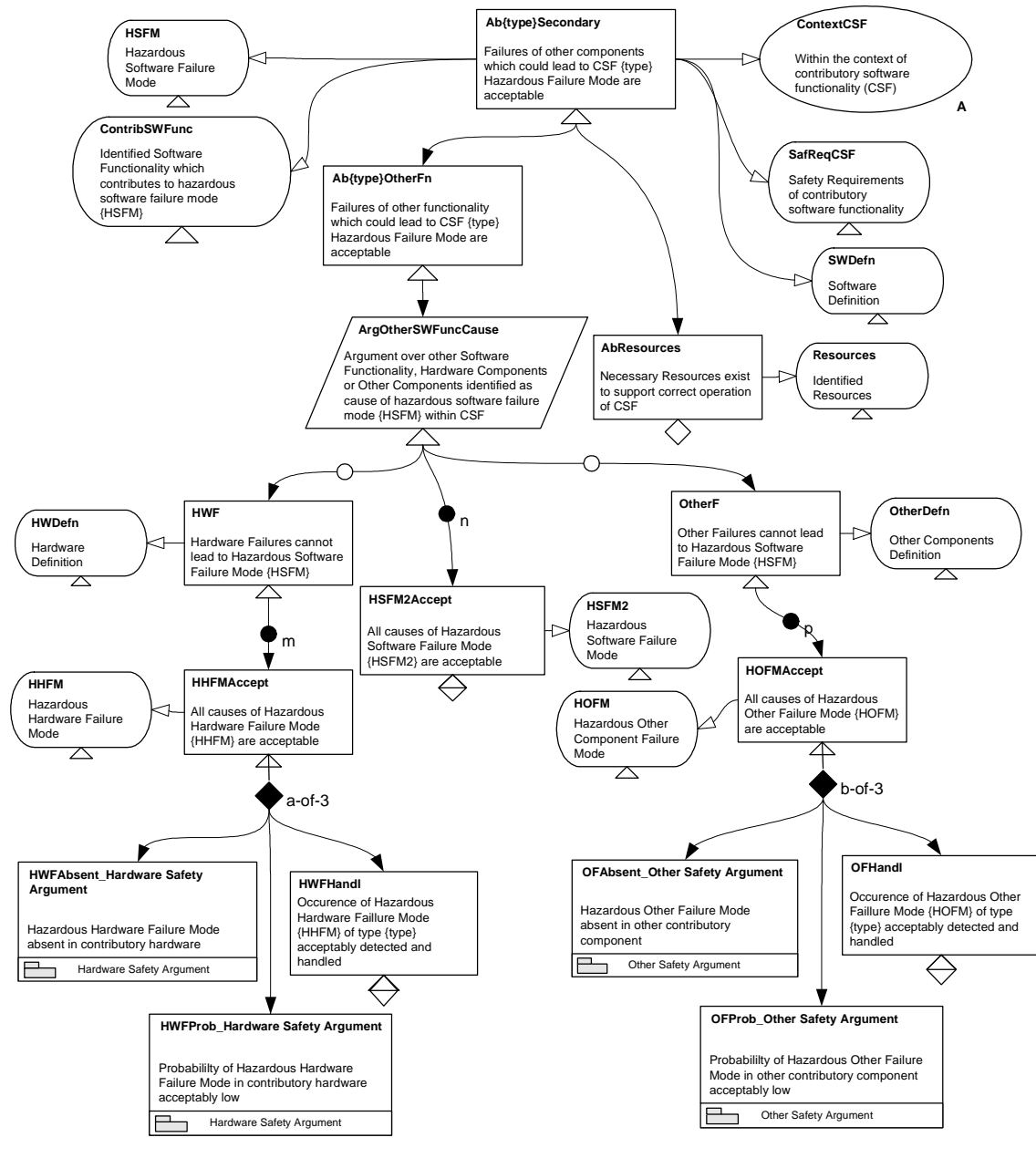


Effects of Other Components

Author(s)	Rob Weaver, John McDermid, Tim Kelly		
Created	18/09/00	Last Modified	20/04/04

Intent	The intent of this pattern is to argue that the effects of other components (software, hardware or other) are acceptable with respect to the hazardous software failure mode under consideration.
Also Known As	
Motivation	The motivation for this pattern is to be able to argue about failure modes in other components to demonstrate they cannot induce a failure mode in the software functionality under consideration. Hardware and Other component failure modes can be address through showing absence, probability of occurrence or handling of the failure. Software Failure Modes can be addressed in the same way as the original failure mode in another pattern.

