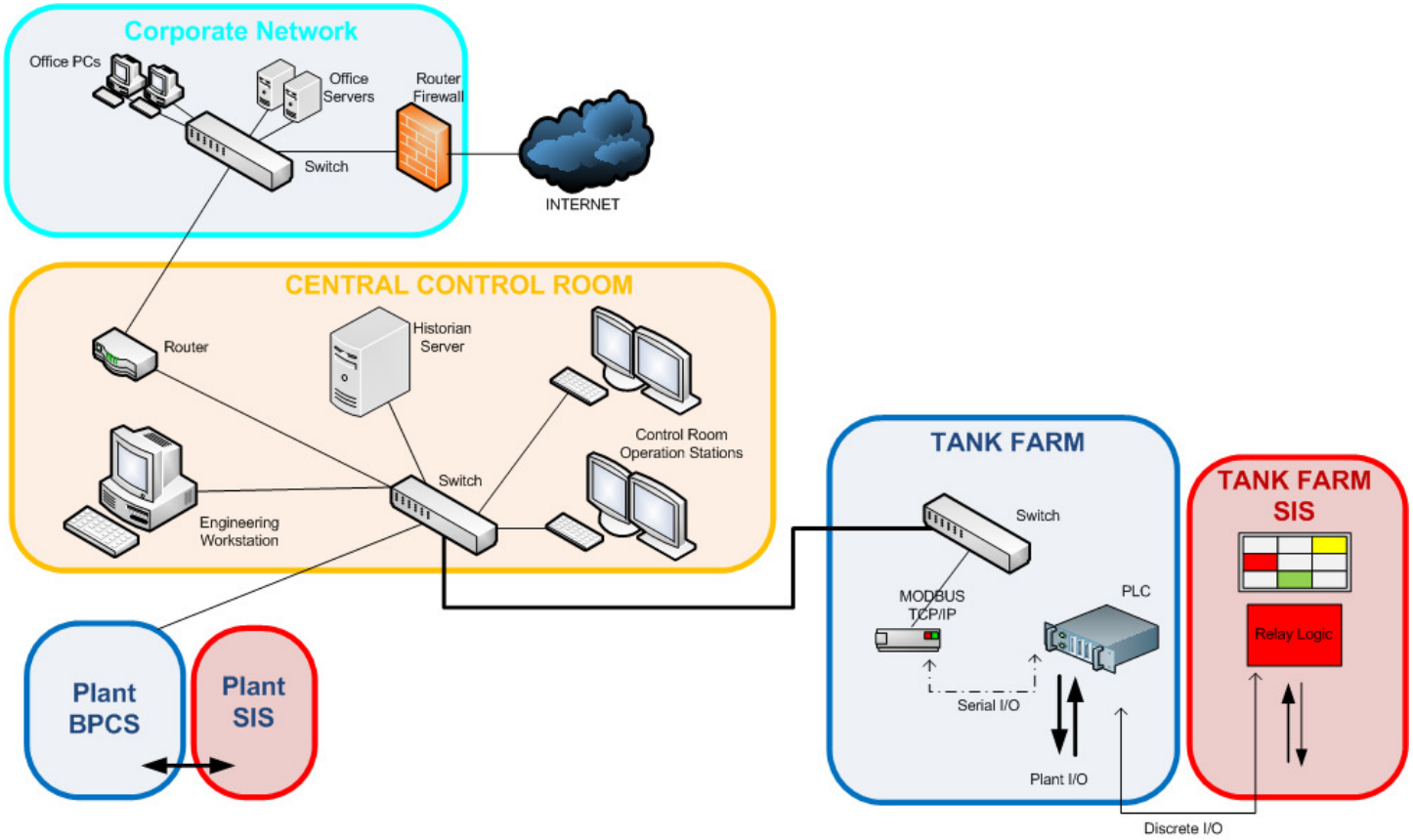
The attacker accumulates the technical information they need in order to attack the system.

HSE Environment Agency SEPA Cyfoeth Naturiol Cymru Natural Resources Wales ONR Office for Nuclear Regulation

5 Move laterally to the ICS

COMAH

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



HSE Environment Agency SEPA Cyfoeth Naturiol Cymru Natural Resources Wales ONR Office for Nuclear Regulation

6 Attack ICS

COMAH

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.

HSE Environment Agency SEPA Cyfoeth Naturiol Cymru Natural Resources Wales ONR Office for Nuclear Regulation

The actual story

COMAH

This is what really happened…

The company was actually called SecureChemCo.

