Project 1





**FDIR**

*Spacecraft fault protection system*

**Euro Team**

|  |  |
| --- | --- |
| **Mikko AHVENNIEMI** | 20096680 |
| **Pierre ALAUZET** | 20096699 |
| **Julien COLIN** | 20096706 |
| **Benoît STARCK** | 20096705 |

**Table of contents**

October 15th, 2009

**CS554 - Design for Software & Systems**

[**Illustration table** 3](#_Toc242777895)

[**Introduction** 4](#_Toc242777896)

[**1.** **Problem understanding** 5](#_Toc242777897)

[1.1. Business case & system context 5](#_Toc242777898)

[**1.1.1.** **FDIR utility** 5](#_Toc242777899)

[**1.1.2.** **System requirements** 5](#_Toc242777900)

[1.2. Problem frames 5](#_Toc242777901)

[**1.2.1.** **Domains identification** 5](#_Toc242777902)

[**1.2.2.** **Context Diagram** 5](#_Toc242777903)

[**1.2.3.** **Problem frames** 5](#_Toc242777904)

[**2.** **Functional requirements (use-case model)** 6](#_Toc242777905)

[2.1. Use-case diagram 6](#_Toc242777906)

[**2.1.1.** **Actors description** 6](#_Toc242777907)

[**2.1.2.** **Use-case diagram** 6](#_Toc242777908)

[**2.1.3.** **Use-case specifications** 7](#_Toc242777909)

[2.2. Sequence diagrams 9](#_Toc242777910)

[**2.2.1.** **Fault recovery** 9](#_Toc242777911)

[**2.2.2.** **Safe response in case of hazardous conditions** 10](#_Toc242777912)

[**2.2.3.** **Critical failure** 10](#_Toc242777913)

[**3.** **Non-functional requirements** 11](#_Toc242777914)

[3.1. Identified quality attributes 11](#_Toc242777915)

[**3.1.1.** **Testability** 11](#_Toc242777916)

[**3.1.2.** **Availability** 11](#_Toc242777917)

[3.2. Improvised quality attributes 11](#_Toc242777918)

[**3.2.1.** **Avaibility** 11](#_Toc242777919)

[**3.2.2.** **Reliability** 11](#_Toc242777920)

[**3.2.3.** **Resilience** 11](#_Toc242777921)

[**3.2.4.** **Response time** 11](#_Toc242777922)

[**4.** **Usability analysis & design** 12](#_Toc242777923)

[a. Preliminary user interface design 12](#_Toc242777924)

[b. Discussion on usability scenarios 12](#_Toc242777925)

[**References** 14](#_Toc242777926)

**Illustration table**

[Figure 1: Use case diagram 6](file:///D:\Documents\UTBM\MON%20CURSUS\GI05\KAIST\Projects\euroteam\Project%201\Part%20Final\CS554_EuroTeam_Project1.docx#_Toc242773046)

**Introduction**

1. **Problem understanding**
   1. Business case & system context
      1. FDIR utility
      2. System requirements
   2. Problem frames
      1. Domains identification
      2. Context Diagram
      3. Problem frames
2. **Functional requirements (use-case model)**
   1. Use-case diagram
      1. Actors description
      2. Use-case diagram

