Functional Hazard Assessment in Product-Lines – A Model-Based Approach

Ibrahim Habli, Tim Kelly, Richard Paige

Department of Computer Science, University of York, York, United Kingdom

Abstract. A product-line can offer the reuse of complete lifecycle assets, comprising planning, development and assessment artefacts. In safety-critical systems engineering, safety assessment artefacts are indispensable assets which are expensive to generate. For safety-critical product-lines, it would be cost-effective to encapsulate these assessment artefacts as reusable assets, i.e. to provide the capability of reusing a product-line function or component in addition to its safety assessment artefacts. In this paper, we focus on Functional Hazard Assessment of a product-line’s functions. We propose a product-line functional hazard model which is integrated with the product-line context and domain models. We also show how this proposed product-line functional hazard model fits within the product-line processes.

Keywords: Product-lines, model-driven development, safety-critical systems, functional hazard assessment

1 Introduction

Reuse is a recognised approach to reducing the development cost of software-intensive systems. Instead of analysing, designing, implementing and verifying a function or a component from scratch every time, it would be more cost-effective to develop it once and reuse it in multiple systems. Specifically, reuse could be more cost-effective if it is managed according to predefined contextual and architectural constraints such as in product-line development. Product-line development is an approach to large-scale and holistic reuse. A product-line can offer the reuse of complete lifecycle artefacts comprising planning, development and assessment artefacts. In safety-critical product-lines, safety assessment artefacts generated from Functional Hazard Assessment (FHA), Fault Tree Analysis (FTA) and Failure Mode and Effect Analysis (FMEA) [1] produce the main evidence supporting claims that the system is acceptably safe to operate within a specific environment. These safety assessment artefacts are indispensable assets which are expensive to generate. To this end, it would be advantageous to encapsulate these artefacts as reusable product-line assets, i.e. to provide the capability of reusing a product-line function or component in addition to its safety assessment artefacts (e.g. its failure mode assessment data). However, to be able to reuse safety assessment artefacts in a trustworthy manner, the relationship between a reusable function or component and its associated safety
assessment artefacts should be explicitly and unambiguously modelled. In other words, it is not enough to emphasise the importance of the process by which the safety assessment information is generated, but also the importance of the model against which the structures, relationships and assumptions underlying the generated assessment information are captured. The safety assessment process is carried out once whereas the generated assessment information, identified and specified against the model, is reused multiple times. In this paper, we focus on Functional Hazard Assessment of a product-line’s functions. We propose a product-line functional hazard model that is integrated with the product-line context and domain models. We also show how this proposed product-line functional hazard model fits within the product-line processes.

This paper is structured as follows. Section 2 presents a brief introduction of FHA, followed by an overview of the modelling approach proposed in this paper (Section 3). Section 4 proposes a product-line functional hazard model and how it interfaces with product-line context and domain models. Section 5 shows how the proposed product-line functional hazard model fits within the product-line’s domain and derivation processes. The paper concludes with a summary in Section 6.

2 Functional Hazard Assessment

Functional hazard assessment (FHA) is an inductive technique which examines the way in which system functions contribute to system safety [1]. FHA identifies failure conditions associated with system functions and the effects these failure conditions can have on overall safety. Failure conditions are typically identified by considering three hypothetical deviations: (1) function not provided, (2) function provided when not required and (3) function provided incorrectly. The effects of each failure condition are then identified, specifically those affecting the intended behaviours of the system, its environment and users. FHA then classifies each function based on the severity of the effects of the function’s failure conditions. Failure conditions leading to deaths or injuries are typically classified as ‘Catastrophic’ or ‘Hazardous’. Less severe failure conditions are typically classified as ‘Major’ or ‘Minor’. Finally, system safety requirements are defined, addressing each failure condition in accordance with the severity of its classification (i.e. rigour in specifying and meeting the safety requirements of a function is proportionate to the criticality of the function).

3 Approach Overview

System safety aspects and the way in which they are identified and assessed cannot be considered in isolation from the system’s context, functions and dependencies. This is mainly because safety is a consequential attribute; i.e. safety conditions such as hazards, failure conditions and failure modes are an outcome of certain system functionalities and behaviours in a given environment. This is why system hazards are typically identified given the safety analysts’ understanding of the system functions and their environment. For example, safety conditions are stated given certain
assumptions about data sampling rate, level of independence, expected operation modes, maintenance procedures and end-user training. In this paper, we focus on one particular class of safety conditions: *Functional Hazards*. Functional hazards are functional failure conditions with hazardous consequences, e.g. loss of braking capability or inadvertent engine thrust control. These failure conditions cannot be identified and analysed without a sufficient understanding of the system functions and the way in which they interact with one another and with their environment. Specifically, in a product-line, functions are typically captured in the domain model as high-level *features*. The product-line environment, on the other hand, is defined in the context model. As such, any product-line functional hazard model should interface with the product-line context and domain models.

