Lecture 4 — Safety Critical Standards

David J. Pearce

School of Engineering and Computer Science
Victoria University of Wellington

Safety Standards

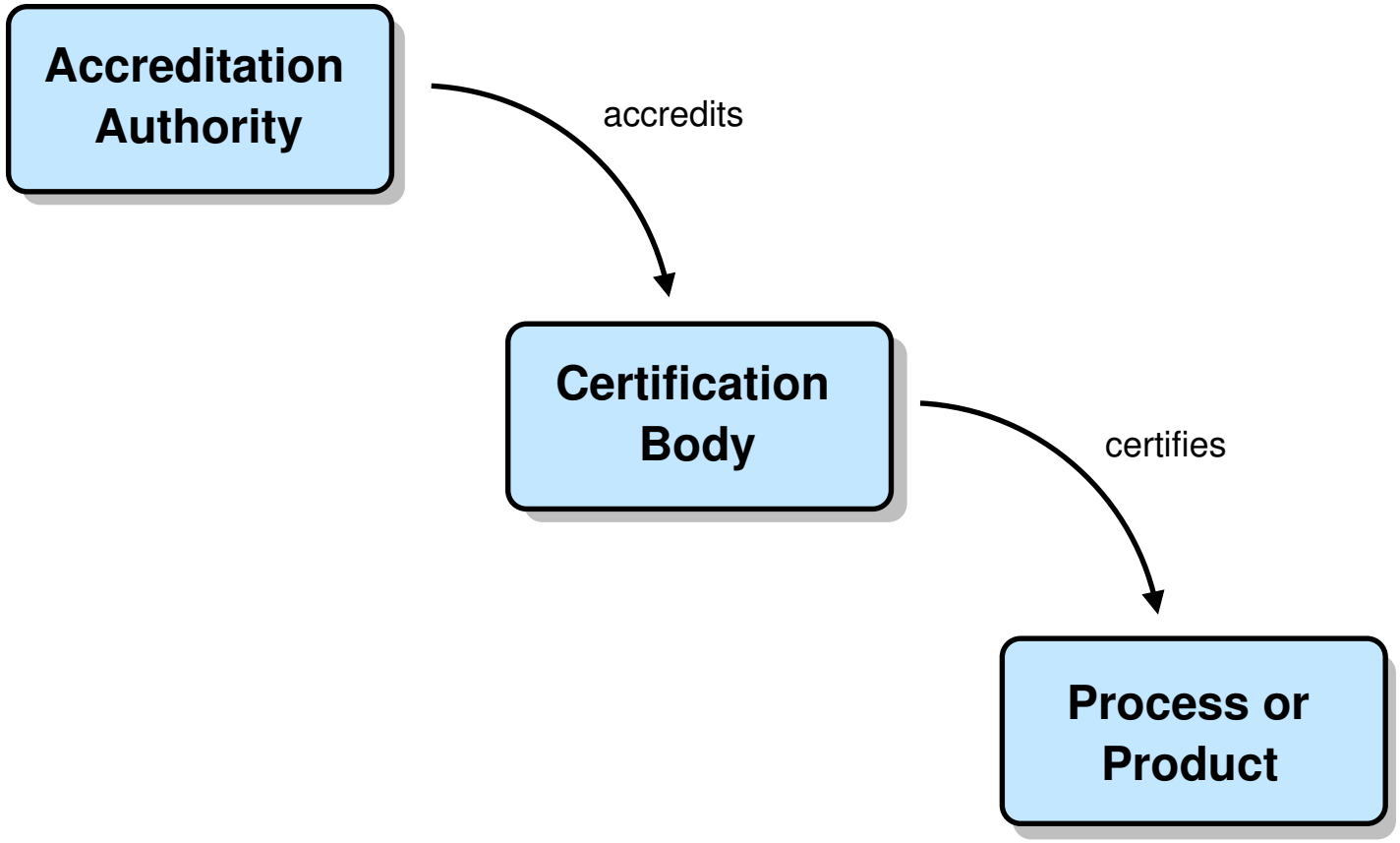
"*It is said that the good thing about standards is that, if you don't like one, then there is always another that you can apply instead.*"

–Hobbs'16

"*All too often, writers of standards focus on question of what constitutes good practice, and lose sight of what the followers of those standards truly need to demonstrate in order to show safety. Safety is demonstrated not by compliance with prescribed processes, but by assessing hazards, mitigating those hazards, and showing that the residual risk is acceptable.*"

–Rae'07

Accreditation and Certification



(image reproduced from Hobbs'16)

Why Standards?

