Operational Hazard Analysis

Dr MURRAY BAILES
Functional Directions Pty Ltd
murraycbailes@gmail.com

Abstract

Operational Hazard Analysis (OHA) is an innovative, context-guided analysis method that enables the characterisation of systems safety risk and the specification of the Operational Safety Requirements, Systems Safety Requirements, and safety arguments for a capability.

OHA is derived from the concepts of DEF(AUST) 5679, an Australian standard for Safety Engineering for Defence Systems, that is applied to the abstract, implementation agnostic, operational domain model of a US Department of Defense Architecture Framework (DoDAF) style architecture.

The OHA method employs three causal chain viewpoints to characterise system safety risk. The first viewpoint, an accident scenario, characterises how a hazardous system output (operational hazard) can coexist with co-effectors in the systems deployment-context to result in an accident. External mitigations may be added to an accident scenario to mitigate the characterised risk. The second viewpoint, a hazard causal scenario, characterises how causal factors within the operation of the system can result in an operational hazard. Internal mitigations can be added to a hazard causal scenario. The final viewpoint, an input vulnerability analysis, characterising the potential for erroneous system inputs to result in the causal factors identified in the hazard causal scenario. The initial deployment-context-based accident analysis informs the subsequent hazard causal analysis that in turn informs the input vulnerability analysis.

Operational hazards provide the basis of Operational Safety Requirements (OSR) that specify the safety goal of prohibiting the occurrence of the operational hazards. External mitigations and internal mitigations provide the basis of the Systems Safety Requirements (SSR). The argument for systems safety is defined by the traceability between the OSR goal of hazard prohibition and the SSR that specify the mitigations that aims to achieve that goal.

Within this paper the OHA method is demonstrated using the operational model, for a hypothetical Aerial Firefighting Management System.

1 Introduction

The content of this paper has, for the most part, been derived from a PhD Thesis, titled Operational Hazard Analysis and the Safety-Aware Concept Development Method that was published in February 2022 (Bailes, M). Due to the space limitations the information within this paper have been significantly reduced from that provided in the thesis and readers are referred to the thesis should additional information regarding the concepts within be sought.

To understand the risks of a system it is first necessary to have a clear specification of the system's functionality and interfaces that place it within the context of its deployment (Hollnagel, 2012). *OHA* utilises the abstract operational system model of a capability architecture as the source of the system's specification that is used in the analysis of the system safety.

The *OHA* method employs three complementary event-sequence viewpoints to collectively characterise the beginning-to-end flow of safety risks, with the first viewpoint developed used to depict the potential safety outcomes (*accidents*) modelled in the context of the system deployment. This enables the knowledge gained from the analysis of the safety outcomes to inform the subsequent construction of the hazard causal scenario and input vulnerability analysis viewpoints, that are developed in that order.

The likelihood of a hazard occurring is frequently employed in safety and risk analysis, however *OHA* follows the guidance of DEF(AUST)5679 in undertaking a consequence-based analysis that only considers the possibility that a hazard may exist and that it may result in an accident. The concept of likelihood applies to the concrete systems of the real world and has no meaning within an abstract system. It may however be possible to infer a likelihood to an abstract concept when a one-to-one correspondence can be established between an abstract concept and a real-world instantiation allowing a low likelihood of a co-effector to be used as a mitigating factor for the associated hazard. The probability of an abstract hazard occurring cannot be inferred in the absence of the design of an implementation however abstract co-effectors depicted on an Accident Scenario (*AS)* may, in some cases be assigned a probability, based on observations and measurements of a concrete real-world equivalent. A low probability of the occurrence of a co-effector can therefore provide the basis of a mitigation in *accident scenario* analysis.

2 OHA and Def(Aust)5679

DEF(AUST)5679 Issue 2, Safety Engineering for Defence Systems (2008) was selected as the basis of the proposed OHA method as this standard begins the analysis using a black-box representation of the system under consideration, allowing the analysis to start without knowledge of the internal operation of the capability. DEF(AUST)5679 uses accident scenarios to characterise the hazardous states of the outputs of the system in the context of the system deployment.

In contrast to the IEC-61508 consequence and likelihood characterisations of risk, DEF(AUST)5679 uses a consequence-based analysis that does not utilise probability in the characterisation of risk which makes it suitable for the analysis of abstract hazards, for which a probability of occurrence cannot be determined.

OHA specialises the DEF(AUST)5679 method by tailoring the safety assessment to the analysis of the abstract operational system of a capability architecture. *OHA* extends DEF(AUST) 5679 by using additional event sequence viewpoints to enable an out-side-in characterisation of the *safety-significant* causal chains of the system under consideration using a safety-specific data model, shown in Figure 2.

Whereas both DEF(AUST)5679 and *OHA* utilise an *accident scenario* (*AS)* viewpoint to depict how hazardous states of a system output can result in an *accident* in the system deployment context, *OHA* introduces two additional, complementary, viewpoints. The first, a *Hazard Causal Scenario* (*HCS)* characterises how *causal factor* sequences in the system structure can result in an *operational hazard* on the system boundary. The second, an *Input Vulnerability Analysis (IVA),* depicts how the provision and receipt of the system inputs, could contribute to the *causal factors* of the system.

It may also be a possible to ascribe probability of failure to the provision and receipt of external inputs, based on real world measurements of an selected external service provider, in a similar manner to the use of observations and measurements of real-world co-effectors can be used to infer a probability on their abstract co-effector representations.

OHA AS, *HCS* and *IVA* collectively provide a mechanism to characterise the full initiating event, risk event and final risk outcome event causal sequences that are commonly used in safety analysis.

Whereas DEF(AUST)5679 uses two levels of requirement to specify safety, OHA utilises three with the systems safety requirements used by the standard renamed as OSR. DEF(AUST)5679 uses component safety requirements to specify the safety-related functions of the implementation that aims to achieve the hazard prohibition specified by a system safety requirement however these a not used by the OHA menthod. *OHA* introduces a new type of *system safety requirement (SSR),* which has no equivalent in the standard, with OHA SSRs specifying the abstract implementation-agnostic mitigations that aim to achieve the goal of the hazard prohibition specified by a parent *OSR*.

As the design progresses further traceability can be established within the capability architecture, from the abstract, implementation-agnostic *SSR* to the *system requirements* that specify the concrete components of the implementation to complete the top-to-bottom systems safety specification.

Within a capability architecture, a *system requirement* is used to specify both the system requirements of the implementation while also performing the role of component safety requirements as they are utilised by DEF(AUST)5679. The use of a common requirement type, for both systems and safety engineering, allows the use of the capability architecture requirements specification and verification framework by both the systems safety and systems engineering disciplines further integrating their products and processes.

The safety-related aspects of a system requirement can be determined from the traceability in the architecture established between the abstract *SSR* and the *system requirements* that specify the implementation, removing the need to create another requirement type for the specification of safety in the system domain of the architecture. The resulting requirements structure uses traceability between each requirement type to create a requirements-based framework for the presentation of systems safety that traverses the abstract-to-concrete system boundary of the architecture. Traceability between an *OSR* and the *SSR* within the operational domain of the architecture framework provides the structure of an abstract, implementation-agnostic argument for the safety of the capability, whose adequacy can be determined based on the level of confidence that the *SSR* will ensure that the *OSR* will not be violated. Further traceability between the abstract *SSR* and the *systems requirements* that specify the components of the implementation completes the specification of systems safety.

It is possible to use the OHA method to assign a level of harm that can result from an accident, where that level of harm can either be expressed as a consequence, as per the hazard analysis guidelines of IEC-61508 (2019), or to express that harm using quantified levels of consequence identified as a severity, as per the processes of DEF(AUST)5679 and MIL-STD-882 (2012).

It is highlighted that the OHA method and its products are self-contained within the operational domain of a capability architecture leading to the identification of the abstract safety requirements for a capability that does not consider the probability or likelihood of the occurrence of identified hazardous events, because abstract events cannot be ascribed a probability or likelihood. To complete the safety assessment of the concrete systems of an implementation, the analysis can use the outputs of the OHA when considering the modes of operation of the physical components of the implementation, and the likelihood of the occurrence of the identified hazardous events within those physical components, for which probabilities of failures can be measured or estimated. OHA identifies the safety risk that is inherent to a capability type by specifying what needs to occur to ensure safety operation, expressed as a set of abstract SSR. It does not specify how those needs are to be achieved, nor the likelihoods of failing to meet those needs, within any specific implementation.

OHA makes no assertions regarding the choice of the safety analysis methods to be applied to components of the implementation. Choices of safety analysis techniques may depend on the availability of an industry specific variant of IEC-61508 for the type of capability under consideration or a requirement to use a specific standard within a particular application domain, such as the use of MIL-STD-882 for defence projects, with that choice guiding the use of either accident severity or consequence in OHA to meet the needs of the selected analysis technique.

Aerial Firefighting Management System Example

To demonstrate the *OHA* method a case study has been developed for a hypothetical Aerial Firefighting Management System (AFMS). Within this paper, this case study is used to provide examples of *OHA* outputs. Figure 1 below depicts the AFMS Operational Concept that is used as an input into the *OHA* process.

