
MEDCONF 2013
FEHLERTOLERANZ
SICHER
SOFTWARE ITEMS
SAFETY CLASSIFICATION
RISK CONTROL MEASURE
SEGREGATION
BEST PRACTICES IM UMGANG MIT DEN EN 62304-BEGRIFFEN: SOFTWARE ITEMS, CLASSIFICATION, SEGREGATION, RISK CONTROL & CO.

ERNI
enables & delivers

INHALT

„Wie erstelle ich eine fehlertolerante, robuste Medizinprodukte-Software und erfülle gleichzeitig die Anforderungen der EN 62304“

1. Die Ausgangssituation
2. Lösung
   a) Ein robustes, fehlertolerantes System
   b) Ein sicheres System (EN 62304)
3. Zusammenfassung

AUSGANGSSITUATION

- Zu entwickelndes Medizingerät
- Hauptanforderungen
- Rahmenbedingungen

ZU ENTWICKELNDES MEDIZINGERÄT

MEDICAL DEVICE

any instrument, apparatus, implement, machine, appliance, implant, in vitro reagent or calibrator, software, material or other similar or related article, intended by the MANUFACTURER to be used, alone or in combination, for human beings for one or more of the specific purpose(s) of

- diagnosis, prevention, monitoring, treatment or alleviation of disease,
- diagnosis, monitoring, treatment, alleviation of or compensation for an injury,
- investigation, replacement, modification, or support of the anatomy or of a physiological PROCESS,
- supporting or sustaining life,
- control of conception,
- disinfection of MEDICAL DEVICES,
- providing information for medical purposes by means of in vitro examination of specimens derived from the human body,

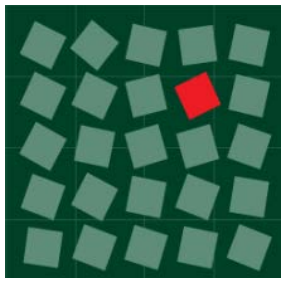
and which does not achieve its primary intended action in or on the human body by pharmacological, immunological or metabolic means, but which may be assisted in its function by such means

MEDICAL DEVICE SOFTWARE

SOFTWARE SYSTEM that has been developed for the purpose of being incorporated into the MEDICAL DEVICE being developed or that is intended for use as a MEDICAL DEVICE in its own right

ANFORDERUNGEN

- …
- The system shall be implemented with at least two microcontrollers to monitor each other.
- A breakdown of the user interface software or user interface controller shall not influence the essential performance
- The system shall execute a self-reset in case of an error whenever possible e.g. (watchdog failures, unhandled exception, transient errors).
- …



robust, fehlertolerant

- ...
- The safety classification (according to EN 62304) shall be assigned so that the implementation effort is as low as possible.
- …

