COM4506/6506: Testing and Verification in Safety Critical Systems

Dr Ramsay Taylor

Contents

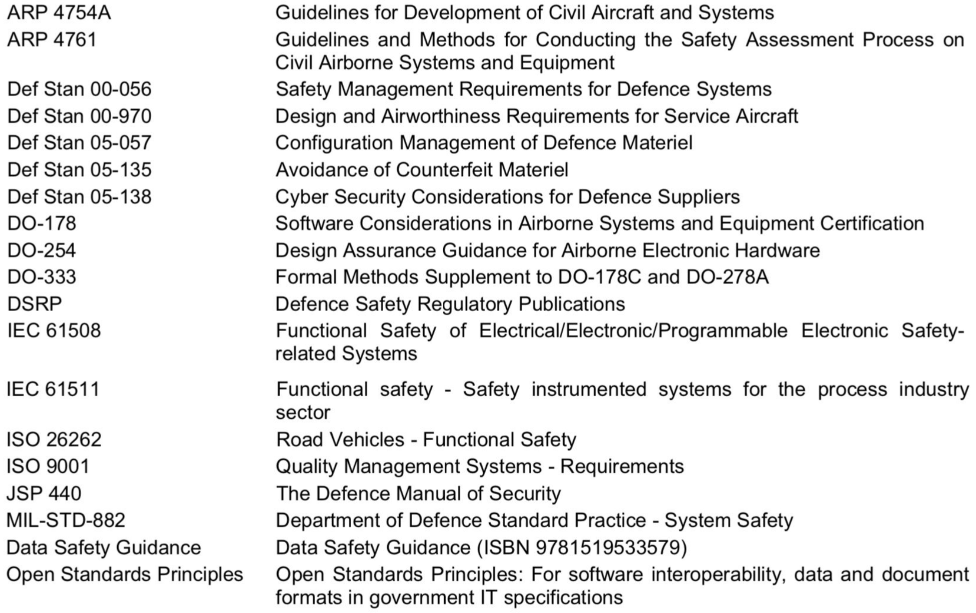
- Is my System Safety Critical?
- Is my System *very* Safety Critical?
- Do I have to have a *technical* solution to that?

What is and isn’t “Safety Critical”?

A safety-critical system is a system whose failure or malfunction may result in one or more of the following outcomes:

- death or serious injury to people
- loss or severe damage to equipment/property
- environmental harm

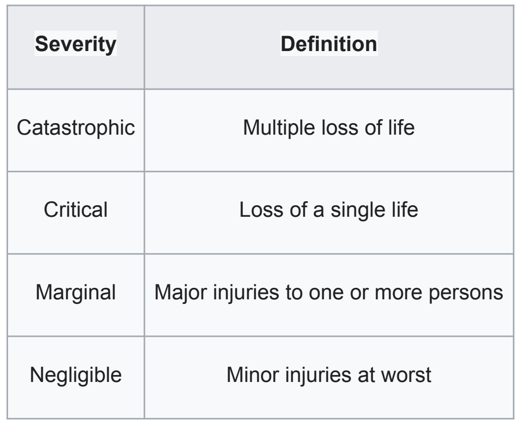
Says Who?



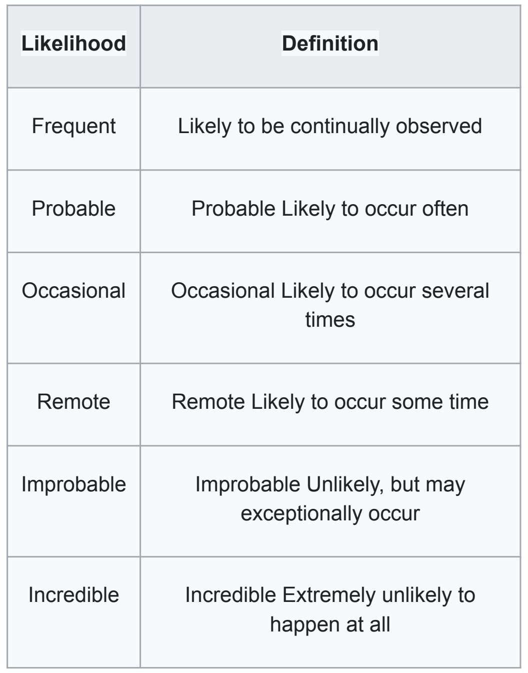
ARP 4754A	Guidelines for Development of Civil Aircraft and Systems
ARP 4761	Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment
Def Stan 00-056	Safety Management Requirements for Defence Systems
Def Stan 00-970	Design and Airworthiness Requirements for Service Aircraft
Def Stan 05-057	Configuration Management of Defence Materiel
Def Stan 05-135	Avoidance of Counterfeit Materiel
Def Stan 05-138	Cyber Security Considerations for Defence Suppliers
DO-178	Software Considerations in Airborne Systems and Equipment Certification
DO-254	Design Assurance Guidance for Airborne Electronic Hardware
DO-333	Formal Methods Supplement to DO-178C and DO-278A
DSRP	Defence Safety Regulatory Publications
IEC 61508	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems
IEC 61511	Functional safety - Safety instrumented systems for the process industry sector
ISO 26262	Road Vehicles - Functional Safety
ISO 9001	Quality Management Systems - Requirements
JSP 440	The Defence Manual of Security
MIL-STD-882	Department of Defence Standard Practice - System Safety
Data Safety Guidance	Data Safety Guidance (ISBN 9781519533579)
Open Standards Principles	Open Standards Principles: For software interoperability, data and document formats in government IT specifications

