UNIVERSITÄT ZU LÜBECK
INSTITUTE FOR SOFTWARE ENGINEERING
AND PROGRAMMING LANGUAGES

Software Engineering im Wintersemester 2021/2022

Prof. Dr. Martin Leucker, Malte Schmitz, Stefan Benox, Julian Schulz, Benedikt Stepanek, Friederike Weilbeer, Tom Wetterich

Übungszettel 12 (Lösungsvorschlag)

31.01.2022

Abgabe bis Donnerstag, 3. Februar um 23:59 Uhr online im Moodle.

Aufgabe 12.1: Systems Engineering

2 Punkte, leicht

Erläutern Sie die zentralen Unterschiede zwischen Systems Engineering und Software Engineering. Gehen Sie dabei auch auf den Begriff System ein.

▼ Lösungsvorschlag

INCOSE Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities, 4th Edition definiert:

> Systems engineering (SE) is an **interdisciplinary approach** and means to **enable** the **realization of successful systems**.
>
> It **focuses** on defining **customer needs** and required functionality **early in the development cycle**, documenting requirements, and then proceeding with design synthesis and system validation while **considering the complete problem**: operations, cost and schedule, performance, training and support, test, manufacturing, and disposal.
>
> SE **integrates all** the **disciplines** and specialty groups into a **team effort** forming a structured development process that proceeds from concept to production to operation.

> SE **considers both** the **business and** the **technical needs** of all customers **with the goal** of providing a **quality product that meets** the **user needs**.

(Zitiert nach und Hervorhebung übernommen aus der Vorlesung von Stefan Schlichting, UNITY AG: „Model-based Systems Engineering in the Context of Interoperability Medical Device Systems“)

Einige exemplarische zentrale Unterschiede zwischen Systems Engineering und Software Engineering sind:

- Systems Engineering ist ein interdisziplinärer Ansatz, der nicht nur die Softwareentwicklung, sondern auch andere Disziplinen wie Robotik, Mechanik, Elektrotechnik und viele weitere mehr mit einbindet.
- Der Fokus beim Systems Engineering liegt insbesondere auf den Anforderungen und dem Architekturdesign, sowie Verifikation und Validierung. Dabei liegt der Schwerpunkt des Systems Engineering jeweils auf dem Gesamtsystem.
- Die zentrale Herausforderung beim Systems Engineering ist die Kommunikation, sowie die Koordinierung und Abstimmung zwischen den verschiedenen Disziplinen, die an der Erstellung der Systems beteiligt sind.

Als System bezeichnen wir dabei gerade nicht nur Software-Systeme, sondern jede Zusammenstellung von Komponenten, deren Wechselwirkung einen Mehrwert bietet, die also durch ihre Interaktion ein höheres Ziel verfolgen. Diese Definition ist absichtlich sehr breit, sodass fast alles ein System sein kann. Deswegen ist die Definition der Systemgrenzen eine zentrale Aufgabe des Systems Engineering.

Aufgabe 12.2: Architekturdefinition im Systems Engineering

2 Punkte, leicht

Erläutern Sie das Konzept RFLP und diskutieren Sie die verschiedenen Architektur-Sichten, die Sie in der Vorlesung kennen gelernt haben!

▼ Lösungsvorschlag

Der RFLP-Ansatz verfolgt eine schrittweise Verfeinerung der Systemdefinitionen basierend auf den Anforderungen. Aus den **R**equirements wird eine **F**unktionale Architektur abgeleitet, die zu einer **L**ogischen Architektur und schließlich zu einer **P**rodukt-Architektur konkretisiert wird. Dabei wird zunächst auf einer groben Abstraktionsebene begonnen und schrittweise weiter über die Systemanforderungen zu den Subsystem-Anforderungen und schließlich den einzelnen Komponenten verfeinert, bis am Ende eine genaue Beschreibung von Software-, Hardware- und Elektronik-Komponenten steht.

Der RFLP-Ansatz betrachtet dabei verschiedene Sichten auf die Systemarchitektur:

- Die Anforderungen,
- die funktionale Architektur,
- die logische Architektur und
- die Produkt-Architektur.

Die funktionale Architektur beschreibt dabei die Funktion des Systems aus der Perspektive der Anforderungen. Hier geht es nur darum, was das System tut, aber nicht wie. Die logische Architektur beschreibt, welche Komponenten des Systems die Aufgabe wie umsetzen ohne auf Implementierungsdetails einzugehen. Erst die Produkt-Architektur beschreibt im Detail die konkrete Implementierung und die genauen Software-, Hardware- und Elektronik-Komponenten.

