

Architecture Framework for Software Safety

Havva Gulay GURBUZ
Nagehan PALA ER
Bedir TEKINERDOGAN

29.09.2014

Bilkent University
Computer Engineering Department
&



Agenda

- Introduction & Motivation
- Case study: Avionics Control Computer System
- Meta-model for Software Safety
- Viewpoints for Software Safety
 - Hazard Viewpoint
 - Safety Tactics Viewpoint
 - Safety-Critical Viewpoint
- Conclusion & Future Work

Introduction

- ❑ Currently, an increasing number of systems:
 - Controlled by software
 - Rely on the correct operation of the software

- ❑ A safety-critical system:
 - Malfunctioning of software could result in death, injury or damage to environment

- ❑ To mitigate these serious risks:
 - The architecture of safety-critical systems needs to be carefully designed and analyzed

Introduction

- A common practice for modeling software architecture
 - Software architecture viewpoints to model the architecture for particular stakeholders and concerns

- Existing architecture viewpoints
 - general purpose
 - do not explicitly focus on safety concern in particular

- We propose an architecture framework for modeling architecture for software safety to address the safety concern explicitly and assist the architect.

Introduction

- ❑ The architecture framework is based on a meta-model that has been developed after a thorough domain analysis. The framework includes three coherent set of viewpoints each of which addresses an important concern.
- ❑ The framework is not mentioned as a replacement of existing general purpose frameworks but rather needs to be considered complementary to these.
- ❑ The application of the viewpoints is illustrated with a case-study on safety-critical avionics control computer system.

Avionics Control Computer System



Case Study – Requirements

Requirement	Explanation
<i>Display aircraft altitude data</i>	Altitude is defined as the height of the aircraft above sea level. Altitude information is shown to pilots, as well as, also used by other avionics systems such as ground collision detection system. Pilots depend on the displayed altitude information especially when landing.
<i>Display aircraft position data</i>	Position is the latitude and longitude coordinates of the aircraft received from GPS (Global Positioning System). Route management also uses aircraft position. Aircraft position is generally showed along with the other points in the route. Pilots can see the deviation from the route and take actions according to the deviation.
<i>Display aircraft attitude data</i>	Attitude is defined with the angles of rotation of the aircraft in three dimensions, known as roll, pitch and yaw angles. For instance, the symbol, called as ADI (Attitude Direction Indicator), is used to show roll and pitch angles of the aircraft.
<i>Display fuel amount</i>	Fuel amount is the sum of fuel in all fuel tanks. Fuel amount is generally represented with a bar chart in order to show how much fuel remains in the aircraft.
<i>Display radio frequency channel</i>	The radio frequency channel is used to communicate with ground stations.

