http://www.engineersjournal.ie/2016/11/01/process-safety-failures-heat-exchangers/

The pen is mightier than the switch

The value of effective, clear and concise documentation to through-life plant safety

Ross Campbell CEng FSEng MIET MInstMC

20th November 2019

SYSTEMS AND ENGINEERING TECHNOLOGY

FRAZER-NASH CONSULTANCY

Frazer-Nash Today

- Systems and Engineering Consultancy
- Core engineering skillset
  - Mechanical, EC&I, electronics, software, civil
- Specialist groups
  - Modelling, HF, cyber, TEA, fire, info. systems
- Experience of regulated industries
- Reduce risk, improve resilience
- 80% of income is repeat business
- Prefer to sell solutions … not man hours
- Established market sectors:
  - Transport, industry & infrastructure
  - Power & energy
  - Defence

IOP Institute of Physics
Accredited Company Training Scheme

IET Accredited Scheme

Institution of MECHANICAL ENGINEERS

INVESTORS IN PEOPLE

ISO 14001 DNV REGISTERED

PROOF

- Introduction – the contributing role of safety documentation to incidents.
- Why isn’t all safety documentation effective, clear and concise?
- The importance of understanding safety reports.
- The link with Asset Management.
- Putting pen to paper…

Introduction – the contributing role of safety documentation to incidents

Columbia Space Shuttle Disaster (2003)

All seven crew were killed when the shuttle disintegrated during atmospheric entry. A piece of foam insulation broke off during launch which damaged the shuttles wing structure. Similar damage had occurred on previous launches but without the same fatal outcome.

The independent investigation was critical of NASA's decision making and risk assessment processes and noted "organizational barriers to effective communication of safety critical information".

Davis Besse Nuclear Power Station (2002)

Erosion of the 6-inch-thick (150 mm) carbon steel reactor head, caused by a persistent leak of borated water.

Among other shortfalls the incident investigation highlighted inadequate processes for assessing safety of the plant, inadequate safety culture, inconsistent and incomplete company policies on safety as root causes.

Introduction – the contributing role of safety documentation to incidents

BBC Sign in | News | Sport | Weather | iPlayer

NEWS

Home | UK | World | Business | Politics

Business | Your Money | Market Data

Ethiopian Airlines crash: Boeing faces safety questions over 737 Max 8 jets

Ethiopian Airlines Boeing 737 pilots 'could not stop nosedive'

Flawed analysis, failed oversight: How Boeing, FAA certified the suspect 737 MAX flight control system

Sources: Seattle Times, EE Times, Gregory Travis, Philip Koopman

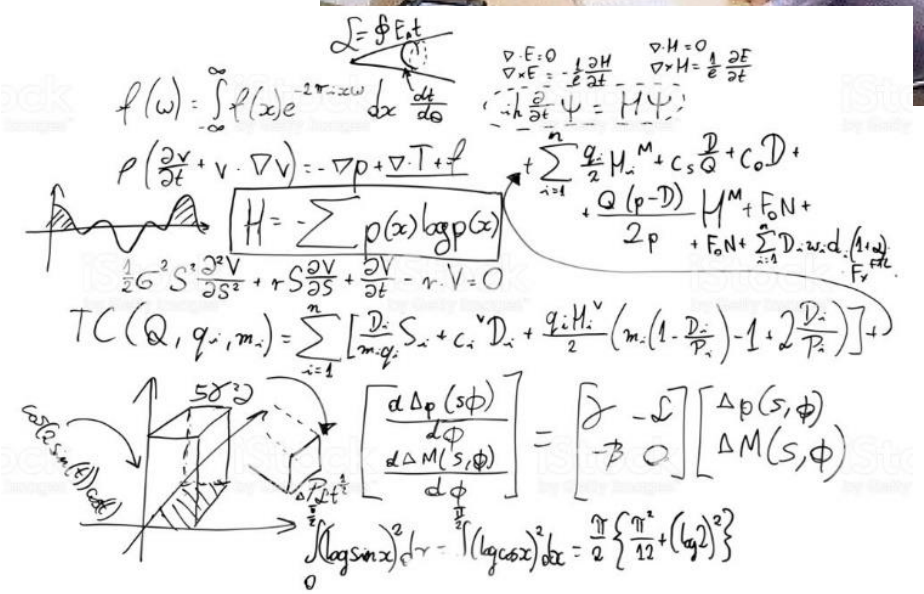
- Boeing 737 Max 8 – Crashes in 2018 and 2019.
  - The fundamental issues for both crashes was the MCAS systems.
  - The result of system failure was incorrectly assessed and not updated when the system configuration was change.
  - This resulted in a single AoA sensor input to system despite 2 sensors being present.
  - Misunderstanding of system authority and reactivation behaviour
  - Pilot training insufficient and flight manual did not document MCAS behaviour or its possible malfunctions