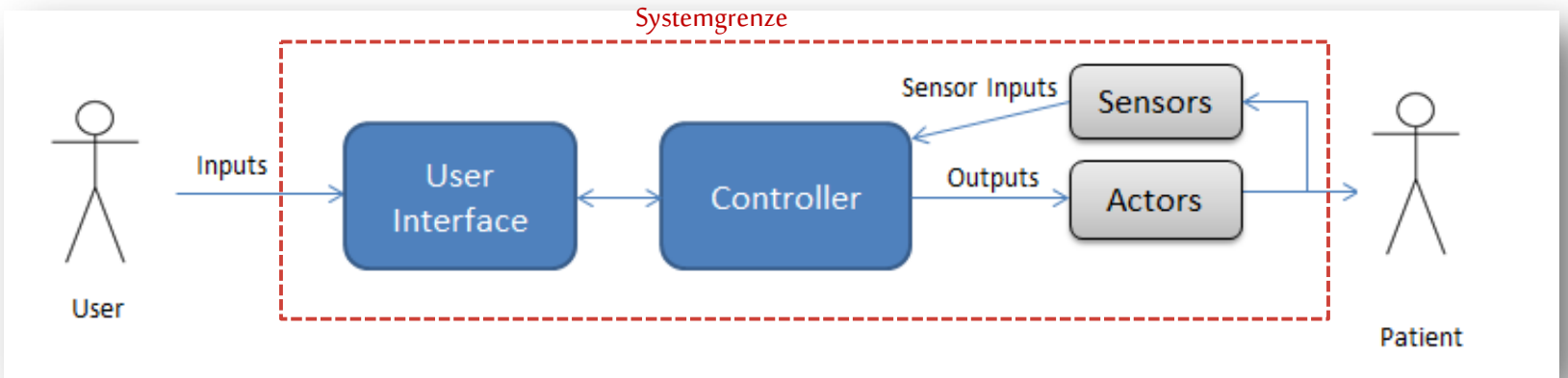
safe

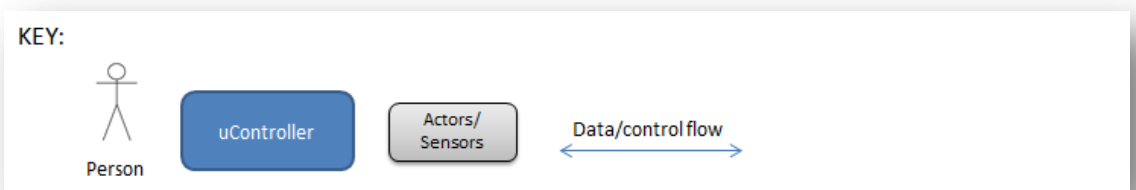
LÖSUNG – ERSTER TEIL

- Design eines fehlertoleranten, robusten Systems

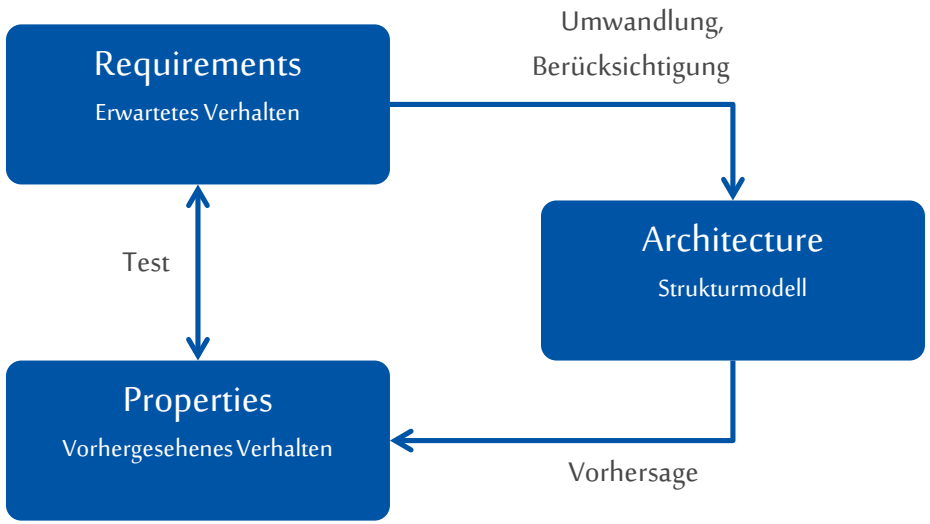
SYSTEMDESIGN

- Erster Überblick



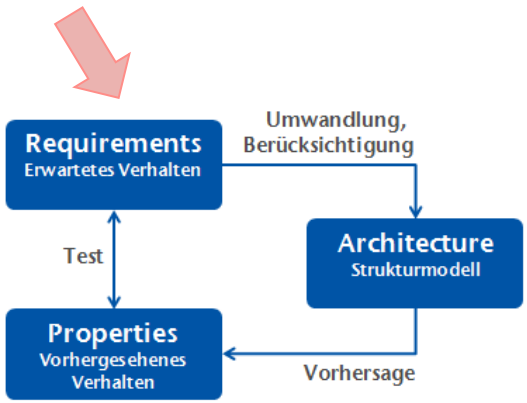


DESIGN PROZESS

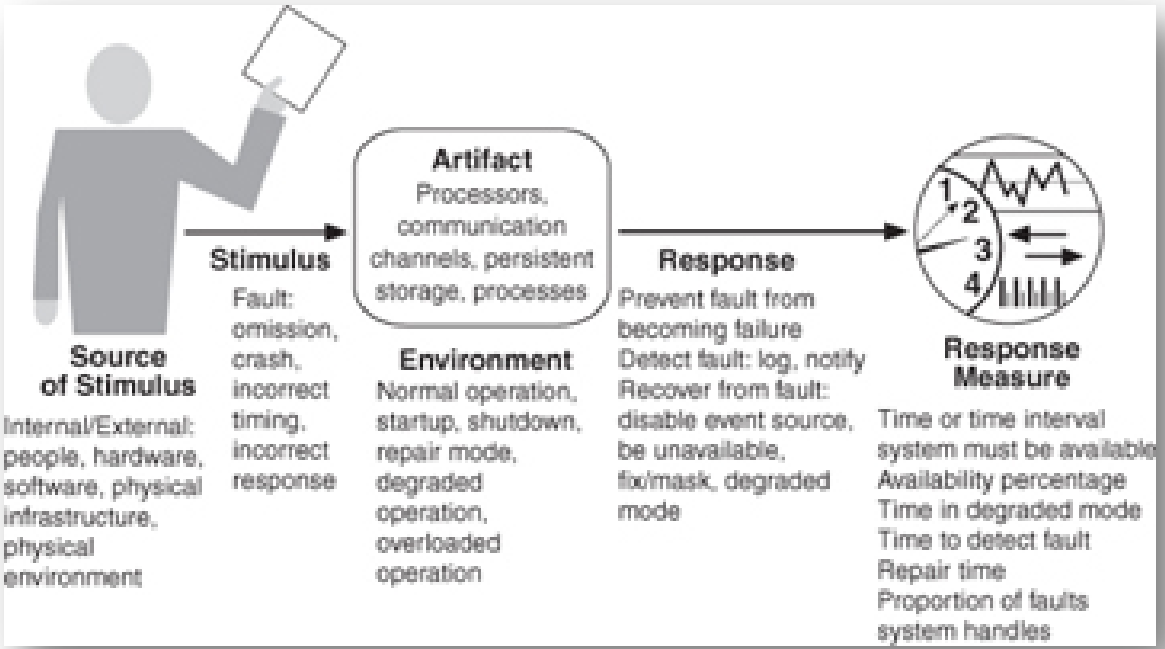


REQUIREMENTS

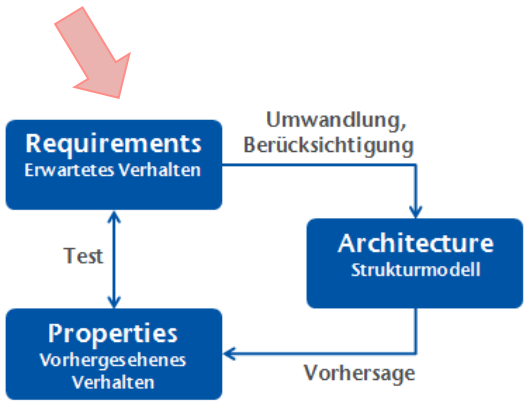
- Anforderungen
  - ...
  - The system shall be implemented with at least two microcontrollers to monitor each other.
  - A breakdown of the user interface software or user interface controller shall not influence the essential performance
  - The system shall execute a self-reset in case of an error whenever possible e.g. (watchdog failures, unhandled exception, transient errors).
  - ...
  - ...
  - The safety classification (according to EN 62304) shall be assigned so that the implementation effort is as low as possible.
  - ...
- Relevante Quality Attributes:
  - Safe → Sicher
  - Fault tolerant → Fehler tolerant
  - Reliability → Zuverlässigkeit
  - Dependability → Verlässlichkeit
  - Availability → Verfügbarkeit