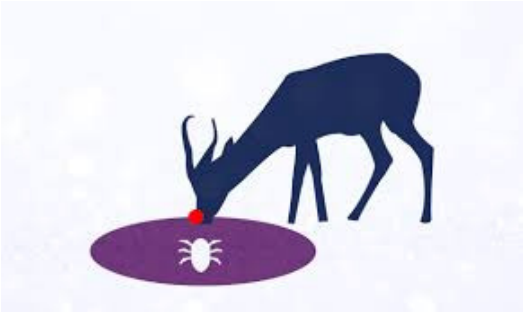
And they'd followed good practice with respect to cyber security

HSE Environment Agency SEPA Cyfoeth Naturiol Cymru Natural Resources Wales ONR Office for Nuclear Regulation

1 Compromise the supply chain

COMAH

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



A4 - Supply Chain Security: The operator has minimised the risk to information stored by the supplier by putting in place robust processes for handling information.

A4 - Supply Chain Security: The operator stipulates Cyber Essentials as a minimum requirement, which decreases the likelihood that the attack will be successful.

HSE Environment Agency SEPA Cyfoeth Naturiol Cymru Natural Resources Wales ONR Office for Nuclear Regulation

2 Send an email from the supply chain containing malware

COMAH

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 COMAH operator’s enterprise desktop.

B6 – Staff awareness and training: The operator has provide general awareness training which reduces the likelihood that the malware is activated

A4 Supply chain: The operator has recognised the corporate network as an internal third party and stipulates Cyber Essentials as a minimum requirement, which decreases the likelihood that the attack will be successful.

HSE Environment Agency SEPA Cyfoeth Naturiol Cymru Natural Resources Wales ONR Office for Nuclear Regulation

3 Establish persistent access to the enterprise network

COMAH

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

A4 Supply chain: The operator has recognised the corporate network as an internal third party and stipulates Cyber Essentials as a minimum requirement, which decreases the likelihood that the attack will be successful.

HSE Environment Agency SEPA Cyfoeth Naturiol Cymru Natural Resources Wales ONR Office for Nuclear Regulation

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

COMAH

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

B3 – Data Security: Key documents are encrypted at rest and when sent between systems.

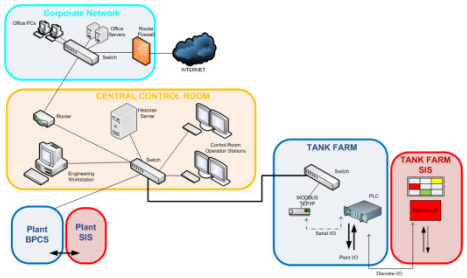
C1 : Security Monitoring : Access to key design documentation is logged and any anomalous activity investigated.

HSE Environment Agency SEPA Cyfoeth Naturiol Cymru Natural Resources Wales ONR Office for Nuclear Regulation

5 Move laterally to the ICS

COMAH

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



B4 – System Security: Well-maintained IT/ICS perimeter systems prevent the attacker from gaining access by exploiting vulnerabilities.

B4 – System Security: System architecture, patch management (patches are deployed at the top levels of the ICS) and devices are hardened to minimise vulnerabilities.

B2 - Identity and Access Control: Appropriate technical controls prevents credentials from the enterprise being reused for ICS making it harder for the attacker to move laterally.

C1 : Security Monitoring : Analysts review system logs and discover evidence of the attacker's actions in the network.

HSE Environment Agency SEPA Cyfoeth Naturiol Cymru Natural Resources Wales ONR Office for Nuclear Regulation

6 Attack ICS

COMAH

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.

B5 – Resilient networks and systems: The operator had recognised the Modbus TCP/IP as vulnerable and physically segregated from other networks

B5 – Resilient networks and systems: The operator had further segregated the SIS by requiring a hardwired enable for any overrides

D1 & D2 – Response & Recovery Planning/Lessons Learned: Impact from the incident is minimised as an effective response plan is put in place.