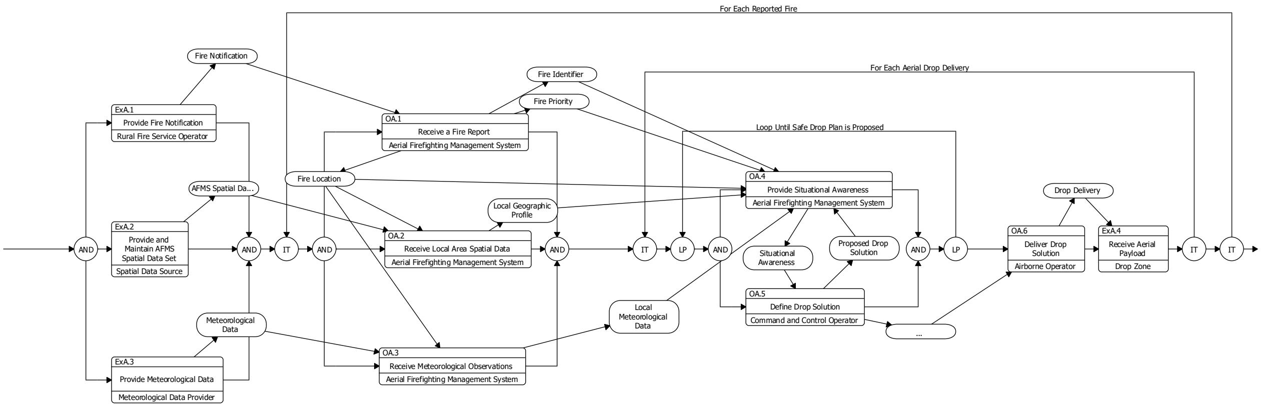

For Each Reported Fire
For Each Aerial Drop Delivery
Loop Until Safe Drop Plan is Proposed
Fire Notification
ExA.1
Provide Fire Notification
Rural Fire Service Operator
AFMS Spatial Da...
ExA.2
Provide and Maintain AFMS Spatial Data Set
Spatial Data Source
Meteorological Data
ExA.3
Provide Meteorological Data
Meteorological Data Provider
AND
AND
IT
AND
Fire Identifier
Fire Priority
OA.1
Receive a Fire Report
Aerial Firefighting Management System
Fire Location
Local Geographic Profile
OA.2
Receive Local Area Spatial Data
Aerial Firefighting Management System
OA.3
Receive Meteorological Observations
Aerial Firefighting Management System
AND
Local Meteorological Data
IT
LP
AND
OA.4
Provide Situational Awareness
Aerial Firefighting Management System
Situational Awareness
Proposed Drop Solution
OA.5
Define Drop Solution
Command and Control Operator
...
AND
LP
Drop Delivery
OA.6
Deliver Drop Solution
Airborne Operator
ExA.4
Receive Aerial Payload
Drop Zone
IT
IT

Figure 1 AFMS Operational Concept

3 OHA Safety Specific Data Extensions

The *OHA* method uses a set of safety specific data types that is depicted in Figure 2 and described below. For the purposes of *OHA*, an output *operational hazard* is a hazardous output of a boundary operational activity of the capability operational model. To support the OHA method the system model must identify the provision and receipt of the system inputs, the emergent behaviour of the system and then the provision and receipt of the system outputs in the context of the system deployment.

The analysis begins by considering how an output *operational hazard*, a hazardous state of a boundary activity that can create a hazardous system output, can coexist with one or more *co-effectors* in the systems deployment context to result in an *accident*. The analysis is completed at the other end of the hazardous causal chains by considering how *input operational hazards,* can create a hazardous system input that can also co-exist with one or more *co-effectors* to result in a *causal factor* in the system structure that was identified in the *HCS* analysis.

Co-effectors are states that exist in the system deployment context that are depicted on an AS viewpoint as co-existing with an identified output *operational hazard* to result in an *accident. Co-effectors* can also be depicted on an IVA viewpoint as co-existing with an *input operational hazard* to result in a *causal factor* that was identified in the preceding *HCS* analysis.

Causal factors are hazardous states of an operational activity within the system's structure that represent events in the causal chain that can result in the occurrence of an output *operational hazard*. In the *OHA IVA* viewpoint *causal factors* can also be the result of an *input operational hazard*.

External mitigations are identified from the context-based AS and IVA viewpoints to establish the assumptions and requirements of system safety based on analysis of the capability type within its deployment context. Each *external mitigation* is then considered against the developing structure of the capability operational concept to identify the design and/or operational mitigations of system safety. OHA *external mitigations* inform the development of the operational model, the identification of the *causal factors* and *internal mitigations* of the system.

Internal mitigations identify additional functionality, or constraints on existing functionality of the system under consideration, that mitigate the risk of an *operational hazard* or *causal factor*.

OHA uses *accident scenarios* (AS) to depict the relationships between *operational hazards*, *co-effectors*, *accidents*, and *external mitigations*. *Accidents* are assigned a severity to indicate a level of harm associated with its occurrence.

OSR define the safety goals of the capability that prohibit the occurrence of an *Operational Hazard*.

SSR specify either an *internal mitigation* that mitigates a *causal factor* in the system structure or an *external mitigation* that mitigates an *operational hazard, co-effector* or *accident* that can occur in the deployment context of the system. A *SSR* aims to achieve the prohibition of the *operational hazard* specified by an *OSR*.

SSR are implemented by *system requirements* that specify the element of the system design that implement the *internal mitigation* that the SSR specifies.

External mitigations identify the basic assumptions of systems safety, while the *internal mitigations* identify an aspect of an *external mitigation* that has been incorporated into the system design. The 'informed by' relationship between mitigation types is used to denote that an *external mitigation* informs an aspect of an *internal mitigation* that has been incorporated into the functionality of the operational concept. For example, the *external mitigation* EM.3 Identify Environmental Sensitivities in the Drop zone identified in the *AS* depicted in Figure 4 informs the identification of the internal mitigations IM.6 Spatial Data to Identify Environmental Sensitivities and IM.3 Situational Awareness to Highlight Environmental Sensitivities depicted in the *HCS* depicted in Figure 7

Corresponding to the 'informed by' relationship between *external mitigations* and *internal mitigations* is the 'refined by' relationship between the *SSR* that specify an *external mitigation* and the *SSR* that specify the *internal mitigation*. This relationship, and the rationale field of each mitigation help to define the assumptions behind the development of the requirements-based argument for systems safety.

The resultant requirements framework of *OSR*, *SSR* and the *system requirements* creates a top-to-bottom specification of the system safety of the capability that crosses the abstract to physical system domains of the architecture.

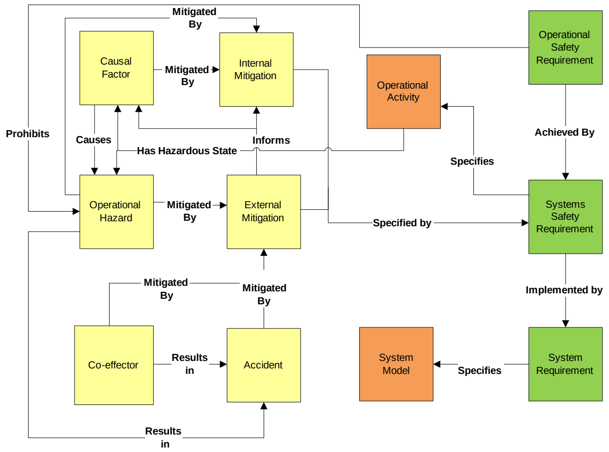


Figure 2 Operational Hazard Analysis Safety Management Schema

4 Perform Operational Hazard Analysis

The *OHA* method begins with analysis of the capability operational model to identify the potential hazardous states of the system outputs of each operational activity on the system boundary.

For each hazardous state of a system output (*operational hazard*) of an activity on the system boundary, an *AS* is developed to characterise how that state could coexist with *co-effectors*, in the context of the system deployment, to result in an *accident*. A consequence *severity* is determined for each *accident depicted on an AS.*

External mitigations can be added to an *AS* to reduce the risk of identified *operational hazards* and/or *co-effectors* and/or *accidents*. The responsibility for the provision of each *external mitigation* is then determined. Where it is determined that the responsibility for the provision of an *external mitigation* is entirely, or partially, provided by the functionality of the capability under development, *OHA* proceeds to the construction of a *HCS* to characterise how the *causal factors* within the system structure could result in the occurrence of the *operational hazard. Internal mitigations* can be added to a *HCS* to reduce the risk of a *causal factor* or *operational hazard*, Where an *internal mitigations*, provides some or all of an *external mitigation* then that *internal mitigation* is said to be ‘informed by’ the related *external mitigation.*

Following the completion of the *HCS* analysis an *IVA* is performed to consider how potential states of a system input could contribute to the occurrence of a *causal factor* in the operation of the system..

At the completion of the development of the *AS*, *HCS and IVA*, the identified *operational hazard*, *external mitigation*, and *internal mitigations* provide the basis for the specification of the *OSR* and *SSR* of the capability. Traceability between the OSR and SSR is established to create the structure of the implementation-agnostic argument for systems safety.

Although it is not possible to ensure that all *operational hazards*, *co-effectors*, *accidents* and *causal factors*, and their respective *internal mitigations* and *external mitigation* have been identified within the analysis, the approach of systematically considering how each output from each boundary operational activity could create potential hazardous states is a systematic process that enables a level of confidence in the completeness of the analysis of the operational concept of a capability. As with any safety or risk analysis, the final verification of the assessment is via peer and stakeholder review.

Because the *operational hazards* are initially identified simply as unsafe outputs, with the subsequent *AS* context analysis allowing the refinement of the *operational hazard* set, there are minimal requirements for application domain or risk analysis knowledge to begin *OHA*.

4.1 Construct Accident Scenario

The *accident scenario*, the first viewpoint that is constructed in the OHA method, depicts how the *operational hazards* can co-exist with *co-effectors* to result in an *accident* in the context of the capability deployment. The understanding of the deployment context gained from the *AS* analysis informs the subsequent construction of the *HCS* and *IVA* viewpoints. In a top-down development process OHA is performed on the abstract operational domain model of the capability, prior to the design of the implementation, and therefore it is not possible to assign a likelihood to the occurrence of an abstract *operational hazard*. As discussed in Section 1 it may however be possible to infer a likelihood to the occurrence of an abstract *co-effector* where a one-to-one correspondence can be established between the abstract *co-effector* and a real word equivalent. The probability of the *operational hazard* itself being realised (if indeed it could be calculated) does not affect the mitigation determination, beyond the simple fact that the *operational hazard* may plausibly be realised. In cases where significant mitigation cannot be identified for an *AS* of high severity, consideration must be given to the possibility of altering the operational context to introduce appropriate mitigations.