“In some areas, the need for standards is very clear. If there were no standards defining the shape and size of the electrical sockets in our houses, then it would be impossible to buy an electrical device with confidence that it would connect to the electrical supply”

“Historically, the creation of standards ... has often been driven by disasters. A disaster occurs and the public demands it never occur again.”

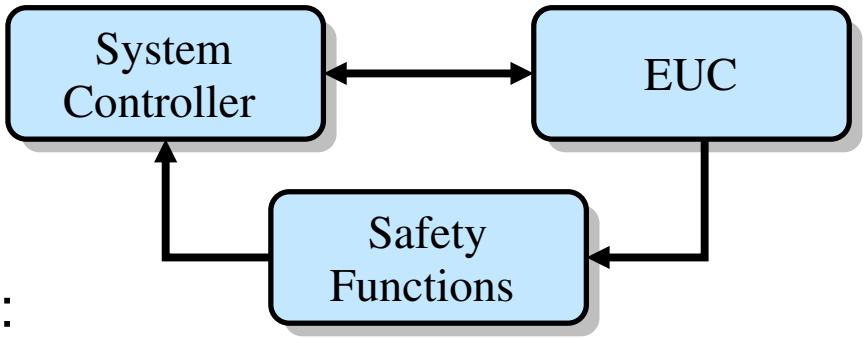
–Hobbs’16

Safety Critical Standards: *Overview*

- **IEC 61508, Software Considerations in Airborne Systems and Equipment Certification** *(generic standard)*.
- **ISO 26262, Road vehicles - Functional safety** *(adaptation of IEC 61508 for automotive Electric/Electronic Systems)*.
- **DO-178C, Software Considerations in Airborne Systems and Equipment Certification**.
- **DEFSTAN 00-55, Requirements for Safety Related Software in Defense Equipment** *(UK Department of Defense)*.

IEC 61508: *Overview*

"*IEC 61508 and its derivatives are firmly rooted in the idea that the study of device safety is the* **study of device failure**." –Hobbs'16



- Assumptions:
  - **Some equipment** providing a function (Equipment Under Control)
  - A **system controller** for that equipment
  - One or more **safety function(s)** which mitigate the **risk**

See "*An Introduction to the Safety Standard IEC 61508*", Redmill, Journal of the System Safety Society, 1999.

Functional Safety: *What is It?*

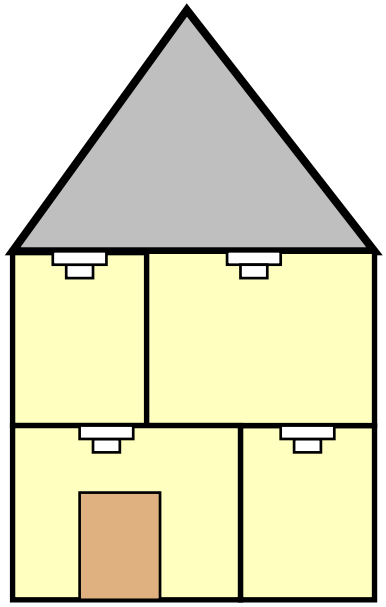
functional safety*: something must continue to* function *in order to keep the system safe*

–Hobbs'16

Functional safety *is the part of the overall safety of a system or piece of equipment that depends on the system or equipment operating correctly in response to its inputs, including the safe management of likely operator errors, hardware failures and environmental changes*

–Wikipedia

Functional Safety: *What is It?*



Tenants must:

- not damage, remove, or disconnect a smoke alarm
- replace dead batteries during the tenancy if there are older-style smoke alarms with replaceable batteries
- let the landlord know if there are any problems with the smoke alarms as soon as possible.

