Assignment Sheet 1:   
Introduction to Safety Requirements Engineering

Due: Sunday, 2/14/2021, 23:59h

|  |  |
| --- | --- |
| **Team Name** | An98Wi00 |

|  |  |  |  |
| --- | --- | --- | --- |
| **Student 1** |  |  |  |
| **Student 2** |  |  |  |

We will assign quasi-anonymous team names to facilitate a double-blind calibrated peer review. Your Team Name is the first two letters of the mother of whomever you decide is Student 1, followed by the 2-digit birthyear of Student 1, followed by the first two letters of the father of Student 2, followed by the 2-digit birthyear of Student 2. Example:

Student 1: Cynthia, mother is Louise, Cynthia was born in 1997

Student 2: Mark, father is Robert, Mark was born in 2001

🡪 Team Name: Lo97Ro01

Rather than your mother’s or father’s, you may use any other first name that isn’t your own, as long as you consistently use the same one throughout the semester.

Grading Task 1 (*15 Points*)

Assign **up to 2 points for the accuracy** (and applicability) of the description of the chosen example. Ask yourself, if the description of the example gives you a clear picture. If you have open questions, deduct a quarter or half a point, depending how critical the missing information is to properly understand the example.

Assign **up to 3 points for the analysis of RE involvement**:

* Zero points if you merely state that “no RE was done” or “RE was done insufficiently”
* One point for “hindsight lessons” derived from the description (e.g., “there should have been a requirement to prevent X”)
* Two to three points for a detailed description in what way inadequacy in requirements or in the way RE was conducted contributed to the situation.

If the example uses an NTSB, NHTSA, or similar official report (i.e., not a news website), please make not of it.

Please use the below grading template to grade each case example from each time. Leave one sentence of a rationale for point deductions or for explanations what was particularly well done.

Grading Scheme

**Team Name:** *Ch99Sa00*

|  |  |  |
| --- | --- | --- |
| **Case Example Name** | **Mars Polar Lander Failure** | |
| **Points** | **Rationale** |
| **Description** | 2 + 1 | The description was very concise and provided adequate information about the dev. Project failure. The sources used were also both from common sites such as news, but also a .gov website. Which I added +1 extra credit points for providing an official report. |
| **Analysis of RE**  **Involvement** | 3 | The RE paragraph provided that there were “hindsight” lessons that were learned. As well as providing the report that showed what went wrong within the requirements engineering process. |
| **TOTAL** | 6 | (over 5 due to extra credit from the article references) |

|  |  |  |
| --- | --- | --- |
| **Case Example Name** | **Explosion of the Ariane 5** | |
| **Points** | **Rationale** |
| **Description** | 2 + 1 | The description provided a wonderful report on what occurred during the failure/accident. As well as properly notifying what the mistake costed, both with lives and money. For the sources, I decided to add another point of extra credit. Due to the abundance of links that I would not deem as news outlets. |
| **Analysis of RE**  **Involvement** | 3 | The RE paragraph showed the exact error within the Requirements engineering process that caused this mistake/failure to happen. It was very clear that the mistake made was since there was an error within keeping the software update to date/maintaining the software. |
| **TOTAL** | 6 | Article references which were non news based, both the Description and RE involvement paragraphs were superb in showing what happened and where things went wrong. |

|  |  |  |
| --- | --- | --- |
| **Case Example Name** | **Example 3** | |
| **Points** | **Rationale** |
| **Description** | 1.75 + 1 | The description provided great insight about what occurred, and what the cost of this error was. But I was a bit confused/curious when I read the sentence about people who wore the helmets vs who did not (it says that helmets were not required for two paramedics). I wish I was able to know if those 2 people died, and the ones with helmets lived. Or if there was no difference and everyone suffered either death or the injuries. The description also references NTSB sources, and the articles/sources linked are not from major news outlets. So, I provided 1 bonus point, and subtracted .25 for the helmet controversy I explained before. |
| **Analysis of RE**  **Involvement** | 3 | The RE paragraph adequately described what went wrong within the RE process, as well as what caused the issue to happen in the first place. Also, NTSB article was referenced multiple times (already gave 1 extra credit point for that within the description paragraph). |
| **TOTAL** | 5.75 | Provided extra 1 point due to sources being .gov/NTSB sources. |