4.1.1 AFMS Accident Scenario Example

Figure 3 depicts an example *AS* from the AFMS case study. This first version of each *AS* does not include *external mitigations*, as these are added to the second *AS* in each set as depicted in Figure 4.

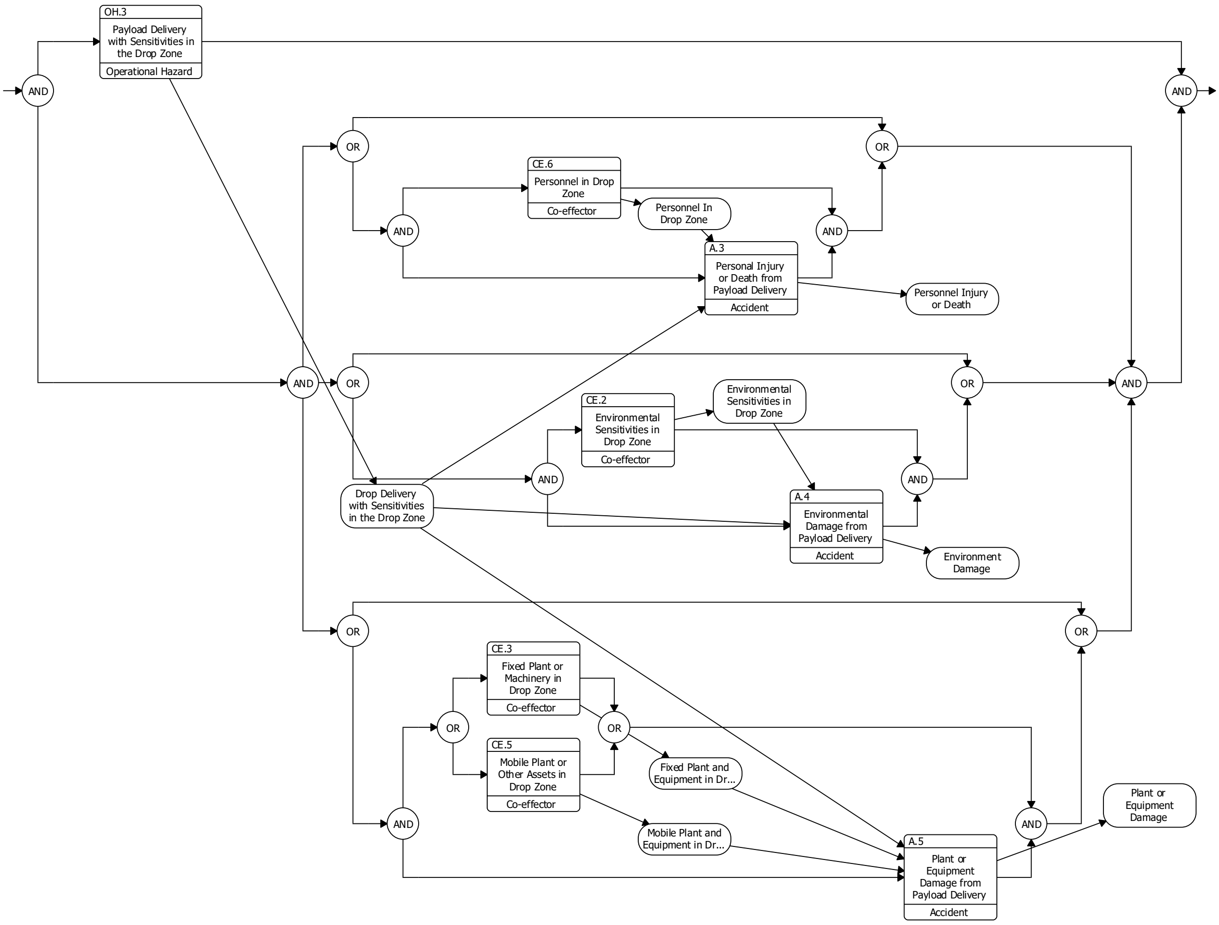

OH.3
Payload Delivery with Sensitivities in the Drop Zone
Operational Hazard
AND
AND
OR
OR
CE.6
Personnel in Drop Zone
Co-effector
Personnel In Drop Zone
AND
AND
A.3
Personal Injury or Death from Payload Delivery
Accident
Personnel Injury or Death
AND
OR
OR
AND
CE.2
Environmental Sensitivities in Drop Zone
Co-effector
Environmental Sensitivities in Drop Zone
AND
AND
Drop Delivery with Sensitivities in the Drop Zone
A.4
Environmental Damage from Payload Delivery
Accident
Environment Damage
OR
OR
CE.3
Fixed Plant or Machinery in Drop Zone
Co-effector
OR
OR
CE.5
Mobile Plant or Other Assets in Drop Zone
Co-effector
Fixed Plant and Equipment in Dr...
Mobile Plant and Equipment in Dr...
AND
AND
Plant or Equipment Damage
A.5
Plant or Equipment Damage from Payload Delivery
Accident

Figure 3 AS.1.1 Payload Delivery with Sensitivities in the Drop Zone (without mitigation)

Table 1 identifies selected traceability for the accidents depicted on AS.1.1 depicted on Figure 3.

Table 1 AS.1 Accident to Operational Hazard and Co-effector Set Traceability

Accident	Is the Result of Operational Hazard	Co-existing with Co-effector
A.3 Personal Injury or Death from Payload Delivery		
	OH.3 Payload Delivery with Sensitivities in the Drop Zone	
		CE.6 Personnel in Drop Zone
A.4 Environmental Damage from Payload Delivery		
	OH.3 Payload Delivery with Sensitivities in the Drop Zone	
		CE.2 Environmental Sensitivities in Drop Zone
A.5 Plant or Equipment Damage from Payload Delivery		
	OH.3 Payload Delivery with Sensitivities in the Drop Zone	
		CE.3 Fixed Plant or Machinery in Drop Zone
		CE.5 Mobile Plant or Other Assets in Drop Zone

Table 2 identifies selected traceability for the *operational hazard* characterised on AS.1, as depicted on Figure 3.

Table 2 AS.1 Operation Hazard, Operational Activity and Accident Traceability

Operational Hazard	Hazardous State of	Results in	Accident Severity
OH.3 Payload Delivery with Sensitivities in the Drop Zone	OA.6 Deliver Drop Solution		
		A.3 Personal Injury or Death from Payload Delivery	Catastrophic
		A.4 Environmental Damage from Payload Delivery	Critical
		A.5 Plant or Equipment Damage from Payload Delivery	Marginal

Figure 4 depicts the final version of AS.1 to which *external mitigations* have been added to the viewpoint depicted in Figure 3.