Aufgabe 12.3: SysML

3 Punkte, mittel

Recherchieren Sie die verschiedenen SysML-Diagramme und erläutern Sie jeweils kurz, welche Verwandtschaft zu UML-Diagrammen besteht.

▼ Lösungsvorschlag

- Das Anforderungsdiagramm (*Requirement Diagram*) ist ein neues Diagramm in SysML, das keine Entsprechung in UML hat. Es stellt Anforderungen an ein System und insbesondere Beziehungen zwischen den Anforderungen dar. Im Gegensatz zum Anwendungsfalldiagramm liegt der Fokus beim Anforderungsdiagramm auf der Hierarchie der Anforderungen und den Beziehungen zwischen den Anforderungen. Beim Anwendungsfalldiagramm geht es primär um die Interaktion der Nutzer mit dem System.
- Das Aktivitätsdiagramm (*Activity Diagram*) ist eine leichte Erweiterung des UML-Diagramms um Kompatibilität mit anderen SysML-Diagrammen, zum Beispiel dem Blockdefinitionsdiagramm.
- Das Sequenzdiagramm (*Sequence Diagram*), das Zustandsdiagramm (*State Diagram*), das Anwendungsfalldiagramm (*Use Case Diagram*) und Paketdiagramm (*Package Diagram*) stehen in SysML unverändert zur Verfügung.
- Das Blockdefinitionsdiagramm (*Block Definition Diagram*) ist eine Abwandlung des UML-Klassendiagramms. Dabei werden insbesondere Aggregationen und Kompositionen verwendet, um Blöcke hierarchisch zu untergliedern.
- Das Interne Blockdiagramm (*Internal Block Diagram*) ist eine Abwandlung des UML-Kompositionsstrukturdiagramms. Es gehört zu einem bestimmten Block und zeiht dessen gekapselten strukturellen Inhalt: Teile, Eigenschaften, Konnektoren, Ports und Schnittstellen. Anders ausgedrückt, ist es eine White-Box-Perspektive eines gekapselten Black-Box-Blocks.
- Das Zusicherungsdiagramm (*Parametric Diagram*) ist ein neues Diagramm in SysML, das keine Entsprechung in UML hat. Es ist eine Spezialisierung eines Internen Blockdiagramms, das mathematische Regeln (*Constraints*) über die internen Eigenschaften eines Blocks beschreibt.

Aufgabe 12.4: Risikoanalyse

5 Punkte, mittel

In dieser Aufgabe führen wir eine Risikoanalyse für vernetzte Medizingeräte durch.

Methodik zur Risikoanalyse

Sie haben in der Vorlesung folgende Methodik zur Risikoanalyse kennen gelernt:

Zunächst ergibt sich aus der Eintrittswahrscheinlichkeit (*Risk Likelihood*) und der Schwere des Eintritts (*Severity of Impact*) die Risikoklasse (*Risk Class*):

		Risk Likelihood		
		Low	**Medium**	**High**
Severity of Impact	**High**	Class 2	Class 1	Class 1
	Medium	Class 3	Class 2	Class 1
	Low	Class 3	Class 3	Class 2

Dann ergibt sich aus der Risikoklasse (*Risk Class*) und der Wahrscheinlichkeit, dass ein Problem erkannt wird, (*Probability of Detection*) die Priorität des Risikos (*Risk Priority*):

		Probability of Detection		
		Low	**Medium**	**High**
Risc Class	**Class 1**	High	High	Medium
	Class 2	High	Medium	Low
	Class 3	Medium	Low	Low

Basierend auf der so ermittelten Priorität des Risikos können schließlich Maßnahmen zur Risikokontrolle (*Risk Control Measures*) definiert werden.

Szenario vernetzter Medizingeräten

In dieser Aufgabe betrachten wir ein Szenario mit folgenden vernetzten Medizingeräten:

- Ein *Fußschalter* mit einem zentralen Schalter und zwei kleineren Schaltern an der Seite.
- Eine *chirurgische Fräse*, deren Drehzahl eingestellt werden kann.
- Ein *Display*, das die aktuell eingestellte Drehzahl der Fräse anzeigt.

Diese drei verschiedenen Geräte kommunizieren über eine Netzwerkprotokoll miteinander: Der zentrale Schalter des Fußschalters aktiviert die Fräse. Diese fräst nur, solange der Schalter betätigt wird. Mit den beiden kleinen Schalter kann die

Drehzahl der Fräse angepasst werden. Einer erhöht den Wert bei Betätigung, der andere erniedrigt ihn. Das Display zeigt jederzeit die aktuelle Drehzahl an.

