

Evolution of Risk & High Reliability System Concepts over 50 years

Howard Witt

Review of key* international events

With Discussion on how these changed risk and reliability thinking and actions internationally & locally

* Caveat

Naturally, there was no single event that was the sole cause of changed thinking. In many cases techniques pre-existed. However, I believe the events discussed were significant in bringing the new thinking to a broader audience.

FC Holden Sedan - 1958

FJ Holden - 1953

Latest Model
Commodore SV6



New Price \$37,000

(Standard Sedan) £1,023



1960s - Space Race - FMEA

FMEA was developed NASA as a formal design methodology in the 1960s.

US MIL-STD-1629 (Developed in 1970)

“Procedures For Performing
A Failure Mode, Effects and Criticality Analysis”

Specifies Worksheets to be completed during
Design, Production and Operation.



The worksheets should be living documents and
referenced repeatedly during project life



Australia has adopted many IEC “Dependability” Standards.
It is likely that Australia will also adopt IEC 60812:2006-01

**Analysis techniques for system reliability –
Procedure for failure mode
and effects analysis (FMEA)**

Hazard and Operability Studies (HAZOP)

Developed in the early 1970s by Imperial Chemical Industries Ltd.

ICI Plant OHS Lost Time Injuries ↓

“Significant Incidents” ↑

↑ Plant size, temperature and pressures.

A formal systematic critical examination of a process (new or existing facilities) to assess the potential impact of **Deviation** from Design Specifications.

Performed by an expert team using a set of guidewords:

e.g. when considering Flow rate in a process line,
the guide word

MORE OF = High Flow rate

LESS THAN = Low Flow rate.

Scenarios that may result in an Incident or an Operational Problem are identified.

The Consequences and Measures to reduce the associated Risk are then discussed and Actions recorded where appropriate.

Well accepted in the process industries for plant safety and operability improvements.

HAZOP Guidewords and their Generic Meanings

Deviations from the intended design are generated by coupling the guideword with a variable parameter or characteristic of the plant or process, such as reactants, reaction sequence, temperature, pressure, flow, phase, etc. i.e.

Guideword + Parameter = Deviation

Standard guidewords

- No (not, none) None of the design intent is achieved
- More (more of, higher) Quantitative increase in a parameter
- Less (less of, lower) Quantitative decrease in a parameter
- As well as (more than) An additional activity occurs
- Part of Only some of the design intention is achieved
- Reverse Logical opposite of the design intention occurs
- Other than (other) Complete substitution. Another activity takes place.

Other useful guidewords

- Where else Applicable for flows, transfers, sources and destinations
- Before/after The step (or some part of it) is effected out of sequence
- Early/late The timing is different from the intention
- Faster/slower The step is done/not done with the right timing

Flixborough

On 6/1/1974, a massive Vapor Cloud Explosion destroyed a UK chemical plant

- 28 employees died and 36 were injured
- Hundreds of off-site injuries
- Approx. 1,800 homes and 170 businesses damaged



Change Control - Compliance

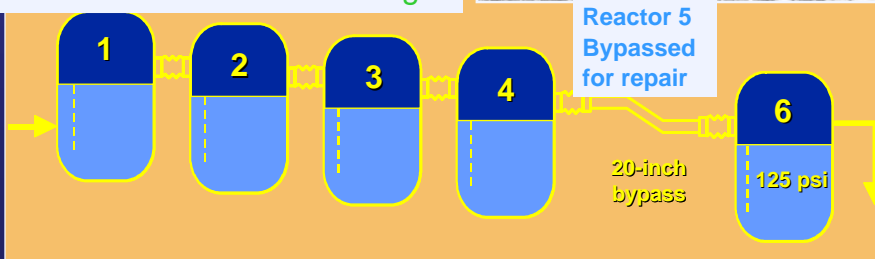
“Hurry up”