—tenancy.govt.nz

Hazards and Risk: *What are they?*

"The iceberg is the **hazard***; the* **risk** *is that a ship will run into it. One* **mitigation** *might be to paint the iceberg yellow to make it more visible."*

–Hobbs'16

Hazard

Potential source of harm caused by equipment

Risk

Probability of a hazardous event combined with its severity

Mitigation

Attempt to reduce the risk of a hazardous event

- **IEC61508**: *Can never be perfect safety (i.e. zero risk)*

IEC61508: *Likelihood of Occurence*

Category	**Definition**	**Failures / yr**
Frequent	Many times in system lifetime	> 0.001
Probable	Several times in system lifetime	$0.0001 - 0.001$
Occasional	Once in system lifetime	$0.0001 - 0.00001$
Remote	Unlikely in system lifetime	$10^{-5} - 10^{-6}$
Improbable	Very unlikely to occur	$10^{-6} - 10^{-7}$
Incredible	Cannot believe that it could occur	$< 10^{-7}$

- Q) How do we **estimate** probability of software failure?

IEC61508: *Consequences*

Category	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	Catastrophic	Critical	Marginal	Negligible
Frequent	I	I	I	II
Probable	I	I	II	III
Occasional	I	II	III	III
Remote	II	III	III	IV
Improbable	III	III	IV	IV
Incredible	IV	IV	IV	IV

I= *Unacceptable in any circumstance*

II= *Undesirable: tolerable only if mitigation impracticable or costs grossly disproportionate to improvements*

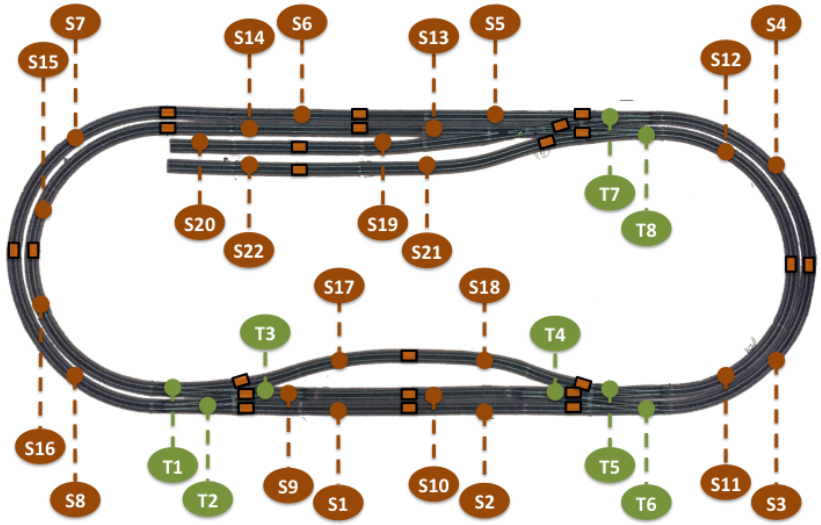
III= *Tolerable if cost of mitigation would exceed improvement*

IV= *Acceptable as it stands, though it may need to be monitored*

DO-178C: *Severity Classifications*

Classification	Effect	Likelihood
Catastrophic	*Multiple casualties with likely loss of airplane*	Extremely Improbable
Hazardous	*Reduced capability of airplane or crew resulting in large reduction in safety margins or extreme increase in crew workload or serious/fatal injury to small number of occupants*	Extremely Remote
Major	*Reduced capability of airplane or crew resulting in reduction in safety margins or significant increase in crew workload or physical distress to passengers including possible injuries*	Remote
Minor	*Does not significantly reduce airplane safety, and involves crew actions well within capability or some physical discomfort to passengers.*	Reasonably Probable
None	*Has no effect on safety*	Probable