![Fig. 1. Overall Structure of the Product-Line Models](image)

An overview of the interrelationships between the functional hazard, context and domain models is depicted in Figure 1 (a more detailed description of these models is presented in the next section). The context model captures information regarding the structure of the physical, operating, support, maintenance and regulatory environment of the product-line systems. Broadly speaking, the context model defines external constraints that these systems need to respect. Without a clear definition of these, implicit contracts and dependencies between these systems and their support environment could be violated, leading to uncertainties regarding the assumed safe behaviours of the systems. The domain model, on the other hand, considers the structures of, and interactions between, *features* provided by systems in a domain. A feature is a set of related capabilities and characteristics that represent a logical unit of functionality for the stakeholders of the product [2] [3]. Features in a domain model have explicit associations with one another and with environmental factors (e.g. particular functions deployed only during certain operational phases). Finally, the functional hazard model captures failure conditions, effects, severity classification and safety requirements which relate to specific functional and environmental configurations, as defined in the context and domain models.

One special characteristic of product-line development is variation management. The product-line context and domain models capture how products, derived from the product-line’s assets, are permitted to vary from one another. These products vary in terms of the functions they provide or the environment in which they can be deployed. Because of the interdependency between the product-line’s functions, environment and functional hazards, functional hazards are not immune from the impact of functional and contextual variation. The nature and severity of functional hazards assumed to be associated with a certain reusable function may change due to certain permitted configurations of the variation points defined for that function.
Uncertainties in the traceability between a function and the hazards that may be posed by that function, due to certain product-line variations, are dangerous and unacceptable in the safety domain. Seemingly simple variations in the original and new deployment of reusable functions may contribute to the occurrence of hazards or failure modes previously assumed to be irrelevant to the system [5].

To this end, the management of variations and the way in which they affect safety, however minor, is a prerequisite for trusted reuse. We believe that the impact of variation on safety can be identified, traced and controlled by integrating the product-line functional hazard model with the context and domain models. By adopting a model-based approach to managing the safety impact of product-line variation, product-line functions, along with their associated functional hazard information, can be reused with greater confidence and without the need for the reassessment of these functions whenever reused in the derivation of new products.

![Variability Metamodel](image)

**Fig. 2.** Example Generic Variability Metamodel [5]

Many models for describing variability have been proposed in the product-line literature [5] [6] [7] [8] [9] [10]. In essence, a variability metamodel comprises variability points (figure 2). Variability points specify places in an artefact where variability can arise [11]. Variability points are bound by engineers to create concrete variants of variable artefacts or attributes. Variability points are often interdependent in that the binding of one variability point may restrict the binding of other variability points. For example, for safety, a choice of relevant operation modes and their criticality in a context model may dictate the binding of certain variability points regarding the level of partitioning in the design model. This in turn may have impact on how the bound design artefact could contribute to system hazards identified in the safety models. In this report, we do not prescribe a specific structure for the variability metamodels. The context, domain and functional hazard models defined in the next section are generic and can easily be interfaced with variability models which comprise, as a minimum, explicit variability points and the resulting variants.

## 4 Product-Line Functional Hazard Model

In this section, we propose a functional hazard model for product-line development. This model defines the relationships between, on the one hand, product-line
functional and environmental variants and, on the other hand, their corresponding failure conditions, effects, classifications and safety requirements.

Fig. 3. Product-Line Functional Hazard Model

The product-line functional hazard model is depicted in Figure 3 (please note that, for presentation purposes, the depicted model is an abstraction of the original model which is created in the form of an Ecore model [12]). In the model in Figure 3, a 'failure condition', which is a subtype of a 'condition' and associated with a 'functional variant', can lead to one or more 'effects' (an effect is also a subtype of a 'condition'). Each effect is associated with a 'classification' based on the severity of this effect from the safety perspective. It is important to note that the two elements 'Functional Variant' and 'Contextual Variant' are the main source of the variation. The 'failure condition', 'effect', 'classification' and 'safety requirement' model elements can also vary, though in a subsequential manner. That is, variation in failure conditions, effects, classifications and safety requirements, within the scope of the FHA, is not indigenous and is a consequent of the variation in functional specifications and the environment (e.g. operation phase, temperature and behaviour of other internal and external functions). A failure condition occurs and leads to certain effects due to, and in the context of, a certain configuration of functional variants and contextual variants. When this configuration varies, the failure condition and its associated effects may also vary. Similarly, the classification of the same failure condition effect in a product-line may vary. For example, in-flight engine shutdown may be classified as 'Minor' for one aircraft whereas classified as 'Hazardous' for another. This depends on the various ways in which the aircraft and engine product-lines are configured (e.g. variation in the number of engines fitted). In
particular, the impact of variation in functions and external conditions is captured in Figure 3 in the following association classes:

**Failure Condition and Effect Association Class:** The relationship between a failure condition and its effects is governed by specific conditions which are associated with certain configurations of functional and contextual variants. These configurations may vary, and as a result, the causal relationship between failure conditions and effects may vary accordingly. For example, the same failure condition of a function may lead to different effects in a product-line FHA depending on the various permitted configurations of this function within certain environments.

