SECEs: It’s time for a rethink

Martin Worth

People who care about their assets choose PIM

A Brief History of Me
A career in context

5th July 1988
Graduated

6th July 1988
Piper Alpha disaster

October 1988
Graduate Control & Instrument Engineer & Safety Engineer

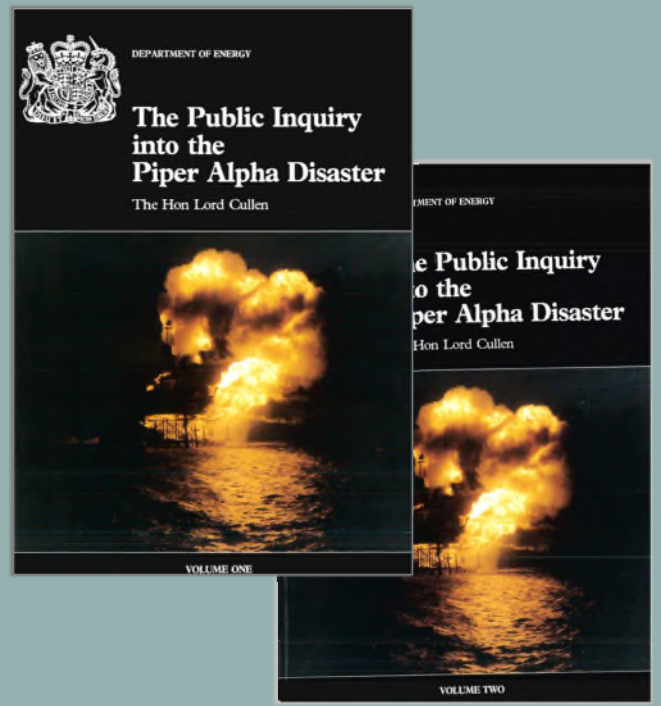
1994 - 2000
Technical Safety / Fire / Exp / Safety Cases

2000 - 2010
Technical Safety Lead
Talisman Energy

June 2011
One of founding PIM Directors

The Origin of the Safety Case
Another brief history

- Seven days after the incident, a public inquiry was directed to be held.
- The two volume “Public Inquiry into the Piper Alpha Disaster” was completed and released in October 1990.
- It made 106 recommendations for changes to North Sea safety procedures:
- These recommendations were all accepted and led to the adoption of the Offshore Installations (Safety Case) Regulations 1992.



The Forthwith Studies
(in advance of and in preparation for the Safety Case)

Areas identified as requiring priority attention

Typically produced by large teams within the operators, ultimately evolving and expanding into

THE SAFETY CASE

Emergency Systems Review (ESR)

Smoke & Gas Ingress (SGI)

Fire Risk Analysis (FRA)

Evacuation, Escape & Rescue (EER)

Cullen Inquiry Expectations

The Cullen Inquiry made it clear what was the expectation, purpose and benefit of a Safety Case regime: -

Paragraph 17.35
... a matter of ensuring that every company **produces an FSA** [Formal Safety Assesment] to **assure itself** that its operations are safe ...
... secondarily ... A matter of **demonstrating** this **to the regulatory body**.

Paragraph 17.36
... show ... that the company has a **suitable safety management system** ...

Paragraph 17.37
... a demonstration that the **hazards ... have been identified and assessed** ... are under control ... exposure of personnel has been minimised.
... should ... feature a **demonstration that the threat from these hazards to the arrangements for refuge for, and evacuation and rescue of , personnel ..., is under control**.

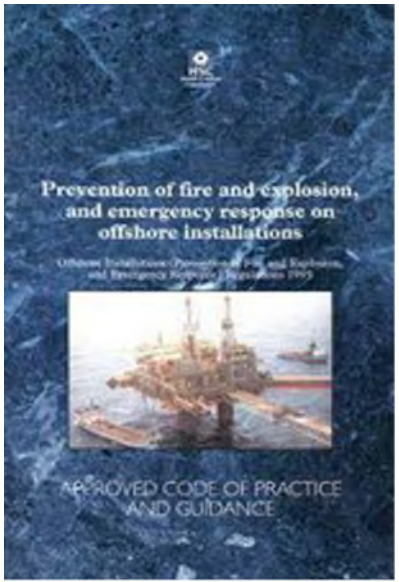
Paragraph 17.38
... installation ... possesses a **temporary safe refuge (TSR [TR])** ... and escape routes.
... it is proposed that **QRA [Quantified Risk Assessment]** be required [to demonstrate the adequacy thereof].