attitude of management

- Overworked staff did not take time to properly analyze their actions



Need for proper design and HAZOP of Mods and Changes



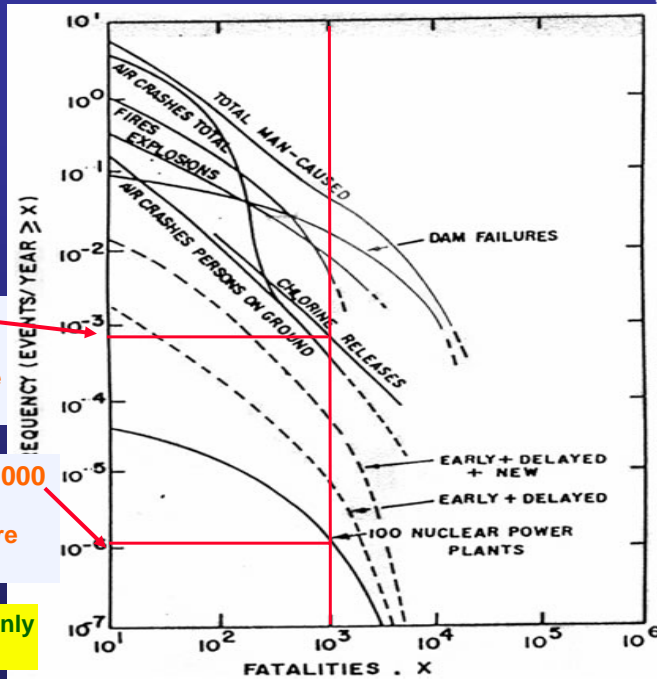
WASH 1400 Societal Risk Summary

In USA
Next year and Every Year

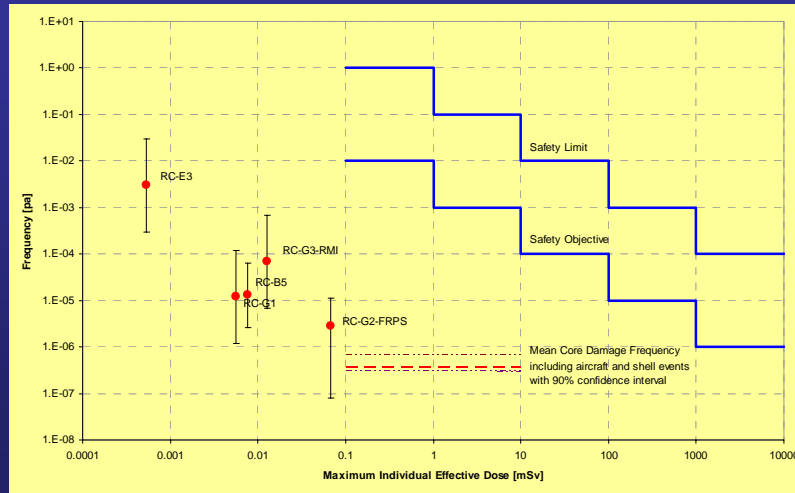
1 chance in a 1,100 that US chlorine release will kill more than 1,000 people.

1 chance in a 1,000,000 That US nuclear accident will kill more than 1,000 people.

Nowadays - Commonly called a FN curve



Comparison of OPAL PSA results with ARPANSA Safety Limits & Objectives



1975 - WASH 1400 Report - PSA

Early Reactor Licensing based on MCA Approach

(MCA - Maximum Credible Accident)

The Large Break LOCA (Loss Of Coolant Accident)

An ~ 30 inch reactor cooling system pipe has a **Guillotine Break** and the high pressure steam-water mixture discharges from the pipe.

WASH 1400 evaluated *all* accident sequences that might lead a **Core Melt**.

WASH 1400 - Reactor Safety Study (also called the *Rasmussen Report* after Professor Norman Rasmussen of MIT).

- Transients, small break Loss Of Coolant Accidents, and Human Error are more important risks – than MCA

Set the foundation for **Probabilistic Safety Assessment (PSA)** or **Probabilistic Risk Assessment (PRA)**.

In the early 1990's, all US nuclear plant licensees submitted plant-specific Individual Plant Examinations (IPE) for NRC review.