Structure



Participants	Abs{type} Secondary	The overall objective of the argument - to provide sufficient support for the claim that secondary causes of a particular type of Software failure mode are acceptable.
	HSFM	This context identifies the Hazardous Software Failure Mode, for which this pattern develops the secondary argument.
	ContribSWFunc	This context describes the software functionality that may have a contributing effect to the cause of the software failure mode.

	SafReqCSF	The safety requirements of the contributory software functionality are given as a basis for developing evidence.
	ContextCSF	An assumption is made that only circumstances in which the Contributory Software Functionality (CSF) operates are considered during analysis of the failure mode.
	SWDefn	This Software Definition should give a clear description of the system software. From the model it should be possible to determine how the failure mode contributes to the system level hazard and how other software failures contribute to the failure mode.
	Ab{type}OtherFn	This claim is associated with failures of other functionality within the system. The goal is that failures associated with other functionality which may induce the failure mode within the CSF are acceptable.
	AbResources	This claim is associated with resources in the system on which the CSF is dependent. The goal states that all necessary resources are available within the system, such that failure mode will not be induced in the CSF.
	Resources	This context identifies the resources on which the CSF relies.
	ArgOtherSW FuncCause	This strategy describes the argument approach – decomposing across other functional components (software, hardware, other)
	HWF	This claim asserts that no hardware failures can induce the software failure mode
	HWDefn	This Hardware Definition should give a clear description of the system hardware. From the model it should be possible to identify the hardware contributions to the software failure mode.
	HSFM2Accept	This claim asserts that no other software failures can induce the original software failure mode
	OtherF	This claim asserts that no other component failures can induce the software failure mode

	OtherDefn	This Other Components Definition should give a clear description of the other components of the system. From the model it should be possible to identify the contribution of other components to the software failure mode.
	HHFMAccept	This claim asserts that a particular hardware failure mode which can induce the software failure mode is acceptably and cannot cause the software failure mode to occur.
	HHFM	This context identifies the Hazardous Hardware Failure Mode, which can induce the software failure mode – the subject of this pattern.
	HWFAbsent_ Hardware Safety Argument	This away goal to the hardware safety argument places a requirement on that argument that the Hardware Failure is absent
	HWFProb_ Hardware Safety Argument	This away goal to the hardware safety argument places a requirement on that argument that the probability of occurrence of the Hardware Failure is acceptably low
	HWHandl	This goal asserts the claim that the hardware failure mode can be detected and handled by the software component which it can affect.
	HOFMAccept	This claim asserts that a particular other component failure mode which can induce the software failure mode is acceptably and cannot cause the software failure mode to occur
	HOFM	This context identifies the Hazardous Other Component Failure Mode, which can induce the software failure mode – the subject of this pattern.
	OFAbsent_Other Safety Argument	This away goal to the Other safety argument places a requirement on that argument that the Other Component Failure is absent
	OFProb_Other Safety Argument	This away goal to the Other safety argument places a requirement on that argument that the probability of occurrence of the Other Component Failure is acceptably low
	OFHandl	This goal asserts the claim that the other component failure mode can be detected and handled by the software component which it can affect.