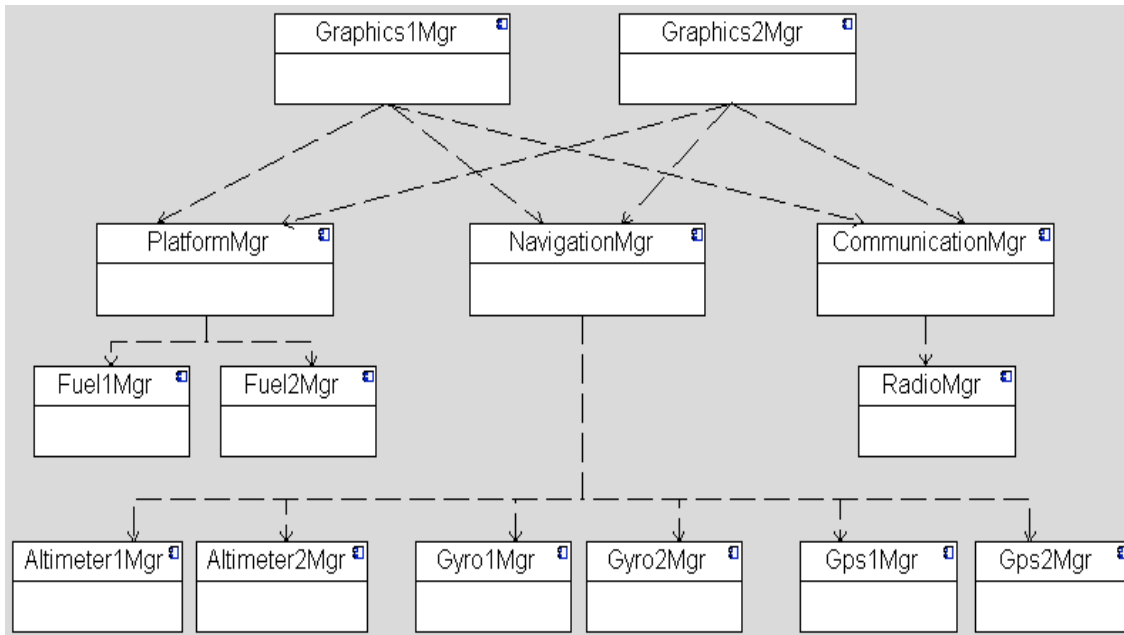
Case Study – Hazard Analysis

Hazard	Possible Causes	Consequence	Severity
HZ1 Displaying wrong altitude data	Loss of/Error in altimeter, Loss of/Error in communication with altimeter, Error in display	Aircraft crash	Catastrophic
HZ2 Displaying wrong position data	Loss of/Error in GPS, Loss of/Error in communication with GPS, Error in display	Aircraft crash	Catastrophic
HZ3 Displaying wrong attitude data	Loss of/Error in gyroscope, Loss of/Error in communication with gyroscope, Error in display	Aircraft crash	Catastrophic
HZ4 Displaying wrong fuel amount	Loss of/Error in fuel sensor, Loss of/Error in communication with fuel sensor, Error in display	Aircraft crash	Catastrophic
HZ5 Displaying wrong radio frequency	Loss of/Error in radio, Loss of/Error in communication with radio, Error in display	Communication error	Negligible