Dabei wird eine Implementierung mit *episodische Nachrichten* verwendet, d.h. der Fußschalter sendet eine Nachricht an die Fräse, sobald eine seiner Tasten gedrückt oder losgelassen wird. Die Fräse sendet eine Nachricht an das Display, sobald sich die Drehzahl ändert.

Risiken

Betrachten Sie in diesem Szenario folgende Risiken:

1. **Nachrichtenverlust zur Fräse.** Eine einzelne Nachricht vom Fußschalter zur Fräse geht im Netzwerk verloren.
2. **Nachrichtenverlust zum Display.** Eine einzelne Nachricht von der Fräse zum Display geht im Netzwerk verloren.
3. **Verbindungsverlust.** Die Netzwerkverbindung geht dauerhaft verloren durch kaputte Netzwerkkomponenten, sodass die gesamte Kommunikation nicht mehr funktioniert.
4. **Fehlbedienung.** Die beiden Schalter zum Anpassen der Drehzahl werden verwechselt, sodass die Drehzahl versehentlich erhöht statt erniedrigt wird oder anders herum.
5. **Fehlinterpretation.** Die Zahl auf dem Display wird falsch interpretiert, sodass von einer falschen Drehzahl ausgegangen wird.
6. **Fehlkonfiguration Fußschalter.** Die Geräte werden falsch vernetzt, sodass nicht bekannt ist, welcher Fußschalter welche Fräse steuert.
7. **Fehlkonfiguration Display.** Die Geräte werden falsch vernetzt, sodass nicht bekannt ist, welches Display die Drehzahl der Fräse anzeigt.

Aufgabenstellung

1. Führen Sie eine Risikoanalyse entsprechen der dargestellten Methodik für das beschriebene Szenario vernetzter Medizingeräten unter Berücksichtigung der aufgeführten Risiken durch. (3 Punkte)

▼ **Lösungsvorschlag**

1. **Nachrichtenverlust zur Fräse.**

   Angenommen, es geht die Nachricht verloren, dass der Fußschalter nicht mehr betätigt wird, so wird die Fräse nicht deaktiviert. Es können starke Schäden an Knochen oder Gewebe entstehen, wenn unbeabsichtigt weiter gefräst wird.

   - *Risk Likelihood:* Medium
   - *Severity of Impact:* High
   - *Risk Class:* 1
   - *Probability of Detection:* High
   - *Risk Priority:* Medium
   - *Risk Control Measure*: Personen, die mit der Fräse arbeiten, werden entsprechend geschult, in diesem Fall den Fußschalter erneut zu betätigen, sodass neue Nachrichten verschickt werden.

2. **Nachrichtenverlust zum Display.**

   Wir betrachten die Situation, dass eine Nachricht über eine Änderung der Drehzahl im Netzwerk verloren geht, sodass das Display nicht die aktuell an der Fräse eingestellte Drehzahl anzeigt. Durch die Verwendung der falschen Drehzahl können Schäden an Knochen oder Gewebe entstehen.

   - *Risk Likelihood:* Medium
   - *Severity of Impact:* Medium
   - *Risk Class:* 2
   - *Probability of Detection:* Low
   - *Risk Priority:* High
   - *Risk Control Measure*: Personen, die mit der Fräse arbeiten, werden entsprechend geschult, regelmäßig die korrekte Funktionsweise der Vernetzung zu überprüfen, in dem die Drehzahl geändert wird und überprüft wird, dass diese Änderung am Display angezeigt wird.

3. **Verbindungsverlust.**

   Im schlimmsten Fall geht die Verbindung verloren, während die Fräse aktiviert ist, sodass diese über den Fußschalter nicht mehr deaktiviert werden kann. Es können starke Schäden an Knochen oder Gewebe entstehen, wenn unbeabsichtigt weiter gefräst wird.

   - *Risk Likelihood:* Medium
   - *Severity of Impact:* High
   - *Risk Class:* 1
   - *Probability of Detection:* High
   - *Risk Priority:* Medium
   - *Risk Control Measure*: Personen, die mit der Fräse arbeiten, werden entsprechend geschult, in diesem Fall die Fräse direkt am Handgerät zu deaktivieren.

4. **Fehlbedienung.**

   Wir betrachten die Situation, dass die Drehzahl fälschlicherweise erhöht wurde. Durch die Verwendung der falschen Drehzahl können Schäden an Knochen oder Gewebe entstehen.

