



## Cyber Security

### A Regulator's Perspective

19-11-19

Nic Butcher CEng MIChemE

HM Specialist Inspector – Electrical, Control and Cyber Security

© Crown Copyright, HSE 2019



## Topics

- Who we are and what we do
- Why is cyber security important
- Managing the risk – Approach, Guidance and Challenges
- HSE Progress Updated
- What this means for operators, suppliers and vendors
- Summary of key points
- Q&A

© Crown Copyright, HSE 2019

# HSE – Who we are



## Working with...

- ▶ Health and Safety Laboratory (HSL)
- ▶ Businesses
- ▶ Workers
- ▶ Safety representatives
- ▶ Local Authorities
- ▶ Chemicals Regulation Directorate
- ▶ Adventure Activities (AALA)
- ▶ Europe and worldwide

## HSE's work

- ▶ Regulating and enforcing health and safety
- ▶ Legislation
- ▶ Better regulation
- ▶ Science, engineering and research
- ▶ Statistics
- ▶ Field operations
- ▶ Hazardous installations
- ▶ Nuclear safety and security

### CEMHD



- ▶ Chemicals Industry
- ▶ Explosives
- ▶ Biosafety and microbiological containment

### Energy Division



- ▶ Offshore oil and gas
- ▶ Gas supply industry
- ▶ Pipelines
- ▶ Mining

## Key Topics

The E,C&I discipline covers four key priority topics and the assessment of Safety Reports.

- Functional Safety
- Explosive Atmospheres
- Electrical Power Systems
- Cyber security

[www.hse.gov.uk/eci](http://www.hse.gov.uk/eci)