HSE Environment Agency SEPA Cyfoeth Naturiol Cymru Natural Resources Wales ONR Office for Nuclear Regulation

Points to make

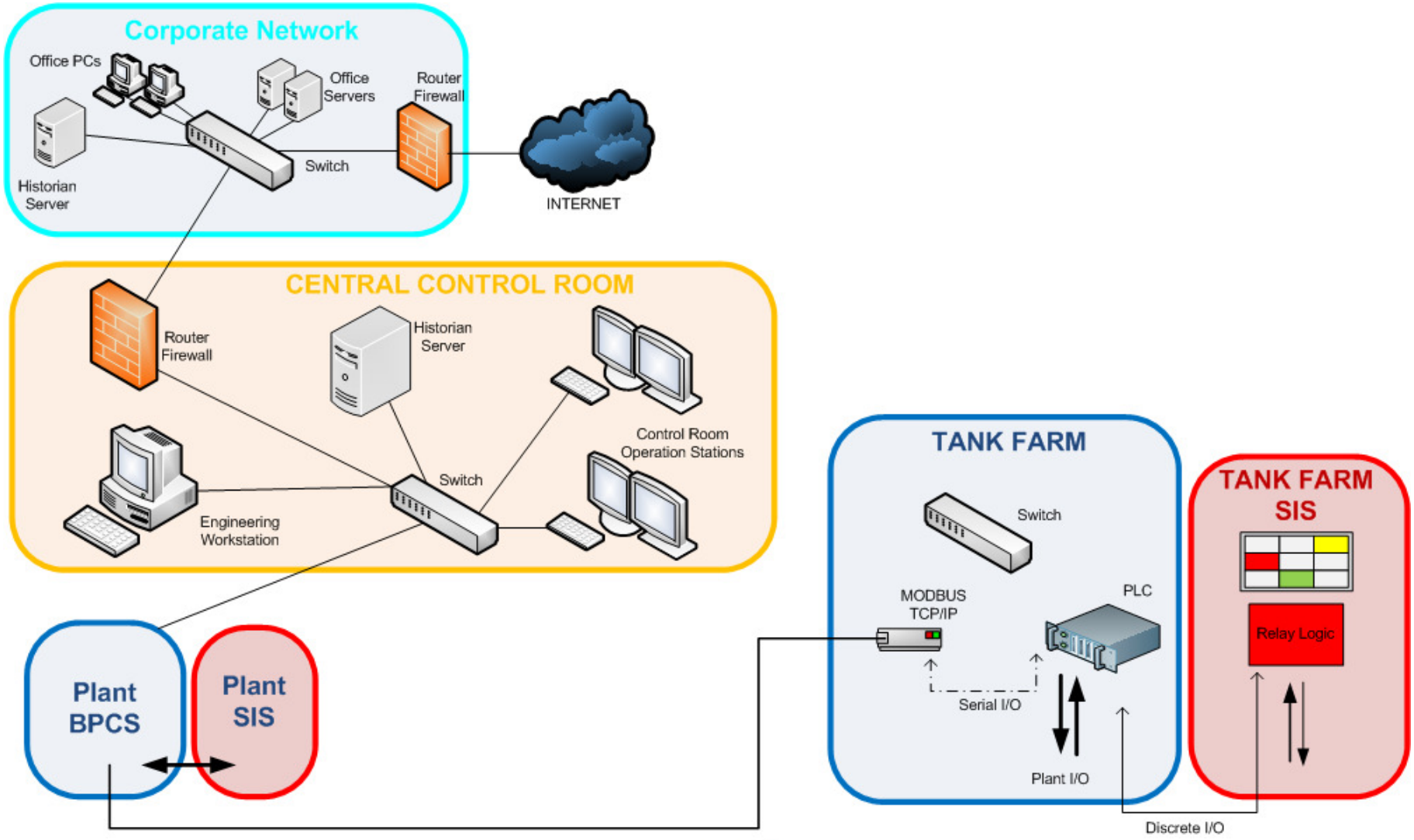
COMAH

- Based upon an example provided by the NCSC describing how ICS could be attacked.
- This sort of architecture is quite common – i.e. reusing network infrastructure to bring PLC control interface to a central control room.
- Path of least resistance – the attacker didn't have break into more complex control system communications or compromise an operator station – targeted Modbus because very well documented and tools exist to analyse and spoof.
- The various parts of the attack are mostly going on at the moment and would not require a very high level of sophistication.

HSE Environment Agency SEPA Cyfoeth Naturiol Cymru Natural Resources Wales ONR Office for Nuclear Regulation

Better ICS Architecture

COMAH



HSE Environment Agency SEPA Cyfoeth Naturiol Cymru Natural Resources Wales ONR Office for Nuclear Regulation