QUALITY ATTRIBUTE SCENARIOS

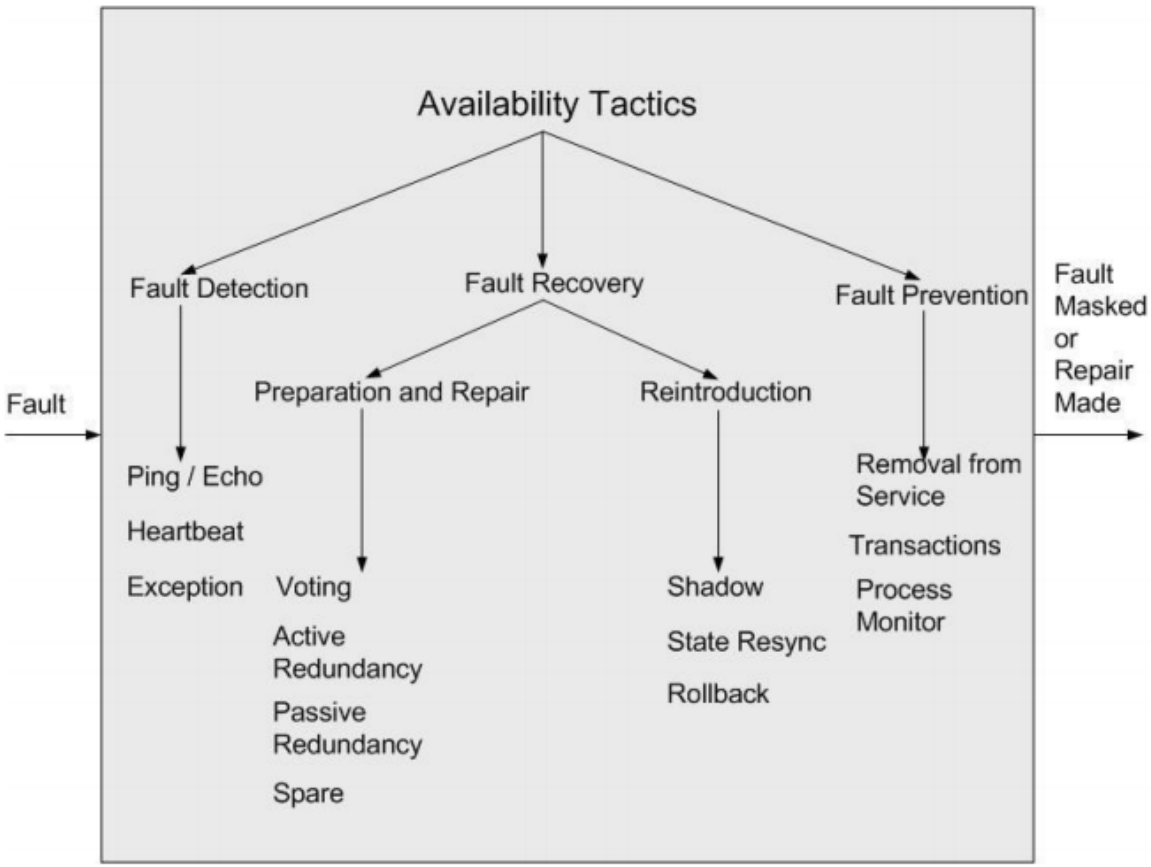


Quelle: http://www.sei.cmu.edu

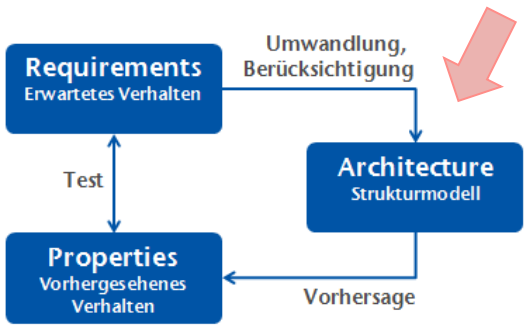


Ziel: Überprüfbare Qualitätseigenschaften

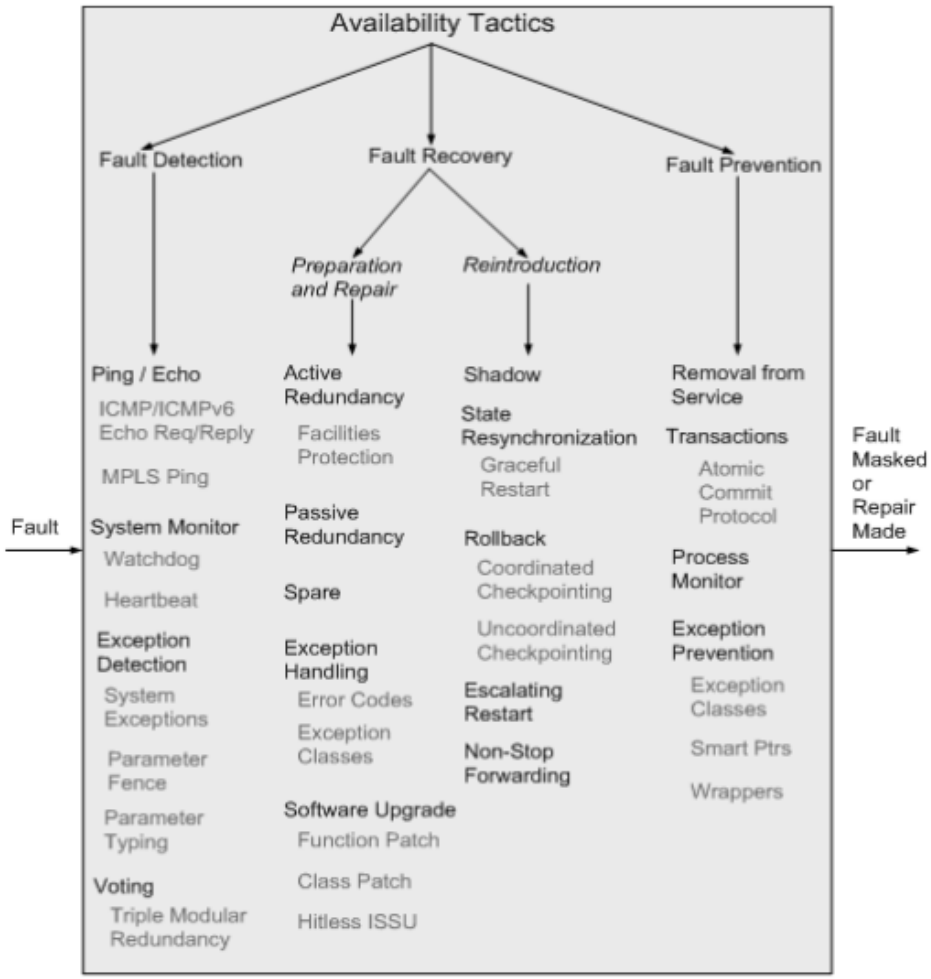
DESIGN TACTICS



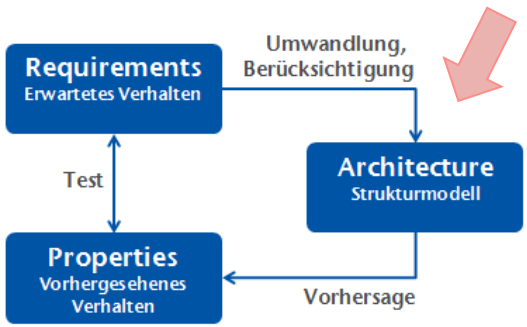