Errors or mis-alignment of safety documentation has been seen across many sectors

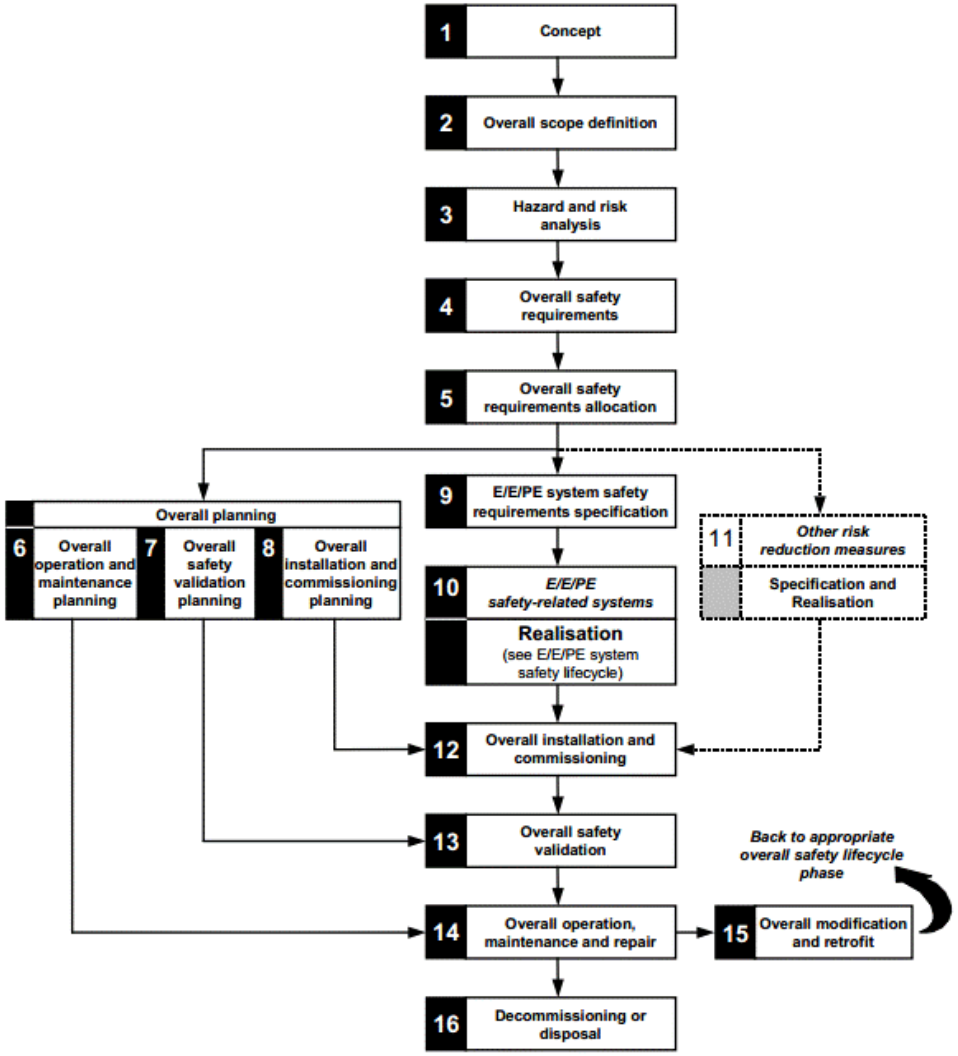
Why isn’t all safety documentation effective, clear and concise?

So its clearly important – so why is it so often flawed?

- Safety documentation can be particularly dry, meetings long and focus on minutia of detail making for long reports.
- You need input from a broad range of stakeholders for it to be both accurate and effective.
- Finalising documentation can be left until projects are well established.
- Assumptions are often made instead of using site based data.
- Budget and time is rarely made for making sure safety documents actually are ‘living’.
- Challenge between EPC and Operational hand-over
- Too much focus can be given to numerical values.

