

GUIDANCE MATERIAL:

SAFETY REQUIREMENTS

1 INTRODUCTION

The purpose of this annex is to provide guidance material on the definition, content, phrasing, criteria of eligibility of safety requirements.

2 MORE DETAIL ABOUT SAFETY REQUIREMENTS

2.1 General

Safety requirements are derived from Safety Objectives. Generally, they specify the potential means to mitigate hazards, i.e. to:

- Prevent occurrence of hazards; associated means are:
 - Precautions for system & equipment design, development, procurement and validation
 - Precautions for procedures design and validation
 - Precautions for people training and licensing
- Reduce the severity of their consequences; associated means are addressing:
 - Detection,
 - Protection, (e.g. software barriers and checkings)
 - Recovery (automatic or human intervention; e.g. provide an automatic switch main/fall-back system or specify an operator manual procedure to activate the fall-back system),
 - Graceful degradation (deliver a reduced service in Degraded mode; e.g. specific procedures while in degraded mode, specific operator training for the degraded mode situations, ...),
 - Other.

The term "Safety Requirement" encompasses both:

- safety related requirements to be met by the system as a "product" and
- those safety related actions to be performed through the processes associated to that product.

Thus Safety Requirements include:

- System and element safety requirements derived from quantitative and qualitative Safety Objectives along the safety assessment process (mainly the FHA and PSSA phases), that have to be

integrated in the System Specification and System Design documents (for the HW and SW), in the Training manual (for Human element) or Operating manual (for Procedures element)

- Completion or modification of already existing system requirements (functional, performance, interoperability), in order to ensure compliance with Safety Objectives,
- Specific "safety evidence demands" (stemmed from the approved recommendations issued along the safety assessment process), to be satisfied in the different stages of the product life-cycle, inside the safety assessment process, or externally but correlated to it. Those "safety evidence demands" might concern:
 - Analysis activities to be addressed by the safety assessment itself (e.g. perform a detailed FMEA or perform a reliability prediction for a specific component in order to ensure that the occurrence rate associated to its failure is acceptable; perform a detailed Human Error analysis for a specific procedure) or
 - Analysis activities external to the safety assessment: Code inspection, Maintenance analysis, Operating Procedure analysis, Training analysis, Transition analysis, specific technical assessments (e.g. electromagnetic compatibility, system behaviour under overloaded conditions, R/F frequency interference and jamming, etc.). These activities are identified during FHA, PSSA or SSA phases and their safety related output is collected during those phases and consolidated by the SSA.
 - Assurance levels for SW and HW covering the different stages of the development process: (e.g. SW Development assurance levels), or specific development precautions to be applied for reducing the likelihood of the occurrence of certain failures,
 - Testing activities, defined for the verification of safety objectives and requirements and of assumptions on which certain safety objectives and requirements were founded. Tests have to be integrated in the Unit, System Integration or Factory acceptance tests plans. Safety related issues of those tests might be specified during the FHA and mostly during the PSSA phase, and then verified during Implementation & Integration, when SSA collects and interprets safety related results. Moreover, Site Acceptance tests might cover some safety validation aspects with respect to users expectations, additionally to verification. Safety related issues of these latter tests are specified

during the FHA, PSSA and SSA phases and are verified and, as far as feasible, validated, during Transfer to operations, when SSA collects and interprets safety-related results.

- Simulation activities, defined for the verification of safety objectives and requirements, associated assumptions, and as far as feasible, for validation of those aspects with respect to users' expectations. Safety issues to be addressed by simulation might be specified during the FHA, PSSA and SSA phases, simulations might be performed any time before Transfer to operations, and SSA collects and interprets safety-related results,
- Demonstration activities, mainly represented by safety-related aspects addressed during trials, aimed at the system safety validation with respect to users' expectation and at the confirmation of some assumption validity. Safety issues to be addressed by trials might be specified during the FHA, PSSA and SSA phases, trials might be performed any time before Transfer to operations, and SSA collects and interprets safety-related results,
- Examination activities, represented by inspections, audits and reviews, can be performed all along the system lifecycle.

In conclusion, some Safety Requirements are intended to directly contribute to the reduction of the risk associated to specific hazards, whilst others represent safety evidence demands, which once satisfied, provide evidence that specific safety requirements are met or that associated assumptions are well founded.

Each Safety Requirement has to be recorded and made traceable to the Safety Objective (and consequently the hazard(s)) that justifies its definition.

The implementation of Safety Requirements has to be monitored along the safety assessment process and traced in SSA documents (usually the Hazard Log). Demands for Safety Evidence will have to be satisfied at different stages of the product life cycle, then their results will be collected and integrated by the SSA process.