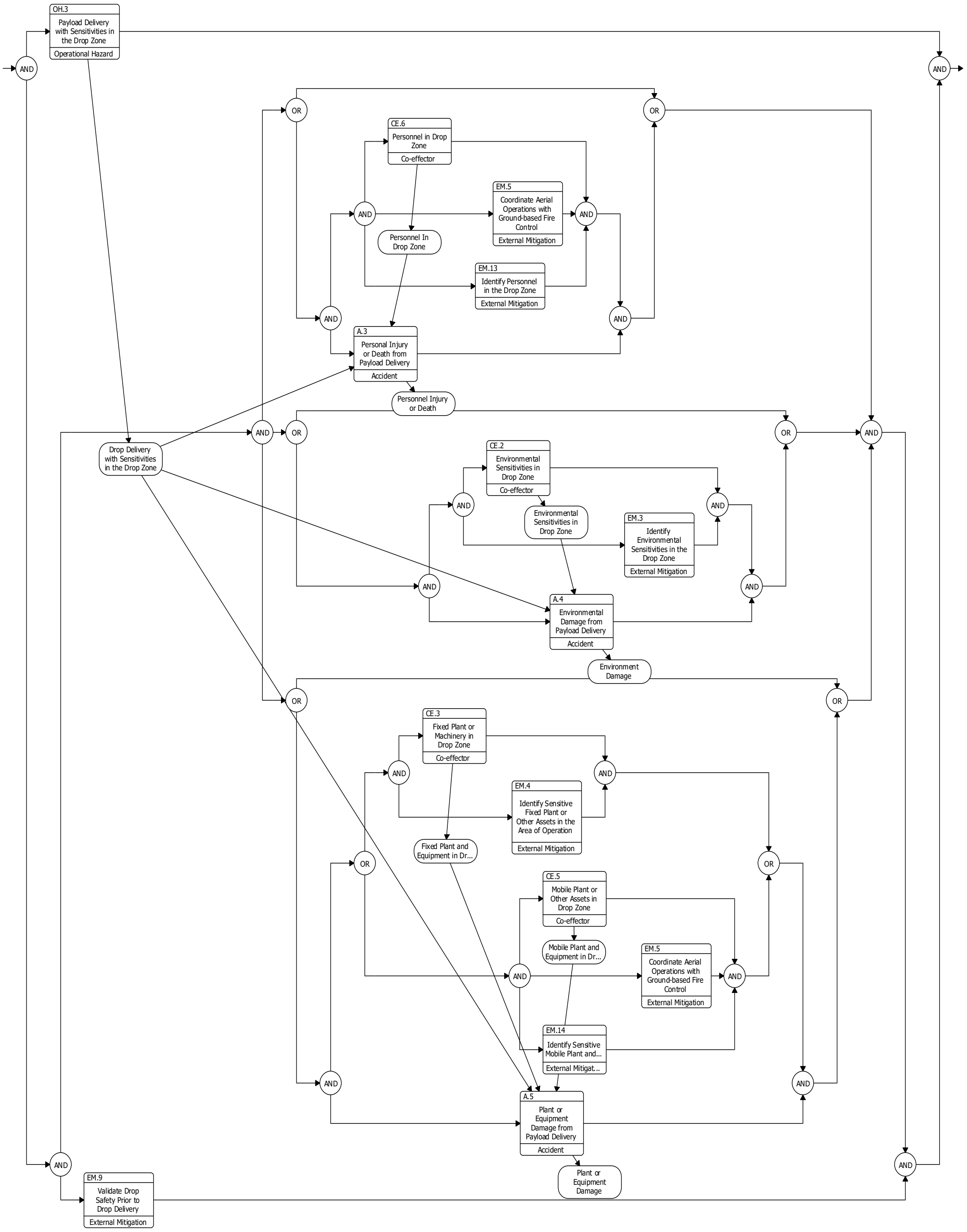

OH.3
Payload Delivery with Sensitivities in the Drop Zone
Operational Hazard
AND
OR
CE.6
Personnel in Drop Zone
Co-effector
EM.5
Coordinate Aerial Operations with Ground-based Fire Control
External Mitigation
Personnel In Drop Zone
EM.13
Identify Personnel in the Drop Zone
External Mitigation
A.3
Personal Injury or Death from Payload Delivery
Accident
Personnel Injury or Death
Drop Delivery with Sensitivities in the Drop Zone
CE.2
Environmental Sensitivities in Drop Zone
Co-effector
Environmental Sensitivities in Drop Zone
EM.3
Identify Environmental Sensitivities in the Drop Zone
External Mitigation
A.4
Environmental Damage from Payload Delivery
Accident
Environment Damage
CE.3
Fixed Plant or Machinery in Drop Zone
Co-effector
EM.4
Identify Sensitive Fixed Plant or Other Assets in the Area of Operation
External Mitigation
Fixed Plant and Equipment in Dr...
CE.5
Mobile Plant or Other Assets in Drop Zone
Co-effector
Mobile Plant and Equipment in Dr...
EM.5
Coordinate Aerial Operations with Ground-based Fire Control
External Mitigation
EM.14
Identify Sensitive Mobile Plant and...
External Mitigat...
A.5
Plant or Equipment Damage from Payload Delivery
Accident
Plant or Equipment Damage
EM.9
Validate Drop Safety Prior to Drop Delivery
External Mitigation

Figure 4 AS.1.2 Payload Delivery with Sensitivities in the Drop Zone (with mitigations)

Table 3 identifies selected traceability for the *co-effectors* for OH.3 depicted on Figure 4.

Table 3 AS.1 Co-effector Traceability

Co-effector	Co-effector can 'result in' the Accident	Co-effector 'mitigated by' External Mitigation
CE.2 Environmental Sensitivities in Drop Zone		
	A.4 Environmental Damage from Payload Delivery	
		EM.3 Identify Environmental Sensitivities in the Drop Zone
		EM.9 Validate Drop Safety Prior to Drop Delivery
CE.3 Fixed Plant or Machinery in Drop Zone		
	A.5 Plant or Equipment Damage from Payload Delivery	
		EM.4 Identify Sensitive Fixed Plant or Other Assets in the Area of Operation
		EM.9 Validate Drop Safety Prior to Drop Delivery
CE.5 Mobile Plant or Other Assets in Drop Zone		
	A.5 Plant or Equipment Damage from Payload Delivery	
		EM.5 Coordinate Aerial Operations with Ground-based Fire Control
		EM.9 Validate Drop Safety Prior to Drop Delivery
CE.6 Personnel in Drop Zone		
	A.3 Personal Injury or Death from Payload Delivery	
		EM.5 Coordinate Aerial Operations with Ground-based Fire Control
		EM.9 Validate Drop Safety Prior to Drop Delivery
		EM.13 Identify Personnel in the Drop Zone

Table 4 identifies selected traceability for the external mitigations characterised on AS.1 depicted on Figure 3 and Figure 4.

Table 4 AS.1 External Mitigation Traceability

External Mitigations	External Mitigation Specified by	External Mitigation Mitigates Co-Effector
EM.3 Identify Environmental Sensitivities in the Drop Zone	SSR.3 Environmental Sensitivities in the area of operation shall be identified.	CE.2 Environmental Sensitivities in Drop Zone
EM.4 Identify Sensitive Fixed Plant or Other Assets in the Area of Operation	SSR.4 Fixed plant, equipment of other assets in the area of operation shall be identified.	CE.3 Fixed Plant or Machinery in Drop Zone
EM.5 Coordinate Aerial Operations with Ground-	SSR.5 AFMS operations shall be coordinated with ground-based firefighting	CE.5 Mobile Plant or Other Assets in Drop Zone

based Fire Control	operations to control access of personnel or members of the public in the area of operation.	
		CE.6 Personnel in Drop Zone
EM.9 Validate Drop Safety Prior to Drop Deliver	SSR.9 The AFMS aerial node operator shall perform a visual inspection of the area of operation. If any safety hazards are detected the drop will be abandoned, and the drop planning iteration will be restarted.	CE.2 Environmental Sensitivities in Drop Zone
		CE.3 Fixed Plant or Machinery in Drop Zone
		CE.4 Fixed Navigation Obstacle in Area of Operation
		CE.5 Mobile Plant or Other Assets in Drop Zone
EM.13 Identify Personnel in the Drop Zone	SSR.26 The presence of personnel in the area of operation shall be identified	CE.6 Personnel in Drop Zone

4.2 Construct Hazard Causal Scenario

A *Hazard Causal Scenario (HCS)* is the inward-looking event sequence that complements the outward-looking *Accident Scenario*. The structure of a *HCS* is based on the structure of the operational activity model. In the construction of a *HCS*, selected operational activities from the operational model, and their outputs, are replaced by their hazardous state representations, where a *causal factor* is used to represent the hazardous state of an internal operational activity and, as per their use in an *accident scenario*, *operational hazards are used to* represent hazardous states of an operational activity on the system boundary.

Following the replacement of all affected operational activities with their hazardous state representations, any original operational activity that is not involved in the casual event sequence may be removed from the *HCS*, so that only those operational activities that can cause, or contribute to the occurrence of the *operational hazard* remain. Following the removal of the non-involved operational activities, any empty branches of the Boolean constructs of the scenario logic can also be removed.

The resulting, simplified, *HCS* depicts how internal states of the system can cause, or contribute to the occurrence of an *operational hazard* on the system boundary, with superfluous information having been removed from the characterisation to provide a simplified, more easily understood viewpoint.

Each *operational hazard* that appears in an *AS* that also identifies an *external mitigation*, the provision of which is determined to be within the scope of the capability, is to be characterised in a *HCS*. Notwithstanding the need to ensure that the full set of causal chains for each *operational hazard* are fully depicted within the set of *HCS*, the number, and content, of each *HCS* is at the discretion of the analyst.

HCS are used to depict how an *internal mitigation* mitigates either a *causal factors* or *operational hazard* of the capability. The identification of *causal factors* and *internal mitigations* is informed by the *external mitigations* that were identified by the *accident scenario* analysis. Where the partial or full implementation of the *external mitigation* is determined to be within the capability operational concept then that *external* mitigation informs the identification of the *causal factors* and *internal mitigations* of the capability.

4.2.1 Constructing and Interpreting a Hazard Causal Scenario

When constructing and interpreting the logic of a *HCS* there is a need to differentiate between the Boolean logic that originated from the operational concept, from the logic that expresses the relationship between the *operational hazard* or *causal factor* hazardous states of each operational activity and the *internal mitigations* that reduce the associated risk.

In the construction of a *HCS* selected operational activities are replaced by their hazardous state representation(s) i.e. a *causal facto*r or an *operational hazard*. If a selected operational activity has more than one hazardous state that is to be depicted on the same *HCS*, then each hazardous state is placed on its own branch of an OR gate.

When constructing the final *HCS* in each set that includes the *internal mitigation*, each *causal factor* and its *internal mitigation(s)* are placed on alternate branches of an AND gate. This use of an AND gate indicates that the *internal mitigation* mitigates the related *causal factor*, with that AND gate then placed in the HCS logic in the location previously occupied by the subject *causal factor*.

When evaluating whether the *internal mitigations* that mitigate each *causal factor* on a HCS adequately mitigates the associated risk, each location of the operational concept logic that originally contained an operational activity is evaluated individually. To differentiate the branches of the Boolean logic that contained an operational activity within the operational concept, from the logic of the constructs of the safety argument, each branch of the operational concept logic that is depicted on a *HCS* is annotated with the letters OC to indicate its origin came from the operational concept. Hence the evaluation of the Boolean logic of a HCS is delimited by the branches of the logic that are annotated with the letters OC.

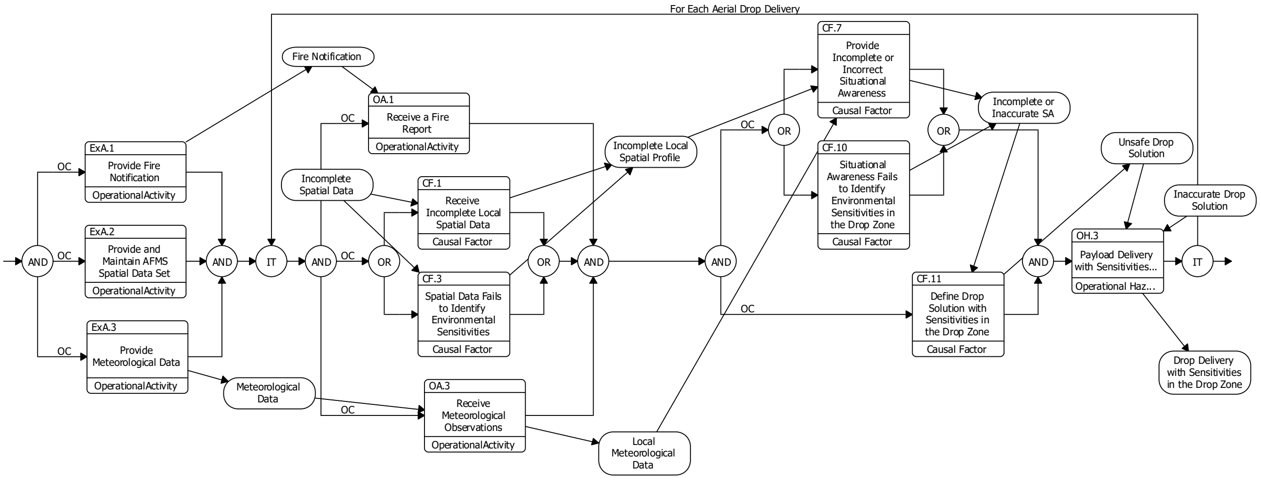
For each HCS the evaluation of the adequacy of the risk reduction achieved by the *internal mitigations* is performed for each *operational hazard* and *causal factor* that are depicted on that scenario, rather than for the operational activity that can have multiple identified hazardous states. Where multiple hazardous states have been identified for an operational activity each hazardous state can be characterised using a single or multiple event viewpoints, to collectively depict the full set of hazardous states of each operational activity.

