Hazard Analysis and FMECA

Prof. Chris Johnson,
School of Computing Science, University of Glasgow.
johnson@dcs.gla.ac.uk
http://www.dcs.gla.ac.uk/~johnson

University of Glasgow

Introduction

- Hazards:
  - Create risk of accident or incident;
  - Risk of fire from hazard of matches, lightning etc.
- Hazard analysis:
  - Component of risk assessment.
- FMECA/FMEA:
  - Failure Modes, Effects and Criticality Analysis;
  - Primarily qualitative approaches;
  - Methodological support reduces subjectivity?

University of Glasgow

Hazard Analysis

- Safety case
  - Argument why proposed system is safe;
  - Key argument is that hazards are identified;
  - Significant risks are then mitigated.

- Lots of Hazard Analysis techniques:
  - fault tress (see later);
  - cause consequence analysis;
  - HAZOPS;
  - FMECA/FHA/FMEA...

University of Glasgow

Failure Modes, Effect and Criticality Analysis

- Technique has its origins in the Cold War:
  - MIL STD 1629A (1977!);
  - Amazing that it is still a core technique.
- Relatively simple idea:
  - Analyse each potential failure;
  - Determine impact of system(s);
  - Assess its criticality;
  - Fix the major concerns.
- Compare this with IEC61508?
  - Hazard analysis to identify SIL,
  - Software tools etc appropriate to integrity level.

University of Glasgow

Failure Modes, Effect and Criticality Analysis

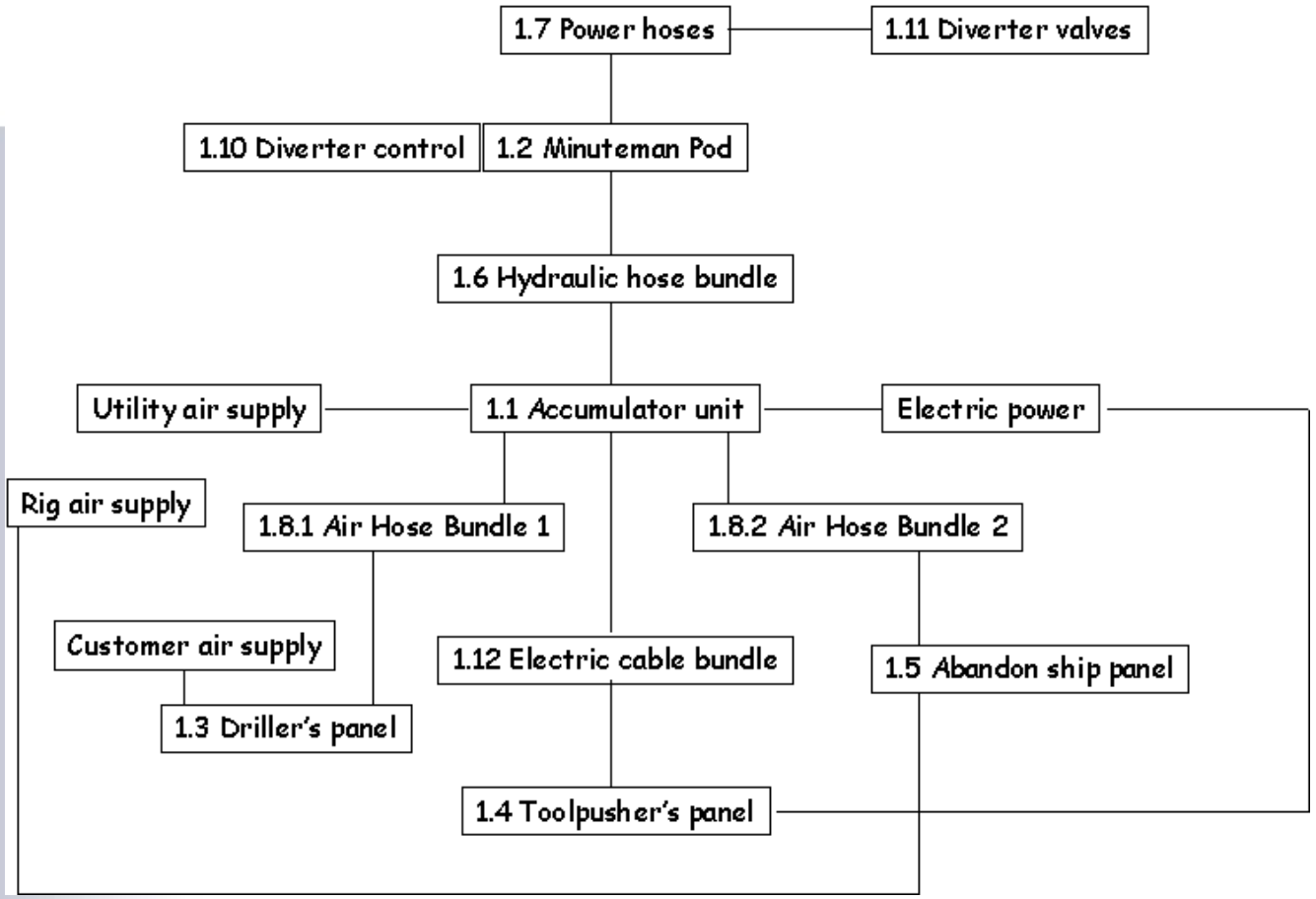
1. Construct functional block diagram.
2. Use diagram to identify any associated failure modes.
3. Identify effects of failure and assess criticality.
4. Repeat 2 and 3 for potential consequences.
5. Identify causes and occurrence rates.
6. Determine detection factors.
7. Calculate Risk Priority Numbers.
8. Finalise hazard assessment.