2.2 People

People (human) element safety requirements address:

- The training process (specific safety-related aspects to be addressed by manuals, simulations, etc. or by the organisation of that process), including the competency and performance checking

- The licensing process,
- The staffing levels, rostering, call-out arrangements, specific skills/qualifications required for systems operation and maintenance, etc.

Note that HMI safety requirements concern the equipment, although their specification and verification & validation is strongly connected to the human element.

Generally, Safety Requirements for Human Element will take the form of training requirements for using the new automated system or procedure.

In a highly automated environment, the training of ATCO should address the functioning of the automated system as well as its limitations (to avoid over reliance on the automated system).

Hazard analysis results should be used also in ATCO training to point out potential hazards and how they are controlled in the design of the automated system or operational procedures.

2.3 Procedures

Procedure safety requirements address:

- Procedures design constraints and recommendations (e.g. provide a recovery action inside a safety related procedure, like "pilot should readback clearance"; design a specific fall-back procedure to cope with a system degradation, etc.),
- The procedures development and verification & validation process.

SAAP (Safety Assessment of ATM Procedures) is in charge of developing the Procedure Assurance Level.

The part of SAAP dealing with the allocation of PAL is the following:

The following steps should be performed to allocate a PAL:

1. Identify the likelihood that, once the procedure fails, this procedure failure can generate an end effect which has a certain severity (do that for each effect of a hazard) (See figure 2.3.1);
2. Identify the PAL for that couple (severity, likelihood) using the matrix here after;
3. This has to be done for all the hazards due to the procedure.

The final PAL of an ATM procedure is the most stringent one.

Effect Severity	1	2	3	4
Likelihood of generating such an effect				
Very Possible	PAL1	PAL2	PAL3	PAL4
Possible	PAL2	PAL3	PAL3	PAL4
Very Unlikely	PAL3	PAL3	PAL4	PAL4
Extremely Unlikely	PAL4	PAL4	PAL4	PAL4

Note: It should be noted that PAL1 is so stringent that it should nearly never be allocated for the following reasons:

1. PAL1 means somehow that the procedure “can directly kill once it fails” as having a Severity1 effect is “Very Possible” (very limited means to mitigate procedure failure(s). This can only be tolerable in extremely exceptional circumstances;
2. PAL1 is so demanding to be satisfied. As the objectives and associated evidences are so stringent, the cost and development duration and effort are very high;
3. Allocating PAL1 means that an extremely low level of performance is accepted. The procedure will be requiring such separation minima, such safety margin, such operational checking that it will be acceptable to use it to expedite traffic only in extremely exceptional circumstances.

It could be the same for PAL2 with of course less stringency.

That is why an objective for PAL 1&2 requests to have the Senior Management signing it (CEO for PAL1 and Director of Operations for PAL2)... because this kind of procedure should not be the recommended practise.

This means that mainly PAL3 and PAL4 will be allocated.

Very Possible: This effect will certainly occur due to procedure failure.

Possible: This effect may happen (it is not unreasonable to expect such effect to happen due to procedure failure).

Very Unlikely: it is not expected to have such an effect more than exceptionally and in some extreme cases throughout the system lifetime.

Extremely Unlikely: Such an effect is not expected to happen throughout the system lifetime.