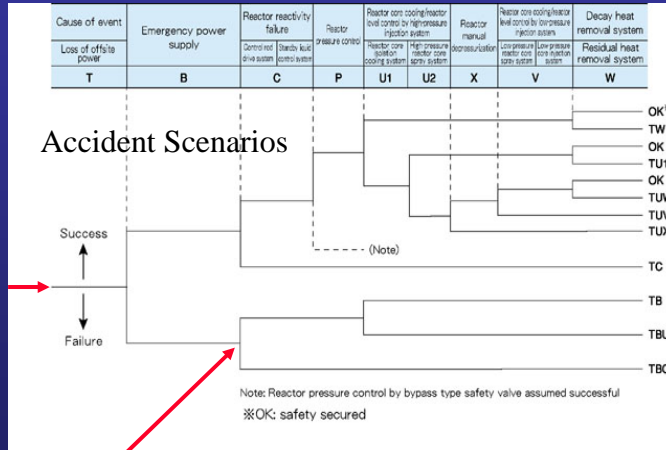
PSA - Event tree

Estimate Likelihood and Consequence of Each Sequence

For Each PIE

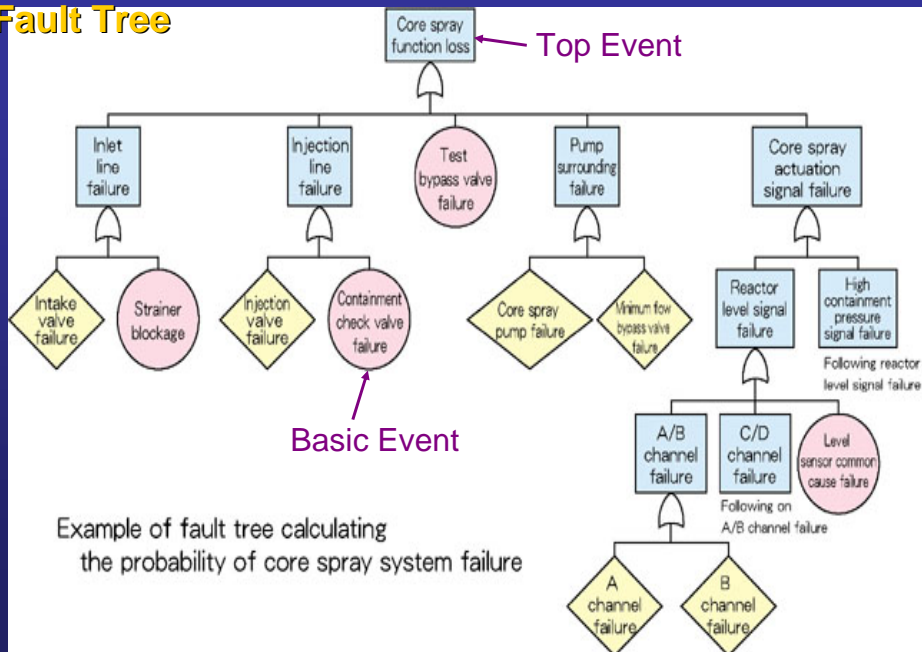
Postulated Initiating Event

Start Here



Use Fault Tree to Estimate Probability of System Failure Under Conditions Expected at these Points in Sequence

Fault Tree

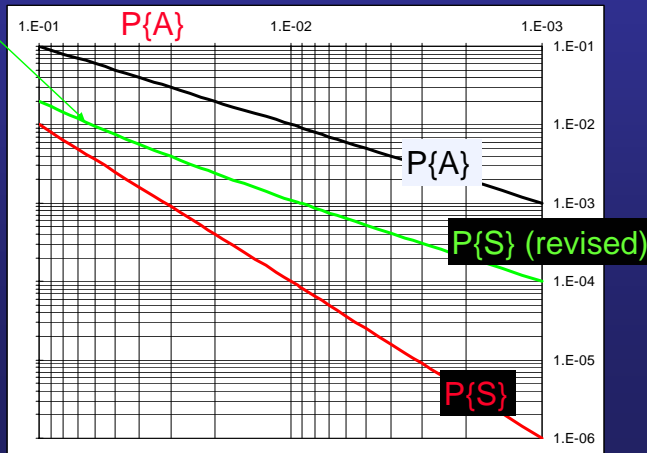
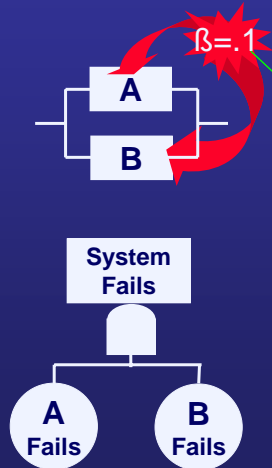