University of Glasgow

Failure Modes, Effect and Criticality Analysis

- Step 1: Functional Block Diagram
- Establish scope of the analysis.
- Break system into subcomponents.
- Different levels of detail?
- Some unknowns early in design?

Minuteman Example



- Ack: J.D. Andrews and T.R. Moss, Reliability and Risk Assessment, Longman, Harlow, 1993 (ISBN-0-582-09615-4).

University of Glasgow

Failure Modes, Effect and Criticality Analysis

- Step 2: Identify Failure Modes
- Many different failure modes:
  - complete failure;
  - partial failure;
  - intermittant failure;
  - gradual failure;
  - etc.
- Not all will apply?
- Compare with HAZOPS guidewords

FMECA - Step 3: Assess Criticality

10. Hazardous without warning: Very high severity ranking when a potential failure mode affects safe operation or involves non-compliance with a government regulation without warning.

9. Hazardous with warning: Failure affects safe product operation or involves noncompliance with government regulation with warning.

8. Very High: Product is inoperable with loss of primary Function.

7. High: Product is operable, but at reduced level of performance.

6. Moderate: Product is operable, but comfort or convenience item(s) are inoperable.

5. Low: Product is operable, but comfort or convenience item(s) operate at a reduced level of performance.

4. Very Low: Fit & finish or squeak & rattle item does not conform. Most customers notice defect.

3. Minor: Fit & finish or squeak & rattle item does not conform. Average customers notice defect.

2. Very Minor: Fit \& finish or squeak \& rattle item does not conform. Discriminating customers notice defect.

1. None No effect

University of Glasgow

Failure Modes, Effect and Criticality Analysis

- Step 4: Repeat for potential consequences
- Can have knock-on effects.
- Additional failure modes.
- Or additional contexts of failure.
- Iterate on the analysis.

University of Glasgow

Failure Modes, Effect and Criticality Analysis

- Step 5: Identify Cause and Occurence Rates
- Modes with most severe effects first.
- What causes the failure mode?
- How likely is that cause?
- risk = frequency x cost

FMECA - Step 5: Identify Occurrence Rates

- Very High: Failure almost inevitable
  - Rank 10: 1 in 2
  - Rank 9: 1 in 3
- High: Repeated failures
  - Rank 8: 1 in 8
  - Rank 7: 1 in 20
- Moderate: Occasional failures
  - Rank 6: 1 in 80
  - Rank 5: 1 in 400
  - Rank 4: 1 in 2000
- Low: Relatively few failures
  - Rank 3: 1 in 15,000
  - Rank 2: 1 in 150,000
- Remote: Failure is unlikely
  - Rank 1: 1 in 1,500,000

Failure Modes, Effect and Criticality Analysis

- Step 6: Determine detection factors.
  - Type (1):These controls prevent the Cause or Failure Mode from occurring, or reduce their rate of occurrence.
  - Type (2): These controls detect the Cause of the Failure Mode and lead to corrective action.
  - Type (3): These Controls detect the Failure Mode before the product operation, subsequent operations, or the end user.
- Can we detect/control failure mode?

Failure Modes, Effect and Criticality Analysis

10. Absolute Uncertainty: Control does not detect a potential Cause of failure or subsequent Failure Mode; or there is no Design Control

9. Very Remote: Very remote chance the Design Control will detect a potential Cause of failure or subsequent Failure Mode

8. Remote: Remote chance the Design Control will detect a potential Cause of failure or subsequent Failure Mode

7. Very Low: Very low chance the Design Control will detect a potential Cause of failure or subsequent Failure Mode

6. Low: Low chance the Design Control will detect a potential Cause of failure or subsequent Failure Mode

5. Moderate: Moderate chance the Design Control will detect a potential Cause of failure or subsequent Failure Mode

4. Moderately High: Moderately high chance the Design Control will detect a potential Cause of failure or subsequent Failure Mode

3. High: High chance the Design Control will detect a potential Cause of failure or subsequent Failure Mode

2. Very High: Very high chance the Design Control will detect a potential Cause of failure or subsequent Failure Mode

1. Almost Certain: Design Control will almost certainly detect a potential Cause of failure or subsequent Failure Mode

University of Glasgow

Failure Modes, Effect and Criticality Analysis

- Step 7: Calculate Risk Priority Numbers
- Risk Priority Numbers (RPN)
- RPN = S x O x D, where:
  - S - severity index;
  - O - occurence index;
  - D - detection index.
- A partial number line 0..1,000.