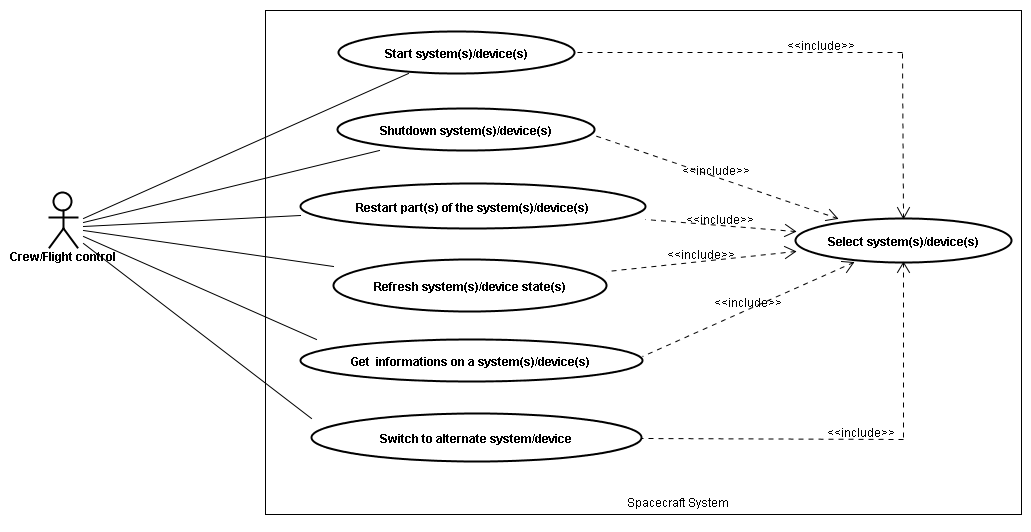


Figure 1: Use case diagram

* + 1. Use-case specifications

|  |  |
| --- | --- |
| Name | Start system(s)/device(s) |
| Actors | Crew / Flight control |
| Description | User can start device(s) or system(s) of the spacecraft system whenever he wants or because it was shutdown |
| Precondition | - System(s) are off  - One or several device(s) or system(s) have been selected |
| Events flow | 1. Click on the “start” button  2. Wait for the system to start |
| Post-condition | System(s) has been started |
| Exception | - System states could be already turned on while it is still displayed as “off” on the FDIR system |

|  |  |
| --- | --- |
| Name | Shutdown system(s)/device(s) |
| Actors | Crew / Flight control |
| Description | User can shutdown device(s) or a part(s) of the spacecraft system whenever he wants or in case of failure |
| Precondition | - Devices or parts of the system have to be running  - One or several device(s) or system(s) have been selected |
| Events flow | 1. Click on the “shutdown” button |
| Post-condition | System(s) has been shutdown |
| Exception | - System states could be already turned off while it is still displayed as “running” on the FDIR system |

|  |  |
| --- | --- |
| Name | Restart part(s) of the system(s)/device(s) |
| Actors | Crew / Flight control |
| Description | User can restart a device or a part of the spacecraft system whenever he wants or in case of failure |
| Precondition | - Device or part of the system has to be running  - Requested system(s)/device(s) have been selected |
| Events flow | 1.  2. Click on the “restart” button |
| Post-condition | System is restarting |
| Exception | - System states could be already turned off while it is still displayed as “running” on the FDIR system |

|  |  |
| --- | --- |
| Name | Refresh system(s)/device(s) states |
| Actors | Crew / Flight control |
| Description | User can refresh the states of any device or system to see if this one is still working correctly or not |
| Precondition | - Device or part of the system has to be running  - Requested system(s)/device(s) have been selected |
| Events flow | 2. Click on the “refresh” button |
| Post-condition | System is refreshing |
| Exception |  |

|  |  |
| --- | --- |
| Name | Switch to alternate system/device |
| Actors | Crew / Flight control |
| Description | If the device is not responding or if there is a failure, user may switch to another system/device |
| Precondition | - Select **one and only one** system or device  - Requested part has been selected |
| Events flow | 2. Click on the “switch” button |
| Post-condition | Alternate system takes the control. |
| Exception | If the alternate system is broken as well, it may generate a fatal error of the system |

|  |  |
| --- | --- |
| Name | Get information on a system(s)/device(s) |
| Actors | Crew / Flight control |
| Description | User may seek information about any device or system on the spacecraft |
| Precondition | - Device has to be working and available for requested action  - Requested system(s)/device(s) have been selected |
| Events flow | 2. Click on the “GetInfo” button |
| Post-condition | Information about the selected system appears on the screen. |
| Exception |  |

|  |  |
| --- | --- |
| Name | Select system(s)/device(s) |
| Actors | Crew / Flight control |
| Description | User can select any system or device in order to issue commands |
| Precondition |  |
| Events flow | 1. Select the requested part(s) |
| Post-condition | The chosen part is selected. |
| Exception | The chosen part is still not selected. |

* 1. Sequence diagrams

We build several sequence diagrams in order to explain in detail the use case diagram and specification. Indeed, as the FDIR system is not represented in the use cases, we need to see how it is interacting with the spacecraft, the crew and the ground controller.

Three sequence diagrams are presented in this part: *Fault recovery*, *Safe response in case of hazardous* **conditions** and *Critical failure*.

* + 1. Fault recovery

Fault recovering scenario shows interactions between the FDIR system and the spacecraft when a fault is detected. FDIR is controlling several values. If one is in an out-of-tolerance state, it be automatically returned to the FDIR which will start the fault localization process. Once the fault has been located, FDIR will be able to proceed to several actions like *recovery*, *shutdown* or *retry*.

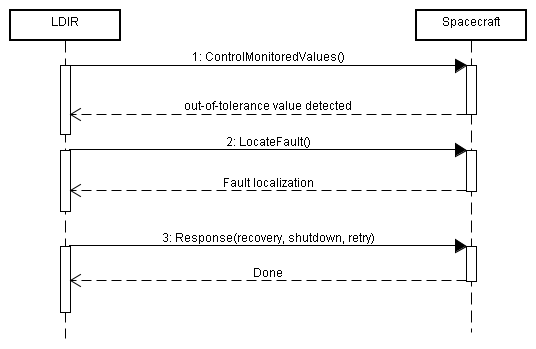


Figure 2: Sequence diagram - Fault recovery

* + 1. Safe response in case of hazardous conditions

This scenario start after that FDIR has detected a hazardous condition of problem in the spacecraft. After having isolated the problem, FDIR is able to proceed to two different actions depending of the kind of spacecraft (unmanned or manned spacecraft).