System Failure Probability Estimate Dependent Failure

Let $P\{A\}$ = Probability Item A failing

$$P\{S\} = P\{A\&B\} = P\{A\} * P\{B|A\} = P\{A\}^2$$

(if $P\{A\} = P\{B\}$ and events independent)



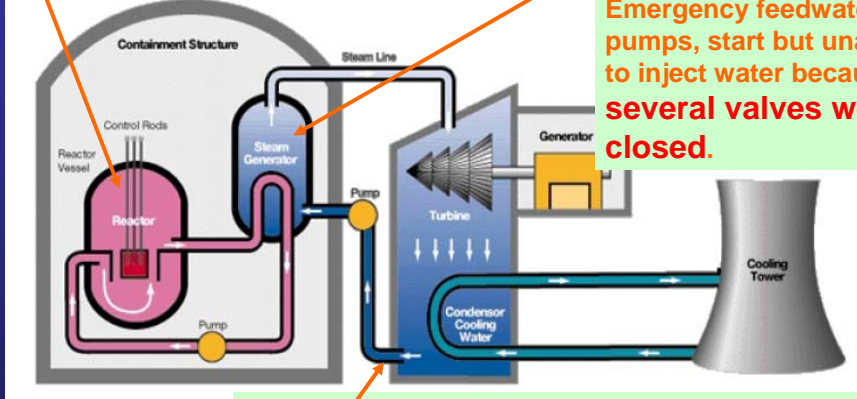
1978 - Three Mile Island Human Factors Knowledge Sharing - INPO (Industry "Club")

In March 1979, an event occurred at the [redacted] that resulted in the first case of Melted Fuel in a full scale Commercial Nuclear Power Plant.

Three Mile Island Incident Sequence

3 Heats, pressure rises - reactor shutdown

2 Design with little water - converted to steam within minutes. Emergency feedwater pumps, start but unable to inject water because several valves were closed.



1 A valve failed closed, reducing water supply to the steam generator. The main feedwater pumps and the turbine tripped within seconds.

Three Mile Island Sequence (Cont)

4 Relief valve opened correctly but failed to re-close after pressure dropped below the set-point - ongoing discharge to the quench tank

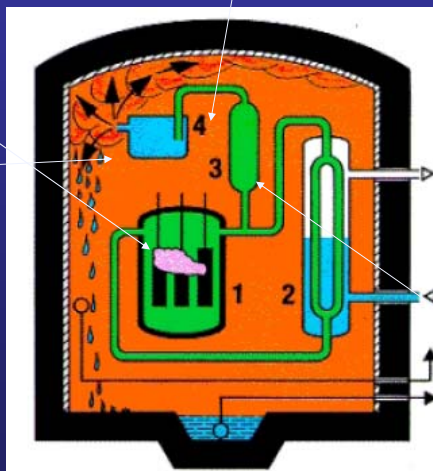
5 Pressure dropped

7 Rupture disc opens - steam released to containment

8 water (about 10-15 feet above the fuel) flashed to steam.

11 Steam void grows fuel melts

12 Water added cooling restored.



6 Due to poor control board design and a failure to indicate the valve position properly, the operators did not know the valve was open

9 Indicated water level stayed high

10 Operators turned off emergency water injection pumps & cooling pumps

Three Mile Island - Fallout

One cancer fatality due to the accident expected over subsequent 30 yr.

The Kemeny Commission which was appointed by President Carter found improvements were needed in:

- * Operator training
- * Emergency planning
- * Dissemination of industry information
- * Use of probabilistic safety assessment and analysis of more probable events.

INPO (Institute of Nuclear Power Operations)

“The electric utilities recognized their responsibilities” (were told to get their act together or the Nuclear Regulatory Commission would).

An industry self-assessment group was formed - the Institute of Nuclear Power Operations (based in Atlanta). INPO:

- Evaluates events and practices in the US nuclear industry and disseminates recommendations
- Conducts periodic assessments of each US utility, including operations, maintenance, engineering, training, radiation protection, chemistry, and corporate support; the results factor into the Insurance Ratings of the utility. - Staffed by officers from other similar Power Reactors
- Provides specialized training programs for utility personnel, including plant managers.