**Effect and Classification Association Class:** A failure condition in a product-line FHA may lead to one or more effects. However, once an effect occurs, its classification may depend on functional and contextual variants other than those affecting the occurrence of the failure condition(s). Therefore, it is important to explicitly capture separately the functional and contextual variants that affect classification.

**Safety Requirement Association Class:** Derived safety requirements are one of the outputs of an FHA – “Assignment of requirements to the failure conditions to be considered at the lower level” [1]. Safety requirements are not only associated with failure conditions, but also with the classification of these failure conditions. Safety requirements for the same failure condition in a product-line can differ when the failure condition has more than one classification – i.e. due to permitted variation that can affect classification. To this end, a safety requirement in the FHA model in Figure 3 is linked with the association that relates a failure condition to its effect. Similarly, a safety requirement in the FHA model is linked with the association that relates the effects of a failure condition to its classification. In this way, we can ensure that the integrity and rigour associated with defining and meeting the safety requirement is proportionate to the classification of the failure condition addressed by that safety requirement. In short, variation in safety requirements is a function of variation in (1) the association leading to failure conditions and (2) the association influencing the classification of these failure conditions.

### 5 Product-Line Functional Hazard Assessment Process

In this section, we present an approach to integrating FHA into the product-line’s domain engineering and application engineering phases. The role of the FHA in the domain engineering phase is to examine the failure conditions associated with each variant of a function addressed in the feature model by producing the function’s effects, classification and associated safety requirements. These product-line failure conditions, effects, classifications and safety requirements are captured against the product-line functional hazard model defined in the previous section. This enables functional hazard data to be reused whenever a function in the feature model is selected in the derivation of a new product as part of the product-line. As shown in Figure 4, the FHA is the first safety assessment method applied in the product-line domain engineering phase and is highly associated with the product-line domain and
context analysis. The relationship between the FHA activity and the context and domain modelling activity is bidirectional. When a function is captured as a feature in the feature model, and its environment defined in the context model, each variant of the function, given its specified context, is examined in the FHA to determine its failure conditions, effects, classifications and safety requirements.

![Product-Line Safety Process](image)

**Fig. 4. FHA in the Product-Line Domain Engineering Phase**

The FHA results also play a role in constraining certain configurations of features or contextual assumptions which may pose unacceptable safety conditions. For example, the functional hazard data may show that the severity of certain failure condition effects of a function (represented as a feature) are unacceptable within the agreed scope of a product-line and may therefore result in imposing constraints on the selection of that function (e.g. it may be within the scope of the product-line to address **hazardous** but not **catastrophic** events). Furthermore, as part of defining the functional variants of the product-line’s feature model, decisions and assumptions can be made regarding independence between the product-line’s functions (e.g. to avoid common mode failures). Decisions and assumptions concerning independence, affecting safety, should be explicitly captured and managed as part of the product-line FHA. In the product-line feature model, constraints should be established, based on the product-line FHA results, that restrict feature compositions that can violate assumed independence between functions, e.g. independence between functions and their monitors.

In the product-line’s application engineering phase, the functional hazards posed by each function, reused in the derivation of a new product, should be identified and analysed. However, this analysis is not carried out from scratch. Each product function, along with its associated contextual conditions, are fed into the product FHA activity, which in turn checks for potential matches with functional and contextual variants whose failure conditions have been previously captured in the product-line functional hazard model. Whenever there is a match, relevant failure condition data should be added to the product functional hazard model and linked with the product’s requirements and contextual conditions. In the case of mismatches,
the safety analysts need to examine the sources of these mismatches. For example, mismatches can due to product-specific functions or product-specific contextual assumptions. Safety analysts should analyse these new functions or contextual assumptions and generate their corresponding failure conditions, effects, classifications and safety requirements. These failure conditions, effects, classifications and safety requirements should not only be added to the product FHA model, but should also be added to the product-line FHA model and therefore should be available for reuse, where relevant, in the analysis of future products.

6 Summary

We have proposed a product-line functional hazard model, which is integrated with the product-line context and domain models. We have also proposed a way in which this functional hazard model fits within the product-line processes. We are currently validating the functional hazard model against a number of safety assessment processes as defined in some aerospace and automotive standards. We are also working on a generic safety assessment metamodel for product-lines which could be integrated with a product-line’s context, domain and reference architecture models.

References