Case Study – Safety Requirements for Hazard HZ1

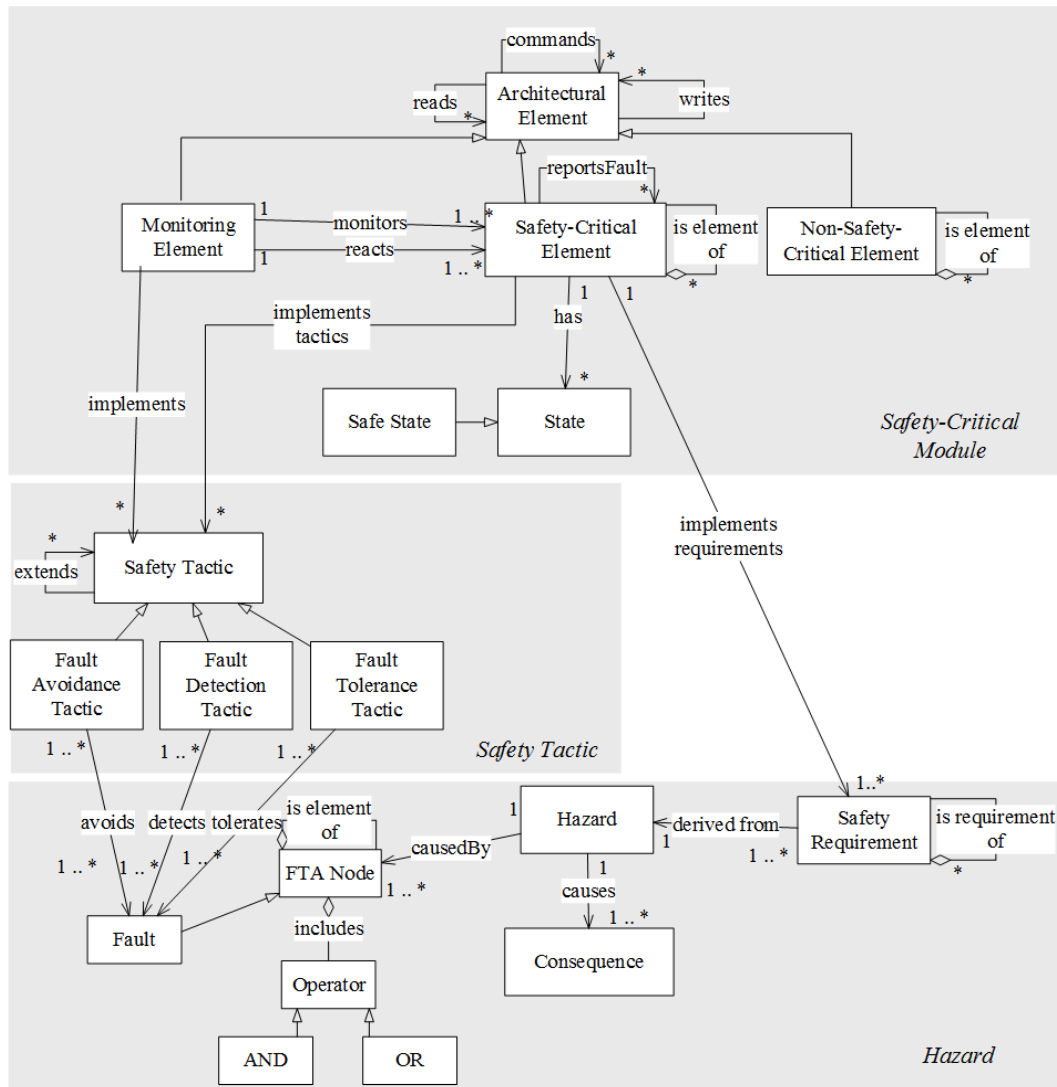
ID	Definition
SR1	Altitude data shall be received from two independent altimeter devices.
SR2	If one of the altitude data cannot be received, the altitude data received from only one of the altimeter device shall be displayed and a warning shall be generated.
SR3	If both of the altitude data cannot be received, the altitude data shall not be displayed and a warning shall be generated.
SR4	If the difference between two altitude values received from two altimeter devices is more than a given threshold, the altitude data shall not be displayed and a warning shall be generated.
SR5	Altitude data shall be displayed on two independent display devices.

Component & Connector View



- ❑ Existing general purpose views do not directly address the safety concerns. For example, the information about whether a component is safety-critical is not explicit.
- ❑ The goal of providing safety concerns in views is two-fold:
 1. Communicating the design decisions related with safety concerns through views
 2. Accomplishing safety analysis of the architecture from views