1978 – Airline Industry RCM (Reliability Centred Maintenance)

US airline industry in the 1960s/1970s

- Increasing preventive maintenance led to higher operating costs; but
- Did NOT provide the required improvement in safety and reliability.

In 1978, Nowlan & Heap of United Airlines published a document

'Reliability Centred Maintenance' (RCM).

This detailed a fundamental shift in the "then current" maintenance instruction development approach (MSG-2).

The Nowlan and Heap report served as the basis for **MSG-3**.

Since 1980, MSG-3 has been revised five times.

The latest is MSG-3 R2003.1

Australia has adopted many IEC "Dependability" Standards. Including

**AS IEC 60300.3.11—2004 Dependability management
Part 3.11: Application guide—Reliability centred maintenance**

Clause 5.2 Calls on use of FMEA to determine functional failures

1986 - Chernobyl

The term '**Safety Culture**' was first introduced in INSAG's# *Summary Report on the Post-Accident Review Meeting on the Chernobyl Accident.*



INSAG International Nuclear Safety Advisory Group - IAEA

IAEA* Definition

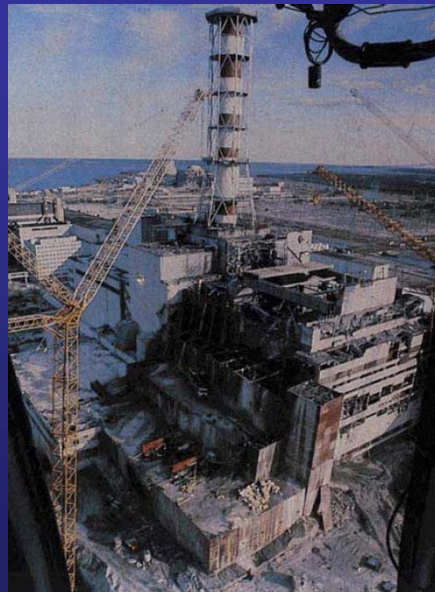
Safety Culture is that assembly of characteristics and attitudes in organisations and individuals which establishes that, as an overriding priority, nuclear plant safety issues receive the attention warranted by their significance.



* International Atomic Energy Agency, VIENNA 1991 Safety Series 75-INSAG-4

Good Safety Culture:-

- Good safety Attitudes in Staff AND Effective Organisational Safety Management Systems and Practices.
- Ongoing Assessment of the Safety Significance of Events, and Issues, and giving then the appropriate level of attention.



A Safety Culture



Stages of Safety Culture Development

Rule Based

Safety Management is Determined by Regulations and Rules

Performance Monitoring Based

Good Safety Performance becomes an Organisational Goal

Process Based

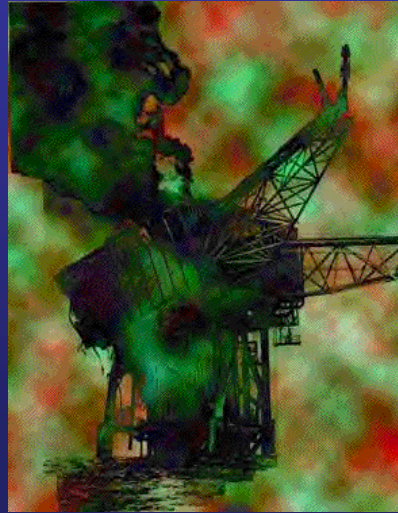
Safety Performance is seen as Dynamic and Continuously Improving



1988 - Piper Alpha Disaster Safety Case

Income of ~ £3.5m (\$6.25 Million US) a day

- North Sea oil production platform operated by Occidental Petroleum (Caledonia) Ltd.
- Produced around 10% of the then oil and gas production from the North Sea.
- Began production in 1976,
- An explosion and resulting fire destroyed it on July 6, 1988, killing 167 men, only sixty two crewmen survived.



Piper Alpha Disaster - 1988

The **Cullen Enquiry** was set up in November 1988 to establish the cause of the disaster.

In November 1990, it concluded that the initial condensate leak was the result of maintenance work being carried out simultaneously on a pump and related safety valve.

Piper Alpha's operator, was found guilty of having **inadequate maintenance procedures**

A second phase of the enquiry made far-reaching safety recommendations, all of which were accepted by industry.