The Regulations

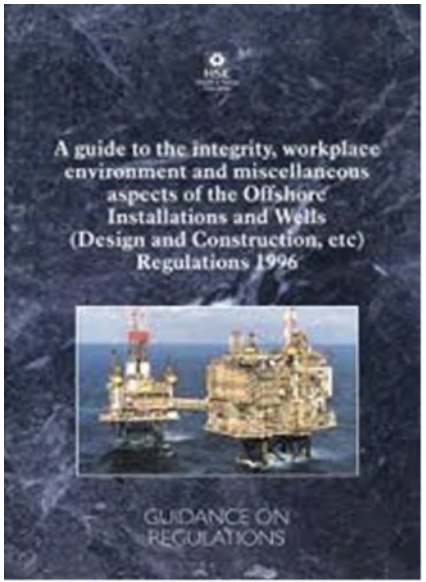
Safety Case Regulations

+

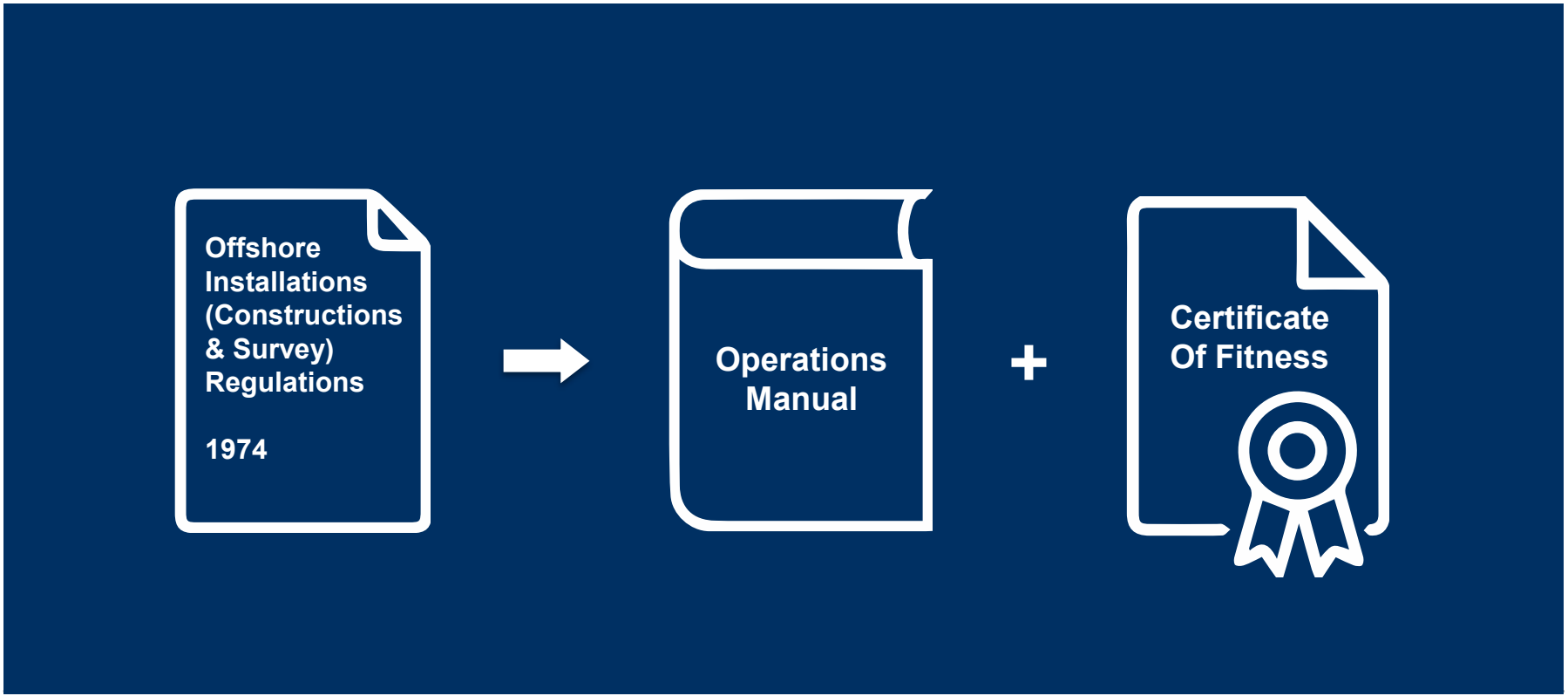
PFEER Regulations



DCR Regulations



Footnote – What came before the Safety Case?



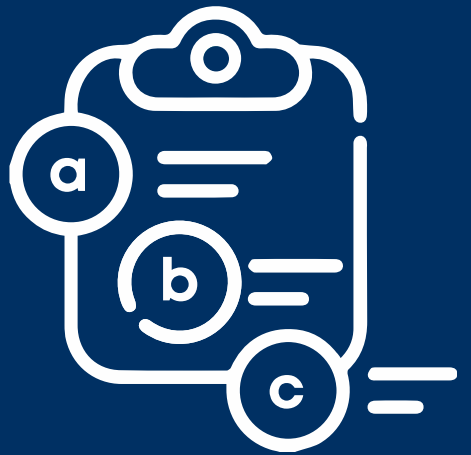
Not just a Safety Case, but a Case for Safety Goal Setting and Self Assessment

A key requirement in [the Safety Case Regulations] regulation 16 is for duty holders to demonstrate in their safety cases that:

(a) all **hazards** with the potential to cause a **major accident** as defined have been identified;

(b) the **risks** have been evaluated; and

(c) **measures** have been, or will be, taken to control those risks so as to ensure compliance with the relevant statutory provisions.