Meta-model for Software Safety



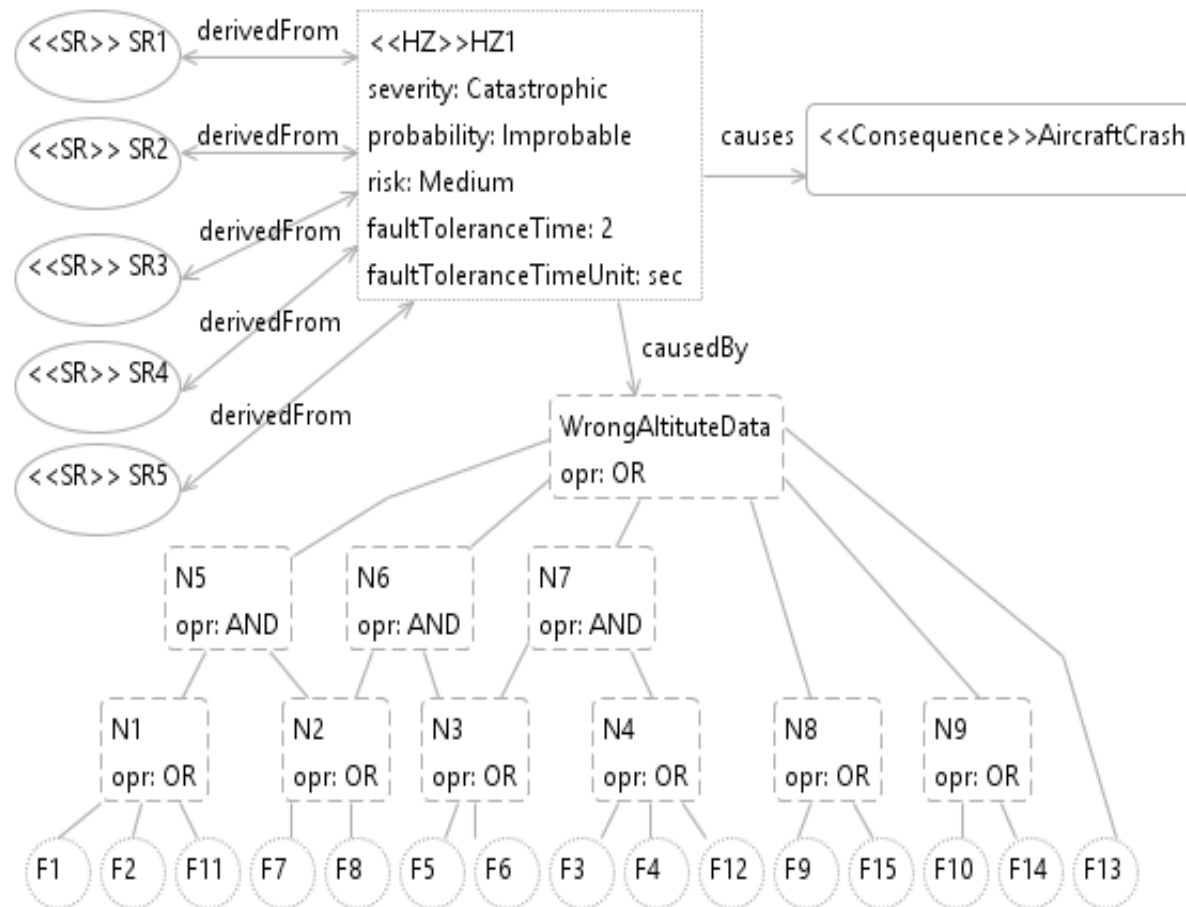
Hazard Viewpoint

Section	Description
<i>Overview</i>	This viewpoint describes the identified hazards, their possible causes and consequences, derived safety requirements from these hazards and possible faults in the system.
<i>Concerns</i>	<ul style="list-style-type: none"> • Which safety requirements are derived from which hazards? • Which faults can cause which hazards? • What are the possible consequences of the identified hazards?
<i>Stakeholders</i>	Software Architect, Safety Engineer
<i>Constraints</i>	<ul style="list-style-type: none"> • One or more safety requirements can be derived from a hazard. • A hazard can cause one or more consequences. • A hazard can be caused by one or more FTA Nodes.
<i>Elements</i>	<p>The diagram illustrates the elements and relationships in the Hazard Viewpoint. It is organized into two rows and three columns.</p> <p>Top Row (Concepts):</p> <ul style="list-style-type: none"> Hazard: Represented by a dashed box containing the text: <<HZ>>, severity:, probability:, risk:, faultToleranceTime: 0, and Fault Tolerance Time Unit:. Consequence: Represented by a rounded rectangle containing the text: <<Consequence>>. Safety Requirement: Represented by an oval containing the text: <<SR>>. <p>Bottom Row (Instances):</p> <ul style="list-style-type: none"> Fault: Represented by a dashed circle. FTA Node for AND: Represented by a dashed box containing the text: FTANode and opr: AND. FTA Node for OR: Represented by a dashed box containing the text: FTANode and opr: OR. <p>Relationships (Bottom Row):</p> <ul style="list-style-type: none"> A double-headed arrow labeled "derivedFrom" connects Hazard and Consequence. A single-headed arrow labeled "causes" points from Hazard to Consequence. A single-headed arrow labeled "causedBy" points from Consequence to Safety Requirement.
<i>Relationships</i>	<p>derivedFrom</p> <p>causes</p> <p>causedBy</p> <p>derived from</p> <p>Causes</p> <p>caused by</p>


