Building Cybersecurity into your Safety Case

Nigel Stanley

Chief Technology Officer

Operational Technology and Industrial Cybersecurity

TÜV Rheinland

Safety Case Symposium 2018 Singapore

Agenda

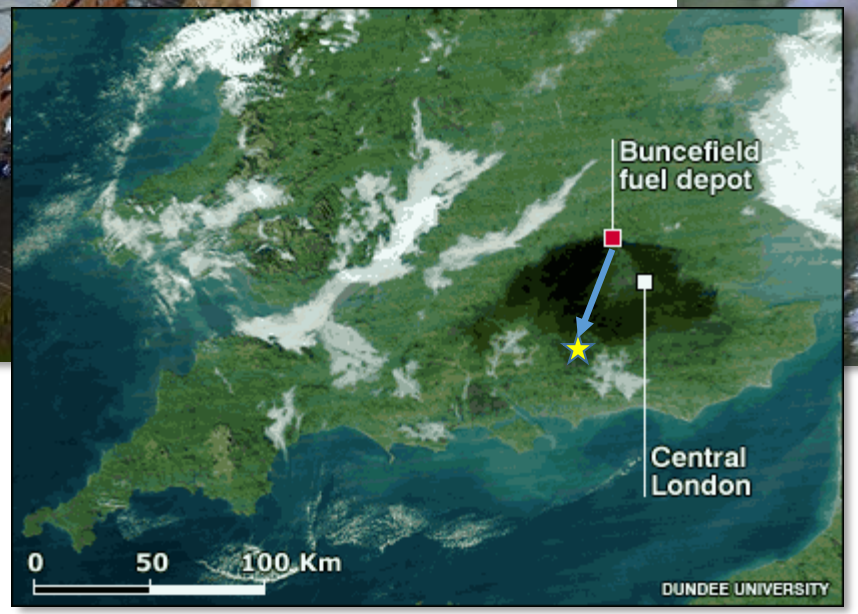
- A short story
- Safety and security are now inextricably linked
- Safety case walkthrough with some selected touch points
- Next steps

Agenda

- A short story
- Safety and security are now inextricably linked
- Safety case walkthrough with some selected touch points
- Next steps

Buncefield, UK

06:01 hrs Sunday 11th December 2005



- Fuel-air explosion in a vapour cloud of evaporated leaking fuel
- The “biggest incident of its kind in peacetime Europe”
- 0 fatalities!

- Site risk assement – tank farm risk LOW
- IT systems in the “bomb proof“ basement
- 600 people normally on site

Next time will the “stuck gauge“ be a cybersecurity event?

Source: http://cryptome.org/eyeball/hemel/hemel-eyeball.htm
BBC News

Agenda

- A short story
- Safety and security are now inextricably linked
- Safety case walkthrough with some selected touch points
- Next steps

Functional Safety and Cybersecurity

Cybersecurity

Defence against negligent and wilful actions to protect devices and facilities

Functional Safety

Defence against random and systematic technical failure to protect life and environment

Relation between Functional Safety & Cybersecurity

Generic Standard for Functional Safety: IEC 61508:2010.

7.4.2.3

If the hazard analysis identifies that malevolent or unauthorised action, constituting a security threat, as being reasonably foreseeable, **then a security threats analysis** should be carried out.

NOTE 3 For guidance on security risks analysis, **see IEC 62443** series.

7.5.2.2

If security threats have been identified, then a vulnerability analysis should be undertaken in order to specify **security requirements**.

NOTE Guidance is given in **IEC 62443** series.

Singapore Cybersecurity Bill

Passed into law on February 5th 2018

- Singapore's Cybersecurity Bill aims to strengthen the protection of Critical Information Infrastructure (CII)
- CII are identified as computers and computer systems that are necessary for the continuous delivery of essential services, the loss or compromise of which would have a debilitating effect on the availability of the essential services in Singapore
- CII owners are ultimately responsible for the cybersecurity of their respective CII
- CII owners should carry out the necessary risk assessments and due diligence while deciding on vendors to engage and conditions to impose on them

Source: https://www.opengovasia.com/articles/singapores-cybersecurity-bill-passed-into-law-minister-addresses-concerns

Triton – a Seminal Moment

Reported December 2017

- The attacker gained remote access to a safety instrumented system (SIS) engineering workstation and deployed the TRITON attack framework to reprogram Triconex SIS controllers
- SIS controllers entered a failed safe state ☺
- Target – CNI but otherwise not publicly revealed (likely ME)
- Attribution – not publicly revealed (likely nation state)

Source: https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html

Agenda

- A short story
- Safety and security are now inextricably linked
- Safety case walkthrough with some selected touch points
- Next steps

Example walk through

- Methodology
  - Reviewed safety case assessment guide http://www.mom.gov.sg/workplace-safety-and-health/major-hazard-installations/preparing-for-safety-case
  - Applied a cybersecurity “lens” to selected elements of the guide
  - “What should be considered from a cybersecurity point of view?”