Quelle: http://www.sei.cmu.edu



WEITERE DESIGN TACTICS

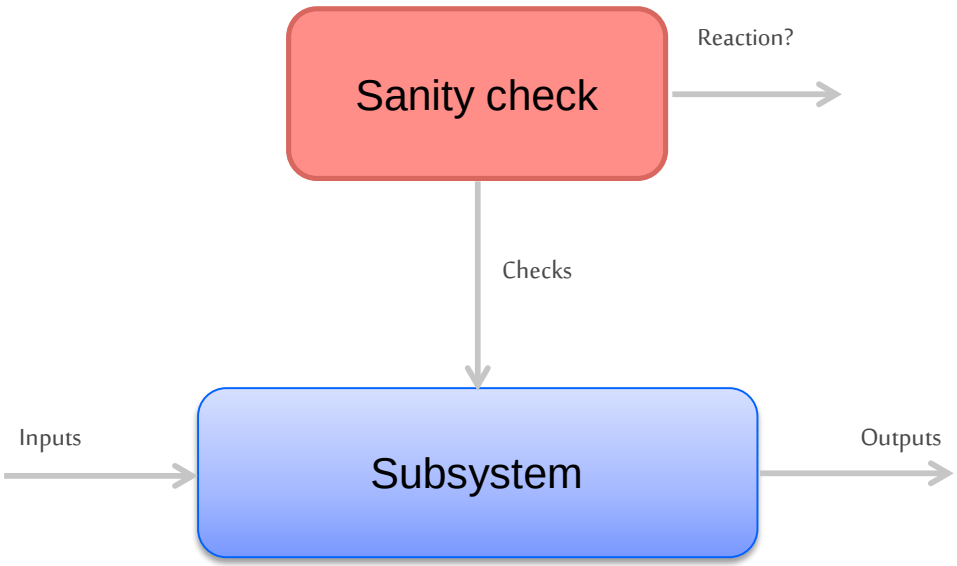


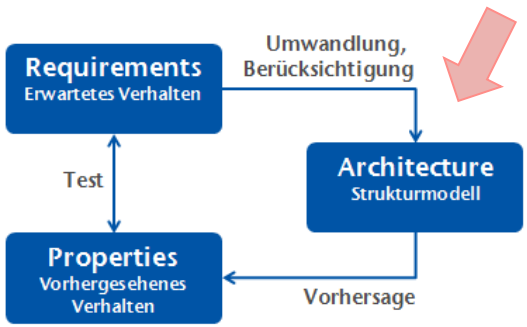
Quelle: http://www.sei.cmu.edu



DESIGN PATTERN: «SANITY CHECK PATTERN»