Footnote: Goal Setting?
What did we have before?

Prescriptive Regulations

Offshore Installations: Guidance on design, construction and certification

Fourth edition – 1990

HSE BOOKS

611 pages

2.3.1 REQUIREMENT TO CERTIFY OFFSHORE INSTALLATIONS

Regulation 3(1) requires that there be in force a valid Certificate of Fitness in Respect of an Offshore Installation before it can be:

…

In practice the function of certification is performed by six bodies appointed by the Secretary of State. These are:

- American Bureau of Shipping
- Bureau Veritas
- Germanischer Lloyd
- Lloyd's Register of Shipping
- Offshore Certification Bureau

Footnote: Certificate of Fitness

Contents

Formal Safety Assessment Process
Goal Setting

1. Identify Major Accident Hazards (MAH)
2. Identify Measures and Barriers
3. Specify Measures (SECEs & Performance Standard Criteria)
4. Apply the Performance Standard process (Maintain / Assure / Verify)

SCR2015 Reg. 2

"major accident" means—

(a) an event involving a fire, explosion, loss of well control or the release of a dangerous substance causing, or with a significant potential to cause, death or serious personal injury to persons on the installation or engaged in an activity on or in connection with it;

(b) an event involving major damage to the structure of the installation or plant affixed to it or any loss in the stability of the installation causing, or with a significant potential to cause, death or serious personal injury to persons on the installation or engaged in an activity on or in connection with it;

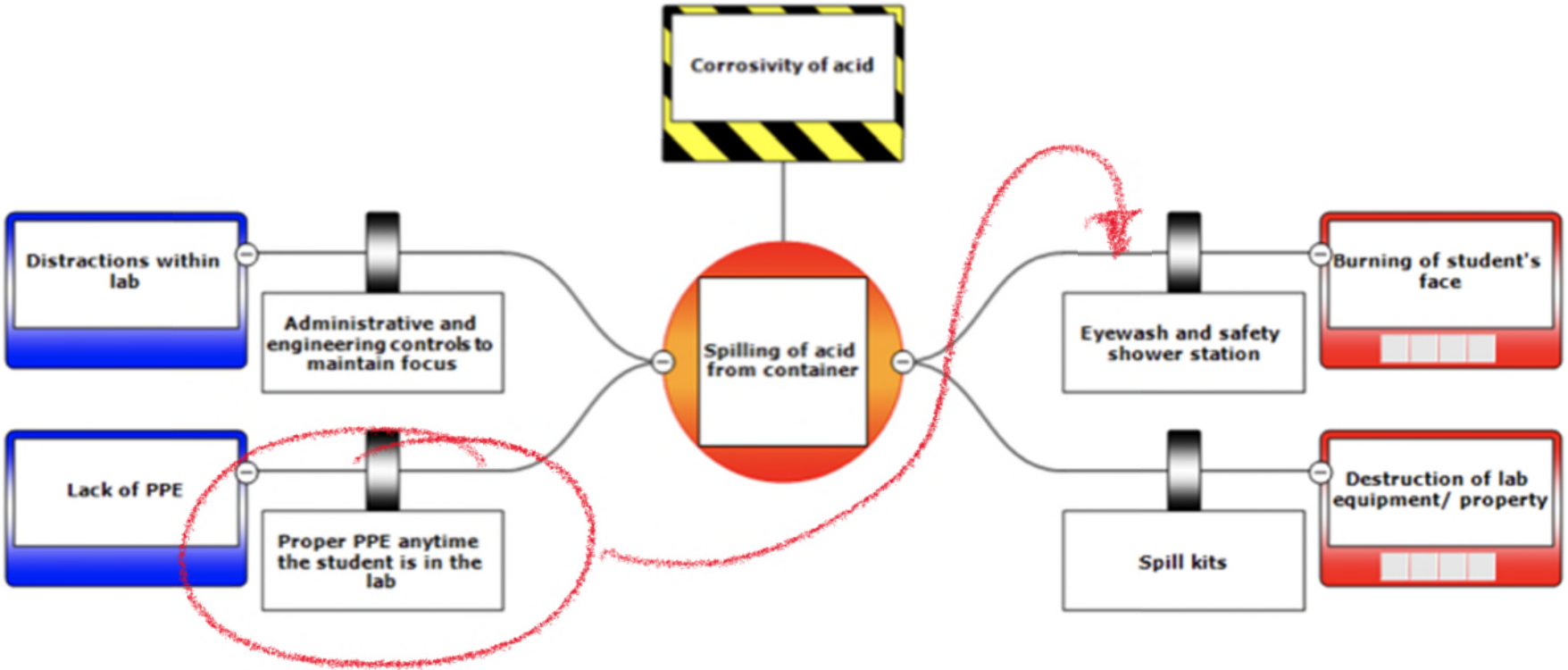
(c) the failure of life support systems for diving operations in connection with the installation, the detachment of a diving bell used for such operations or the trapping of a diver in a diving bell or other subsea chamber used for such operations;

(d) any other event arising from a work activity involving death or serious personal injury to five or more persons on the installation or engaged in an activity on or in connection with it; or

(e) any major environmental incident resulting from any event referred to in paragraph (a), (b) or (d)

Bow tie Diagram – Visualisation of Measures

Real World Example of Bowtie and Measures



Measures are called SECEs in the Regulations
Safety and Environmental Critical Elements

SCR2015 Reg. 2

"safety and environmental–critical elements" means such parts of installation and such of its plant (including computer programs), or any part of those:-

a) The **failure** of which **could cause** or contribute substantially to a **major accident**; or

b) A **purpose** of which is to **prevent or limit the effect** of, a **major accident**

Footnote: Why are there two types of SECE?