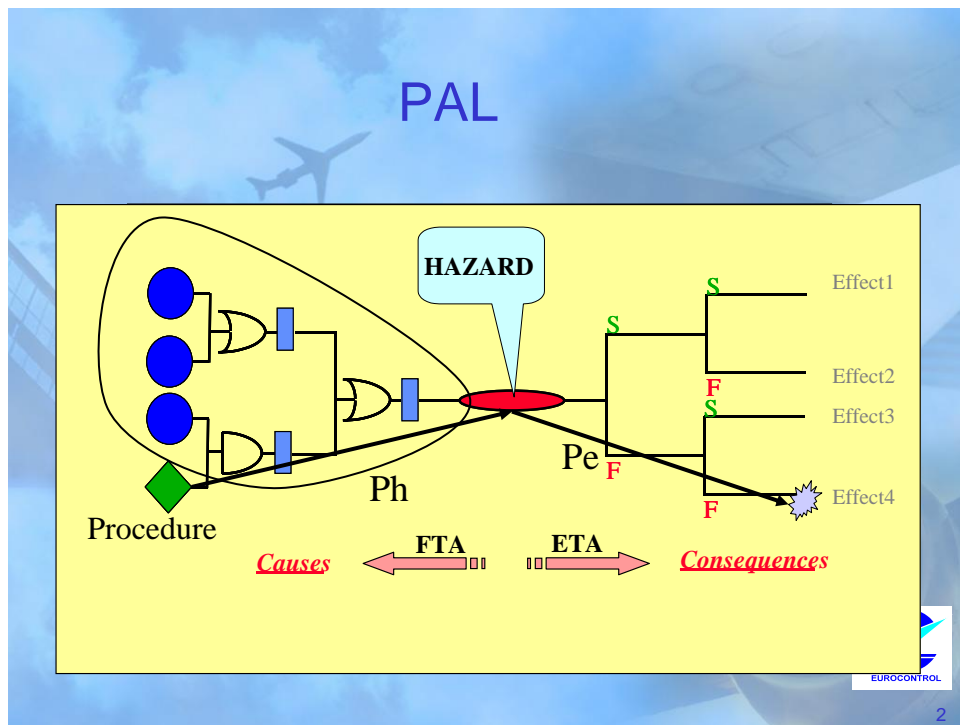


Figure 2.3.1: Relationship between Procedure failure, hazard and effects.

Example of PAL allocation: This procedure will be allocated a PAL = PAL3 as it the most stringent (for both hazards).

1st CASE: Safety Objectives were allocated using Method 1 or 3 (See FHA Chapter 3 Guidance Material G “Methods for Setting Safety Objectives). So all effects, due to ATM Procedure failure, are taken into consideration.

This Procedure will be allocated a PAL = PAL3 as it is the most stringent PAL (for both hazards).

Effect Severity	1	2	3	4
Likelihood of generating such an effect				
Very Possible	PAL1	PAL2	PAL3	PAL4
Possible	PAL2	PAL3	PAL3	PAL4
Very Unlikely	PAL3	PAL3	PAL4	PAL4
Extremely Unlikely	PAL4	PAL4	PAL4	PAL4

Procedure error leading to Hazard1

Procedure error leading to Hazard2:

The way to read the table is the following:

For Hazard 1:

- If it is “Extremely Unlikely” that once the procedure fails, it generates Hazard1 and an effect having a severity 1, then this procedure should be allocated a PAL4;
- If it is “Possible” that once the procedure fails, it generates Hazard1 and an effect having a severity 2, then this procedure should be allocated a PAL3;
- If it is “Very Possible” that once the procedure fails, it generates Hazard1 and an effect having a severity 3, then this procedure should be allocated a PAL3;
- If it is “Very Possible” that once the procedure fails, it generates Hazard1 and an effect having a severity 4, then this procedure should be allocated a PAL4;

For Hazard 2:

- If it is “Extremely Unlikely” that once the procedure fails, it generates Hazard2 and an effect having a severity 1, then this procedure should be allocated a PAL4;
- If it is “Extremely Unlikely” that once the procedure fails, it generates Hazard2 and an effect having a severity 2, then this procedure should be allocated a PAL4;

- If it is “Very Unlikely” that once the procedure fails, it generates Hazard2 and an effect having a severity 3, then this procedure should be allocated a PAL4;
- If it is “Possible” that once the procedure fails, it generates Hazard2 and an effect having a severity 4, then this procedure should be allocated a PAL4.

2nd CASE: Safety Objectives were allocated using Method 2 or 4 (See FHA Chapter 3 Guidance Material G “Methods for Setting Safety Objectives). So only the worst credible scenario which has been used to set safety objectives is taken into consideration.

This ATM Procedure will be allocated a PAL = PAL3 as it is the most stringent PAL (for both hazards which have a worst credible hazard effect having a severity 3).

Effect Severity	1	2	3	4
Likelihood of generating such an effect				
Very Possible	PAL1	PAL2	PAL3	PAL4
Possible	PAL2	PAL3	PAL3	PAL4
Very Unlikely	PAL3	PAL3	PAL4	PAL4
Extremely Unlikely	PAL4	PAL4	PAL4	PAL4

Procedure error leading to Hazard1:



Procedure error leading to Hazard2:



The way to read the table is the following:

For Hazard 1: As the Worst Credible effect of Hazard 1 has a Severity 3 (FHA result), then

- If it is “Very Possible” that once the procedure fails, it generates Hazard1 and an effect having a severity 3, then this procedure should be allocated a PAL3;

For Hazard 2: As the Worst Credible effect of Hazard 1 has a Severity 3 (FHA result), then

- If it is “Very Unlikely” that once the procedure fails, it generates Hazard2 and an effect having a severity 3, then this procedure should be allocated a PAL4.

2.4 Equipment

Product safety requirements include system or component architecture constraints & recommendations (protection, detection, recovery, degraded mode strategy, type of fault tolerance mechanism), and operational contingencies (operational limitations, preventative and corrective maintenance).

Example of issues that might be subject to product safety-related requirements for a HW component:

- Power-up/Power-down,
- Input/output control,
- Operation at the limits,
- Error detection and processing,
- Main/fallback switch-over,
- System degraded modes and transition to/from nominal mode,
- HW watchdog,
- Etc.