Quelle: "Real-Time Design Patterns: Robust Scalable Architecture for Real-Time Systems"
(Bruce Powel Douglass)



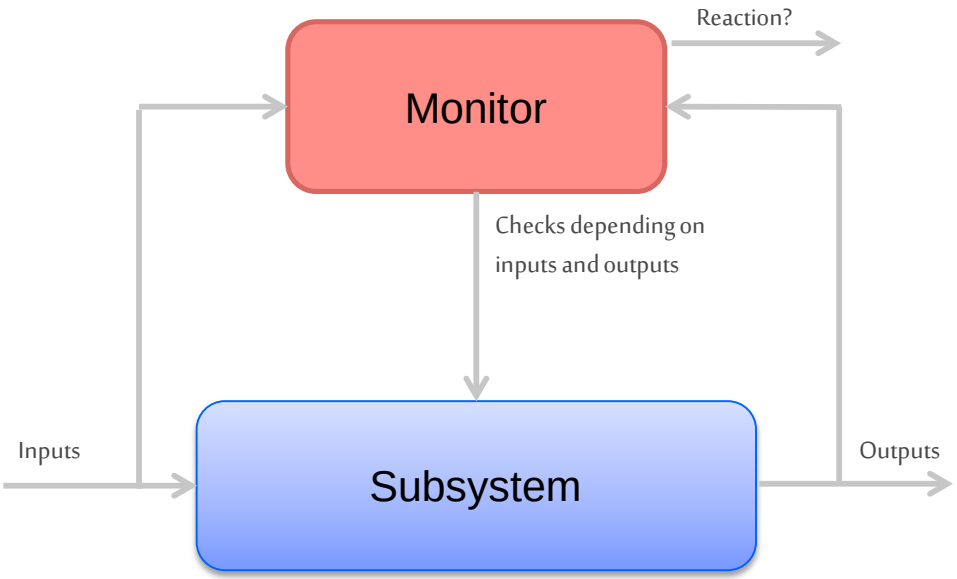


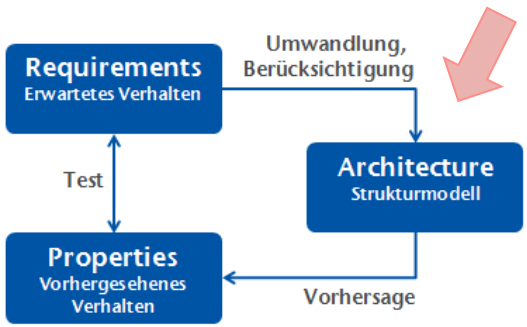
Design tactics:

- Fault detection → system monitor
- Fault prevention → removal from service (failsafe)