Measures

“Measures” is mentioned 49 times in this document

- Identify
- Specify
- Assess
- Implement
- ALARP

e.g. Principle 15

OFFSHORE MAJOR ACCIDENT REGULATOR

Offshore Petroleum Regulator
for Environment & Decommissioning

HSE

Assessment Principles for Offshore Safety Cases (APOSC)

Title	Assessment Principles for Offshore Safety Cases		
Publication Date	August 2021 (Rev:001)	**Document Identification**	APOSC
Review Due	August 2022	**Internal Reference**	2021/174769
Target Audience	All OMAR Inspectors All stakeholders	**Document Owner**	HSE ED 7

Principle 15

Measures taken to manage major accident hazards should be described

66. A hierarchical approach should be used for managing major accident hazards, taking account of the effect of each measure in a balanced and integrated way.
The recommended hierarchy is:

a. elimination and minimisation of hazards by design (inherently safer design)
b. prevention (reduction of likelihood)
c. detection (transmission of information to control point)
d. control (limitation of scale, intensity and duration)
e. mitigation of consequences (protection from effects).

Performance Standards / Safety Critical Elements

Typical Lists of Safety Critical Elements.

Performance Standards are written for each SECE.

No. of SECEs can vary depending on philosophy

001 Hydrocarbon Containment Systems.docx
002 Ignition Prevention Systems
003 Fire and Gas Systems
004 ESD System
005 Pipeline Systems and Riser ESDVs
006 Topsides Isolation and Blowdown Valves
007 Well Isolation and Containment.docx
008 Emergency Communications
009 Structural
010 Egress and Escape
011 Temporary Refuge
012 Emergency Power
013 Helicopter Support Systems
014 TEMPSC
015 Tertiary Means of Escape
016 Standby Vessel and FRC
017 PPE
018 Active Fire Protection
019 Navigational Aids
020 Lifting Equipment
021 Ventilation
022 Passive Fire Protection and Explosion Protection

P1	Structural Integrity	P2	Legs Jacking & Locking System
P3	Collision Avoidance System	P4	Process Containment Integrity
P5	Pipelines & Riser Integrity		
P7	Prevention of Rotating Equipment Failures	P8	Process Area Ventilation
P6	Process Shutdown System	P9	Well Containment
P10	Relief Systems	P11	HVAC Systems
P12	Ignition Prevention Systems	P14	Drilling System
P15	Ballast System and Stability Management	P16	Anchoring & Mooring System
P17	Crane & Lifting Equipment	P18	Corrosion Prevention & Corrosion Monitoring
C1	Flammable Gas detection	C2	Fire Detection
C3	Fire & Gas Control System	C4	Emergency Isolation
C5	Riser / Pipeline ESDVs	C6	Reservoir Isolation & Containment
C7	SSIV SSBV	C8	MACs
C9	Emergency depresurisation	C10	Toxic Gas detection
C11	Oxygen Depletion Detection	C12	Drainage & Containment
C13	Drilling Well Control System	C14	HIPS System
M1	Dropped Object Protection	M2	Blast Resistant Construction
M3	Fire Mitigation	M4	Temporary Refuge
M5	Fire Pumps	M6	Firewater main
M7	Firewater Systems	M8	Foam Systems
M9	Liquid & Gaseous Extinguishing Systems	M10	Portable / Trolley Mounted Extinguishers
E1	Alarm & PA System	E2	Egress & Access Routes
E3	Emergency Lighting	E4	Helideck
E5	Internal Communications	E6	External Communications
E7	Lifeboats (TEMPSC) & Boat Landings	E8	Liferafts
E9	Maintained Power Supplies	E10	Means of Escape to Sea
E11	Personnel Protective Equipment	E12	Rescue& Recovery Facilities

No need to FEAR PFEER!