© Crown Copyright, HSE 2019

# HSE – What we do – prevention



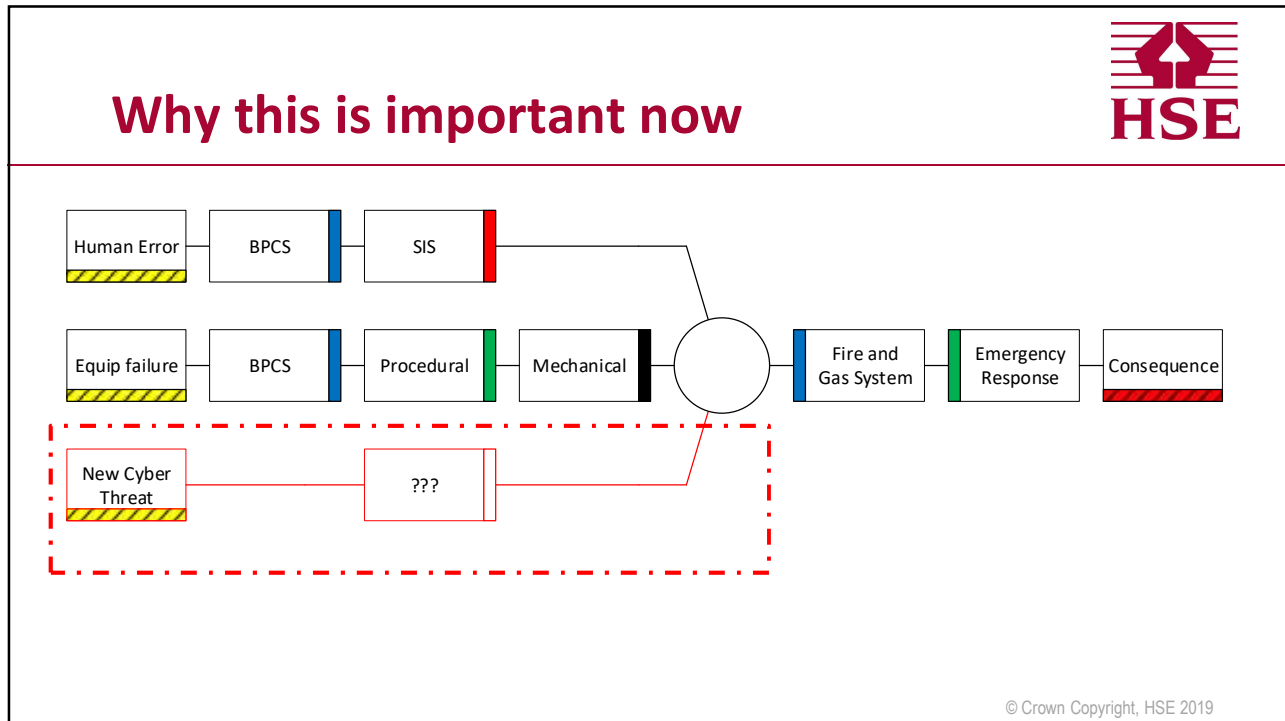
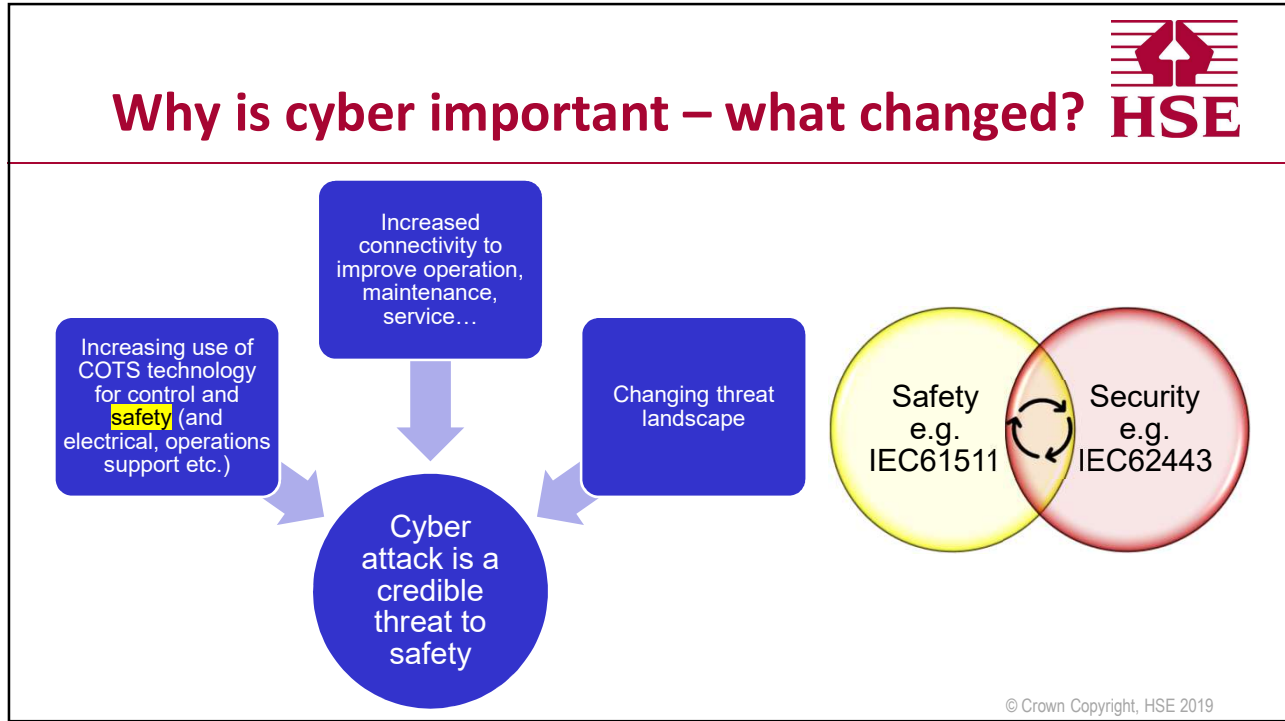
Search - The Guardian UK edition -

