# FHA Profile

**Dave Banham**

**Version: 0.3**

**Date: 26 Sept 2018**

This information is provided by Rolls-Royce in good faith based upon the latest information available to it; no warranty or representation is given; no contractual or other binding commitment is implied.

Copyright © 2018 Rolls-Royce

# TABLE OF CONTENTS

1. FHA Profile ........................................ 4

1.1. RR FHA Profile Diagram ........................................ 6

1.1.1. Stereotypes ........................................ 7

1.1.1.1. RR FHA Failure Mode ........................................ 7

1.1.1.2. RR FHA Final Effect of Failure ........................................ 9

1.1.1.3. RR FHA Likelihood Qual Score ........................................ 9

1.1.1.4. RR FHA Severity Score ........................................ 10

1.1.1.5. RR FHA Situation ........................................ 11

© 2018 Rolls-Royce

# NOTE TO READERS

An automated document generator that uses a set of rules to extract information from a model and then render it as text and diagrams has produced this document. Consequences of this are: presentation of the same information more than once due to the model's reuse of the same facts; deep section nesting due to the natural hierarchies in the model.

© 2018 Rolls-Royce

# 1. FHA PROFILE

Disclaimer: The SysML lightweight extension profile described herein does not wholly or partly represent an approved method of performing *Functional Hazard Assessment* in Rolls-Royce plc. The profile's use is therefore experimental. (C.f. TRL4) As such, additional care must be taken to avoid mistakes in any aspect of the profile's design and implementation (including the associated Microsoft Excel based model data extractor), or in the profile's application, irrespective of whether the guidance for its use is strictly followed or not.

This SysML lightweight extension profile allows a Functional Hazard Assessment (FHA) against system functions to be performed and captured in the system's MBSE model(s).

Functional Hazard Analysis is defined by SAE ARP 4761 and is applied early in the safety engineering lifecycle. At the earliest stage in the lifecycle, high-level (i.e. "system") functional requirements are a source of definition for the desired system functions and are amendable to an initial FHA. These functional requirements and other forms of analysis (e.g. mission analysis) that elicitate function requirements can be further developed by the use of functional models that describe the system functions in terms of what they logically produce, what they logically need, and what they are logically dependent on. These more detailed (but still high level) models can then be further refined using FHA. In both applications, the result of the FHA is to identify concerns that can be resolved by the reworking the functional requirements and functional model(s), and by the addition of safety requirements. These safety requirements can then be refined into additional system functionality to satisfy them. A further application of FHA can then be initiated to assess these new functions.

FHA is similar to HAZOP (IEC61882:2016), in that both methods seek to find undesirable and potentially hazardous effects that could arise from functional failures. Both methods make use of contextualised guidewords to systematically assess these failure modes, the most obvious of which is the "No" (or "None") guideword meaning the function completely fails to deliver. Other typical guidewords include "too much" and "insufficient" for example.

Note that this profile does not (currently) provide the means to capture a list of the guidewords in the model. This is an open point of discussion, but the reason for not