Estimated cost to Occidental Petroleum more than £8.5 Billion (\$15.2 Billion US).



Piper Alpha

27

- For safety - modules organised so that the most dangerous operations were distant from the personnel areas.
- **A conversion from oil to gas production broke this safety concept, for example the gas compression next to the control room.**
- **Two large compressors, compressed the gas for transport to the coast. On the morning of July 6, compressor A's pressure relief valve was removed for overhaul. The now open pressure tube was temporarily sealed with a plate. Because the work could not be completed by 18:00, the plate remained.**
- **On-duty custodian busy, the duty engineer omitted to inform him of the condition of compressor A - Placed the worksheet in the control centre and left.**
- **Sheet lost. - Coincidentally there was another worksheet for the general overhaul of compressor A that had not yet begun.**
 - Compressor B stopped suddenly and could not be restarted.
 - Compressor A was switched on. **→ Fire**

The control room was abandoned. → Fire pumps not started.

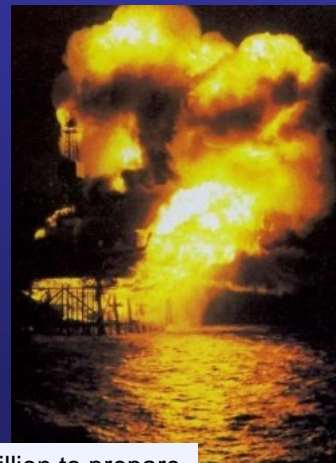
Design did not anticipate the possibility of the destruction of the control room.

Piper Alpha Disaster - 1988

28

As details of the causes of the disaster emerged every offshore Operator undertook wide-ranging assessments of their installations and management systems.

- Improvements to **"Permit to work"** management systems
- Relocation of some pipeline emergency shutdown valves
- Installation of sub-sea pipeline isolation systems
- Mitigation of smoke hazards
- Improvements to evacuation and escape systems
- Initiation of **Formal Safety Assessments**



Each **Safety Case** cost, on average, about £1 Million to prepare.

Source: Offshore Operators Website



28 January 1986

Challenger explodes 73 seconds into its launch, killing all seven crew members



1 February 2003

Columbia, re-entry at 10,000 mph, disintegrates. All 7 astronauts are killed

Key Organizational Culture Findings

- What NASA Did Not Do

1. Maintain Sense Of Vulnerability
2. Combat Normalization Of Deviance
3. Establish an Imperative for Safety
4. Perform Valid/Timely Hazard/Risk Assessments
5. Ensure Open and Frank Communications
6. Learn and Advance the Culture

25/9/1998 – Longford Major Hazard Facility Legislation in Vic

- Explosion – 2 Fatalities
 - Fire took 2 days to extinguish
- Large \$ Cost - Insurance \$150 million - overall ~ \$13 billion
- Royal Commission to Report in 3 months
- Found Esso at fault and that the accident was Practicably Preventable