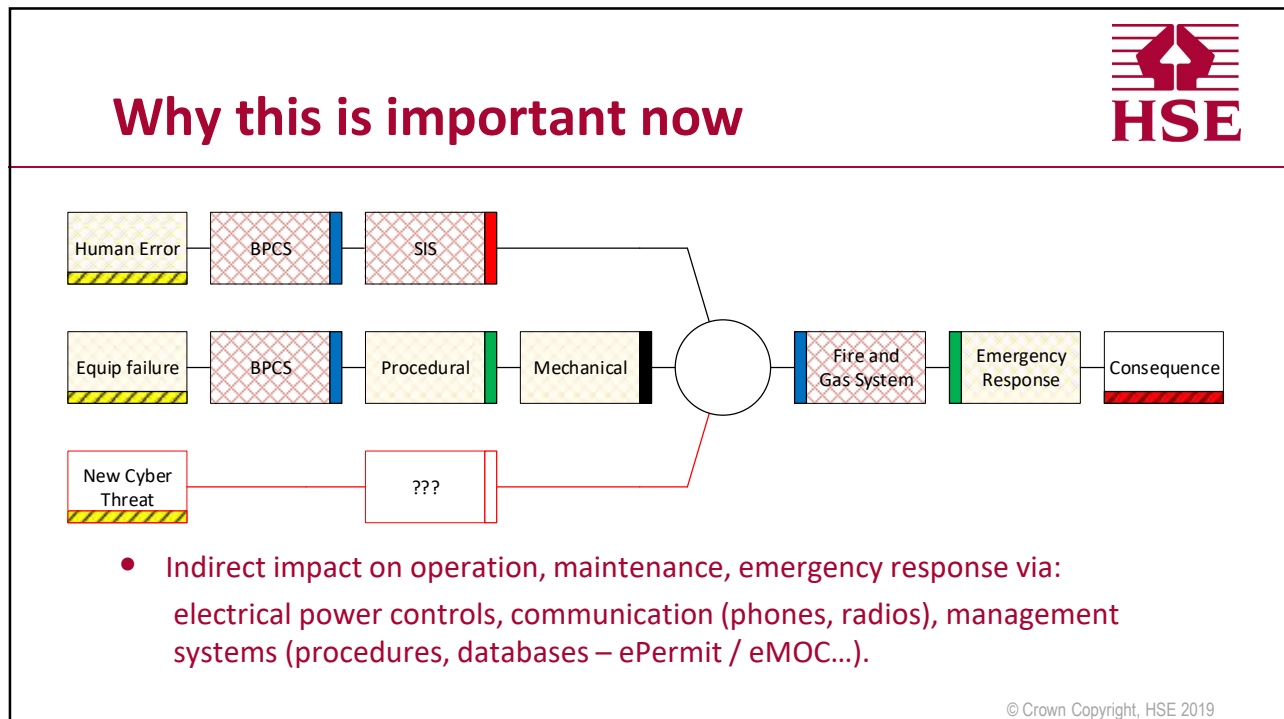
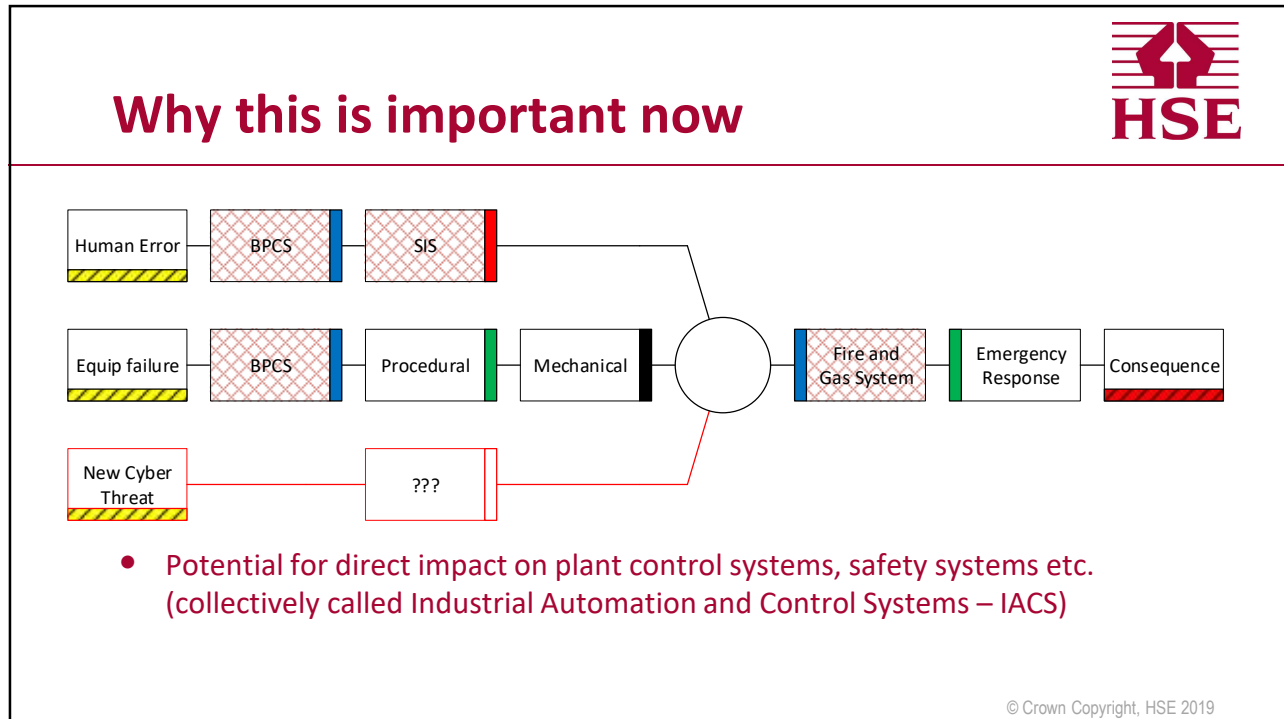
### The Guardian