Example of issues that might be subject to product safety-related requirements for a SW component:

- Initialisation/stop,
- Input/output control,
- Interface/control of the data flow,
- Data integrity,
- Data management,
- Operation at the limits,
- Error detection and processing,
- Master/slave switch-over,
- Main/fallback switch-over,

- System degraded modes and transition to/from nominal mode,
- HW support,
- Memory sizing and timing,
- FIFOs and buffers,
- Interruptions,
- SW watchdog,
- Etc.

Process safety requirements include specific actions and precautions to be taken during development, verification of implementation or testing (unit, integration, Factory acceptance or Site acceptance). For the Software, the Assurance levels associated to the design, development and verification & validation activities allow to systematically assign a set of process safety requirements to a component, in function of the level of severity associated to its failure (see [EUROCONTROL/Recommendations for ANS SW]).

Equipment safety requirements might be qualitative or quantitative.

Quantitative safety requirements might be deterministic or probabilistic.

- Deterministic: time to switch-over, maximum tolerable time of service interruption, maximum tolerable time for a maintenance intervention, etc;
- Probabilistic:
 - Safety (freedom of accidents),
 - Reliability (mission success or continuity of proper service),
 - Availability (readiness for use),
 - Integrity (correctness of data),
 - Maintainability (ability to be maintained).

Note that quantitative safety objectives and requirements, at a higher level, result into lower level requirements addressing reliability, availability, integrity, and maintainability through allocation process.

2.4.1 Hardware Safety Requirements

The safety requirements allocated to hardware elements of the architecture can be directly derived from the quantitative approach by applying Fault Tree Analysis for example and using the result of the decomposition of the safety objective.

Similar to the assurance levels for SW, HW Assurance Levels are being defined.

2.4.2 Software Assurance Level (SWAL)

2.4.2.1 SWAL Basics

A specific Safety Requirement for software consists in identifying a SoftWare Assurance Level (SWAL), which intends to provide the level of confidence that risks associated with the use of software in safety related ground-based ATM systems, are reduced to an acceptable level.

A SWAL establishes a level of confidence that the overall software lifecycle has been conducted in a sufficiently disciplined manner to limit the likelihood of development errors that could impact safety during operations.

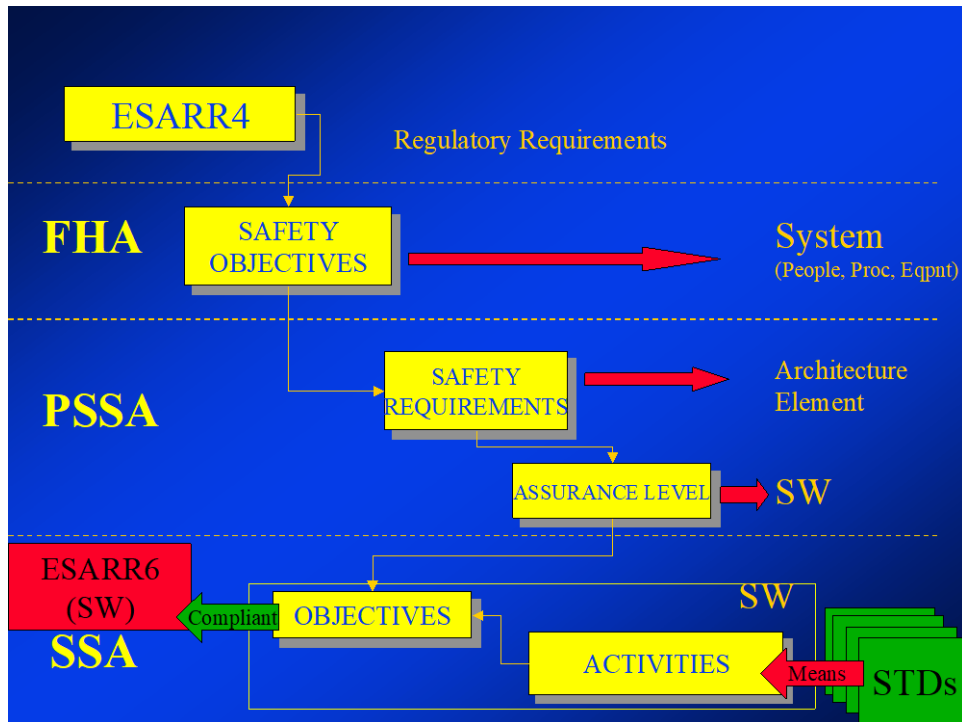


Figure 2.4.2.1: Software Assurance Level allocation

The first step to allocate a SWAL (SoftWare Assurance Level) consists in identifying the (sub-)function embedding/encapsulating this software and its associated safety requirements.