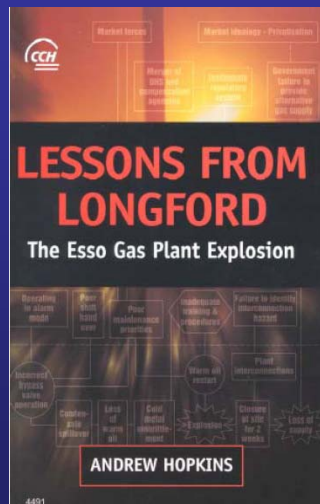


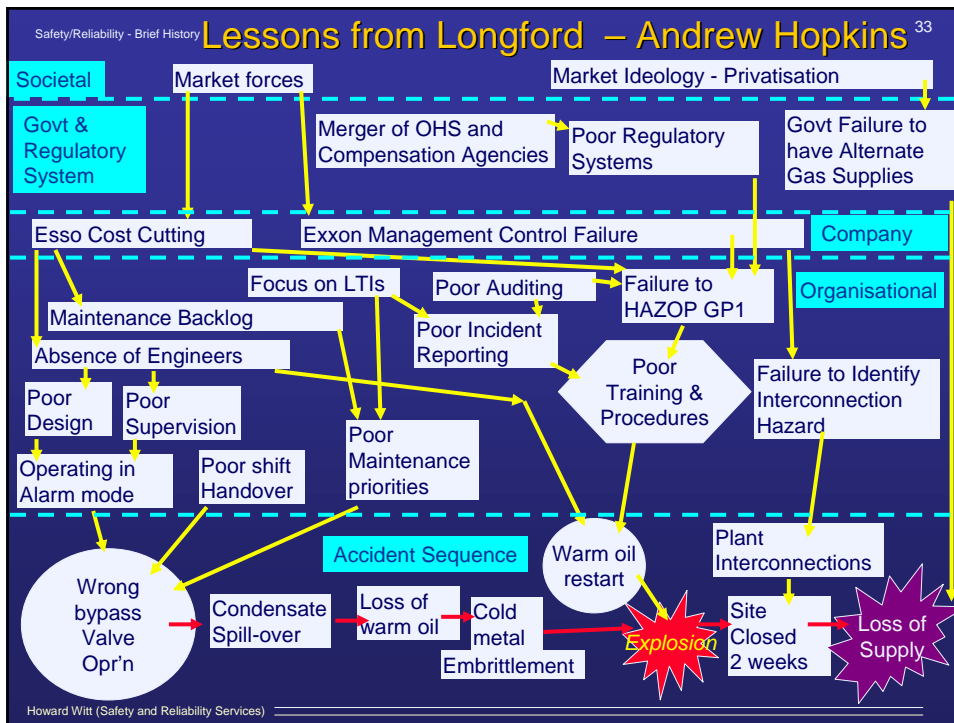
Cause Sequence

- Pump S/D hot oil flow to heat exchanger GP905 stops
- Flow of cold product continues
- GP905 drops to -30 C weld becomes brittle
- 4 hr later hot oil flow restarts
- Thermal stress – weld crack
- GP905 Rips open – Gas Explosion

This photograph shows the extinguished structure. The 3/4" steel plating has been ripped apart like a tin can.

Good Reference





Safety/Reliability - Brief History **Esso Found Guilty** 34

The OH&S Act requires employers to identify, as far as is practicable, workplace hazards.

- Absolute safety is seen as an unachievable ideal, and much hangs on that phrase "as far as is practicable".
- For any alleged breach, a court will consider the accepted methods, standards, codes of practice, safety management systems and so on utilized within the industry in question.

For the jury to find the company guilty on this charge, it had to be satisfied on two "elements" of the charge, namely:-

- the hazard of cold embrittlement existed
- the company had a practicable means of identifying the hazard, **that it did not employ**

Howard Witt (Safety and Reliability Services)

Australian Standard & Code of Practice

Australian Safety and Compensation Council

(ASCC) - October 2005.

- replaces the **National Occupational Health and Safety Commission (NOHSC)** which issued "WORKSAFE STANDARDS AUSTRALIA".
- Like its predecessor, the ASCC comprises representatives from Federal, State and Territory Governments, the Australian Council of Trade Unions (ACTU) and the Australian Chamber of Commerce and Industry (ACCI).

1996 Standard reissued in 2002

**National Standard
[NOHSC:1014(2002)]**

1996 Code of Practice still current
Practical Guidance on how to
comply

**NATIONAL CODE OF PRACTICE
FOR THE CONTROL OF
MAJOR HAZARD FACILITIES
[NOHSC:2016(1996)]**

Objectives of National Standard

The objective of the National Standard is to prevent major accidents and near misses, and to minimise the effect of any major accident and near misses, resulting from the activities of major hazard facilities.

It attempts to achieve this by requiring operators to:

- identify and assess all hazards and implement control measures to reduce the likelihood and effect of a major accident;
- provide information to the relevant public authority and the community, including other closely located facilities, regarding the nature of the hazards at a major hazard facility and emergency procedures in the event of a major accident;
- report and investigate major accidents and near misses, and take appropriate corrective action; and
- record and discuss the lessons learnt and the analysis of major accidents and near misses with employees and employee representatives.