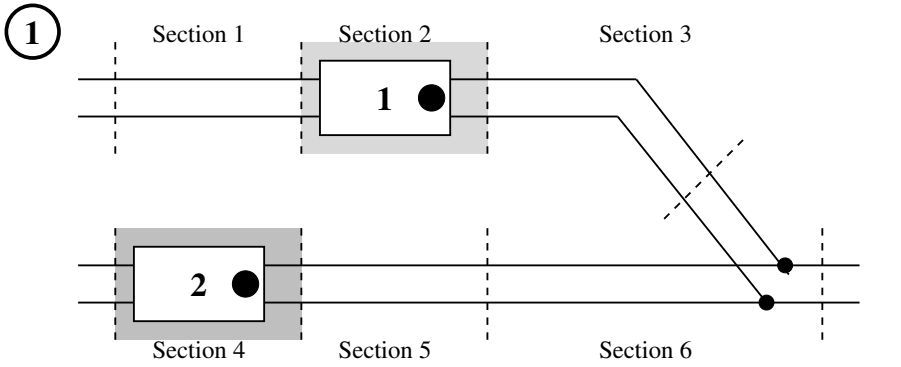
An Example — A (Model) Railway

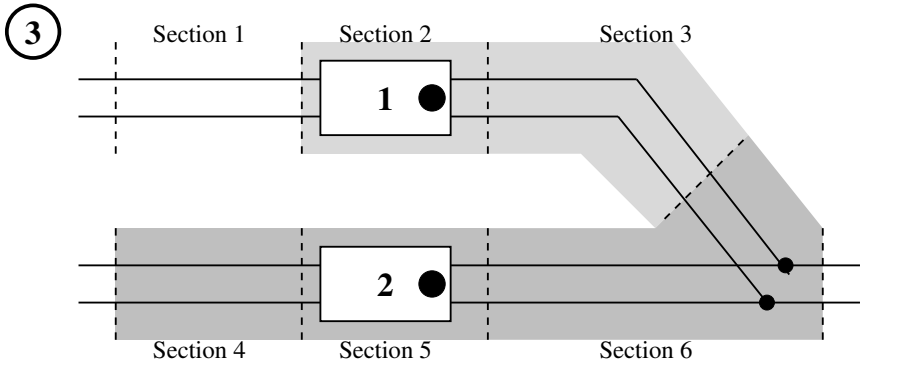


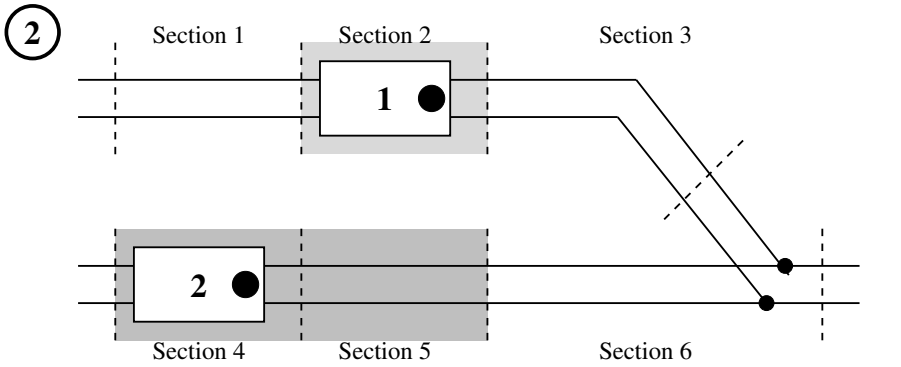
- Track broken up into 22 distinct **sections** to prevent collisions
- Layout consists of eight software controlled **turnouts**
- Layout includes one **diamond crossing**

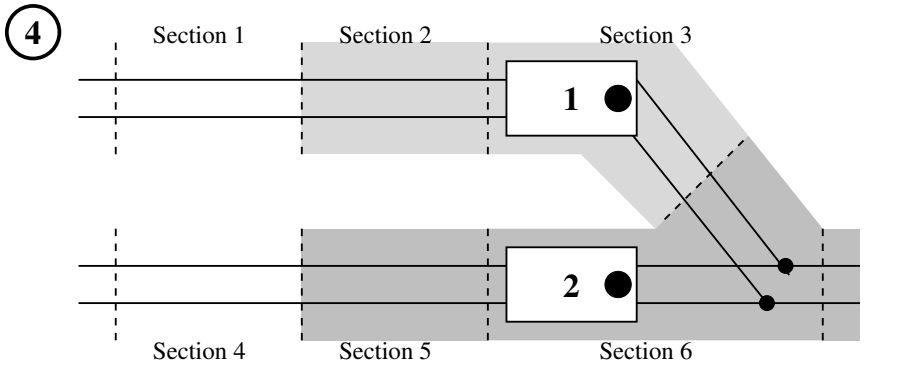
See `https://www.youtube.com/watch?v=RurklTTb6Xg`

An Example — Interlock Sequence









An Example — Hazards and Risks

- *What is the Equipment Under Control?*
- *What is the System Controller?*
- *What are the Safety Functions?*
- *What are the Hazards?*
- *What are the Risks?*