From: Def Stan 00-055

How critical is this System?



Severity	Definition
Catastrophic	Multiple loss of life
Critical	Loss of a single life
Marginal	Major injuries to one or more persons
Negligible	Minor injuries at worst



Likelihood	Definition
Frequent	Likely to be continually observed
Probable	Probable Likely to occur often
Occasional	Occasional Likely to occur several times
Remote	Remote Likely to occur some time
Improbable	Improbable Unlikely, but may exceptionally occur
Incredible	Incredible Extremely unlikely to happen at all

From IEC 61508

How critical is this System?

Frequency/ Severity				
	Catastrophic	Critical	Marginal	Negligible
Frequent	1	1	1	2
Probable	1	1	2	3
Occasional	1	2	3	3
Remote	2	3	3	4
Improbable	3	3	4	4
Incredible	4	4	4	4

From IEC 61508

What are we supposed to do about it?

Mitigate the hazards!

- Training
- Testing
- Verification
- Design
- ...Do something else!

Are we supposed to make it completely safe?

9.3 PE Risk Reduction and Mitigation

The Contractor shall ensure that, for each configuration of the PE, the PSS Risk to Life posed by the known impact of normal or unintended behaviour of the PE is addressed by;

a) Implementation and documentation of appropriate risk reduction or mitigation, and;

b) Provision of evidence that PE Safety Requirements are satisfied (Objectives 3 and 4).

DEF STAN 00-055 Part 1 Issue 4

Are we supposed to make it completely safe?

Risks cannot be totally removed from most Safety Critical Systems.

Instead, you need to aim for ***As Low As Reasonably Practicable (ALARP)***

This will always be a balance between what could possibly be done, the requirements of the system, and *cost.*

Pricing Human life

Value of Preventing a Fatality (VPF) is often misunderstood to mean that a value is being placed on a life. This is not the case. It is simply another way of saying what people are prepared to pay to secure a certain averaged risk reduction. A VPF of £1,000,000 corresponds to a reduction in risk of one in a hundred thousand being worth about £10 to an average individual. VPF therefore, is not to be confused with the value society, or the courts, might put on the life of a real person or the compensation appropriate to its loss

(Health and Safety Executive, 2001:*Reducing Risks, Protecting People*).

Whole Life Safety

The “Harm” caused by a system doesn’t end when you turn it off.

Disposal costs mostly relate to the physical and electronic components of a system, rather than the software.

However, Software *evolution* can introduce safety concerns and/or violate the original mitigation strategies.

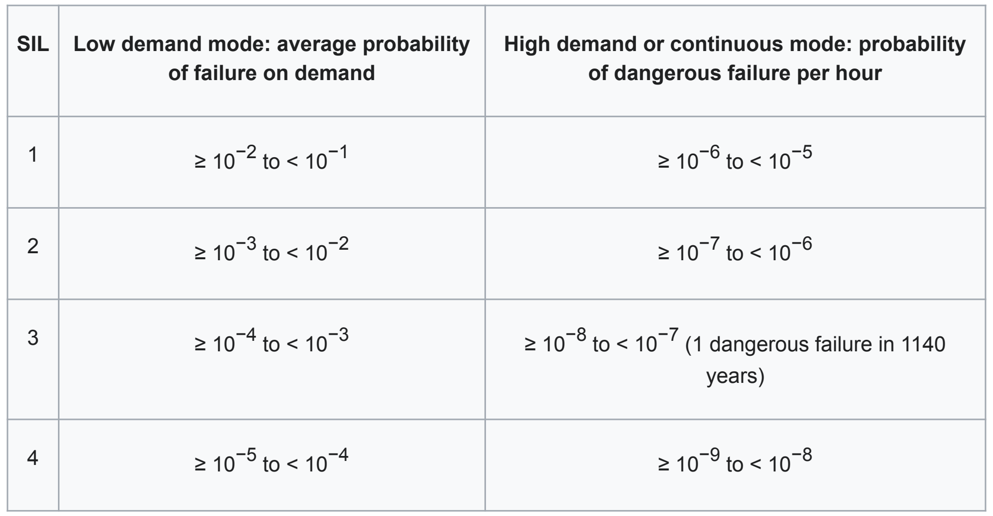
How critical is this System *Function*?