Major Hazard Facility Law

- All jurisdictions expected to have legislation by 2003*
- To date only Victoria and Queensland have specific Major Hazard Facility law in place

* National Occupational Health & Safety Commission
MAJOR HAZARD FACILITIES - Annual Situation Report 2003

Victorian WorkCover Authority

The Victorian Occupational Health and Safety (Major Hazard Facilities) Regulations – 1 July 2000

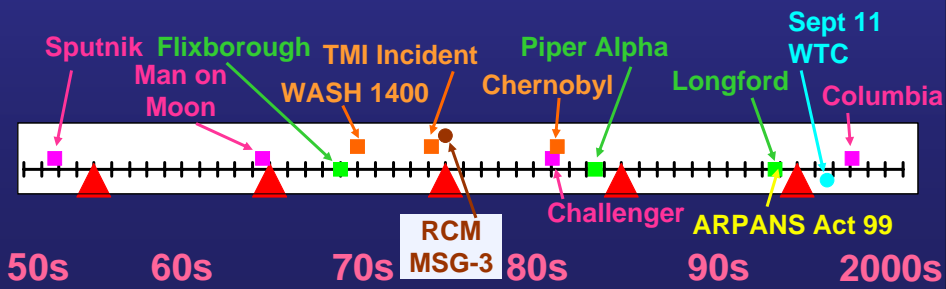
They give effect to the National Standard and the recommendations of the Longford Royal Commission.

In 2003 the Victorian WorkCover Authority had assessed

- 39 Safety Cases and
- issued 37 licences.

Timeline

- Conservative Design
- Max Credible Accident
- Defense in Depth
- Fail Safe
- HAZOP
- PSA
- RCM
- Asset Mgmt
- Safety Culture
- Safety Case
- Security Culture
- Human Factors
- Information Sharing



Changing Expectations

Personal Responsibility

I (he) was paralytic don't know how I (he) got home → Drink less & Designated Driver

Vehicles

Backyard Mechanic Minimal Safety Features → New Safer Car with 4 yr Warranty

Law/Rules

Expected a fair chance to avoid detection → Accept random testing and Speed Cameras

Most men smoke Most women don't → Fewer men smoke More women smoke

Changes in Safety Thinking

Traditional

- Concerned about people hurting themselves
- Fix plant problems safely when/if they arise
- Trial and error
- say “Be Careful!”
Blame Operator
- Attention limited to incidents that injure.

Loss Prevention

- More concern of about incidents that arise from the technology
- Hazards are to be identified and considered during design
- Formal and systematic approaches adopted
- Consider Man Machine Interface
- Attention to incidents/near misses that injure, damage plant and profit

Adapted from Lees: Loss Prevention in the process Industries

Generation III US Power Reactors Sales Pitch

Increased Plant Safety - Reduced Cost

Safety and Licensing Certainty

- Certified Design - The AP600 has final design approval from the US NRC.
- No major licensing hurdles once site and construction licenses are granted.

Passive Safety Features

- Once actuated, depend only on natural forces (gravity and natural circulation) to perform safety functions.

Simplicity

- Using experience-based components – No plant prototype or demonstration models.
- Requires no operator actions to maintain a safe configuration following an accident.
- No emergency planning zone beyond the site boundary.
- Greatly reduced operation, maintenance and testing requirements.

Modularisation - Construction costs down

- construction techniques - similar to those applied in ship construction
- 36-month schedule from first concrete pour to the fuel load.
- Reduced skilled craft labour hours needed.
- Much quality assurance inspections completed in the factory (before delivery).

No Power Reactor Projects have been initiated in the United States since the 1970s.

Recurrent Problems Observed

For Safety Related Plant there can be an emphasis on

- Change Control **rather than**
- Conformance Management
 - i.e. proposed changes subject to formal review but no formal review of impact of gradual deterioration
- Hardware only **rather than**
- Total System including Procedures and People

Too easy to adopt the do nothing option

Too easy to assume management systems are adequate/appropriate

50 yrs of Safety and Reliability

Within living memory there has been

An inexorable and relentless Improvement in our Standard of Living and the Safety and Reliability of Systems

Continuation is NOT Inevitable Rapid Decline is Possible

- Reliant on an ongoing prosperity
 - Reliant on social stability and innovation
 - Reliant on ready access to food and resources
 - Reliant on natural systems

We can influence Some of Driving Factors Others we can not.

Of those we can influence we should try to be Wise in our Actions

Remember the Dinosaurs Ruled Once