© 2018 Rolls-Royce

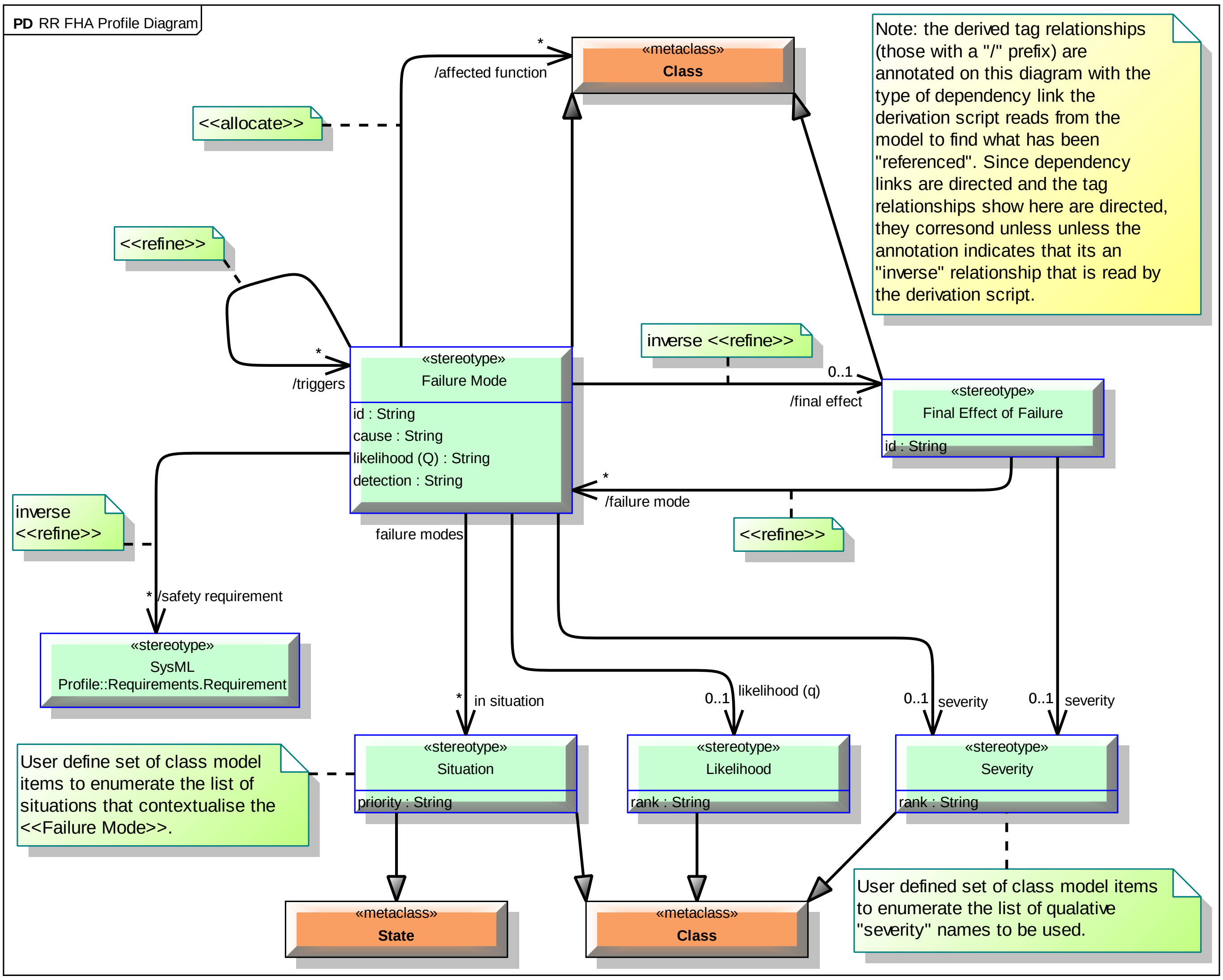
implementing it at this stage is that guidewords can be specific to nature of the functions (and implicitly their input and outputs); for example, continuous functions versus event-triggered functions. This then creates the potential need for multiple guideword lists in the same model, which is difficult to design a profile to facilitate. A downside to not capturing an explicit use of guidewords is that it is not possible to assess how complete the analysis is based on the level of guideword usage per function.

The profile consists of a number of stereotypes and their associated tags. Some of the tags provide the means to store descriptive strings and some provide the means to store references to other stereotyped model items. The profile also defines a small number of toolbar extensions to aid working with the profile.

Whilst the design of the profile aims to allow a wide variety of model item kinds to be used to denote the "system functions", the bulk of the testing to date has been conducted with SysML «Requirement» model items on requirement diagrams.

© 2018 Rolls-Royce

## 1.1. RR FHA Profile Diagram



Note: the derived tag relationships (those with a "/" prefix) are annotated on this diagram with the type of dependency link the derivation script reads from the model to find what has been "referenced". Since dependency links are directed and the tag relationships show here are directed, they corresond unless unless the annotation indicates that its an "inverse" relationship that is read by the derivation script.

User define set of class model items to enumerate the list of situations that contextualise the <<Failure Mode>>.

User defined set of class model items to enumerate the list of qualative "severity" names to be used.

Figure 1 RR FHA Profile Diagram

This profile diagram shows the FHA stereotypes, their value tags, and their reference tag relationships.

There are a number of relationships that need to be established between «Failure Mode» and «Final Effect» model items that require the use of «allocate» and «refine» dependency relationships. These are noted on the affected reference tag connectors on this diagram. Note that as the reference tag connectors are directed (there is an arrowhead) and as the «allocate» and «refine» dependency relationships are directed, the intent is that the direction of use follows the direction between the stereotypes on the profile diagram, unless otherwise indicated by the use of the word "inverse".

© 2018 Rolls-Royce

The «Severity» and qualitative «Likelihood» model items can have a "rank" value assigned. The rank values for all of the severities in a model should be unique. Similarly, the rank values for all of the likelihoods in a model should be unique. This allows a programmatic examination of the model to apply an ordering to the severities and qualitative likelihoods. One application of ordered severities and likelihoods is to allow the risk score to be determined.

The «Situation» model items can have a "priority" value assigned. One application is to allow a programmatic examination of the model to filter, or order, the failure model items based on the situation they have been assigned.

Note that this profile relies heavily on the *name alias* feature of stereotypes and tags to hide their underlying and long names, which is intended to ensure they will not clash with any other profile's stereotypes.

## 1.1.1. Stereotypes

### *1.1.1.1. RR FHA Failure Mode*

Name Alias: Failure Mode

Keyword: Failure Mode

Description: Failure Mode is an element describing a departure of an item from its required or intended operation, function, or behaviour; problems that users encounter.

•The inability of a system, subsystem, or component to perform its required function.