The overall adequacy of the argument for systems safety is evaluated by considering the completeness of the identification of the *operational hazard* or *causal factors* and their related *internal mitigations* for each operational activity, within the context of the emergent behaviour of the operational concept.

4.2.2 AFMS Case Study Hazard Causal Scenario

For the purposes of providing a step-by-step demonstration of the development of a *HCS*, three versions of the example HCS are provided to demonstrate interim products of the three stages of the constructing a *HCS*.

The HCS in Figure 5, Figure 6 and Figure 7 characterise the causal chain resulting from a failure to identify environmental sensitivities within the AFMS spatial data, the resulting incomplete situational awareness leading to the definition of an unsafe drop plan and a subsequent unsafe drop delivery due to environmental sensitivities in the drop zone.



For Each Aerial Drop Delivery
AND
OC
ExA.1
Provide Fire Notification
OperationalActivity
ExA.2
Provide and Maintain AFMS Spatial Data Set
OperationalActivity
ExA.3
Provide Meteorological Data
OperationalActivity
AND
IT
Fire Notification
Meteorological Data
AND
OC
OA.1
Receive a Fire Report
OperationalActivity
Incomplete Spatial Data
OR
CF.1
Receive Incomplete Local Spatial Data
Causal Factor
CF.3
Spatial Data Fails to Identify Environmental Sensitivities
Causal Factor
OA.3
Receive Meteorological Observations
OperationalActivity
OR
AND
Incomplete Local Spatial Profile
Local Meteorological Data
AND
OR
CF.7
Provide Incomplete or Incorrect Situational Awareness
Causal Factor
CF.10
Situational Awareness Fails to Identify Environmental Sensitivities in the Drop Zone
Causal Factor
OR
Incomplete or Inaccurate SA
CF.11
Define Drop Solution with Sensitivities in the Drop Zone
Causal Factor
AND
Unsafe Drop Solution
Inaccurate Drop Solution
OH.3
Payload Delivery with Sensitivities...
Operational Haz...
IT
Drop Delivery with Sensitivities in the Drop Zone

Figure 5 HCS.2.1 Unsafe Payload Delivery Due to Environmental Sensitivities in the drop zone (full model)

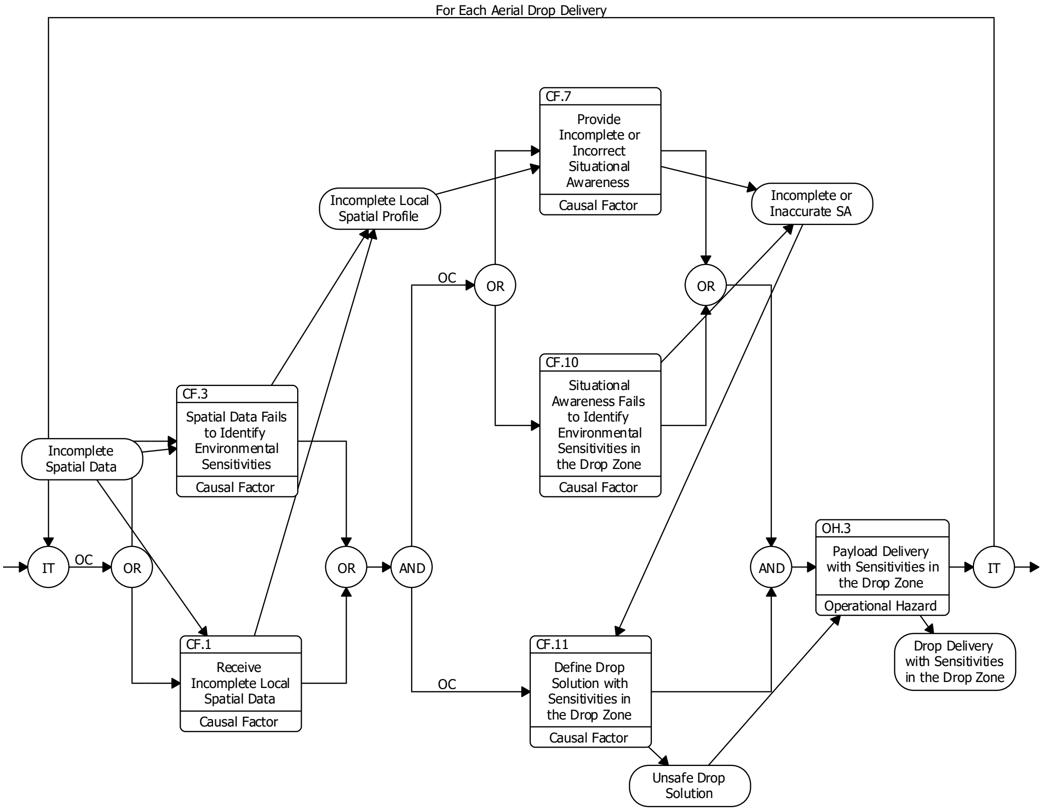

For Each Aerial Drop Delivery
CF.7
Provide Incomplete or Incorrect Situational Awareness
Causal Factor
Incomplete Local Spatial Profile
Incomplete or Inaccurate SA
OC
OR
OR
CF.10
Situational Awareness Fails to Identify Environmental Sensitivities in the Drop Zone
Causal Factor
CF.3
Spatial Data Fails to Identify Environmental Sensitivities
Causal Factor
Incomplete Spatial Data
IT
OC
OR
OR
AND
AND
OH.3
Payload Delivery with Sensitivities in the Drop Zone
Operational Hazard
IT
CF.1
Receive Incomplete Local Spatial Data
Causal Factor
OC
CF.11
Define Drop Solution with Sensitivities in the Drop Zone
Causal Factor
Drop Delivery with Sensitivities in the Drop Zone
Unsafe Drop Solution

Figure 6 HCS.2.2 Unsafe Payload Delivery Due to Environmental Sensitivities in the drop zone (without mitigations)

In Figure 6 the operational activities depicted on Figure 5 that are not involved in the causal chain resulting in the occurrence of OH.3 are removed. Any resulting empty branches of the model logic are also removed to provide a simpler depiction without superfluous information. Figure 7 extends the *HCS* depicted on Figure 6 with the addition of *internal mitigation*.

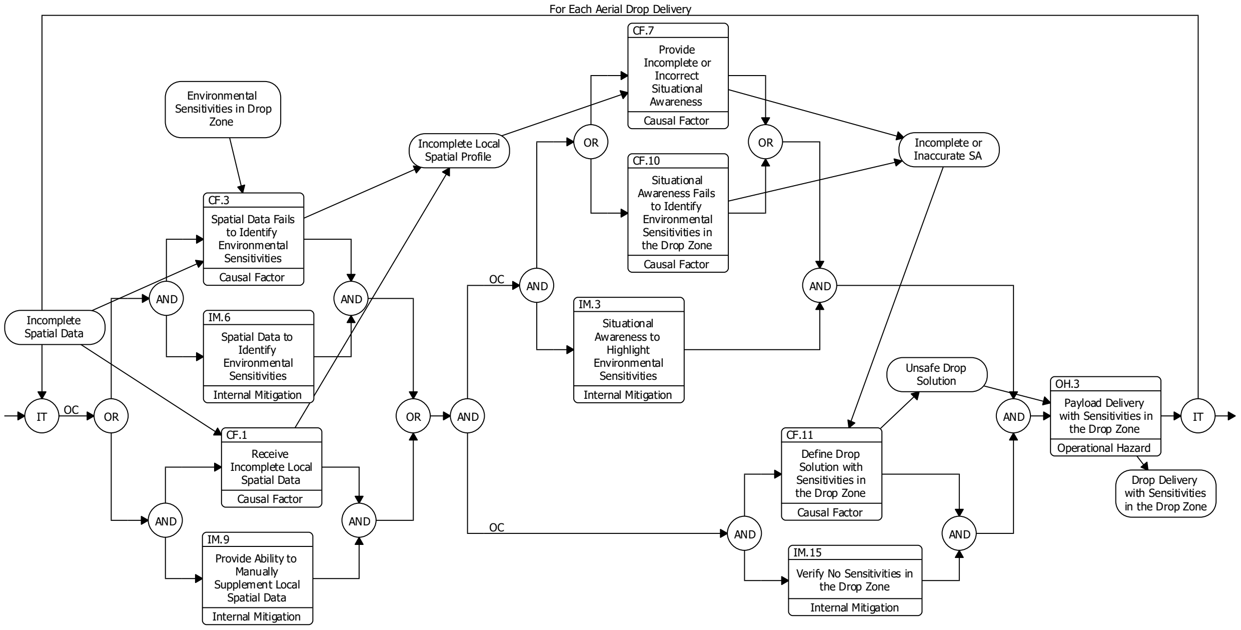

For Each Aerial Drop Delivery
CF.7
Provide Incomplete or Incorrect Situational Awareness
Causal Factor
Environmental Sensitivities in Drop Zone
Incomplete Local Spatial Profile
OR
OR
Incomplete or Inaccurate SA
CF.10
Situational Awareness Fails to Identify Environmental Sensitivities in the Drop Zone
Causal Factor
CF.3
Spatial Data Fails to Identify Environmental Sensitivities
Causal Factor
AND
AND
OC
AND
AND
IM.3
Situational Awareness to Highlight Environmental Sensitivities
Internal Mitigation
Incomplete Spatial Data
IM.6
Spatial Data to Identify Environmental Sensitivities
Internal Mitigation
Unsafe Drop Solution
OH.3
Payload Delivery with Sensitivities in the Drop Zone
Operational Hazard
IT
OC
OR
OR
AND
AND
IT
CF.1
Receive Incomplete Local Spatial Data
Causal Factor
CF.11
Define Drop Solution with Sensitivities in the Drop Zone
Causal Factor
Drop Delivery with Sensitivities in the Drop Zone
AND
AND
OC
AND
AND
IM.9
Provide Ability to Manually Supplement Local Spatial Data
Internal Mitigation
IM.15
Verify No Sensitivities in the Drop Zone
Internal Mitigation