FARS – Functionality / Availability / Reliability / Survivability

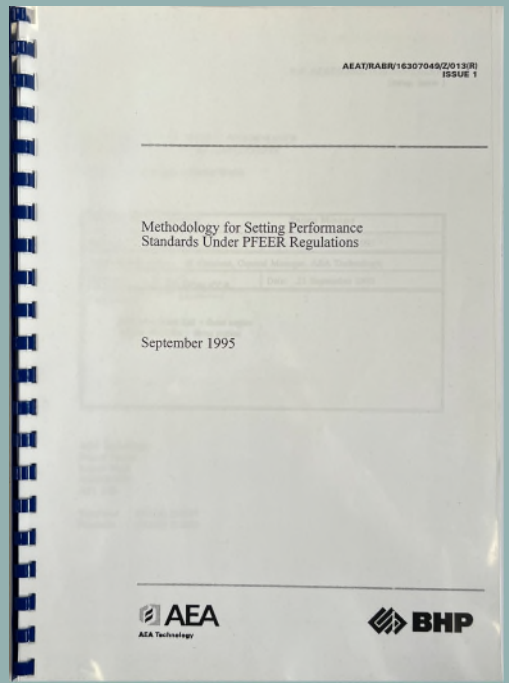
PDMCR – Prevent / Detect / Control / Mitigate / Recover

Paradigm Setting Advertising

Early Attempts

Methodology for Setting Performance Standards
Under PFEER Regulations

September 1995



Early Attempts (c. 1995)

Early “Functionality” Performance Standard for:

Emergency Shutdown System

PERFORMANCE STANDARD PROFORMA		1/3
EMERGENCY SHUTDOWN (ESD) SYSTEM (PSXXX)		
Aim: Automatically sense any abnormal operational and equipment condition, alert the Operator at a continuously manned location and execute timely actions to isolate hazardous inventories and trip non-essential equipment.		
FUNCTIONALITY		
Function	**Criteria**	**Verification**
Annunciate status of ESD valves	Annunciate at the operating console	Confirm by site survey
Leakage past ESD sectioning valves to be acceptable when closed	Leakage rate required to be within acceptable limits	Fire risk analysis to assess if anticipated or measured leakage acceptable
Tripping of non-essential equipment	Annunciate at the operating console	Function test against ESD Philosophy and Cause and Effect Diagrams
Provision of boundary isolation	List of initiators Speed of response	Function test against ESD Philosophy and Cause and Effect Diagrams
Provide shutdown functions on manual initiation	List of initiators	Function test against ESD Philosophy and Cause and Effect Diagrams
Provide facilities to manually initiate ESD	Push button locations	Function test against ESD Philosophy and Cause and Effect Diagrams

Later Attempts (c. 2019)

C4: Emergency Isolation				
Operational Performance Standard				
Functionality				
Function ID	Short Description	Functional Performance Requirements	Means of Operational Assurance	Operational Verification
F1	ESD/USS Shutdown Function	ESD/USS system to continuously monitor process data, equipment status and inputs from other systems, in areas of the site where a major accident could occur. ESD/USS system to continuously monitor and accept signals to initiate appropriate emergency shutdown actions and valve closure signals in accordance with ESD/USS Cause & Effects Diagrams.	Assurance is provided by function testing of the ESD/USS systems ensuring that all associated control functions, trip and alarm points and executive actions including electrical isolations function correctly as per ESD/USS Cause & Effects Diagrams. • Taking credit for any relevant unplanned isolation event, which occurs within the period between scheduled tests. These events should be recorded, investigated and corrected as necessary OR • Planned isolation events (i.e. during planned TAR events), or, scheduled isolation function test if no creditable isolation event has taken place during the proceeding period, ensuring that different initiating elements are used on a rotational basis. Assurance in accordance with procedure L3-NNS-14-020.	Review records to confirm that assurance tasks have been completed, results have been recorded correctly and any required remedial action has been carried out or a plan put in place. Witness assurance testing of the equipment to confirm it is being carried out in accordance with the assurance routine and the equipment meets the requirements of the performance standard. Function test the system ensuring that all associated control functions, trip and alarm points and executive actions function correctly as per Cause & Effects.
F2	ESD Valve Operation, incl. Reaction and Closure Time	Overall time for full ESD/USS Emergency Isolation to be less than 60 seconds from detection of hazard deviation. All ESDVs to close on emergency shutdown with local reset only. (NB! All valves should close within 60 seconds with the exception of ESV5152 which has a 2 minutes timer in the logic).	Assurance is provided by simulation of process shutdown and recording of valve closure times from initiation mechanism.	Review records to confirm that assurance tasks have been completed, results have been recorded correctly and any required remedial action has been carried out or a plan put in place. Witness assurance testing of the equipment to confirm it is being carried out in accordance with the assurance routine and the equipment meets the requirements of the performance standard.