Basics of Mitigation Means Influence

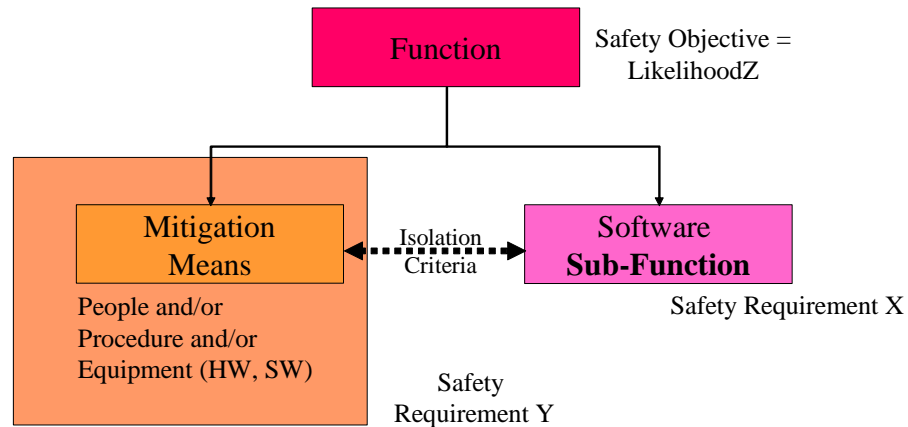


Figure 2.4.2.2: Basics of Mitigation Means Influence

As shown in Figure 2.4.2.2, “Mitigation means” are any kind of internal means (people and/or procedures and/or equipment) designed to control or prevent failures from causing harm and to reduce the expected effects of failures and hazards to a tolerable or acceptable level. In Figure 2.1.1, “Mitigation Means” encompass all the other sub-functions that are part of the function (that has a safety Objective “LikelihoodZ”) and complement the “SW sub-function” to which a SWAL is being allocated.

Figure 2.4.2.2 intends to show that the SWAL definition is commensurate with the Safety Requirements allocated to the software sub-function and not with the Safety Objective of the overall function.

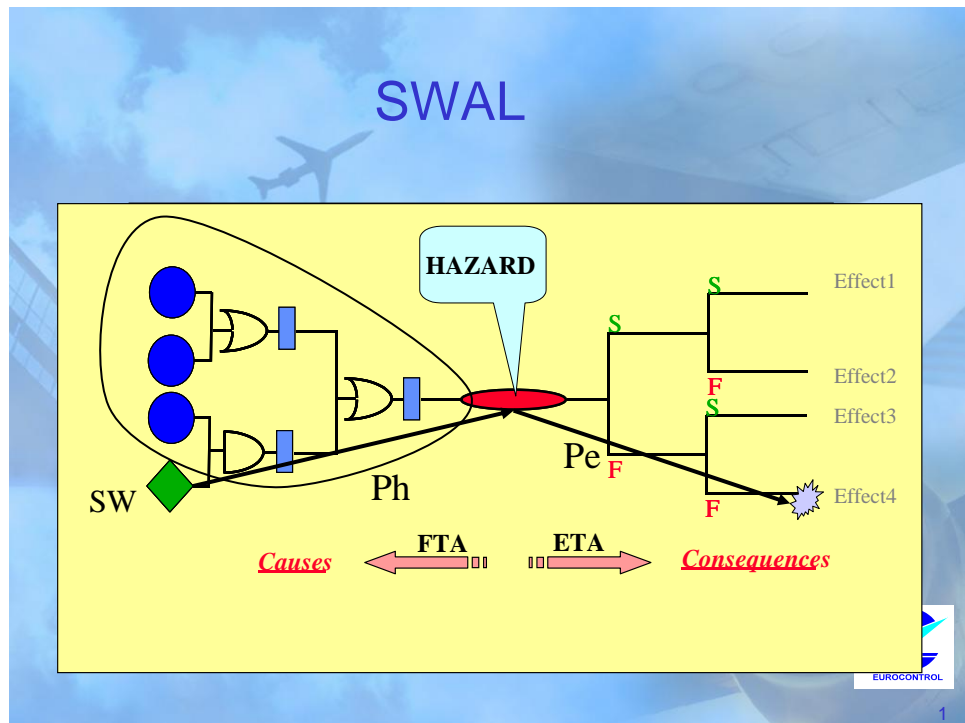


Figure 2.4.2.3: Relationship between SW failure, hazard and effects.

The likelihood ($Ph \times Pe$) that, once software fails, this software failure could generate a certain effect is illustrated in the above figure 2.4.2.3:

- Ph is the probability that, once software fails, this software failure generates a hazard. Ph is commensurate with the ability (probability) of the remaining part of the architecture to mitigate the software failure;
- Pe is the probability that the hazard generates an effect having a certain severity.