Figure 7 HCS.2.3 Unsafe Payload Delivery Due to Environmental Sensitivities in the drop zone (with mitigations)

Table 5 HCS.2 Operational Hazards and Causal Factors Traceability

Hazardous States	Impacted Operational Activity	Mitigated By
OH.3 Payload Delivery with Sensitivities in the Drop Zone	OA.6 Deliver Drop Solution	
CF.1 Receive Incomplete Local Spatial Data	OA.2 Receive Local Area Spatial Data	IM.9 Provide Ability to Manually Supplement Local Spatial Data
CF.3 Spatial Data Fails to Identify Environmental Sensitivities	OA.2 Receive Local Area Spatial Data	IM.6 Spatial Data to Identify Environmental Sensitivities
CF.7 Provide Incomplete or Incorrect Situational Awareness	OA.4 Provide Situational Awareness	IM.3 Situational Awareness to Highlight Environmental Sensitivities
CF.10 Situational Awareness Fails to Identify Environmental Sensitivities in the Drop Zone	OA.4 Provide Situational Awareness	IM.3 Situational Awareness to Highlight Environmental Sensitivities
CF.11 Define Drop Solution with Sensitivities in the Drop Zone	OA.5 Define Drop Solution	IM.15 Verify No Sensitivities in the Drop Zone

Table 6 identifies selected traceability for the internal mitigations characterised on the HCS.2.3 depicted on Figure 7.

Table 6 HCS.2 Unsafe Payload Delivery Due to Environmental Sensitivities in the Drop Zone Internal Mitigation Traceability

Mitigations	Internal Mitigation Specified by
IM.3 Situational Awareness to Highlight Environmental Sensitivities	SSR.14 AFMS Situational Awareness shall highlight environmental sensitivities in the area of operation.
IM.6 Spatial Data to Identify Environmental Sensitivities	SSR.11 The AFMS spatial data shall identify known environmental sensitivities in the area of operation.
IM.9 Provide Ability to Manually Supplement Local Spatial Data	SSR.18 The ability to create points of interest in the spatial dataset based on local operational ground and aerial firefighting observations shall be provided at all AFMS nodes
IM.15 Verify No Sensitivities in the Drop Zone	SSR.30 The AFMS C2 Operator shall verify, against the information provided by the AFMS situational awareness that there are no sensitivities in the drop zone that could negatively impacted by the drop delivery.

4.3 Perform Input Vulnerability Analysis

The *Input Vulnerability Analysis* provides a complementary viewpoint to the *Accident Scenario* by characterising how hazardous states of the system inputs can co-exist with *co-effectors* in the deployment context to result in the occurrence of a *causal factor* in the system structure that was identified in the preceding *HCS* characterisations.

Although the hazardous states of the system inputs may not, strictly speaking, be a hazard that can arise from the emerging behaviour of the system under consideration. the use of the generic operational hazard data class to represent the hazardous states of both an input or an output that crosses the system boundary enables a common notation and method for the characterisation and specification of the *OSR* and *SSR* for both hazardous event types that enables the same format to be used to present the argument for system safety.

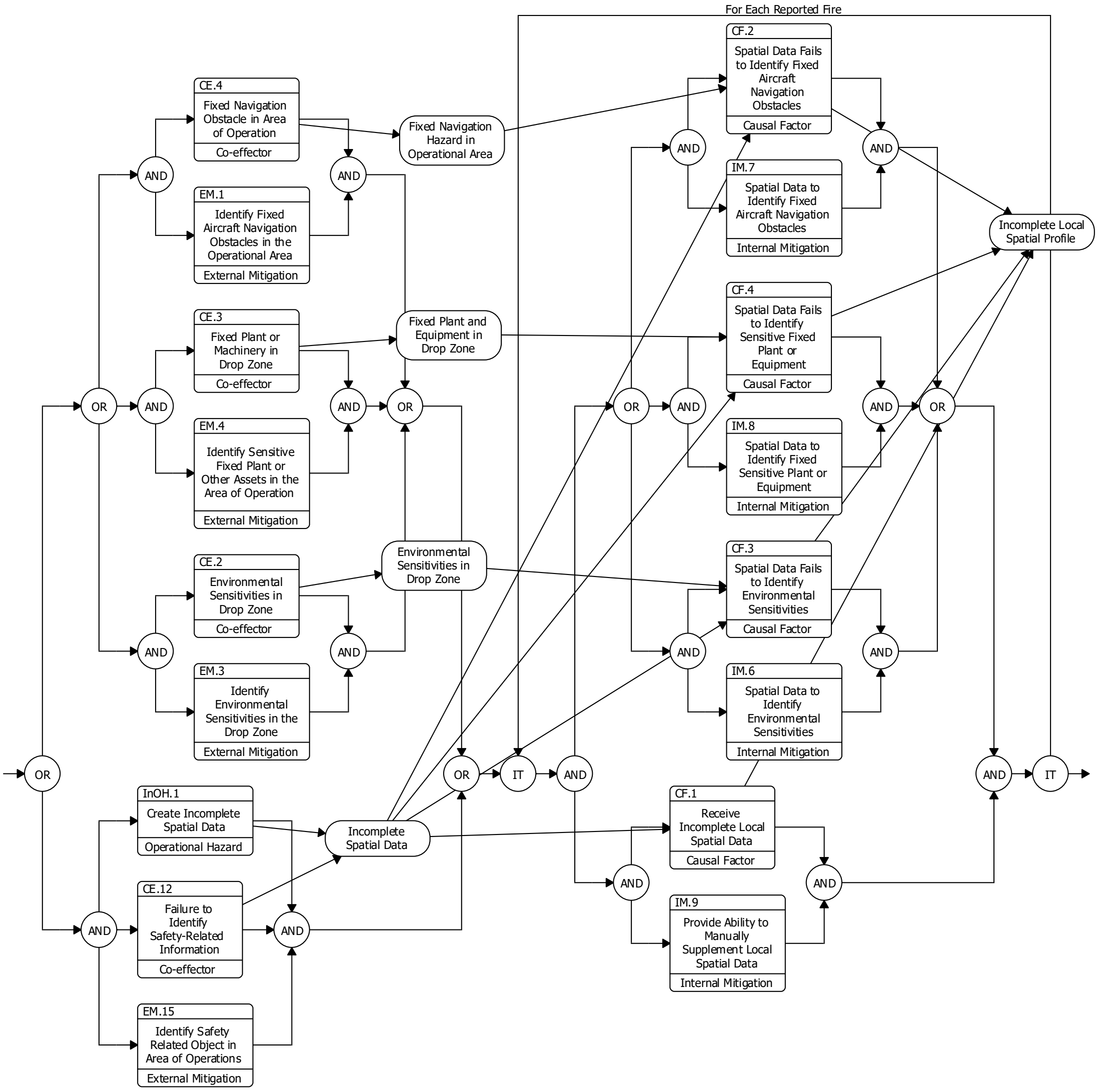
The purpose of the IVA is to take the 'overall' view of systems safety to complete the OHA hazard analysis by considering the system safety characterisations that were developed in the preceding OHA and operational concept development to identify any further issues that can arise from the external provision and internal receipt of the system inputs. The elements depicted on an *IVA* that corresponds to the *accident* depicted in an *accident scenario* are the *causal factors* that were identified in the preceding *HCS* causal chains that can result in a hazardous output *operational hazard*. As the final step in the OHA process the IVA also identifies any issues that arise from the topology of the system as it is to be deployed in its operational context. For example, when the topology of the AFMS capability was considered it was recognised that the AFMS will typically operate as a distributed system that will rely of inter-node communications provided by an external service provider. In the AFMS OHA analysis the need for AFMS operations to be coordinated with ground-based operations was identified, as was the need to be able to supplement the AFMS spatial data with the observations of ground-based operators, however within a distributed application this functionality relies on external inter-node communication. It was also recognised that an inter-node communication failure could result in the inability to send and receive a fire report between distributed AFMS nodes. Similarly, a failure to receive accurate meteorological data in the drop planning activity can affect payload delivery accuracy that can impact on the safe delivery of an aerial payload. The system level implications of these factors are to be included in the IVA analysis.

As per the *HCS*, the *IVA* viewpoint is constructed from the logic of the capability operational model where the operational activities on either side of the system boundary that either provide or receive the selected system input are replaced by their hazardous state representations. IVA *co-effectors* are any external dependencies or constraints on the system under consideration that can impact on the provision and receipt of the identified system input.

The identification of the input *operational hazard* and the related *co-effector(s)*, as well as any new *external mitigation* depicted on an *IVA* is informed by the *co-effectors and external mitigations* identified in the preceding *AS* analysis and the *causal factors* and their *internal mitigations* identified in the *HCS* analysis. C*o-effectors* for an IVA identify any dependencies that the capability has on the provision and receipt of the input of interest. To differentiate between the *input operational hazards* identified in an IVA viewpoint and those identified in the preceding *accident scenario* and *HCS* viewpoints, *input operational hazards* are numbered using the InOH numerical identifier, The use of the same *operational* hazard data type to represent both input and output *operational hazards* allows both types to provide the basis of an *OSR* to specifies its prohibition and SSR to specify the related *internal* and *external mitigations*. This also allows the use of the 'achieved by' relationship between the related *OSR* and *SSR* to forms the structure for the argument that the identified *mitigations* achieve the desired *operational hazard* prohibition.

