Fault Modeling

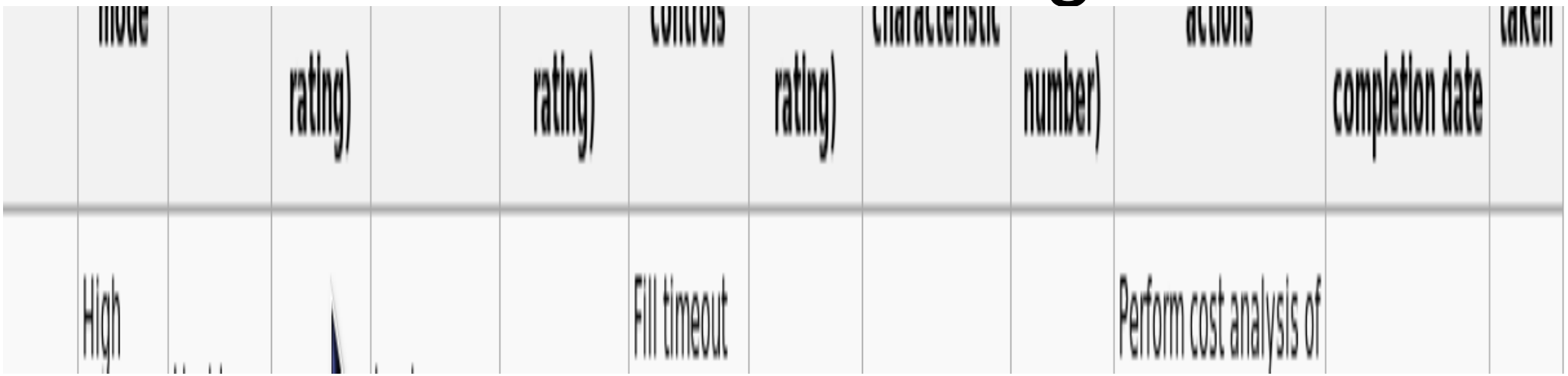
- FMECA – spreadsheet-driven fault modeling
  - Enumerate fault scenarios, effects, and criticality
  - Use the table to drive analysis and testing

From Mil Relibility Guide:

No.	Unit	Function	Failure Mode	Probable Cause	Effect On			Interrupt ?	Crit	Action
					Unit	Sub	System			
1	Output	Outputs file into	Output is incorrect	Inputs are invalid and not detected	n/a	none	mission degraded	no	II	lab repair
2	Output	Outputs file into	Output is incorrect	Inputs are correct but not stored properly	n/a	none	mission degraded	no	II	lab repair
3	Output	Outputs file into	Output is incorrect	Values are not computed to spec	n/a	none	mission degraded	no	II	lab repair

FIGURE 9.8-1: EXAMPLE OF SOFTWARE FMECA

Fault Modeling



- Wikipedia example (FMEA, with risk priority numbers -- 1-10 each)
  - severity
  - occurrence
  - detection
- RPN = S x O x D
- Help prioritize the faults and direct development efforts.

Questions

- Is the spreadsheet a good modeling format? It helps with systematic coverage and categorization of all faults we can think of.
- Modeling use cases – what questions must be answered by the models?
  - To what level have we detailed the causes/effects of each fault?
  - To what degree have we mitigated each fault?
  - Do we know fault severity, occurrence, and detectability?
  - How does the FMECA worksheet information correlate with what we have in the ESMoL model? What information do we need to add to ESMoL?
- Use cases – can we use statistical model checking with fault scenarios to analyze confidence for the design?

Questions

- What about test coverage?
- What information needs to go into test descriptions?
- Modeling: Is it simpler/useful to simply refer to external test specs?