Depending on the method used to set Safety Objectives (See Sam-FHA Chapter 3 Guidance material G) there can be:

- Many Pe probabilities (one Pe per effect of the hazard), to be assessed for each individual effect (when using method 1 or 3 for setting Safety Objectives) or;
- Only one probability Pe (one for the worst credible effect when using method 2 & 4 for setting Safety Objectives).

As it can be difficult to quantify accurately and precisely these probabilities, expert judgement and other means (database, lessons learned, incidents reports) can be used to set those probabilities. Of course as part of the SAM-SSA, appropriate monitoring has to be put in place to ensure that these values are satisfied.

2.4.2.2 SWAL Allocation process

The following steps should be performed to allocate a SWAL (See Recommendations for ANS SW):

1. Identify the likelihood that, once Software fails, this software failure can generate an end effect which has a certain severity (do that for each effect of a hazard) (See figure 2.4.2.3) ;
2. Identify the SWAL for that couple (severity, likelihood) using the matrix here after;
3. This has to be done for all the hazards due to the software.

The final SWAL of software is the most stringent one.

Effect Severity	1	2	3	4
Likelihood of generating such an effect				
Very Possible	SWAL1	SWAL2	SWAL3	SWAL4
Possible	SWAL2	SWAL3	SWAL3	SWAL4
Very Unlikely	SWAL3	SWAL3	SWAL4	SWAL4
Extremely Unlikely	SWAL4	SWAL4	SWAL4	SWAL4

Very Possible: This effect will certainly occur due to software failure.

Possible: This effect may happen (it is not unreasonable to expect such effect to happen due to software failure).

Very Unlikely: it is not expected to have such an effect more than exceptionally and in some extreme cases throughout the system lifetime.

Extremely Unlikely: Such an effect is not expected to happen throughout the system lifetime.

Note: It should be noted that SWAL1 is so stringent that it should nearly never be allocated for the following reasons:


1. SWAL1 means somehow that software “can directly kill once it fails” as having a Severity1 effect is “Very Possible” (very limited means to mitigate SW failure(s). This can only be tolerable in extremely exceptional circumstances;
2. SWAL1 is so demanding to be satisfied. As the objectives and associated evidences are so stringent, the cost and development duration and effort are very high.


2.4.2.3 Example of SWAL allocation

1st CASE: Safety Objectives were allocated using Method 1 or 3 (See FHA Chapter 3 Guidance Material G “Methods for Setting Safety Objectives”). So all effects due to Software failure are taken into consideration.

This Software will be allocated a SWAL = SWAL3 as it is the most stringent SWAL (for both hazards).

Effect Severity	1	2	3	4
Likelihood of generating such an effect				
Very Possible	SWAL1	SWAL2	SWAL3	SWAL4
Possible	SWAL2	SWAL3	SWAL3	SWAL4
Very Unlikely	SWAL3	SWAL3	SWAL4	SWAL4
Extremely Unlikely	SWAL4	SWAL4	SWAL4	SWAL4

SW failure leading to Hazard1: 

SW failure leading to Hazard2: 

The way to read the table is the following:

For Hazard 1:

- If it is “Extremely Unlikely” that once SW fails, it generates Hazard1 and an effect having a severity 1, then this SW should be allocated a SWAL4;
- If it is “Possible” that once SW fails, it generates Hazard1 and an effect having a severity 2, then this SW should be allocated a SWAL3;
- If it is “Very Possible” that once SW fails, it generates Hazard1 and an effect having a severity 3, then this SW should be allocated a SWAL3;
- If it is “Very Possible” that once SW fails, it generates Hazard1 and an effect having a severity 4, then this SW should be allocated a SWAL4;


For Hazard 2:


- If it is “Extremely Unlikely” that once SW fails, it generates Hazard2 and an effect having a severity 1, then this SW should be allocated a SWAL4;
- If it is “Extremely Unlikely” that once SW fails, it generates Hazard2 and an effect having a severity 2, then this SW should be allocated a SWAL4;
- If it is “Very Unlikely” that once SW fails, it generates Hazard2 and an effect having a severity 3, then this SW should be allocated a SWAL4;
- If it is “Possible” that once SW fails, it generates Hazard2 and an effect having a severity 4, then this SW should be allocated a SWAL4.

2nd CASE: Safety Objectives were allocated using Method 2 or 4 (See FHA Chapter 3 Guidance Material G “Methods for Setting Safety Objectives). So only the worst credible scenario which has been used to set safety objectives is taken into consideration.

This Software will be allocated a SWAL = SWAL3 as it is the most stringent SWAL (for both hazards which have a worst credible hazard effect having a severity 3).