4.3.1 AFMS Input Vulnerability Analysis Example

Figure 8 depicts the *Input Vulnerability Analysis* viewpoint example for the AFMS Spatial Data input.



For Each Reported Fire
CE.4
Fixed Navigation Obstacle in Area of Operation
Co-effector
Fixed Navigation Hazard in Operational Area
EM.1
Identify Fixed Aircraft Navigation Obstacles in the Operational Area
External Mitigation
CE.3
Fixed Plant or Machinery in Drop Zone
Co-effector
Fixed Plant and Equipment in Drop Zone
EM.4
Identify Sensitive Fixed Plant or Other Assets in the Area of Operation
External Mitigation
CE.2
Environmental Sensitivities in Drop Zone
Co-effector
Environmental Sensitivities in Drop Zone
EM.3
Identify Environmental Sensitivities in the Drop Zone
External Mitigation
InOH.1
Create Incomplete Spatial Data
Operational Hazard
Incomplete Spatial Data
CE.12
Failure to Identify Safety-Related Information
Co-effector
EM.15
Identify Safety Related Object in Area of Operations
External Mitigation
CF.2
Spatial Data Fails to Identify Fixed Aircraft Navigation Obstacles
Causal Factor
IM.7
Spatial Data to Identify Fixed Aircraft Navigation Obstacles
Internal Mitigation
Incomplete Local Spatial Profile
CF.4
Spatial Data Fails to Identify Sensitive Fixed Plant or Equipment
Causal Factor
IM.8
Spatial Data to Identify Fixed Sensitive Plant or Equipment
Internal Mitigation
CF.3
Spatial Data Fails to Identify Environmental Sensitivities
Causal Factor
IM.6
Spatial Data to Identify Environmental Sensitivities
Internal Mitigation
CF.1
Receive Incomplete Local Spatial Data
Causal Factor
IM.9
Provide Ability to Manually Supplement Local Spatial Data
Internal Mitigation
AND
OR
IT

Figure 8 IVA.1 AFMS Spatial Data IVA

Table 7 IVA.1 Operation Hazard, Operational Activity and Co-effector and Causal Factor Causal Chain

Operational Hazard	Hazardous State of	Co-exists with Co-effectors	To Result in Causal Factor
InOH.1 Create Incomplete Spatial Data	ExA.2 Create and Maintain AFMS Spatial Data Set		
		CE.12 Spatial Data Fails to Identify Safety-Related Information	
			CF.1 Receive Incomplete Local Spatial Data
		CE.3 Fixed Plant or Machinery in Drop Zone	
			CF.2 Spatial Data Fails to Identify Fixed Aircraft Navigation Obstacles
		CE.2 Environmental Sensitivities in Drop Zone	
			CF.3 Spatial Data Fails to Identify Environmental Sensitivities
		CE.4 Fixed Navigation Obstacle in Area of Operation	
			CF.4 Spatial Data Fails to Identify Fixed Aircraft Navigation Obstacles

Table 8 IVA.1 Causal Factors, Operational Activity and Operational hazard and Co-effector Causal Chain

Causal Factor	Result of Operational Hazard	and Co-effector	Mitigations
CF.1 Receive Incomplete Local Spatial Data			IM.9 Provide Ability to Manually Supplement Local Spatial Data
	InOH.1 Create Incomplete Spatial Data		EM.15 AFMS to Identify Safety Related Objects
		CE.12 Spatial Data Fails to Identify Safety-Related Information	EM.15 AFMS to Identify Safety Related Objects
CF.2 Spatial Data Fails to Identify Fixed Aircraft Navigation Obstacles			IM.7 Spatial Data to Identify Fixed Aircraft Navigation Obstacles
	InOH.1 Create Incomplete Spatial Data		EM.15 AFMS to Identify Safety Related Objects
		CE.4 Fixed Navigation Obstacle in Area of Operation	EM.1 Identify Fixed Aircraft Navigation Obstacles in the Operational Area
			EM.9 Validate Drop Safety Prior to Drop Delivery
CF.3 Spatial Data Fails			IM.6 Spatial Data to

to Identify Environmental Sensitivities			Identify Environmental Sensitivities
	InOH.1 Create Incomplete Spatial Data		EM.15 AFMS to Identify Safety Related Objects
		CE.2 Environmental Sensitivities in Drop Zone	EM.3 Identify Environmental Sensitivities in the Drop Zone
			EM.9 Validate Drop Safety Prior to Drop Delivery
CF.4 Spatial Data Fails to Identify Sensitive Fixed Plant or Equipment			IM.8 Spatial Data to Identify Fixed Sensitive Plant or Equipment
	InOH.1 Create Incomplete Spatial Data		EM.15 AFMS to Identify Safety Related Objects
		CE.3 Fixed Plant or Machinery in Drop Zone	EM.4 Identify Sensitive Fixed Plant or Other Assets in the Area of Operation
			EM.9 Validate Drop Safety Prior to Drop Delivery

Table 9 identifies selected traceability for the *input operational hazard* that is characterised on Figure 8

Table 9 IVA.1 External Mitigation, Systems Safety Requirements and Causal Factors Traceability

External or Internal Mitigation	Mitigation Specified by	Mitigates Co-effector or Causal Factor
EM.1 Identify Fixed Aircraft Navigation Obstacles in the Operational Area	SSR.1	CE.4 Fixed Navigation Obstacle in Area of Operation
EM.3 Identify Environmental Sensitivities in the Drop Zone	SSR.3	CE.2 Environmental Sensitivities in Drop Zone
EM.4 Identify Sensitive Fixed Plant or Other Assets in the Area of Operation	SSR.4	CE.3 Fixed Plant or Machinery in Drop Zone
EM.15 AFMS to Identify Safety Related Objects	SSR.27	CE.12 Failure to Identify Safety-Related Information
IM.6 Spatial Data to Identify Environmental Sensitivities	SSR.11	CF.3 Spatial Data Fails to Identify Environmental Sensitivities
IM.7 Spatial Data to Identify Fixed Aircraft Navigation Obstacles	SSR.10	CF.2 Spatial Data Fails to Identify Fixed Aircraft Navigation Obstacles
IM.8 Spatial Data to Identify Fixed Sensitive Plant or Equipment	SSR.12	CF.4 Spatial Data Fails to Identify Sensitive Fixed Plant or Equipment
IM.9 Provide Ability to Manually Supplement Local Spatial Data	SSR.18	CF.1 Receive Incomplete Local Spatial Data

5 Requirements Based Safety Argument

Figure 9 describes how the informed by / informs relationship between *internal mitigations* and *internal mitigations* is used to derive the relationships between various SSR. Figure 10 provides an example for the AFMS case study that depicts how the OSR and SSR that were derived from the *operational hazard*, *external mitigation* and *internal mitigations* characterised in the example *AS*, *HCS* and *IVA* viewpoints provided above to create a requirements-based abstract safety argument for the example operational hazard OH.3 Payload Delivery with Sensitivities in the Drop Zone. The safety argument is to be validated by collecting and correlating Objective Quality Evidence (OQE) to verify that the SSR of the argument are upheld.

Each *SSR* specifies both an element of the AFMS operational model and an *internal* or *external mitigation* identified in the hazard analysis. Although not shown on Figure 10 each *SSR* is implemented by a *system requirement* that is, in turn, allocated to an element of the system under construction for implementation and verification. The later part of that traceability is not defined for the AFMS case study for which a corresponding model of the implementation has yet been defined to be defined.

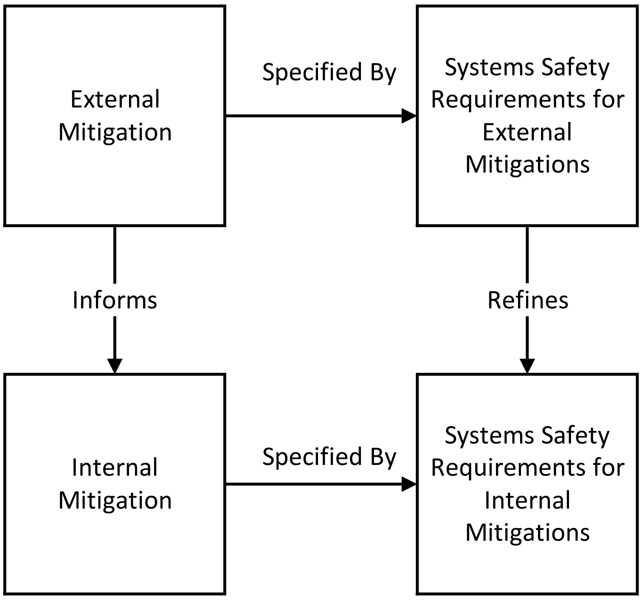

External Mitigation
Specified By
Systems Safety Requirements for External Mitigations
Informs
Refines
Internal Mitigation
Specified By
Systems Safety Requirements for Internal Mitigations

Figure 9 Relationship Between Mitigation Types and Systems Safety Requirement Refinement

Table 10 describes the relationship between selected External Mitigations and the Internal Mitigations that they inform.

Table 10 External Mitigation 'informs' Internal Mitigation.