**Team Name:** *Na99Ma96*

|  |  |  |
| --- | --- | --- |
| **Case Example Name** | *London Ambulance fiasco* | |
| **Points** | **Rationale** |
| **Description** | 1.75 | The description explained the problem and provided details such was when the incident occurred. There was information such as what the effects of this failure was as well. I do wish that there was information pertaining to if anyone died, or if any people were seriously injured since it was stated that there were ambulances that failed to be notified to go to certain areas. Other than that, the description provided a lot of information. |
| **Analysis of RE**  **Involvement** | 3 | The RE paragraph showed that the mistake within the RE process was the lack of communication between the developers and the stakeholders (dispatchers etc.). This paragraph properly showed where the accident could have been resolved if there was a proper RE process when developing the application. |
| **TOTAL** | 4.75 | There were no scholarly sources, or non-news articles for this case. |

|  |  |  |
| --- | --- | --- |
| **Case Example Name** | **$2 billion air traffic control system failed by running out of computer memory** | |
| **Points** | **Rationale** |
| **Description** | 2 | The description explained the problem and the effect that it caused. There was also a reference provided. |
| **Analysis of RE**  **Involvement** | 3 | The RE paragraph explained exactly were they thought things went wrong within the Requirements engineering process. It was very clear that it was due to not paying attention to the restraints that the system had. They also explained the fact that there are now provisions in place this way the problem does not occur again. |
| **TOTAL** | 5 | There were no scholarly sources, or non-news articles for this case. |

|  |  |  |
| --- | --- | --- |
| **Case Example Name** | **Heartland Payment Systems 134 million credit cards compromised** | |
| **Points** | **Rationale** |
| **Description** | 1 | While the description did explain what the failure/accident was. I felt that there was much more information that could have been said. Such as the year or date that this happened. Or if there could have been more information provided on what occurred. I am taking off a point due to lack of information that could have been provided otherwise. |
| **Analysis of RE**  **Involvement** | 2 | While the RE paragraph did state what would be a hindsight finding about the SQL injection attacks, it also provided information such that Heartland was warned for multiple years. As well as the fact they did not consider that the most common attack at the time were SQL injection attacks. There should have been stricter testing within the RE process even before the QA session would have occurred. The paragraph adequately shows that there was not an emphasis on security when developing the product. I decided to give a 2/3 due to the fact that there was a pinpoint on the warnings Heartland missed, but there could have been more emphasis on where exactly within the RE process things went wrong. |
| **TOTAL** | 3 | There were no scholarly sources, or non-news articles for this case. |

**Team Name:** *Pa99Mi99*

|  |  |  |
| --- | --- | --- |
| **Case Example Name** | **Communications company O2 network outage in the UK** | |
| **Points** | **Rationale** |
| **Description** | 2 | The description for this I felt was very detailed in explaining what exactly happened when and where, and for how long people were affected. |
| **Analysis of RE**  **Involvement** | 2 | The RE for this example makes it very clear how the outage was an RE issue and explains goes in depth into what caused the lead up to this issue. However, with that in mind the specific requirement that was not met wasn’t specifically mentioned. It only describes that a full set of possible test cases wasn’t provided and was the culprit for this failure. |
| **TOTAL** | 4 | Don’t forget extra credit? |

|  |  |  |
| --- | --- | --- |
| **Case Example Name** | *National Grid SAP project failure* | |
| **Points** | **Rationale** |
| **Description** | 2 | The description for this I felt was very detailed in what caused this failure, how long it went on for, how much in costs, and what else was affected due to the failure. |
| **Analysis of RE**  **Involvement** | 3 | This RE description was perfect in that is it lists several different requirements issues that lead up to the failure. From management issues to overrun budgets. |
| **TOTAL** | 5 | Don’t forget extra credit? |

|  |  |  |
| --- | --- | --- |
| **Case Example Name** | *Biometric System failure in Heathrow* | |
| **Points** | **Rationale** |
| **Description** | 1 | Description is vague in that it doesn’t directly say what exactly was wrong with the system other than it had potential of a data breach. |
| **Analysis of RE**  **Involvement** | 2 | Most RE related in this is implied but it isn’t clear exactly to what exactly it had to do with this failure. Only saying that it is possible that it wasn’t fully scoped. However, it does say what could’ve been done to prevent the issue |
| **TOTAL** | 3 | Don’t forget extra credit? |