Effect Severity	1	2	3	4
Likelihood of generating such an effect				
Very Possible	SWAL1	SWAL2	SWAL3	SWAL4
Possible	SWAL2	SWAL3	SWAL3	SWAL4
Very Unlikely	SWAL3	SWAL3	SWAL4	SWAL4
Extremely Unlikely	SWAL4	SWAL4	SWAL4	SWAL4

SW failure leading to Hazard1: 

SW failure leading to Hazard2: 

The way to read the table is the following:

For Hazard 1: As the Worst Credible effect of Hazard 1 has a Severity 3 (FHA result), then

- If it is “Very Possible” that once SW fails, it generates Hazard1 and an effect having a severity 3, then this SW should be allocated a SWAL3;

For Hazard 2: As the Worst Credible effect of Hazard 1 has a Severity 3 (FHA result), then

- If it is “Very Unlikely” that once SW fails, it generates Hazard2 and an effect having a severity 3, then this SW should be allocated a SWAL4.

Non-ATM example of allocation of SWAL

System: Navigation system (Hardware and software) in a car using GPS signal:

Assuming that the Severity Classification Scheme defines severity classes as following:

Severity Class 1: Accident

- Death (drivers and occupants and maybe other vehicle occupants or pedestrians);
- Vehicle(s) destroyed.

Severity Class 2: Serious Incident

- Serious injuries (maybe one death);
- Car destroyed.

Severity Class 3: Major Incident

- Major injuries;
- Car damaged.

Severity Class 4: Significant Incident

- Stress, increase of workload to recover the situation;
- Possibly minor car damages.

1°) Navigation system used for indication (as it is today)

OED (Operational Environment Definition): The following operational environment is assumed:

- Drivers have a driving license;
- Drivers have a good vision;
- Drivers have a situational awareness: other traffic, road signals (continuous line, one-way indication, priority signs, ...), direction indication;
- Drivers know their final destination and the navigation system is used only for indication (as described in the User's Manual);
- Road regulations exist and are known by drivers.

Assuming that operational environment, let's assess the following hazard:

- Hazard1: Undetected credible corruption of direction indication (provided by navigation system).

When looking at all effects to allocate a SWAL:

Effect Severity	1	2	3	4
Likelihood of generating such an effect				
Very Possible	SWAL1	SWAL2	SWAL3	SWAL4
Possible	SWAL2	SWAL3	SWAL3	SWAL4
Very Unlikely	SWAL3	SWAL3	SWAL4	SWAL4
Extremely Unlikely	SWAL4	SWAL4	SWAL4	SWAL4

- It is “Extremely Unlikely” that once SW fails, it generates Hazard1 and an effect having a severity 1, then this SW should be allocated a SWAL4 as:
 - The driver controls his/her car and has to assess the credibility of the indication before applying it and so will not apply it (See OED). Thus the probability of applying a credibly corrupted indication is “Extremely Unlikely”;
- It is “Extremely Unlikely” that once SW fails, it generates Hazard1 and an effect having a severity 2, then this SW should be allocated a SWAL4 as;
 - The driver controls his/her car and has to assess the credibility of the indication before applying it (See OED). Thus the probability of applying a credibly corrupted indication is “Extremely Unlikely”;
- It is “Extremely Unlikely” that once SW fails, it generates Hazard1 and an effect having a severity 3, then this SW should be allocated a SWAL4 as:
 - The driver controls his/her car and has to assess the credibility of the indication before applying it (See OED). Thus the probability of applying a credibly corrupted indication is “Extremely Unlikely”;
- It is “Very Possible” that once SW fails, it generates Hazard1 and an effect having a severity 4, then this SW should be allocated a SWAL4 as:
 - The driver spends some time assessing the indication applicability, so it increases driver workload, may stress him/her. Maybe the physical location of the car is not the expected one, but this is impacting performance not safety.

As a conclusion, as far as the hazard “credible corruption of navigation system indication” is concerned, the SWAL allocated to the Navigation system in the OED as described is:

- **SWAL4.**

2°) Navigation system in command (futuristic use)

OED (Operational Environment Definition): The following operational environment is assumed:

- Drivers have to apply navigation system command;
- Drivers are only monitoring the system;
- Drivers do not need a situational awareness: other traffic, road signals (continuous line, one-way indication, priority signs, ...), direction indication. Cars may not have windows!;
- Drivers have only to enter their final destination into the navigation system (as described in the User's Manual);
- Road regulations exist and are known by navigation system.

Assuming that operational environment, let's assess the following hazard:

- Hazard1: Undetected credible corruption of direction command (provided by navigation system).