Think cybersecurity as you build the safety case

Safety Case Assessment Guide

Chapter 3: Major Accident Prevention Policy (MAPP) and Safety & Health Management System (SHMS) Aspects of Safety Case Assessment (part 1)

Safety Case Requirement
3.3 *Senior Level Endorsement* The MAPP shall be set at a **senior level** in the MHI's organisation and be **established in writing**.
3.4 *Roles and Responsibilities* The safety case shall show that all necessary **roles and responsibilities** in the management of MAHs have been clearly **allocated and defined**.
3.8 *External Organisations* The safety case shall show that the MHI has in place arrangements for cooperating with, **communicating information to and securing the cooperation of, external organisations.**

Safety Case Assessment Guide

Chapter 3: Major Accident Prevention Policy (MAPP) and Safety & Health Management System (SHMS) Aspects of Safety Case Assessment (part 1)

- Cybersecurity commentary
  - Do you have a cybersecurity governance statement? Is it signed by the CEO?
  - What related policies and procedures do you have in place? This is your internal "cybersecurity law"
    - Can you legally pursue an errant employee for cybersecurity "offences"?
  - Have you clearly defined cybersecurity roles and responsibilities?
    - How does IT security interface with OT security?
  - Are you actively tracking cybersecurity regulations? (and don't forget data privacy)
  - How is your supply chain involved in your cybersecurity strategy? Is your connected equipment accessible from outside the plant by suppliers/manufacturers?
  - Are you part of a cybersecurity threat and intelligence sharing community?