NOTE: This group did three more on top of the previous that are only from NTSB not sure if these should replace the above, or if +1 should be added to the ones above, etc.

|  |  |  |
| --- | --- | --- |
| **Case Example Name** | **Airplane accident** | |
| **Points** | **Rationale** |
| **Description** | 1 | The description for this I felt was very lacking in detail. It says there was corrosion that caused the issue however no information on the flight number, amount of people injured (if any), location of where it occurred. |
| **Analysis of RE**  **Involvement** | 1 | I don’t believe this is a requirement issue as the only possible RE issue is ability to view the joints that had corrosion. |
| **TOTAL** | 3 | +1 From NTSB |

|  |  |  |
| --- | --- | --- |
| **Case Example Name** | **Airplane accident 2** | |
| **Points** | **Rationale** |
| **Description** | 1.5 | The description for this I felt was very lacking in detail. It says there was damage to elevator control rods from high winds that caused the accident however no information on the flight number, amount of people injured (if any), location of where it occurred. However, it does mention there was a know deficiency in the mechanical gust lock design. |
| **Analysis of RE**  **Involvement** | 1 | The description gave an idea of a possible RE issue but this section only mentions that that the design didn’t take harsh weather into account and that the design could’ve been perfected instead of more on the gust lock design and how its design failed. |
| **TOTAL** | 3.5 | +1 From NTSB |

|  |  |  |
| --- | --- | --- |
| **Case Example Name** | **Airplane accident 3** | |
| **Points** | **Rationale** |
| **Description** | 1.75 | Description of what happened is detailed. However, no info on the aircrafts flight number, and where it was located. |
| **Analysis of RE**  **Involvement** | 1 | I don’t think this is a RE design issue, at least not from what I can tell by the RE involvement description given. |
| **TOTAL** | 3.75 | +1 From NTSB |

|  |  |  |
| --- | --- | --- |
| **Low Quality Example** | | **Score** |
| **Was it a project failure or an accident?** | | **\_\_\_\_\_ / 5,00** |
| X | Development project failure |
|  | Accident |
| **Description of the Failure / Accident:** | |
| The Therac-25 medical accelerator was a radiation therapy device meant to combat tumors. This device unfortunately delivered lethal doses of radiation to several people seriously injuring many, and killing 6. This was a result of a bug within the program's operating system. This bug is known as a datarace, and they can make data unpredictable. When a doctor used the interface, sometimes the configurations assigned to the machines weren't the ones they selected, and intense amount of radiation would be exposed to the patient. | |
| **Involvement of Requirements or the Requirements Engineering Process:** | |
| RE: in this scenario was done irresponsibly. When the program was being developed, an operating system developed by an untrained programmer should not have been the first choice for industry standard medical equipment. All and all the entire development of this program was relatively unorganized, and unreliable. | |

|  |  |  |
| --- | --- | --- |
| **Medium Quality Example** | | **Score** |
| **Was it a project failure or an accident?** | | **\_\_\_\_\_ / 5,00** |
|  | Development project failure |
| *X* | Accident |
| **Description of the Failure / Accident:** | |
| A new information system for better handling of route changes for scheduled flights by air traffic controllers failed on seven occasions between 2014 and 2018. One of the failures was a result of overloaded system memory, and caused thousands of flights to be either delayed or cancelled for several days. This particular failure was caused by a U-2 spy plane that had filed a very complex flight plan that was loaded onto the system memory when the airplane entered the airspace. Unlike most commercial planes which send information back to the air traffic controller to better guide them, this plane did not send this information, which caused the software to begin searching for possible midair collisions involving this plane and all others at all altitudes. | |
| **Involvement of Requirements or the Requirements Engineering Process:** | |
| The failures of the ERAM system would have been found before deployment if the requirements of the project had specified a solution that takes into account the limited system memory of the air traffic controller’s computers. One solution would be to require a memory saving solution in the event of a complex flight plan. This would have been discovered during extreme case testing.  Another solution would be to have minimum system specifications required of the end user, just like many programs do. Using this, they could specify that the air traffic controllers would need to improve their system’s available memory, which would prevent these failures. Another issue was that the requirement for annual testing of the contingency plans for ERAM failure were not implemented. | |