Safety blunders expose lab staff to potentially lethal diseases in UK



This Photo by Unknown Author is licensed under CC BY-SA  
© Crown Copyright, HSE 2019





## Why this is important now



- Cyber threats are not just a new potential cause of an accident / loss of essential service
- They are also a common cause failure mode of existing protection and mitigation layers
- And potential impact to systems used operation, maintenance and emergency response
- Cyber security is therefore considered more like a infrastructure that we need to protect

© Crown Copyright, HSE 2019

## Why this is important – Looking forward



- There is no going back! The use of these technologies is key to effective operation and maintenance of our businesses.
- Building cyber security into our systems also enables future technology:
  - Mobile connectivity for field operation / maintenance
  - Further advanced control (machine learning / AI)
  - Further decentralisation / industrial internet of things
  - Connectivity – open systems / interoperability / cloud services
  - Big data and analytics
  - Digital twins
- And builds capability – Engineers understand the processes and therefore how/where above technologies add value

© Crown Copyright, HSE 2019



## What does the law say?

- Control of Major Accident Hazard Regulations (COMAH) – (there is a similar requirement in offshore Regs)

*“Every operator must take all measures necessary to prevent major accidents and to limit their consequences...”*

- Network and Information Systems Regulations (NIS)

*“An operator ... must take appropriate and proportionate technical and organisational measures to manage risks...”*

- I.e. Goal setting, not prescriptive
- Obligation is on the site operator to manage risks and apply suitable technical and organisational risk controls (apply relevant good practice).

© Crown Copyright, HSE 2019



## What is relevant good practice?

- IEC 62443 standard (in development or recently issued)
- NIST guidance (USA)
- Legacy CPNI guidance (out of date?)
- NCSC guidance and cyber assessment frameworks (new)



- Interpreted into HSE Operational guidance OG86
  - We needed a consistent benchmark for regulation
  - (freely available for industry to use if it wants to use it)

© Crown Copyright, HSE 2019

## Approach



- Not proportionate to regulate all systems
- Identify systems directly relevant to major hazard safety and/or providing an essential service:
  - Mostly these are the process and electrical control and safety systems and associated support systems (IACS) + cyber security countermeasures
- Regulate these systems proportionately to risk and require:
  - A basic level of cyber risk controls across the IACS
  - Special focus on critical systems (e.g. the SIS for safety)
  - In future may supplement additional controls where risks are higher
- Have a 'plan' to manage without other 'essential data / functions' outside the IACS (procedures, databases, eMOC, ePermit etc.)

© Crown Copyright, HSE 2019

## Approach



- First the good news:
  - The majority of cyber risk can be dealt with by relatively simple technical and organisational control measures.
  - Lots of the tools, techniques and processes that we use to manage safety can be applied to cyber security.
  - E.g. a systematic lifecycle approach, proportionality, management systems, human factors.
- However, in some cases, a different way of thinking is necessary... there are some challenges:

© Crown Copyright, HSE 2019

## Challenge – Risk Assessment



Safety Risk	Cyber Risk
Can systematically identify hazards and their causes	Link between cyber threats, vulnerabilities and hazards not clear.
Reasonable to assume no malicious intent and hazards and their causes can be considered individually	Malicious intent a key feature. Need to consider multiple contingencies / common cause failures.
Likelihood based upon predictable failure rates based upon experience	Likelihood not predictable
<u>Therefore:</u> Can systematically and with some confidence identify the required risk controls and manage these robustly – e.g. safety systems	<u>Therefore:</u> difficult to predict cyber risk and impact of countermeasures

© Crown Copyright, HSE 2019

## Challenge – Risk Assessment




- What does this mean...
  - Cannot use existing risk assessments to examine cyber risk
  - Cannot assume that cyber risk is addressed by existing risk control measures (i.e. just protect the SIS)
  - Need a different approach to cyber risk assessment