External Mitigation	Informs Internal Mitigation
EM.1 Identify Fixed Aircraft Navigation Obstacles in the Operational Area	IM.4 Situational Awareness to Highlight Fixed Aircraft Navigation Obstacle ,
	IM.7 Spatial Data to Identify Fixed Aircraft Navigation Obstacles
EM.2 Provide Local Air Space Management	Note: This is a procedural mitigation only
EM.3 Identify Environmental Sensitivities in the Drop Zone	IM.3 Situational Awareness to Highlight Environmental Sensitivities
	IM.6 Spatial Data to Identify Environmental Sensitivities
EM.4 Identify Sensitive Fixed Plant or Other Assets in the Area of Operation	IM.5 Situational Awareness to Highlight Sensitive Fixed Plant or Equipment
	IM.8 Spatial Data to Identify Fixed Sensitive Plant or Equipment
EM.5 Coordinate Aerial Operations with Ground-based Fire Control	IM.9 Provide Ability to Manually Supplement Local Spatial Data
EM.9 Validate Drop Safety Prior to Drop Delivery	Note: this is a procedural mitigation and has no implication for the sysem structure
EM.13 Identify Personnel in the Drop Zone	IM.9 Provide Ability to Manually Supplement Local Spatial Data
	IM.14 Situational Awareness to Highlight Personnel and Mobile Equipment
EM.15 AFMS to Identify Safety Related Objects	IM.6 Spatial Data to Identify Environmental Sensitivities
	IM.7 Spatial Data to Identify Fixed Aircraft Navigation Obstacles
	IM.8 Spatial Data to Identify Fixed Sensitive Plant or Equipment

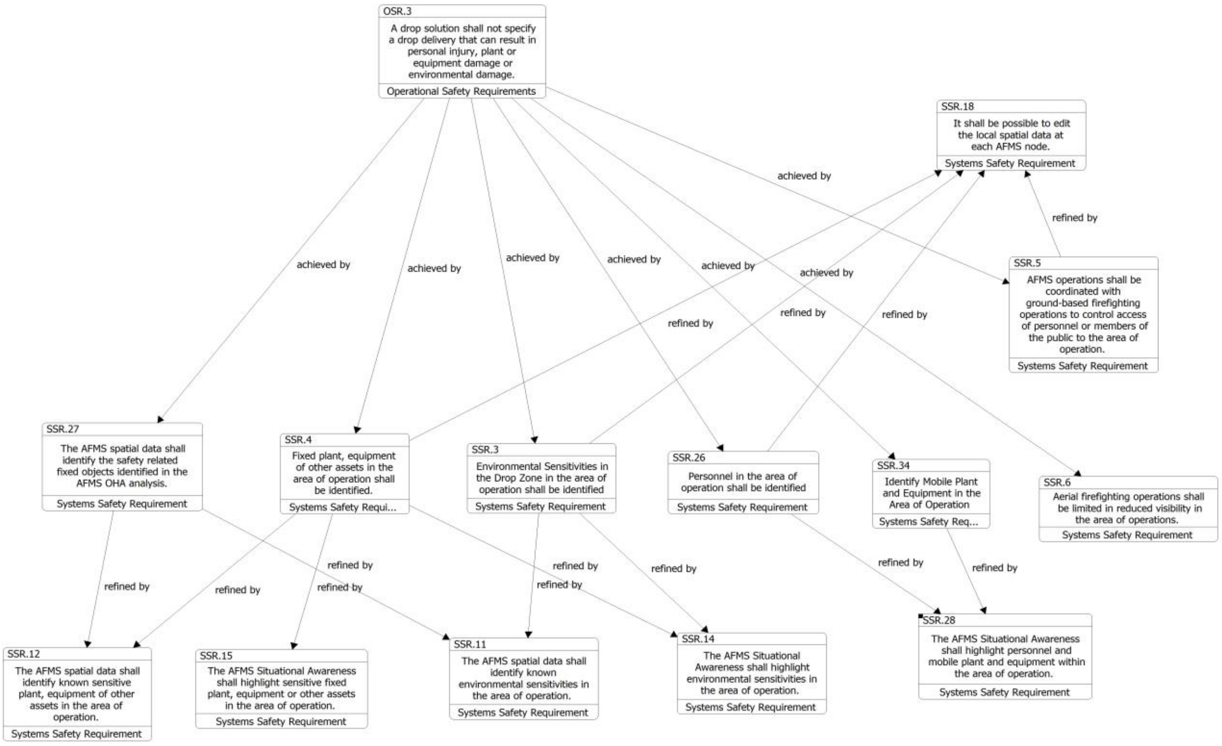

OSR.3
A drop solution shall not specify a drop delivery that can result in personal injury, plant or equipment damage or environmental damage.
Operational Safety Requirements
SSR.18
It shall be possible to edit the local spatial data at each AFMS node.
Systems Safety Requirement
achieved by
refined by
achieved by
achieved by
achieved by
achieved by
achieved by
achieved by
refined by
refined by
refined by
SSR.5
AFMS operations shall be coordinated with ground-based firefighting operations to control access of personnel or members of the public to the area of operation.
Systems Safety Requirement
SSR.27
The AFMS spatial data shall identify the safety related fixed objects identified in the AFMS OHA analysis.
Systems Safety Requirement
SSR.4
Fixed plant, equipment of other assets in the area of operation shall be identified.
Systems Safety Requi...
SSR.3
Environmental Sensitivities in the Drop Zone in the area of operation shall be identified
Systems Safety Requirement
SSR.26
Personnel in the area of operation shall be identified
Systems Safety Requirement
SSR.34
Identify Mobile Plant and Equipment in the Area of Operation
Systems Safety Req...
SSR.6
Aerial firefighting operations shall be limited in reduced visibility in the area of operations.
Systems Safety Requirement
refined by
refined by
refined by
refined by
refined by
refined by
refined by
refined by
refined by
SSR.12
The AFMS spatial data shall identify known sensitive plant, equipment of other assets in the area of operation.
Systems Safety Requirement
SSR.15
The AFMS Situational Awareness shall highlight sensitive fixed plant, equipment or other assets in the area of operation.
Systems Safety Requirement
SSR.11
The AFMS spatial data shall identify known environmental sensitivities in the area of operation.
Systems Safety Requirement
SSR.14
The AFMS Situational Awareness shall highlight environmental sensitivities in the area of operation.
Systems Safety Requirement
SSR.28
The AFMS Situational Awareness shall highlight personnel and mobile plant and equipment within the area of operation.
Systems Safety Requirement

Figure 10 Sample AFMS Requirements Based Safety Argument Example

6 Summary

The *OHA* method presented in this paper specialises the hazard analysis and requirement specification concepts of DEF(AUST)5679 for the analysis of the operational domain model of a generic capability architecture. Performing *OHA* at the concept phase of the system lifecycle allows the results of the analysis to inform the development of the operational concept leading to the development of a safety-aware operational concept.

The process uses *AS* to depict how hazardous states of a system’s external output (*operational hazard*) could co-exist with defined states in the context of the system deployment (*co-effectors*) to result in an *accident*. *External mitigations* can be added to an *accident scenario* to reduce the risk of an *operational hazard*, *co-effector*, or *accident*.

Any aspect of an external mitigations that cannot be provided within the capability operational concept must be identified as the source of a constraint for incorporation into the capability operational procedures.

For any *operational hazard* that is depicted on an *accident scenario* that has an *external mitigation* that is considered to have an implication for the capability operational concept a *HCS* is constructed to characterise how initiating events (*causal factors*) in the system structure can cause the occurrence of the *operational hazard* on the system boundary. *Internal mitigations* can be added to the *HCS* to reduce the risk associated with either a *causal factor* or an *operational hazard* to achieve the required level of risk mitigation. If the required level of risk reduction cannot be achieved, then the feasibility, or structure, of the operational concept for the capability may need reconsidered. No attempt is made in this paper to identify an acceptable level of risk, as that is dependent on the application domain and the risk appetite of the risk acceptance authority.

The method uses *OSR*, to specify that identified *operational hazards* must never occur, and *SSR* to specify the implementation-agnostic safety requirements of the capability. Trace links established from an *operational safety requirement* to one or more *SSR* creates the structure of an abstract, implementation-agnostic, argument for systems safety. Further trace links established between the *SSR* and the *system requirements* that specify the implementation completes the specification of systems safety. Collectively, these processes establish a top-to-bottom safety requirements framework that creates a logical structure to present the argument for systems safety that traverses the operational to system, or abstract to concrete domains of the capability architecture.

Although it is not possible to ensure that all *operational hazards*, *co-effectors*, *accidents* and *causal factors*, and their respective *internal mitigations* and *external mitigation* have been identified within the analysis, the approach of systematically considering how each external output, from each boundary operational activity of the operational activity model can create potential hazardous states enables a level of confidence to be achieved regarding the thoroughness of the analysis. As with any safety or risk analysis, the final verification of the assessment is via peer and stakeholder review.

Since the *operational hazards* are initially identified simply as unsafe outputs, with the subsequent *accident scenario* context analysis driving the refinement of the *operational hazard* set there are minimal requirements for a knowledge of hazard analysis to undertake the *OHA* method with the *external mitigations* identified in the accident scenarios informing the subsequent identification of *causal factors* and *internal mitigations.*

Although *OHA* may be performed independently of a capability architecture, its integration into a MBSE toolset can allow some aspects of the method to be automated, and allow static testing of the analysis to provide confidence in the completeness of both the operational model as well as the *OHA* products. Furthermore, traceability between the operational hazards and causal factor hazardous states of the activities of the operational model can be used to identify the need to revisit the safety assessment in response to changes to the operation concept. The script-based report generation capability of MBSE tools can also provide a repeatable method for generating design documentation and safety analysis artefacts based on the current contents of the living MBSE capability baseline defined within the architecture framework.

Using the AFMS case study to produce sample outputs of *OHA* demonstrated this to be a systematic logical method to perform a top-down safety analysis enabling the development of a safety-aware AFMS operational concept and the derivation of a set of *OSR* and *SSR* for the AFMS that complemented the AFMS operational model and the related operational requirements that specified the implementation-agnostic user needs for the AFMS.

7 References

Australian Department of Defence. (2008). Safety Engineering for Defence Systems, Australian Defence standard DEF(Aust) 5679 / Issue 2, Australian Government.

Bailes, M. (2022) Operational Hazard Analysis and the Safety-aware Concept Development Method. University of Queensland. Brisbane, Australia.

Hollnagel, E. (2012). FRAM, the functional resonance analysis method modelling complex socio-technical systems. Farnham, Surrey, UK England: Ashgate.

International Electrotechnical Commission. (2019). IEC-61508 Functional safety of electrical / electronic / programmable electronic safety related systems.

US Department of Defense. (2012). MIL-STD 882E Department of Defense Standard Practice Systems Safety.