Failure Modes, Effect and Criticality Analysis

- Step 8 - Finalise Hazard Analysis
- Must document the analysis...
- ...and response to analysis.
- Use FMECA forms.
- Several formats and tools.

Documentation

FMECA Worksheet

System: Date: Author: Approved by:

Function	Failure Mode	Failure Effect		Severity	Occurrence rate	Detection Method	Notes
		System	Local				

University of Glasgow

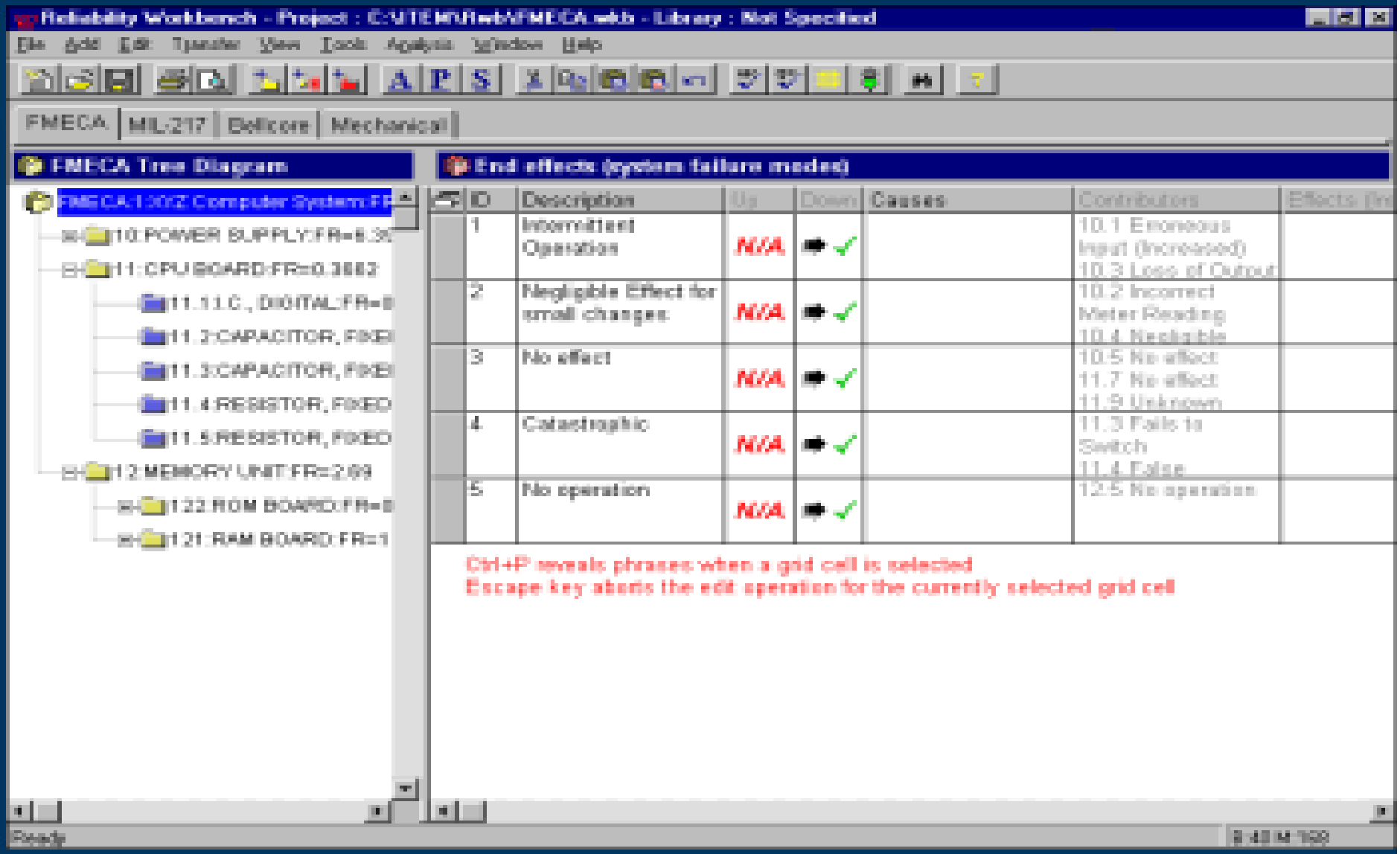
FMECA Tool Support

FMECA, Part PENTIUM PRO

	Item/Description	Name/Function	Failure Mode	Local Effect
1	Pentium Pro Processor. Microprocessor which provides a central processing unit and an internal cache.	Controls the primary operation of the personal computer.	Processor Section Failure	The Pentium Pro Chip Fails.
2			Address Section Failure	The Pentium Pro Chip Fails.
3			Memory Section Failure	Failure of the internal memory of the Pentium Pro causes erroneous information to be generated.
4				
5				
6				
7				
8				

University of Glasgow

FMECA Tool Support



University of Glasgow

Conclusions

- Hazard analysis.
- FMECA/FMEA.
  - qualitative approach;
  - but is it subjective?
- Next more quantitative approaches.

University of Glasgow

Any Questions…