Footnote - Another Complication
Not just Operational Performance Standards

Design

Specification

Fabrication / FAT

Commissioning

Operational

Functionality

Availability / Reliability

Survivability

Decommissioning

Function

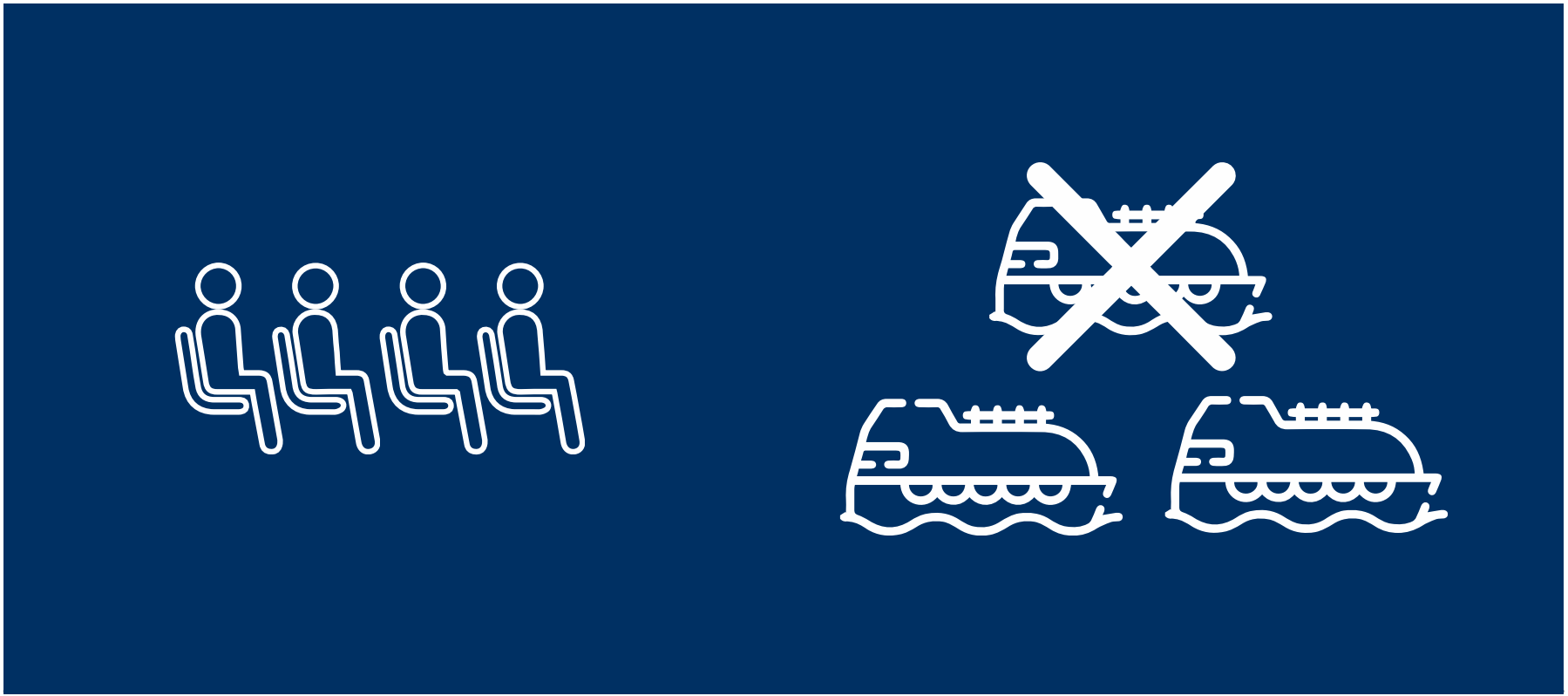
Prioritisation

Type (b) SECE

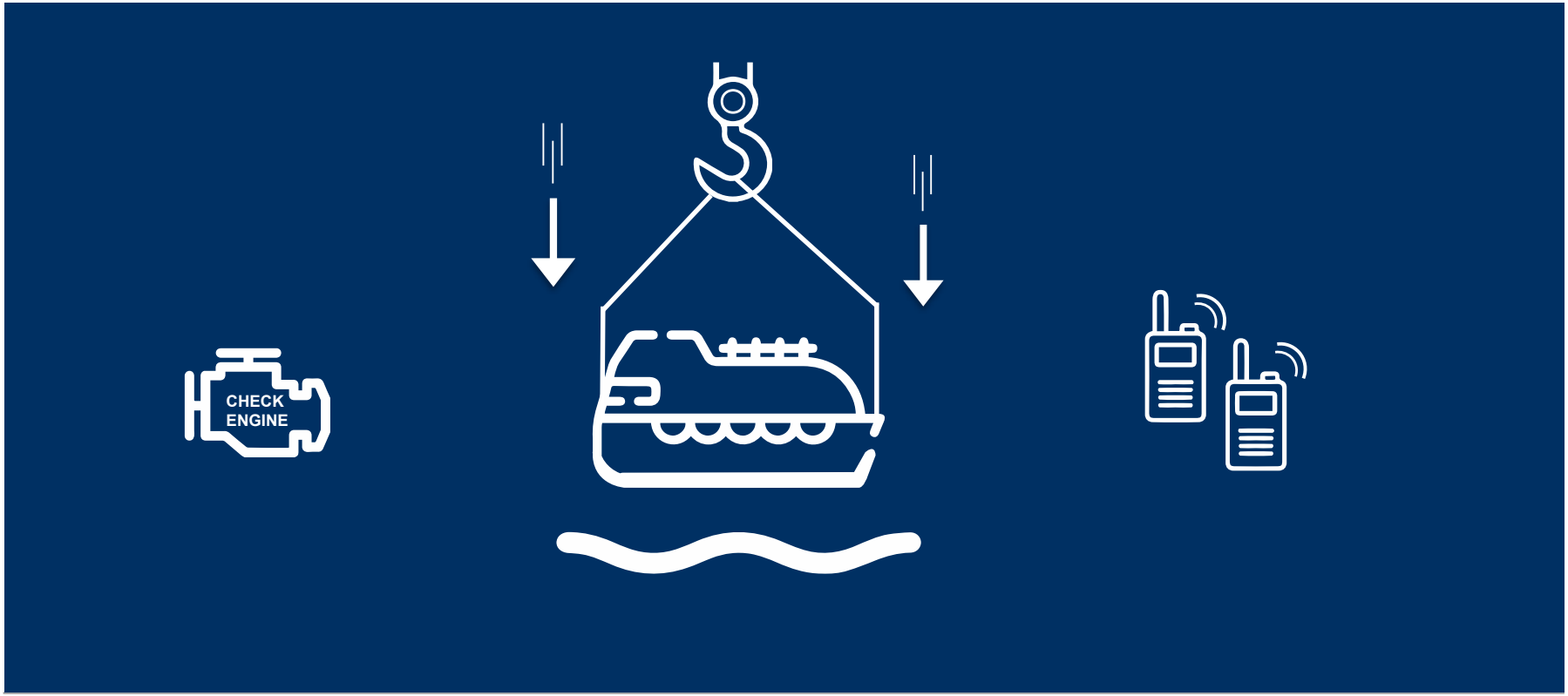
SCR2015 Reg. 2

b) A **purpose** of which is to **prevent or limit the effect** of, a **major accident**