Within an unmanned spacecraft, FDIR will shut down all the non-critical functions in order to focus on the device/system problem and minimize the damages. It will also move the antenna to point toward earth in order to receive human commands and decisions.

Within a manned spacecraft, process is easier because as humans are inside the spacecraft, they can directly interact with the system without needing is functions shutdown process or antenna redirection. Then LDIR is just giving the hand to the crew.

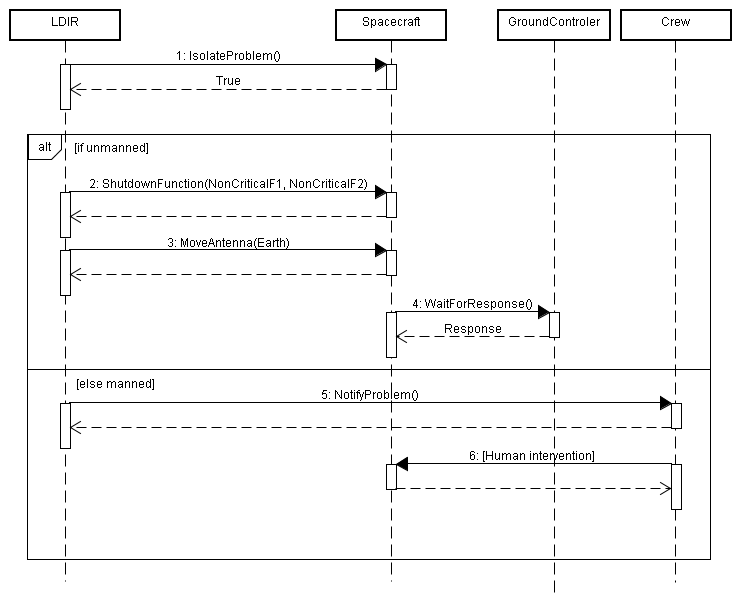
****

Figure 3: Sequence diagram - Safe response in case of hazardous conditions

* + 1. Critical failure

Critical failure scenario starts as the *Fault recovery* scenario (cf. 2.2.1) as we consider the detection of an out-of-tolerance value in the spacecraft. But if a failure cannot be recovered, FDIR system is going thru different decisions and actions. After localizing the error, FDIR is giving the hand to the crew and put itself in a manual mode state. Crew can then execute several actions like *backup*, *shutdown* or *retry*.

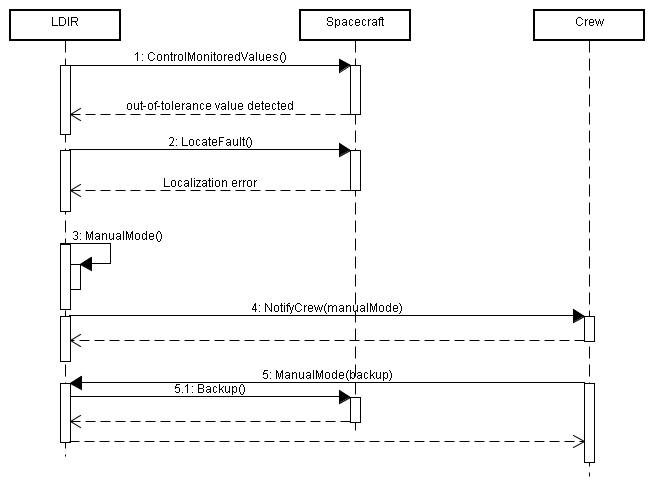
****

Figure 4: Sequence diagram - Critical failure

1. **Non-functional requirements**
   1. Identified quality attributes
      1. Testability
      2. Availability
   2. Improvised quality attributes
      1. Avaibility
      2. Reliability
      3. Resilience
      4. Response time
2. **Usability analysis & design**
3. Preliminary user interface design

Displaying information continuously 🡪 multiple screens but no tabs

Overview of the spacecraft always available 🡪 list of systems & subsystems with information (monitoring values, temperature, pressure)

Professional interface 🡪 non useful features like displaying spacecraft screens. Crew would be formed to be on the spacecraft and do not need to have a visualization of the spacecraft. Title of device or system is enough

Locate the fault 🡪 displaying left panel with spacecraft scheme. List of the systems appearing on the tree should appears on the scheme too. If an alert appears on one system, we should be able to localize it geographically on the scheme.

Keep the control of the spacecraft with safety, observability & commandability 🡪 bottom panel with buttons (shutdown, restart, backup and recovery data)

1. Discussion on usability scenarios

Conclusion

**References**

**Web Sites**

**Articles**

**Books**