Case Study – Faults related with the hazard HZ1

Fault	Description	Fault	Description
[F1]	Loss of altimeter device 1	[F9]	Error in display device 1
[F2]	Loss of communication with altimeter device 1	[F10]	Error in display device 2
[F3]	Loss of altimeter device 2	[F11]	Altimeter1Mgr fails
[F4]	Loss of communication with altimeter device 2	[F12]	Altimeter2Mgr fails
[F5]	Error in altimeter device 1	[F13]	NavigationMgr fails
[F6]	Error in communication with altimeter device 1	[F14]	Graphics1Mgr fails
[F7]	Error in altimeter device 2	[F15]	Graphics2Mgr fails
[F8]	Error in communication with altimeter device 2		

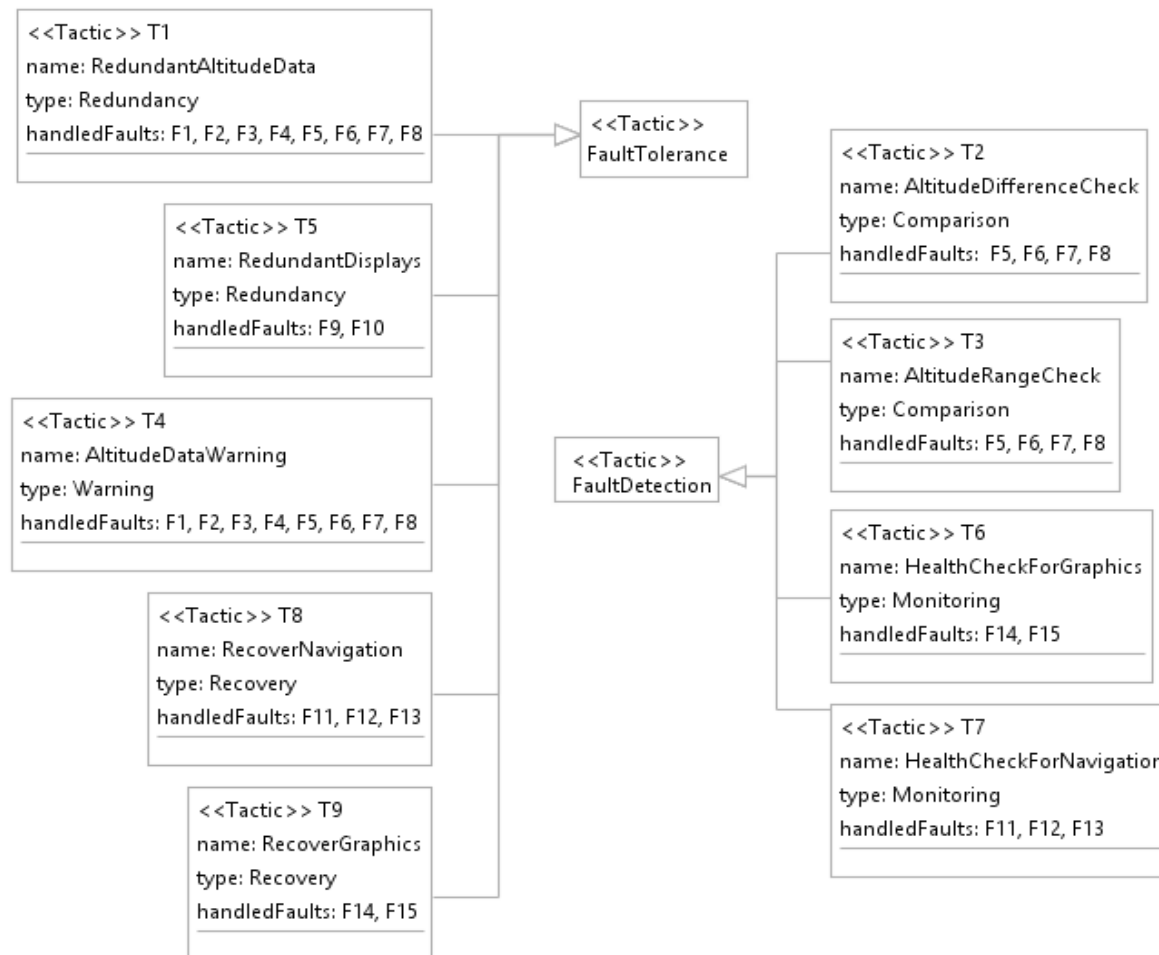
Case Study – Hazard View



Safety Tactics Viewpoint

Section	Description
<i>Overview</i>	This viewpoint describes the safety tactics implemented in the system. Also it shows the faults handled by the safety tactics.
<i>Concerns</i>	<ul style="list-style-type: none"> • What are the applied safety tactics? • Which faults are handled by which safety tactics?
<i>Stakeholders</i>	Software Architect, Safety Engineer, Software Developer
<i>Constraints</i>	<ul style="list-style-type: none"> • A safety tactic can extend different safety tactics.
<i>Elements</i>	<div style="display: flex; align-items: center; justify-content: space-between;"> <div style="border: 1px solid black; padding: 5px; width: 20%;"> <pre><<Tactic>> name: type: handledFaults:</pre> </div> <div style="text-align: center; width: 60%;"> <p>Safety Tactic, Fault Avoidance, Fault Detection, Fault Tolerance</p> </div> </div>
<i>Relationships</i>	 extends