Key Safety Attributes? Criteria?



Key Safety Attributes



Footnote: When did all this come in?

The SECE Management Process

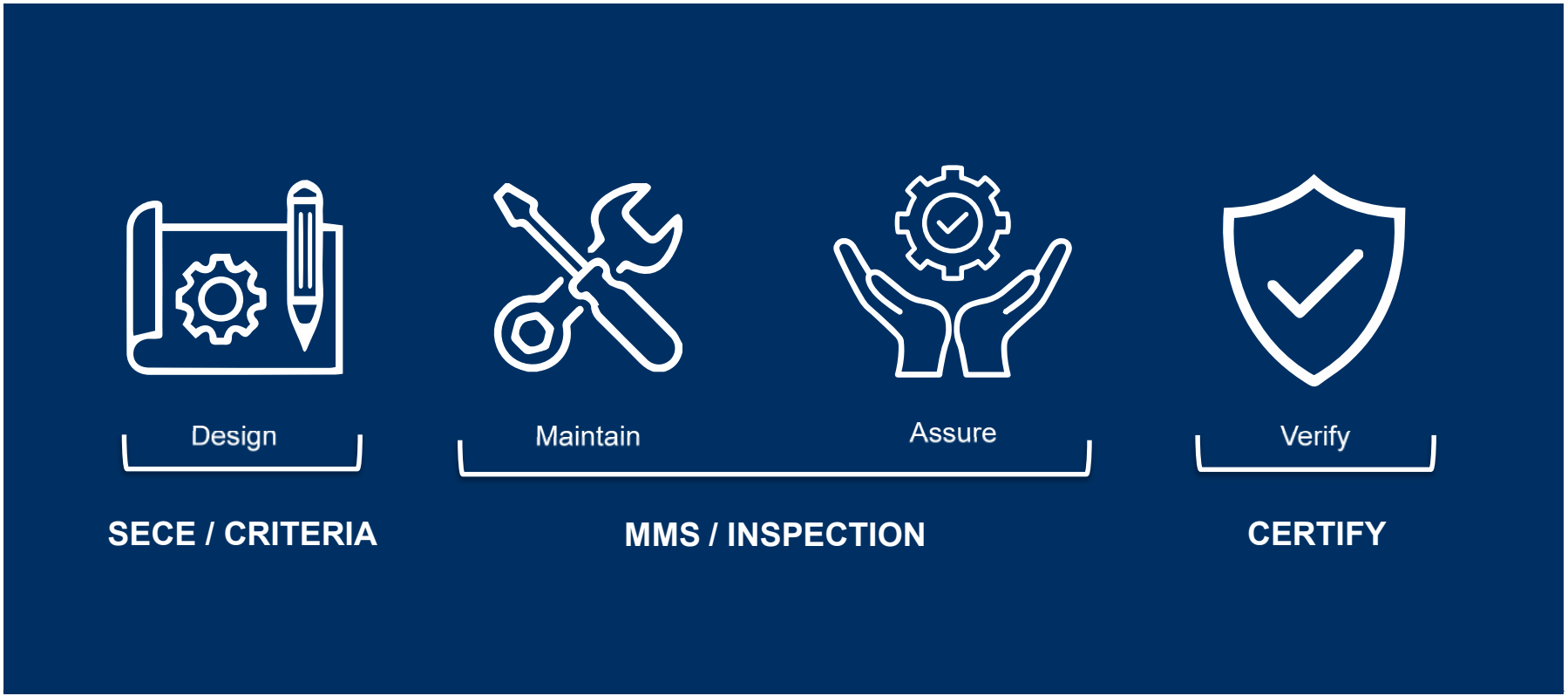
Design

Maintain

Assure

Verify

The SECE Management Process



Type (a) SECE

SCR2015 Reg. 2

a) The **failure** of which **could cause** or contribute substantially to a **major accident.**