© Crown Copyright, HSE 2019




## Challenge – Historical System Design



Historically	{	<ul style="list-style-type: none"> <li>• Proprietary (security by obscurity?)</li> <li>• Not connected</li> <li>• No inbuilt security</li> </ul>
Currently	{	<ul style="list-style-type: none"> <li>• Move to COTS – open and unlimited by design</li> <li>• Increased connectivity</li> <li>• Security ‘bolted on’ – i.e. between the assets</li> <li>• Security at system level, not possible to target</li> </ul>
Future ?	{	<ul style="list-style-type: none"> <li>• Secure by design – i.e. within the assets</li> <li>• Security focused on the critical function</li> <li>• More open connectivity, e.g. for cloud</li> </ul>

© Crown Copyright, HSE 2019

## Challenge – IT v IACS requirements



- The design and management of control and safety systems are well understood by Engineers (don’t break a working system).
- The more recent use of COTS and networking requires and the associated (‘bolt on’) security requires IT support and skills.
- But typical IT approach to cyber security (periodic technology refresh, patching, etc.) don’t work in the IACS world (long life, real-time operations)
- Result: ‘Security Limbo’ – IACS Engineers didn’t have the skills, inclination; IT Engineers didn’t have a suitable approach.
- Requires a new approach and IT + IACS collaboration

© Crown Copyright, HSE 2019

## Addressing challenges within guidance



- Recognise that some of this may need to be modified in future but this is sufficient to progress.
  - Risk Assessment – simplified system level (zone) approach proposed for now – sufficient to determine basic levels of cyber countermeasures.
  - System Design – System level (zone) countermeasures – appropriate approach for basic cyber countermeasures
  - IT v IACS – required clear definition of IACS scope and responsibility but with ability to use IT support with a new approach, e.g. for patching.

© Crown Copyright, HSE 2019

## Progress



Mar 17 OG86  
Edition 1  
Released

Nov 17 – May 18  
Trial Inspections

Nov 18 OG86  
Edition 2  
Released

Jan 19 Cyber  
Inspection at  
COMAH sites

Apr 20  
Combined  
NIS+COMAH  
Cyber Inspection

- followed significant stakeholder engagement
  - aimed at onshore and offshore major hazards only
- Findings indicated:
- Some progress with management systems and protection measures
  - But less progress with detect and respond measures
  - Insufficient detail within the guidance
- Addressed feedback from the trials
  - Reformatted and terminology to be consistent with the NCSC guidance subsequently released
  - New HSE NIS role – guidance also had to cover essential services, not just major hazards
- Operators were already aware via their normal intervention plan
  - Included implementing a secure method of file transfer HSE ↔ operator
- Requires completion of a regulatory framework – currently in progress.

© Crown Copyright, HSE 2019

## What does this mean for operators



- Inspection at major hazard sites:
  - Inspection planned via intervention plan
  - Inspections managed in the usual way
  - HSE will use OG as benchmark to assess compliance
- Inspection as NIS essential service sites:
  - Regulatory framework (planning, enforcement, reporting etc.) for NIS being developed
  - After which combined NIS-major hazard inspections will begin (almost all NIS sites are also major hazard sites).

© Crown Copyright, HSE 2019

## What can operators do now



- Senior management engagement:
  - Guidance for senior managers being developed by CDOIF
  - Recognise the cyber risk to safety (and essential service for NIS sites)
  - Define governance: policy, resources and oversight
  - Recognise this is not a 'project' but ongoing risk management
- Complete a gap assessment against good practice
  - could use OG86 or NCSC CAF, or whatever.
  - Assess risk, understand gaps –
  - Define improvement plan to develop and implement technical and organisational risk countermeasures

© Crown Copyright, HSE 2019

## What does this mean for vendors / suppliers



- Most of the legal requirements fall on the operators but...
  - Operators will be required to seek assurance that their suppliers are managing cyber security risk
  - Operators need supplier's help to meet the requirements
- HSE thinks that future engagement with suppliers and vendors will be helpful for all parties
- In particular:
  - What does good look like for installed systems?
  - How do we integrate systems together securely?
  - What will good look like for new systems, i.e. security by design?

© Crown Copyright, HSE 2019

## Summary



- Cyber attack is a credible risk to safety and essential services now.
- Managing cyber security is necessary to address these risks but also enables future exploitation of new technologies – i.e. builds the cyber capability and infrastructure
- Managing cyber security risk requires a similar approach to other risks but there are some challenges specific to the topic and changes in approach required.
- HSE has developed guidance and started to roll out inspection of this topic on major hazard sites and essential service sites.
- Sites can also use the guidance to begin to address these risks.

© Crown Copyright, HSE 2019

**Q&A**



**[Nic.Butcher@hse.gov.uk](mailto:Nic.Butcher@hse.gov.uk)**

© Crown Copyright, HSE 2019