MISSION READY SOFTWARE
SOFTREL LLC

sales@softrel.com
321-514-4659
http://missionreadysoftware.com

Question: Can I conduct a safety analysis and a software FMEA in one step? Answer: Yes, the failure modes for safety related failures are also failure modes for mission failures

Software Safety Analysis as Per AOP-52 and JSSSH Training

This one-day training class covers the methods for assessing the safety of a software system based on AOP-52 section 4 and the Joint Services Software Safety Handbook Appendix E. The below root causes for software safety related issues are summarized below. Note that these are also root causes for mission related failures and aren't necessarily specific to either safety critical software or to munitions.

Criteria	**Referenced docs**	
	AOP52	**JSSSH**
System design requirements	4.1	E.3
Designed safe states	4.1.3	E.3.1, E.3.18
Safe state return	4.1.4	E.3.2
Circumvent unsafe conditions	4.1.5	E.3.9
External hardware failures	4.1.6	E.3.7
Safety kernel failure	4.1.7	E.3.8
Fallback and recovery	4.1.8	E.3.10
Computing system failure	4.1.9	
Maintenance interlocks	4.1.10	E.4.4
Restoration of interlocks	4.1.11	E.3.5
Simulators	4.1.12	E.3.11
Logging safety errors	4.1.13	E.3.12
Positive feedback mechanisms	4.1.14	E.3.13
Peak load conditions	4.1.15	E.3.14
Ease of maintenance	4.1.16	E.3.4
Endurance issues	4.1.17	E.3.15
Error handling	4.1.18	E.3.16
Standalone processors	4.1.19	E.3.3
I/O registers	4.1.20	E.3.6
Power up initialization requirements		E.4
Power up initialization	4.1.21	E.4.1
Power down transition	4.1.22	
Power faults	4.1.23	E.4.2
System level check	4.1.24	E.4.5
Primary computer failure		E.4.3
Control flow defects		E.4.6
Redundancy management	4.1.25	E.3.17
Isolation and Modularity		E.3.19

sales@softrel.com
321-514-4659
http://missionreadysoftware.com

Criteria	Referenced docs	
	AOP52	JSSSH
Self check design requirements and guidelines	4.3	E.6
Watchdog timers	4.3.1	E.6.1
Memory checks	4.3.2	E.6.2
Fault detection	4.3.3	E.6.3
Operational checks	4.3.4	E.6.4
Safety related events and safety related functions	4.4	
Safety critical computing system functions protection requirements and guidelines	4.5	E.7
Safety degradation	4.5.1	E.7.1
Unauthorized interaction	4.5.2	E.7.2
Unauthorized access	4.5.3	E.7.3
Safety kernel ROM	4.5.4	E.7.4
Safety kernal independence	4.5.5	
Inadvertent Jumps	4.5.6	E.7.5
Load data integrity	4.5.7	E.7.6
Operational reconfiguration integrity	4.5.8	E.7.7
Interface design requirements	4.6	E.8
Feedback loops	4.6.1	E.8.1
Interface control	4.6.2	E.8.2
Decision statements	4.6.3	E.8.3
InterCPU communications	4.6.4	E.8.4
Data transfer messages	4.6.5	E.8.5
External functions	4.6.6	E.8.6
Input reasonableness checks	4.6.7	E.8.7
Full-scale representations	4.6.8	E.8.8
Human interface	4.7	E.9
Operator/computing system interface	4.7.1	E.9.1
Computer human interface issues	4.7.2	
Processing cancelation	4.7.3	E.9.2
Hazardous function initiation	4.7.4	E.9.3
Safety related displays	4.7.5	
Operator entry errors	4.7.6	E.9.4
Safety critical alerts	4.7.7	E.9.5
Unsafe situation alerts	4.7.8	E.9.6
Unsafe state alerts	4.7.9	E.9.7
Critical timing and interrupt functions	4.8	E.10
Safety critical timing	4.8.1	E.10.1
Valid interrupts	4.8.2	E.10.2
Recursive loops	4.8.3	E.10.3
Time dependency	4.8.4	E.10.4

sales@softrel.com
321-514-4659
http://missionreadysoftware.com

Target Audience

Software engineers, software test engineers, software safety engineers

Each course attendee is able to…

- Analyze each software use case, requirement statement, design statement and determine which of the AOP-52 and JSSSH compliance criteria is applicable, met, not met.
- Analyze the effects on safety, mission or both.

Table of contents

The topics for the one-day course are shown below.

Topic	Estimated time
Greetings and introductions	15 minutes
Overview of AOP-52 section 4 and JSSSH Appendix E	45 minutes
Overview of the basic failure modes for software including faulty functionality, faulty timing, faulty sequencing, faulty error handling, faulty data, faulty processing, etc.	1 hour
Discussion of each of the generic safety criteria in these documents and how to assess it in the software documentation	5 hours
How to use the safety analyses in conjunction with other analyses such as the software FMEA	30 minutes

Related Products and Services

Related products	Related services
Requs AI Predict Software FMEA	• Software FMEA analysis service.

Pricing and training options

This class is available as an on-site option or private remote instructor guided. Call 321-514-4659 for a quotation.