When looking at all effects to allocate a SWAL:

Effect Severity	1	2	3	4
Likelihood of generating such an effect				
Very Possible	SWAL1	SWAL2	SWAL3	SWAL4
Possible	SWAL2	SWAL3	SWAL3	SWAL4
Very Unlikely	SWAL3	SWAL3	SWAL4	SWAL4
Extremely Unlikely	SWAL4	SWAL4	SWAL4	SWAL4

- It is "Very Possible" that once SW fails, it generates Hazard1 and an effect having a severity 1, then this SW should be allocated a SWAL1 as:
 - The driver applies the Navigation system command (See OED). Thus the probability of applying a credibly corrupted indication that can kill the driver (and other occupants and maybe other vehicle occupants) is "Very Possible";
- It is "Very Possible" that once SW fails, it generates Hazard1 and an effect having a severity 2, then this SW should be allocated a SWAL2 as:
 - The driver applies the Navigation system command (See OED). Thus the probability of applying a credibly corrupted indication that can seriously injure the driver (and other occupants and maybe other vehicle occupants) and destroys the car is "Very Possible";
- It is "Very Possible" that once SW fails, it generates Hazard1 and an effect having a severity 3, then this SW should be allocated a SWAL3 as:

- The driver applies the Navigation system command (See OED). Thus the probability of applying a credibly corrupted indication that can seriously injure the driver (and other occupants and maybe other vehicle occupants) and destroys the car is “Very Possible”;
- It is “Very Possible” that once SW fails, it generates Hazard1 and an effect having a severity 4, then this SW should be allocated a SWAL4 as:
 - The driver applies the Navigation system command (See OED). Thus the probability of applying a credibly corrupted indication that can stress the driver (and other occupants and maybe other vehicle occupants) and damages the car is “Very Possible”.

As a conclusion, as far as the hazard “credible corruption of navigation system indication” is concerned, the SWAL allocated to the Navigation system in the OED as described is:

- **SWAL1.**

2.4.2.4 SWAL, Objectives, Activities & Evidences

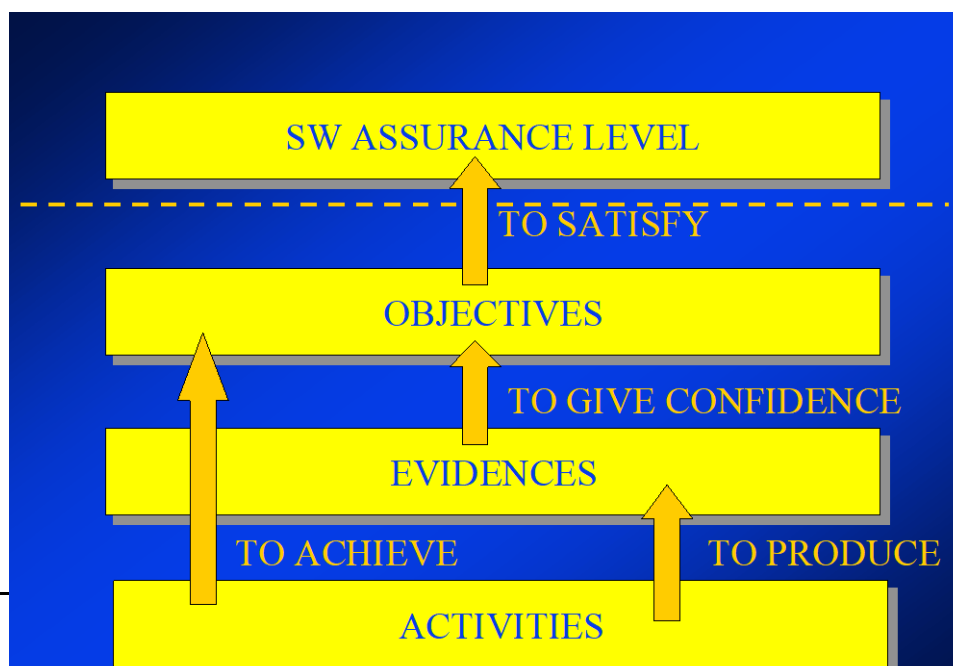
These Software Assurance Levels (SWAL) are designed to provide a level of confidence that the software will be developed and can be integrated in the equipment and then in the system in order to manage risks due to software failure.

The way to provide this level of confidence and assurance is by defining some objectives that will satisfy this level of assurance.

These objectives address the software acquisition, development, integration, maintenance, operation, ... processes of the software lifecycle and identify what is to be done to satisfy a level of assurance;

These objectives intend to give confidence that the assurance level is satisfied by showing evidences.

These evidences are produced by activities, which achieve these objectives. Different activities can produce different evidences, which are acceptable to satisfy objectives. However the same evidence can be produced by different activities.



Activities define how to achieve objectives and to satisfy a level of assurance.

Figure 2.4.2.4: SW AL/Objectives/Evidences/Activities links

This page is intentionally left blank.