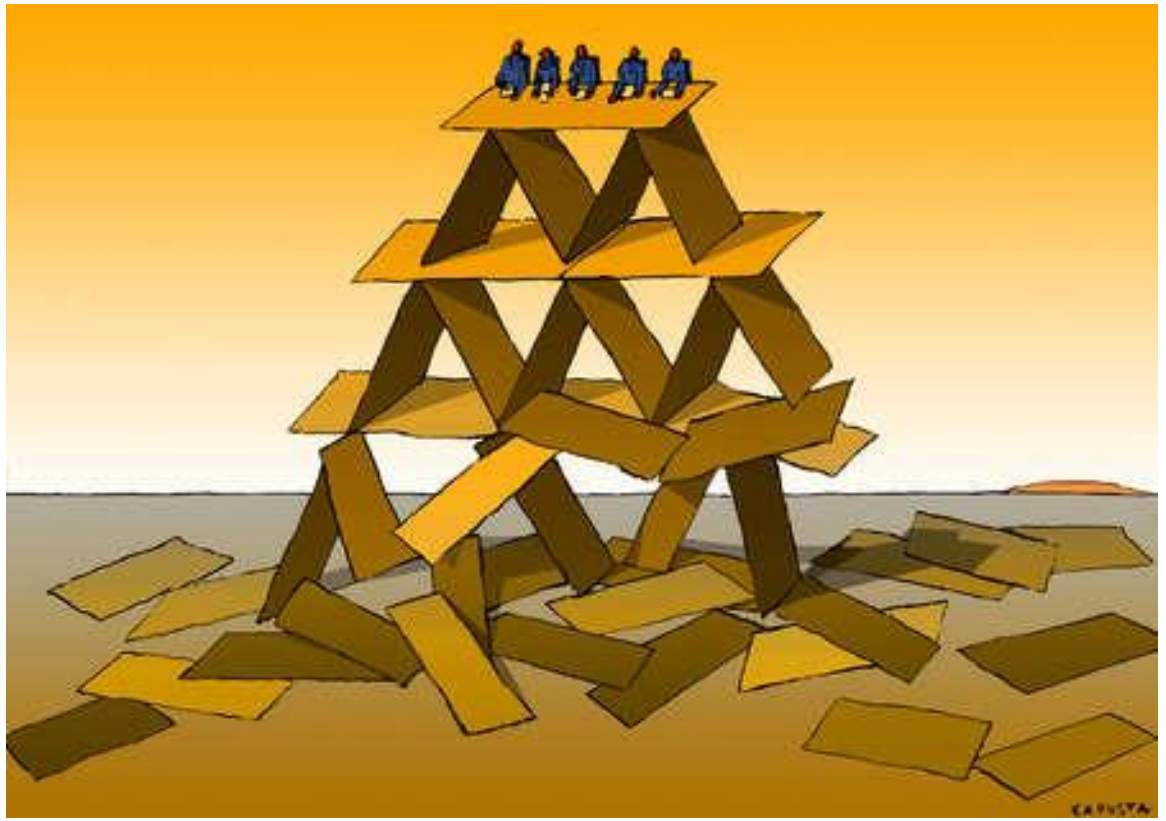


Tracking assumptions



- There is a defined safety lifecycle.
- The flow of data between these is where important information can be missed.
- Assumptions can be the basis of the assessments:
  - These two functions will be independent
  - The function is fully tested every year
  - The system is rarely operated…

Tracking assumptions



- Management of assumptions is key:
  - Testing sensitivity to these assumptions should be performed.
  - What if the function isn't tested fully every year.
  - What if a system starts to fail more frequently.
- Some examples

Independent functions using the same instrument type

Testing of system never having been performed

Boiler controller not controlling pressure and a trip occurring every month

- **Some assumptions are more influential than others - it's important to target your focus**

Moving expectations

- The goal posts are moving - expectations for management of safety documentation is changing:
  - Legacy arguments are always becoming harder to make.
  - IEC61511 now mandates a Functional Safety Assessment 4: Reviewing an in-service safety system.
  - Some organisations use machine learning to interrogate maintenance records and work orders.

Putting pen to paper…

Human errors will always exist, so whilst more ‘switches’ can help, there is a continuous need to improve safety measures that are written with a ‘pen’.

Here are a few ideas that could help:

- Allocate system owners alongside discipline engineers.
- Traceability of requirements and risk mitigations – link functions back to hazard analysis.
- Extracting assumptions from safety documentation and link to operational data.
- Challenge the practicalities of assumptions e.g. 100% proof test coverage.
- Involve end users more by giving operators the responsibility for approving safety related documents
- Test assumption sensitivities – are efforts being focused in the most impactful areas.

Complimenting Asset Management

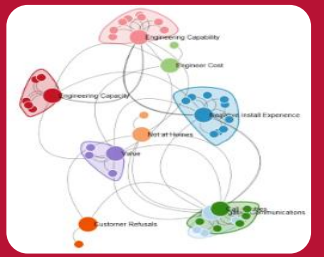
Safety Report

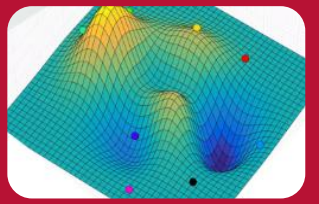
- Assumptions
  - Frequency of failure
  - System Availability
  - Test frequency
  - Repair time
  - Occupancy

Sensitivity Model

Computational Modelling

Analytical Engineering





Asset Management System

- Maintenance Records
- Operational data
- Failure reports
- Availability of Spares

Thank you. Any questions?

Ross Campbell – E,C&I Group Leader

Frazer-Nash Consultancy

Eston Road

Middlesbrough

TS6 6US

Tel: 01642 382 107

r.campbell@fnc.co.uk

www.fnc.co.uk