   - *Risk Likelihood:* High
   - *Severity of Impact:* Medium
   - *Risk Class:* 1
   - *Probability of Detection:* Medium
   - *Risk Priority:* High
   - *Risk Control Measure*: Personen, die mit der Fräse arbeiten, werden entsprechend geschult, stets die eingestellte Drehzahl am Display zu überprüfen.

5. **Fehlinterpretation.**

   Wir betrachten die Situation, dass die auf dem Display angezeigte Drehzahl falsch interpretiert wird. Durch die Verwendung der falschen

Drehzahl können Schäden an Knochen oder Gewebe entstehen.

- *Risk Likelihood:* Low
- *Severity of Impact:* Medium
- *Risk Class:* 3
- *Probability of Detection:* Medium
- *Risk Priority:* Low
- *Risk Control Measure*: Personen, die mit der Fräse arbeiten, werden in der Interpretation der Darstellung der Drehzahl auf dem Display geschult.

6. **Fehlkonfiguration Fußschalter.**

   Wir betrachten die Situation, dass der Fußschalter die falsche Fräse steuert. Durch eine versehentliche Aktivierung der falschen Fräse können Personen verletzt werden.

   - *Risk Likelihood:* Low
   - *Severity of Impact:* Medium
   - *Risk Class:* 3
   - *Probability of Detection:* High
   - *Risk Priority:* Low
   - *Risk Control Measure*: Personen, die mit der Fräse arbeiten, werden entsprechend geschult, dass vor dauerhafter Inbetriebnahme der Fräse stets die korrekte Vernetzung durch eine kurze Aktivierung bei niedriger Drehzahl geprüft wird.

7. **Fehlkonfiguration Display.**

   Wir betrachten die Situation, dass das Display die Drehzahl einer anderen Fräse anzeigt. Durch die Verwendung der falschen Drehzahl können Schäden an Knochen oder Gewebe entstehen.

   - *Risk Likelihood:* Low
   - *Severity of Impact:* Medium

- *Risk Class:* 3
- *Probability of Detection:* Low
- *Risk Priority:* Medium
- *Risk Control Measure*: Das Display zeigt nicht nur die Drehzahl, sondern auch die Aktivierung der Fräse an, sodass Personen, die die Fräse verwenden, unmittelbar erkennen können, ob das Display mit der richtigen Fräse vernetzt wurde.

2. Betrachten Sie nun eine alternative Implementierung mit *periodischen Nachrichten*, d.h. der Fußschalter sendet alle 50 ms eine Nachricht an die Fräse und diese im gleichen Takt an das Display. Wie ändert sich die Risikoanalyse durch diese Anpassung? Entscheiden Sie sich für eine der beiden Implementierungsmöglichkeiten und begründen Sie Ihre Empfehlung. (2 Punkte)

▼ **Lösungsvorschlag**

Die Risiken *Nachrichtenverlust zur Fräse*, *Nachrichtenverlust zum Display* müssen durch diese Anpassung nicht mehr betrachtet werden. Wenn nur eine einzelne Nachricht vom Fußschalter verloren geht, so reagiert die Fräse mit einer maximalen Verzögerung von 50 ms gegenüber dem Normalbetrieb. Wenn nur eine Nachricht von der Fräse an das Display verloren geht, so reagiert das Display mit einer maximalen Verzögerung von 50 ms gegenüber dem Normalbetrieb. In beiden Fällen kann ohne Auswirkungen weiter gearbeitet werden.

Das Risiko *Verbindungsverlust* wird wie folgt angepasst:

3. **Verbindungsverlust.**

   Im schlimmsten Fall geht die Verbindung verloren, während die Fräse aktiviert ist, sodass diese über den Fußschalter nicht mehr deaktiviert werden kann. Es können starke Schäden an Knochen oder Gewebe entstehen, wenn unbeabsichtigt weiter gefräst wird.

   - *Risk Likelihood:* Medium
   - *Severity of Impact:* High
   - *Risk Class:* 1

- *Probability of Detection:* High
- *Risk Priority:* Medium
- *Risk Control Measure*: Die Fräse schaltet sich automatisch ab, sobald über 100 ms keine Nachrichten vom Fußschalter mehr empfangen wurden.

Durch die Anpassung der Implementierung reicht eine technische Risikokontrollmaßnahme aus, um dem Risiko zu begegnen. Das ist einer Risikokontrollmaßnahme in Form einer Schulung deutlich überlegen, da hier menschliches Versagen ausgeschlossen werden kann.

Fazit: Die Implementierung mit periodische Nachrichten hat gegenüber der Implementierung mit episodischen Nachrichten gravierende Vorteile, da hier drei Risiken deutlich besser begegnet werden kann.