Reference: <https://www.oig.dot.gov/sites/default/files/FAA%20Actions%20to%20Address%20ERAM%20Outages%20Final%20Report%5E11-07-18.pdf>

|  |  |  |
| --- | --- | --- |
| **High Quality Example** | | **Score** |
| **Was it a project failure or an accident?** | | **\_\_\_\_\_ / 5,00** |
|  | Development project failure |
| *X* | Accident |
| **Description of the Failure / Accident:** | |
| The 2010 Lexus GX 460 was recalled soon after it was launched due to it failing certain roll over tests. The GX 460 specifically failed a Consumer Reports’ test that was supposed to mimic an alarmed driver might do after exiting a highway ramp too fast. The driver, would approach a sharp turn unusually fast, then releases the accelerator pedal to evaluate the vehicle’s response. Usually, the electronic stability control (ESC) system would prevent the vehicle from skidding, however in this case the ESC took too long kick in for the GX 460 which caused the vehicle to almost slide sideways into the turn. In the real world, this would result in the vehicle hitting either the curb or a barrier and causing a potential rollover risk. No people were hurt while operating these vehicles that was directly caused by the ESC failing in this way. | |
| **Involvement of Requirements or the Requirements Engineering Process:** | |
| It is to be noted that the 2010 Toyota 4Runner, which shares the same underpinnings of the Lexus GX 460, did not fail this test. This means that this problem falls solely on the ESC. The Requirements failed specifically because there was no validation on the conditions for the ESC to engage. The Engineers decided that the system in place was correct, and didn’t bother to properly validate what they had, or even elicit documentation for review to make sure they had matched what the 4Runner had. What resulted was the time interval that existed between loss of traction and the engaging of the ESC was too long. This caused the SUV to behave in an unsafe and dangerous manner. This was remedied by a software update to the ECU that fixed this issue, but should have been caught long beforehand. | |

Reference: <https://www.nbcnews.com/id/wbna36568021>

**Team Name:** *Example Solutions*

|  |  |  |
| --- | --- | --- |
| **Case Example Name** | *Low Quality Solution* | |
| **Points** | **Rationale** |
| **Description** | 1.5 | Description is OK. However, a reference is missing, leading to 0.5 points deducted. |
| **Analysis of RE**  **Involvement** | 0 | This isn't an RE problem, at least not the way it's described here. There are no references to the RE Framework, RE activities, or impact on management.  According to the above description, this was a quality assurance problem, as can be seen by the reference to the datarace “bug”. |

|  |  |  |
| --- | --- | --- |
| **Case Example Name** | *Medium Quality Solution* | |
| **Points** | **Rationale** |
| **Description** | 2 + 1 | The description is adequate and contains sufficient information.  We’re awarding one of the three extra credit points for referencing an “official report,” i.e. by the Department of Transportation |
| **Analysis of RE**  **Involvement** | 1.5 | The description of RE involvement is too implicit. There are no direct references to the RE Framework, RE activities or Requirements in the first paragraph (in fact, it references testing). No points here. The second paragraph references user involvement and hints at the idea that validation would be necessary, however does not explicitly mention validation. |

|  |  |  |
| --- | --- | --- |
| **Case Example Name** | *High Quality Solution* | |
| **Points** | **Rationale** |
| **Description** | 2 | The description is adequate and contains sufficient information. |
| **Analysis of RE**  **Involvement** | 3 | The descriptions of lack of RE are optimal. The solution specifically mentions requirements incompleteness (lack of conditions when ESC should engage), lack of validation of these conditions, and lack of appropriate documentation of testing results (which in this case, act as requirements for improvement of the ESC). The verb “elicit” is used, but is probably extraneous. |