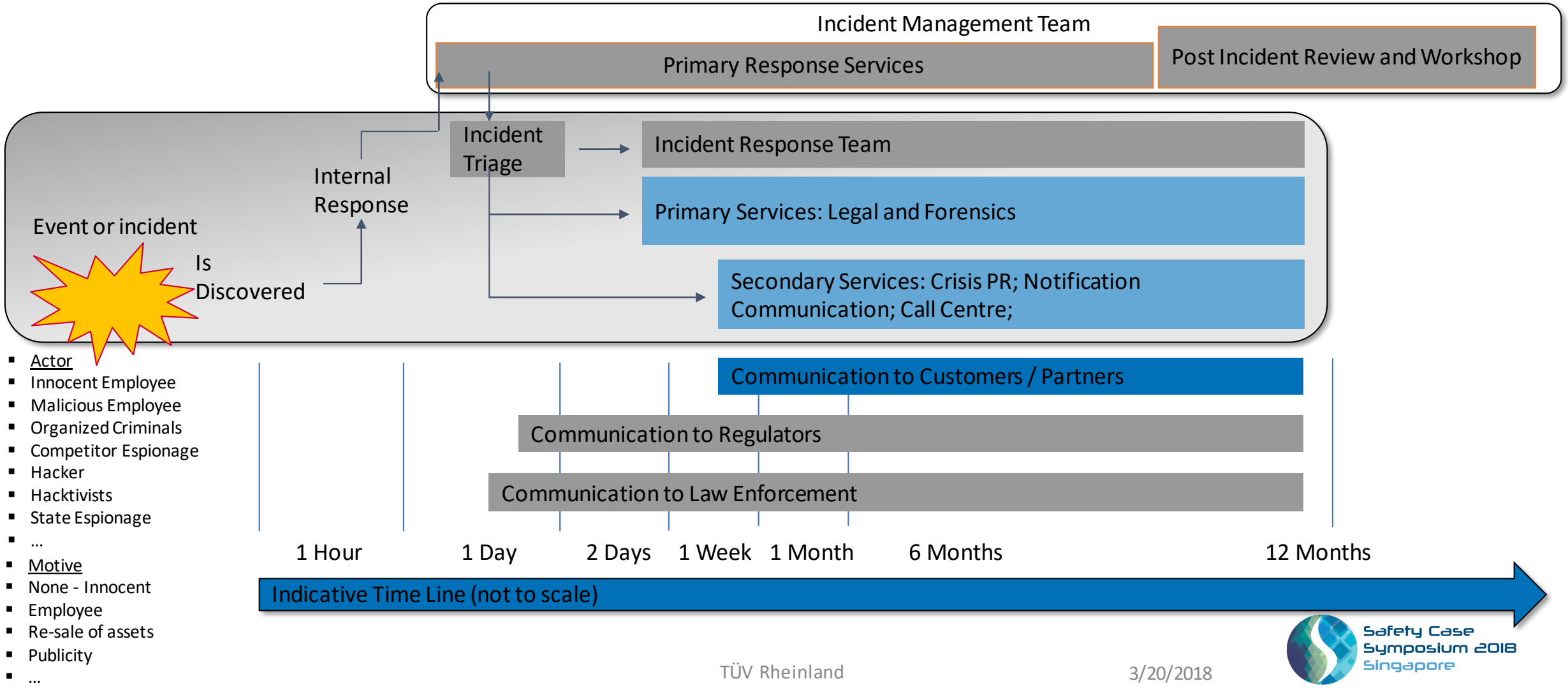
Safety Case Assessment Guide

Chapter 3: Major Accident Prevention Policy (MAPP) and Safety & Health Management System (SHMS) Aspects of Safety Case Assessment (part 2)

Safety Case Requirement
3.10 *Internal Communication* The safety case shall show that the MHI has arrangements for **communicating information important for the control** of MASs within the MHI's organisation.
3.15 Reactive Monitoring The safety case shall show that the MHI has adopted a **system for reporting incidents and near misses**, relating to failure of the protective measures for control of MASs.
3.16 Investigation and Corrective Action The safety case shall show that the MHI has adopted **mechanisms for investigating and taking corrective action**: a) in cases of the proactive performance standards showing a deterioration in risk control measures; and b) in relation to any incident or event

Safety Case Assessment Guide

Chapter 3: Major Accident Prevention Policy (MAPP) and Safety & Health Management System (SHMS) Aspects of Safety Case Assessment (part 2)



- Actor
- Innocent Employee
- Malicious Employee
- Organized Criminals
- Competitor Espionage
- Hacker
- Hacktivists
- State Espionage
- …
- Motive
- None - Innocent
- Employee
- Re-sale of assets
- Publicity
- …

Safety Case Assessment Guide

Chapter 4: Predictive Aspects of Safety Case Assessment (part 1)

Safety Case Requirement
4.1 The safety case shall **describe the sections of the installation** that could give rise to major accidents.
4.2 The safety case shall **identify and describe in detail** all potential MASs.
4.2.1 The safety case shall demonstrate that a **systematic process has been used to identify events and events combinations** which could cause MAHs to be realised.

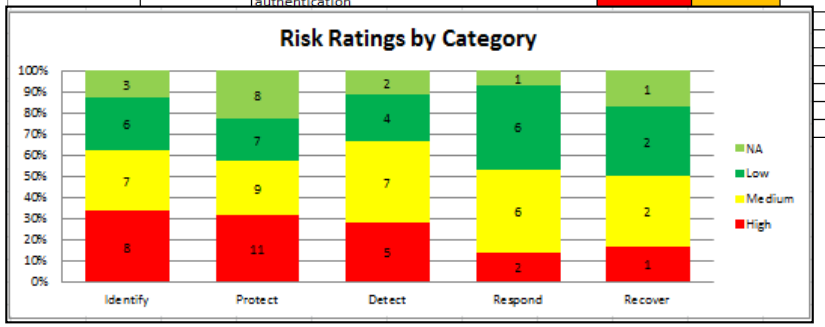
Safety Case Assessment Guide

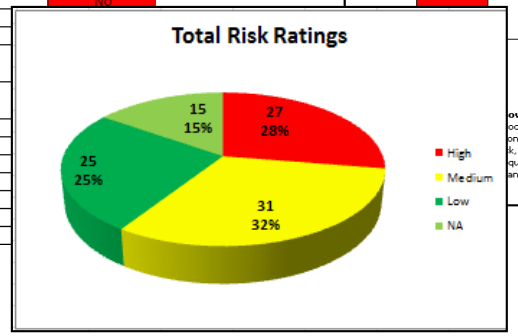
Chapter 4: Predictive Aspects of Safety Case Assessment (part 1)

- Cybersecurity commentary
  - Have you assessed your OT and IT cybersecurity risks?
  - How mature are your controls?
  - What framework did you apply to this assessment?
  - When will you re-evaluate?

