Table of Contents

1. Functional Safety Analysis

Summary:
Functional Safety Analysis is an approach that assesses all the system functions to determine the hazards associated with what the system does. The purpose of Functional Safety Analysis is to identify hazards associated with both the correct and incorrect operation and non-operation of the system, lower level functions and human functions.

1.1. Functional Safety Analysis

1.1.1. Description and Purpose

1.1.1.1.

Functional Safety Analysis is an approach that assesses all the system functions to determine the hazards associated with what the system does.

1.1.1.2.

The purpose of Functional Safety Analysis is to identify hazards associated with both the correct and incorrect operation and non-operation of the system, lower level functions and human functions.

1.1.1.3.

Functional Safety Analysis should be applied to all functions, including those listed below, and should be carried out to the lowest level functions identified in the design:

- Principal Functions
- Subsidiary and Non-obvious Functions
- Warning Functions
- Warnings that provide operator indications and controls
- Functions that protect against hazards
- Functions provided by human operator
- Functions that moderate the effects of failure of other functions

1.1.1.4.

Functional Safety Analysis should examine all functional failures that may give rise to credible hazards, including:

- Those following directly from the behaviour of the function or component being evaluated
- Those due to the effects on another connected function or component (e.g. hazards due to the loss of an oil cooling function)
- Those due to indirect influence (e.g. hazards due to the generation of electro-magnetic interference (EMI) by a component when it has failed)

1.1.1.5.

The first step of Functional Safety Analysis is to create a functional representation of the system, defining the purpose and behaviour of all functions. It is also necessary to define the operational phase of the system, since the effect of a system failure will depend on what the system is doing at the time. All phases of operation should be included; these will include maintenance and emergency phases if applicable.

1.1.1.6.

For each identified function, a set of failure conditions, based on the aspects below should be defined:

- **Normal performance:** What hazards might be associated with the normal operation of the system functions ?
- **Specific degraded performance:** What hazards are introduced if the system is functionally degraded but still active, for example reduced performance from a ventilation system
- **Incorrect functioning, including inadvertent functioning:** An example might be a Radhaz transmission failure, as a result of a physical failure of the interlock, resulting in the radar transmitting when not expected.

- **Absence of function:** There may be, for example, a loss of a function which may result in the inability of the system to complete a required task, or part of that task (such as being able to turn a ship to Port but not to Starboard).
- **Human error:** This may be due to such factors as stopping an activity too soon or performing the right activities, but in the wrong order.
- **Mis-timing of the function occurring,** that is, sequencing too early or too late.

1.1.1.7.

For each of the operational phases, the effects of the failure conditions upon the system should be assessed in order to determine, record (and verify) associated risk factors (severity and probability). Functional Safety Analysis can be supported by a functionally based Failure Modes Effects and Critical Analysis (FMECA) or Fault Tree Analysis (FTA).

1.1.2. When It Might be Used

1.1.2.1.

Functional Safety Analysis should be performed once the required functions have been defined and it should be refined as the implementation of the functions develops. It is therefore an iterative activity that can be refined throughout the project lifecycle as more detail on system functions and sub-functions becomes available.

1.1.3. Advantages, Disadvantages, and Limitations to The Defence Sector or The Particular Domain

1.1.3.1.

Advantages

- Functional Safety Analysis provides an approach for identifying system hazards at an early stage in the procurement cycle when the means of realising functions (e.g. hardware, software or human action) has not been defined.
- Functional Safety Analysis can be used to concentrate effort on critical areas of the system early in the development, leading to fundamental decisions such as whether to use software to realise a function and where redundancy is appropriate.
- Appropriate Safety requirements, including Safety Integrity Levels, can be derived through Functional Safety Analysis.
- The process can be applied to both software and hardware functions.

1.1.3.2.

Disadvantages

- Functional Safety Analysis is not good at examining hazards which relate to system components or system location. It must therefore be used in combination with other techniques.
- The value of Functional Safety Analysis is dependent on the quality of the functional description of the system. If subsidiary or non-obvious functions are not in the functional description, the hazard identification may be incomplete.
- Environmental conditions may alter the effects of failure and may need to be considered e.g. the effects of the loss of “anti-lock” on a car’s brakes may be more serious on wet or icy roads.
- Domain specific knowledge is required to effectively perform Functional Safety Analysis.
- Any interdependence or inter-relationship of system functions needs to be carefully identified so that they are accounted for in the analysis.

1.1.4. Sources of Additional Information

1.1.4.1.

A list of additional information (e.g., Standards, textbooks, and websites) includes but is not limited to:

- SAE ARP 4761: Excellence in Procedure for Safety Assessment [1]
- International Electrotechnical Comission (IEC) 61508 Series [1] (Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems).

1.1.5. Additional Comments

1.1.5.1.

A list of software programs (e.g., Computer tools and related techniques) includes but is not limited to:

- SETTA, a toolset for Automated Safety Analysis designed by DaimlerChrysler, although a simple spreadsheet can support Functional Safety Analysis effectively.

1.1.5.2.

Example:

(Based on SAE ARP 4761: Excellence in Procedure for Safety Assessment [1] Appendix L)

An aircraft may be assessed as having the following operational functions:

- Control Thrust
- Control Flight Path
- Determine Orientation
- Determine Heading & Position
- Control Aircraft on the Ground
- Control Cabin Environment

1.1.5.3.

The function “Control Aircraft on the Ground” can be divided into a number of lower level functions including “Decelerate Aircraft on the Ground”. The functional failure condition considered in this example is loss of deceleration capability (other functional failures could be “reduced deceleration capability” or “inadvertent deceleration”). The phases of operation where deceleration of the aircraft on the ground is required are: Taxi, Landing, and Rejected Takeoff.

1.1.5.4.

The example is documented below in a Functional Block Diagram (FBD) format similar to the FMECA. The example references Failure Condition Severity Classifications and Probabilities, which should be defined.

1.1.5.5.

Example data sheet:

Function	Failure Condition (Hazard description)	Phase	Effects of Failure on Aircraft / Crew	Classification (Severity)	References	Verification / Target Probability
Decelerate Aircraft on the Ground.	1a. Unannunciated loss of deceleration capability.	Landing / Rejected Take Off	Crew unable to decelerate aircraft resulting in high speed overrun.	Catastrophic		Aircraft Fault Tree
	1b. Unannunciated loss of deceleration capability.	Taxi	Crew unable to stop the aircraft on the taxi way or gate, resulting in low speed contact with terminal, aircraft or vehicle.	Major		Remote (1.0 E-5 or better
	1c. Unannunciated loss of deceleration capability.	Landing	Crew selects more suitbale airport, notifies emergency ground support and prepares occupants for a landing overrun.	Hazardous	Emergency landing procedures in case of loss of stopping capability.	Aircraft Fault Tree
	1d. Unannunciated loss of deceleration capability.	Taxi	Crew steers the aircraft clear of any obstacles.	No safety effect		Frequent (1.0 or better)

1.2. Version Control

1.2.0.1.

Version 3.0 to 3.1 Uplift

Links within Sources of Additional Information and Additional Comments have been updated.

Version 2.3 to 3.0 Uplift

Major uplift from the Acquisition System Guidance (ASG) to online version.

Source URL: https://www.asems.mod.uk/toolkit/functional-safety-analysis

Links
[1] https://www.asems.mod.uk/ExtReferences