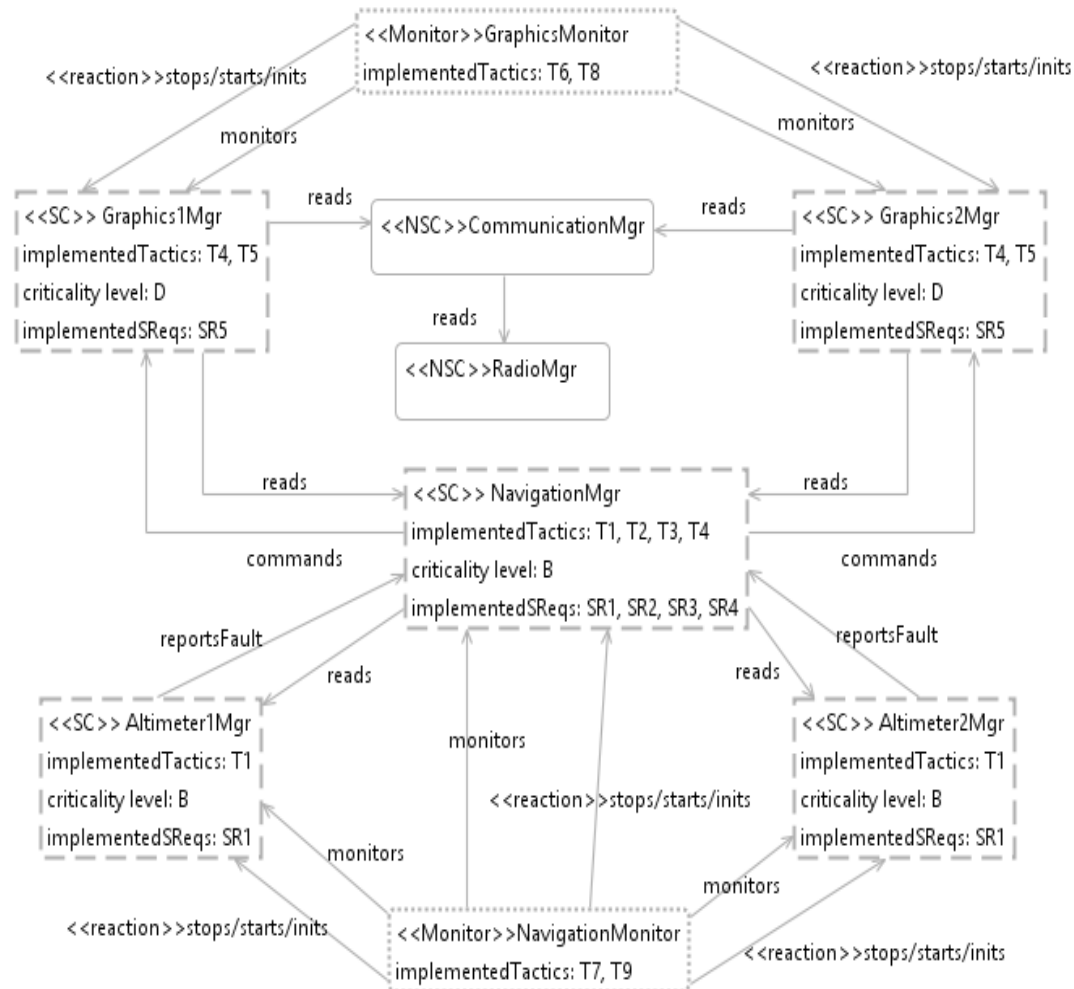
Case Study – Safety Tactics View



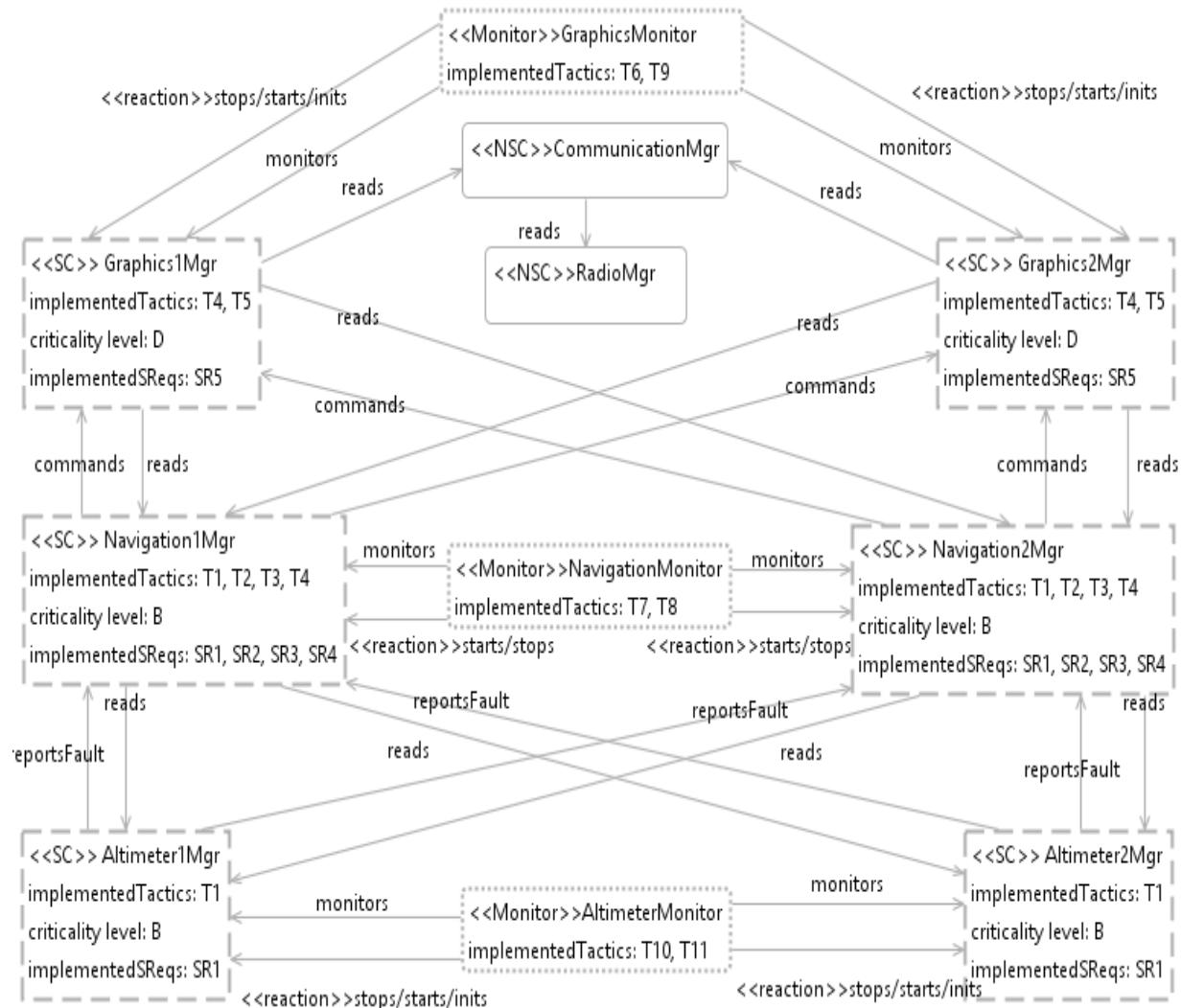
Safety-Critical Viewpoint

Section	Description												
<i>Overview</i>	This viewpoint shows the safety-critical elements, monitoring elements, non-safety-critical elements and relations between them. It presents also the implemented safety tactics by related safety-critical elements and monitoring elements. Additionally it shows the implemented safety requirements by related safety-critical elements.												
<i>Concerns</i>	<ul style="list-style-type: none"> • What are the safety-critical elements and relations between them? • What are the monitoring elements and relations between monitoring and safety-critical elements? • What are the implemented safety tactics and safety requirements by safety-critical elements and monitoring elements? • What are the non-safety-critical elements and relations between them? 												
<i>Stakeholders</i>	Software Architect, Software Developer, Safety Engineer												