•The inability of an item to perform within previously prescribed and specified limits.

Failure Mode base metaclass is UML Class.

| **Name** | **Name Alias** | **Tag Definition Type** | **Description** |
|---|---|---|---|
| RR FHA tag FM id | id | String | A record id for this failure mode. |
| RR FHA tag FM | affected | Reference | |

© 2018 Rolls-Royce

| Name | Name Alias | Tag Definition Type | Description |
|---|---|---|---|
| affected function | function | | |
| RR FHA tag FM cause | cause | String | A description of the possible causes leading to the stated failure mode. |
| RR FHA tag FM likelihood (quantitative) | likelihood (Q) | String | The quantitative likelihood of failure.<br>NB units of measure are up to the analyst - be consistent!<br>Leave blank if the qualitative measure of likelihood is being used. |
| RR FHA FM likelihood (qualitative) | likelihood (q) | Reference | The qualitative likelihood of failure.<br>Leave blank/null if the quantitative measure of likelihood is being used. |
| RR FHA tag FM Severity | severity | Reference | The severity classification of the failure mode. |
| RR FHA tag FM final effect | final effect | Reference | The failure mode's final effect of failure. |
| RR FHA tag FM in situation | in situation | Reference | Operation Situation Classification List / [Note: classification list to be tailored to specific disciplines / standards] |
| RR FHA tag FM trg | triggers | Reference | The antecedent failure modes that may result in this failure mode. |
| RR FHA tag FM | detection | String | Detectability of the functional failure mode |

© 2018 Rolls-Royce

| Name | Name Alias | Tag Definition Type | Description |
|---|---|---|---|
| detection | | | |
| RR FHA tag FM safety requirement | safety requirement | Reference | A safety requirement that provides a risk reduction to this failure mode. |

Table 1 RR FHA Failure Mode Tag Definitions

#### 1.1.1.2. RR FHA Final Effect of Failure

Name Alias: Final Effect of Failure

Keyword: Final Effect

Description: Final Effect of Failure is an element describing the operation of a system or an item as the result of a failure; i.e., the consequence(s) a failure mode has on the operational behaviour, function, or status of a system or an item. [SAE ARP 4761].

Final Effect of Failure base metaclass is UML Class.

| Name | Name Alias | Tag Definition Type | Description |
|---|---|---|---|
| RR FHA tag FEoF id | id | String | A record id for this final effect. |
| RR FHA tag FEoF failure mode | failure mode | Reference | The failure mode(s) for which this final effect is a consequence. |
| RR FHA tag FEoF Severity | severity | Reference | The severity classification of the final effect. |

Table 2 RR FHA Final Effect of Failure Tag Definitions

#### 1.1.1.3. RR FHA Likelihood Qual Score

Name Alias: Likelihood

© 2018 Rolls-Royce

Keyword: Likelihood

Description: Likelihood is a model element that describes a qualitative likelihood score. A set of likelihood model elements describes all of the values in a qualitative likelihood metric.

| **Name** | **Name Alias** | **Tag Definition Type** | **Description** |
|---|---|---|---|
| RR FHA tag Likelihood rank | rank | String | The rank of the qualitative likelihood score in a set of defined qualitative likelihood scores. Used for sorting purposes. A sort order of descending numerical order is proposed; i.e. highest ranked (i.e. most probable) likelihood comes first. A value of 0 means unranked. The assigned rank value to each likelihood in the set should be unique to obtain a strict ordering. |

**Table 3 RR FHA Likelihood Qual Score Tag Definitions**

#### *1.1.1.4. RR FHA Severity Score*

Name Alias: Severity

Keyword: Severity

Description: Severity is a model element that describes a severity score. A set of severity model elements describes all of the values in a severity metric.

| **Name** | **Name Alias** | **Tag Definition Type** | **Description** |
|---|---|---|---|
| RR FHA tag Severity rank | rank | String | The rank of the severity in set of defined severities. Used for sorting purposes. A sort order of descending numerical order is proposed; i.e. highest ranked severity comes first. A value of 0 means unranked. The |

© 2018 Rolls-Royce

| Name | Name Alias | Tag Definition Type | Description |
|---|---|---|---|
| | | | assigned rank value to each severity in the set should be unique to obtain a strict ordering. |

Table 4 RR FHA Severity Score Tag Definitions

### *1.1.1.5. RR FHA Situation*

Name Alias: Situation

Keyword: Situation

Description: A situation model element describes a specific situation that a failure mode can manifest.

| Name | Name Alias | Tag Definition Type | Description |
|---|---|---|---|
| RR FHA tag Severity priority | priority | String | The priority of the situation in the hazard analysis.<br>A numerical descending order scale is suggested (i.e. highest priority value in the set has the highest priority), with 0 meaning unclassified priority or don't care. Situations can have equal priority with the same assigned priority value. |

Table 5 RR FHA Situation Tag Definitions

© 2018 Rolls-Royce