- IEC 62443
- NIST Cybersecurity Framework

Foundational Requirement	Individual Control System Requirements	Details	Risk Rating	Remediation Required	Target SL (SL-T)	Achieved SL (SL - A)	Capability SL (SL - C)	Target SL Met?
FR 1 – Identification and authentication control (IAC)	SR 1.1	Human user identification and authentication	High	High	SL 2	SL 1	SL 0	No
	SR 1.1 RE 1	Unique identification and authentication	Medium	High	SL 2	SL 1	SL 1	No
	SR 1.2	Software process and device identification and authentication	High	Medium	SL 2	SL 3	SL 1	Yes
	SR 1.3	Account management	High	Low	SL 2	SL 1	SL 1	No
	SR 1.4	Identifier management	High	Medium	SL 2	SL 1	SL 1	No
	SR 1.5	Authenticator management	High	Medium	SL 2	SL 2	SL 1	
	SR 1.6	Wireless access management	High	Medium	SL 2	SL 3	SL 1	
	SR 1.6 RE 1	Unique identification and authentication	High	Medium	SL 2	SL 1	SL 1	
	SR 1.7	Strength of password-based authentication	High	Medium	SL 2	SL 1	SL 2	
						SL 1	SL 2	
						SL 1	SL 2	
						SL 1	SL 2	
						SL 1	SL 2	
						SL 1	SL 3	
						SL 1	SL 1	
						SL 1	SL 2	





Function	Maturity Rating	Category	Maturity Rating	Subcategory	Risk Rating	Effort Rating
		Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	3	ID.BE-1: The organization's role in the supply chain is identified and communicated	Low	Medium
				ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	NA	Low
				ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	High	High
				ID.BE-4: Dependencies and critical functions for delivery of critical services are established	Medium	Medium
				ID.BE-5: Resilience requirements to support delivery of critical services are established	Low	Low
		overnance (ID.GV): The policies, ocedures, and processes to manage and onitor the organization's regulatory, legal, k, environmental, and operational quirements are understood and inform the anagement of cybersecurity risk.	2	ID.GV-1: Organizational information security policy is established	High	High
				ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	High	Medium
				ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	Medium	Low

Safety Case Assessment Guide

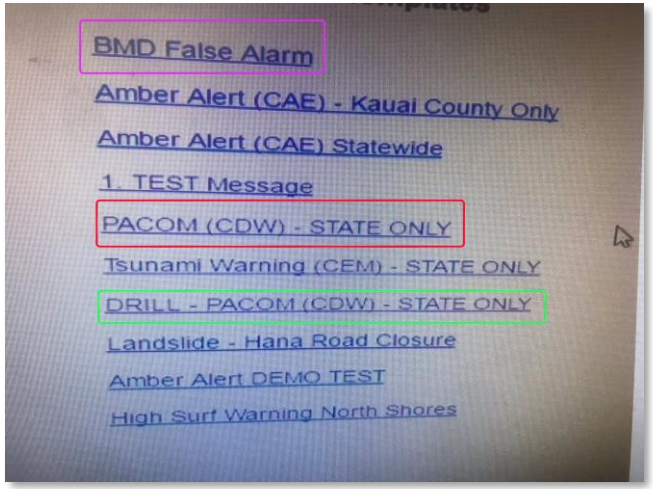
Chapter 4: Predictive Aspects of Safety Case Assessment (part 2)

Safety Case Requirement
4.5 It should be clear that **human factors have been taken into account** in the risk assessment.
4.7.2 Estimates of, or assumptions made about, the reliability of protective systems and the **times for operators to respond** and isolate LOC accidents or others need to be **realistic and adequately justified**.

Safety Case Assessment Guide

Chapter 4: Predictive Aspects of Safety Case Assessment (part 2)

- Cybersecurity commentary
  - How experienced are your teams in managing cybersecurity related incidents?
  - Could they determine if a spurious reading in a control room was a physical or a cybersecurity incident? How would they respond?
  - But more interesting, what about events or incidents caused by users?
    - Incompetent and non-malicious vs competent and malicious
  - How are these risk assessed and mitigated?



Agenda

- A short story
- Safety and security are now inextricably linked
- Safety case walkthrough with some selected touch points
- Next steps

Next steps

- Safety cases need to consider cybersecurity risks
- Cybersecurity issues will only increase
- Legislation and regulations will force your hand – monitor developments with the SG Cybersecurity Bill
- Why wait? It is the right thing to do

And you can no longer be safe if you are not secure

Nigel Stanley

Chief Technology Officer

Operational Technology and Industrial Cybersecurity

TÜV Rheinland

Email: nigel.stanley@us.tuv.com

Safety Case Symposium 2018 Singapore

www.SafetyCaseSymposium.com