<i>Constraints</i>	<ul style="list-style-type: none"> • A safety-critical element can read data from one or more safety-critical elements. • A safety-critical element can write data to one or more safety-critical elements. • A safety-critical element can command one or more safety-critical elements. • A safety-critical element can report fault to one or more safety-critical elements. • A monitoring element can monitor one or more safety-critical elements. • A monitoring element can react (stop/start/init/restart) one or more safety-critical elements. 												
<i>Elements</i>	<p style="text-align: center;"> Safety-Critical Element Non-Safety-Critical Element Monitoring Element </p>												
<i>Relationships</i>	<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="text-align: center; width: 33%;">reads →</td> <td style="text-align: center; width: 33%;">writes →</td> <td style="text-align: center; width: 33%;">commands →</td> </tr> <tr> <td style="text-align: center;">reads</td> <td style="text-align: center;">writes</td> <td style="text-align: center;">commands</td> </tr> <tr> <td style="text-align: center;">reportsFault →</td> <td style="text-align: center;"><<reaction>> →</td> <td style="text-align: center;">monitors →</td> </tr> <tr> <td style="text-align: center;">reportsFault</td> <td style="text-align: center;">reacts</td> <td style="text-align: center;">monitors</td> </tr> </table>	reads →	writes →	commands →	reads	writes	commands	reportsFault →	<<reaction>> →	monitors →	reportsFault	reacts	monitors
reads →	writes →	commands →											
reads	writes	commands											
reportsFault →	<<reaction>> →	monitors →											
reportsFault	reacts	monitors											

Case Study – Safety-Critical View (1st Alternative)



Case Study – Safety-Critical View (2nd Alternative)



Conclusion

- ❑ Designing a safety-critical system requires to show design decisions related to safety concerns explicitly at the architectural level.
- ❑ Existing viewpoint approaches tend to be general purpose.
- ❑ For this purpose, we have introduced the architecture framework for software safety to address the safety concerns explicitly.

Conclusion & Future Work

- Using the viewpoints we could:
 - Analyze the architecture in the early phases of the development life cycle,
 - Analyze the design alternatives,
 - Increase the communication between safety engineers and software developers,
 - Communicate the design decisions related with safety

- Future work:
 - Define metrics and develop tools to analyze several design alternatives for safety-critical systems based on the proposed viewpoints.

Questions?



Thank you.