Collaborations	<ul style="list-style-type: none"> • ContribSWFunc identifies the contributory software functionality on which the Ab{type}Secondary claim is made. • SWDefn, ContribSWFunc, HSFM, Resources should be used to identify the resources for which the claim AbResources is made. • The HWDefn, SWDefn and OtherDefn should be suitable to identify failures of Hardware or Other Components and Other Software Functionality that can contribute to the software failure mode for which this pattern is the subject. • The HWDefn and OtherDefn should be suitable to identify the argument approach for arguing that the hardware or other failure mode is absent, has a low probability of occurrence or can be handled.
Applicability	<p>This pattern identifies the claims about parts of the system (hardware, other software functionality, other components) for an argument for particular software failure mode. It assumes that the failure mode has been identified, classified as a certain type and the Contributory Software Functionality has been identified. It also assumes the contributions of the other parts of the system to the software failure mode can be identified.</p>
Consequences	<p>After instantiating this pattern the following undeveloped goals will remain:</p> <ul style="list-style-type: none"> • AbResources, and • Possibly HSFM2Accept, HWFHandl and OFHandl <p>After instantiating this pattern four away goals may need to be satisfied:</p> <ul style="list-style-type: none"> • HWFAbsent_Hardware Safety Argument, HWFProb_Hardware Safety Argument, OFAbsent_Hardware Safety Argument, OFProb_Hardware Safety Argument <p>To satisfy the decomposition of Ab{type}Secondary the necessary goals need to be decomposed and the away goals satisfied.</p>
Implementation	<p>This pattern should be instantiated in a Top Down fashion. All goals and contexts should be instantiated before continuing to a</p>

	<p>lower level in the pattern. This pattern assumes that the software failure mode has already, along with the contributory software functionality.</p> <p>Failures within hardware, other software functionality or other components which could induce the software failure mode should be identified. For failures within the hardware and other components, the approach for arguing about these failures should be determined.</p> <p>The choice of the three claims (Absence and/or Probability and/or Handling) is an m of n selection. It is up to the implementer to choose what technique(s) will be used, depending upon the detail of the failure mode. Where sufficient evidence cannot be generated about absence, probability or handling of the failure mode alone, it is recommended that a combination of these three types of evidence is used.</p> <p>Possible Pitfalls</p> <ul style="list-style-type: none"> • Not correctly identifying all resources on which the contributory software functionality relies may lead to incorrect or insufficient evidence being developed about the acceptability of the secondary components. • Not correctly identifying all hardware, other software functionality and other component failures which could effect the contributory software functionality may lead to incorrect or insufficient evidence being developed about the acceptability of the secondary components. • Selecting an argument approach for which evidence cannot be generated.
Examples	None provided at this stage.
Known Uses	
Related Patterns	<p><i>Absence Omission Hazardous Failure Mode</i> – This pattern has an undeveloped goal which can be the overall objective of <i>Effects of Other Components</i>.</p> <p><i>Absence Commission Hazardous Failure Mode</i> – This pattern has an undeveloped goal which can be the overall objective of <i>Effects of Other Components</i>.</p>

	<p><i>Absence Early Hazardous Failure Mode</i> – This pattern has an undeveloped goal which can be the overall objective of <i>Effects of Other Components</i>.</p> <p><i>Absence Late Hazardous Failure Mode</i> – This pattern has an undeveloped goal which can be the overall objective of <i>Effects of Other Components</i>.</p> <p><i>Absence Value Hazardous Failure Mode</i> – This pattern has an undeveloped goal which can be the overall objective of <i>Effects of Other Components</i>.</p> <p><i>Hazardous Software Failure Mode Classification</i> – This pattern can be used to decompose the undeveloped goal HSFM2Accept.</p> <p><i>Handling of Hardware/Other Component Failure Mode</i> – This pattern can be used to decompose the undeveloped goals HWFHandl and OFHandl.</p> <p>This pattern forms part of a software safety argument pattern catalogue, which includes the following patterns:</p> <p><i>Component Contributions to System Hazards</i></p> <p><i>Hazardous Software Failure Mode Decomposition</i></p> <p><i>Hazardous Software Failure Mode Classification</i></p> <p><i>Software Safety Argument Approach</i></p> <p><i>Absence of Omission Hazardous Failure Mode</i></p> <p><i>Absence of Commission Hazardous Failure Mode</i></p> <p><i>Absence of Early Hazardous Failure Mode</i></p> <p><i>Absence of Late Hazardous Failure Mode</i></p> <p><i>Absence of Value Hazardous Failure Mode</i></p> <p><i>Effects of Other Components</i></p> <p><i>Handling of Software Failure Mode</i></p> <p><i>Handling of Hardware/Other Component Failure Mode</i></p>
--	---