IMS Workflow

The SECE Management Process

Design

Maintain

Assure

Verify

The SECE Management Process

PIM

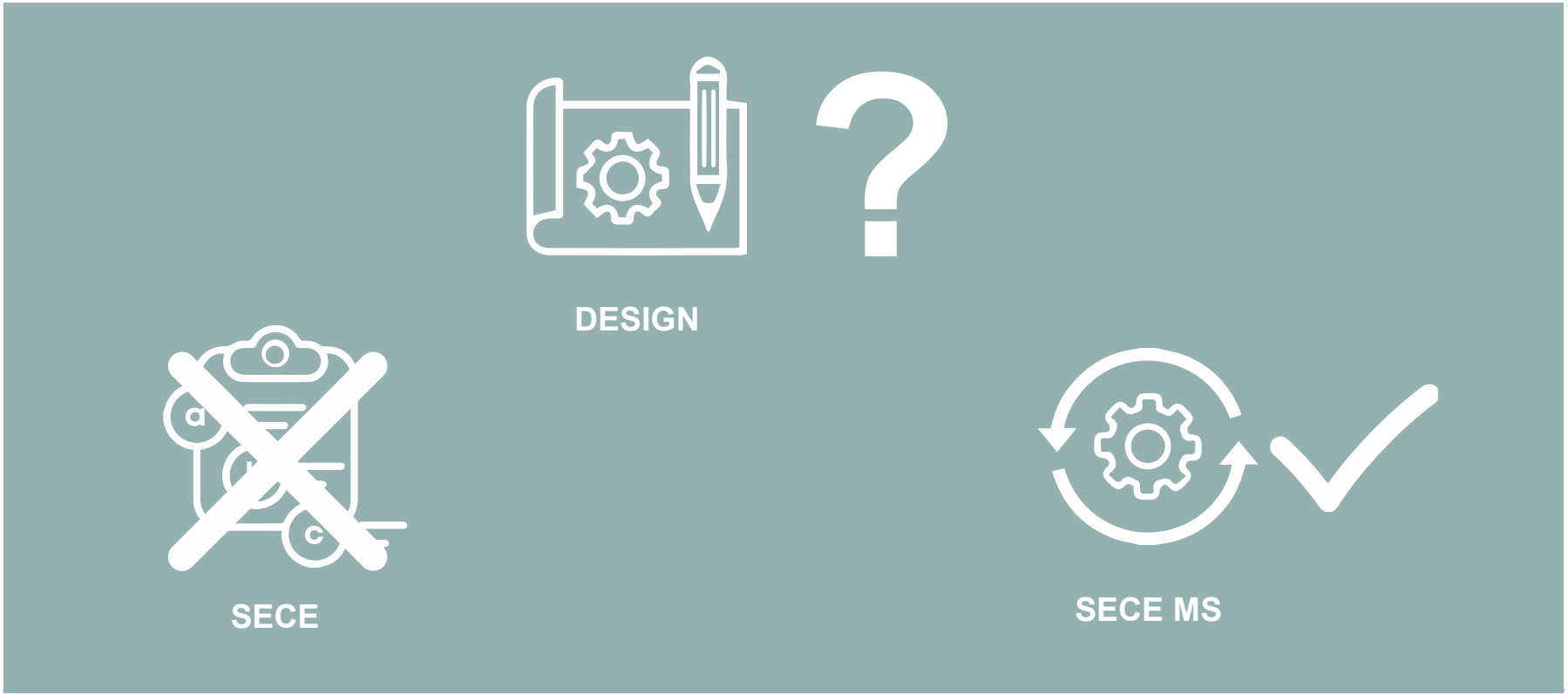
VERIFICATION ≈ CERTIFICATION

It's Fine … It works …

Operators, HSE and Verification Bodies have made it work!!

BUT THERE MIGHT BE A BETTER WAY?

Design



Design

Maintenance

Assurance

- Is the Management System well formulated?
- Is it looking at the correct items?
- Are the inspection tasks correct for the system?
- Are the tasks being carried out correctly?
- Are anomalies being identified and appropriately managed?
- Are there any backlogs at any point of the process?
- Has anything changed that require the Management System to be significantly updated?

Verification

- Examine operators Management System
- Examine inspection and reporting records
- Examine the Operator’s assessment processes
- Ensure Operator is following their own Management System
- Sampling and witnessing

Universal SECE

SECE Management Process

Design of SECE Management System

Maintenance Is the application of the process

Assurance is the audit of the process

Verification is an independent 3rd party audit of the whole process

Benefits and Challenges

Benefits

Less duplication

Less administration

Clearer process

Common process

Challenges

IMS Systems need to be well formulated

Change of mind set

PIM

BUT THAT'S JUST WHAT I THINK!

I WOULD LOVE TO HEAR YOUR THOUGHTS