Individual Software components will be responsible for particular parts of the system - and they may be responsible for *mitigating* some of the risk.

Software doesn’t *fail* in the same way that traditional engineering products do (fatigue, manufacturing flaws, etc.).

We can still quantify the required robustness of Software components based on their probability of failure.

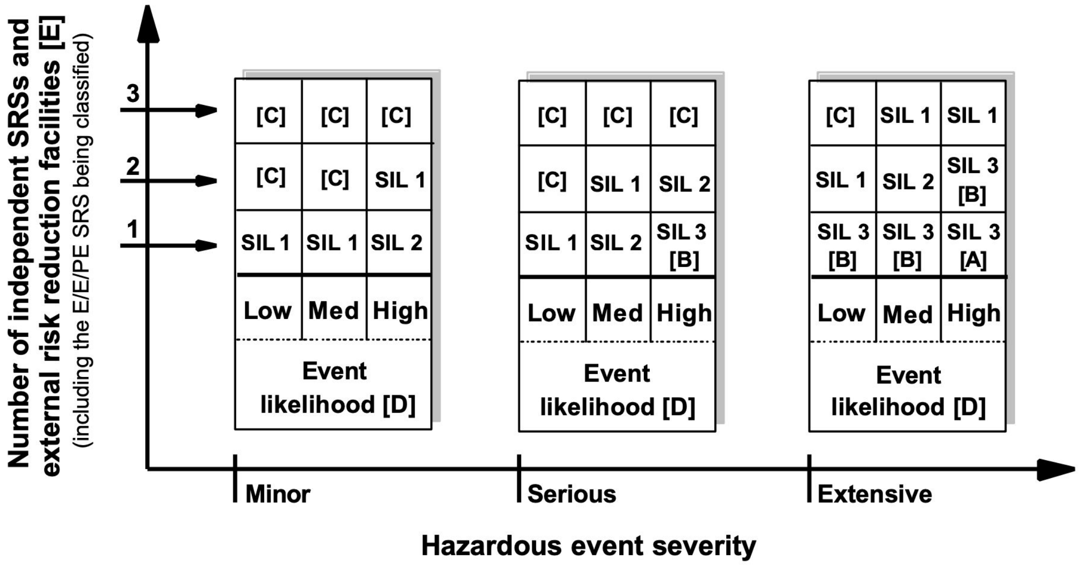
How critical is this System *Function*?



SIL	Low demand mode: average probability of failure on demand	High demand or continuous mode: probability of dangerous failure per hour
1	≥ 10^{-2} to < 10^{-1}	≥ 10^{-6} to < 10^{-5}
2	≥ 10^{-3} to < 10^{-2}	≥ 10^{-7} to < 10^{-6}
3	≥ 10^{-4} to < 10^{-3}	≥ 10^{-8} to < 10^{-7} (1 dangerous failure in 1140 years)
4	≥ 10^{-5} to < 10^{-4}	≥ 10^{-9} to < 10^{-8}

From IEC 61508

How critical is this System *Function*?



Number of independent SRSs and external risk reduction facilities [E]
(including the E/E/PE SRS being classified)
Hazardous event severity
Event likelihood [D]

	Minor			Serious			Extensive		
	Low	Med	High	Low	Med	High	Low	Med	High
3	[C]	[C]	[C]	[C]	[C]	[C]	[C]	SIL 1	SIL 1
2	[C]	[C]	SIL 1	[C]	SIL 1	SIL 2	SIL 1	SIL 2	SIL 3 [B]
1	SIL 1	SIL 1	SIL 2	SIL 1	SIL 2	SIL 3 [B]	SIL 3 [B]	SIL 3 [B]	SIL 3 [A]

From IEC 61508

Summary

- Safety Critical Systems are those with *hazards* that are life or property destructive
- We can classify *how* critical a system is, and that might inform how far we go in verifying it
- We will *mitigate* the hazards, but this doesn't have to be done with Software Testing!
- Ultimately, you will have to present a *Safety Case* and it will be a combination of arguments that get it accepted.