DESIGN PATTERN: «MONITOR-ACTUATOR PATTERN»

Quelle: "Real-Time Design Patterns: Robust Scalable Architecture for Real-Time Systems" (Bruce Powel Douglass)

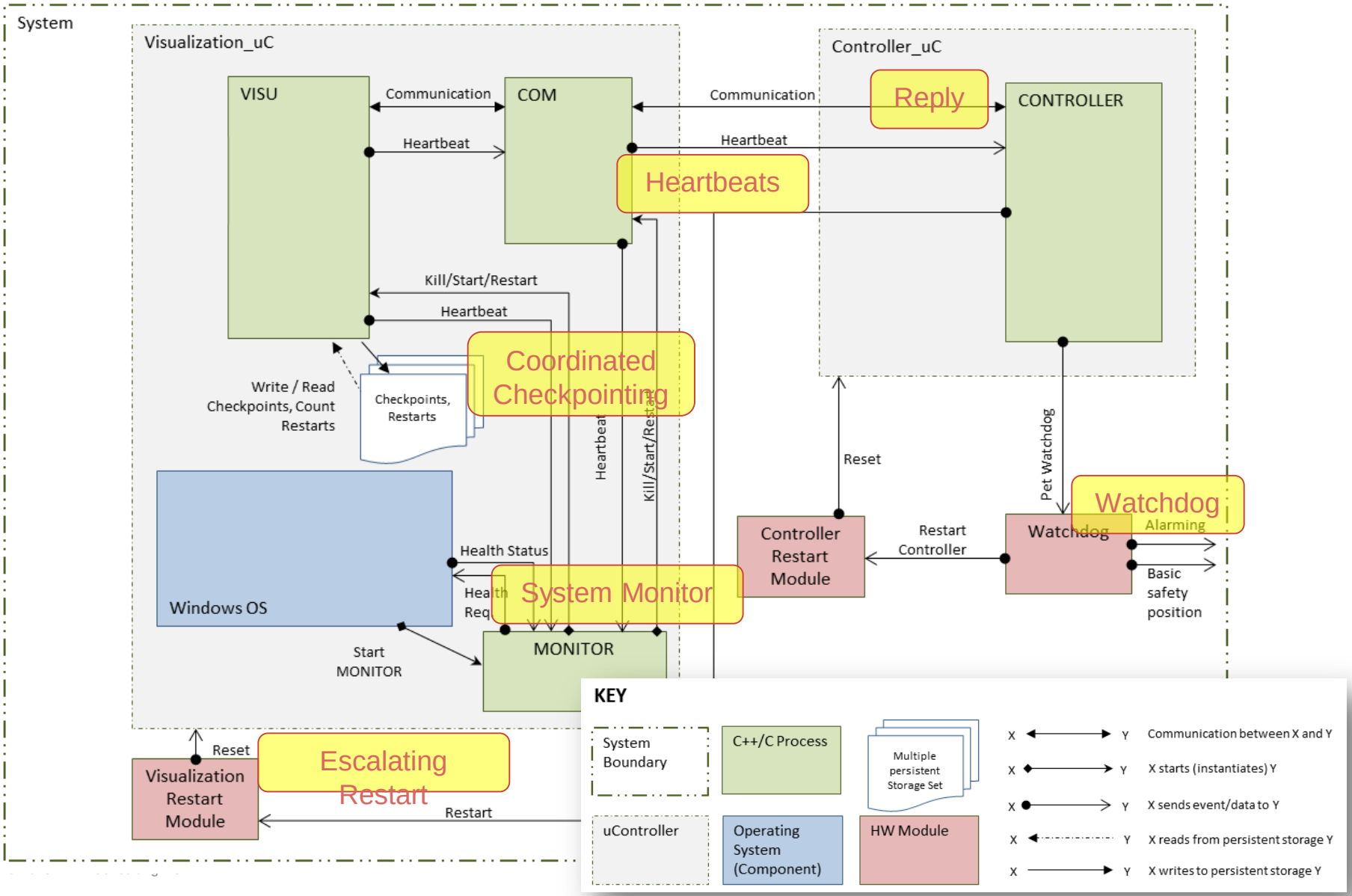




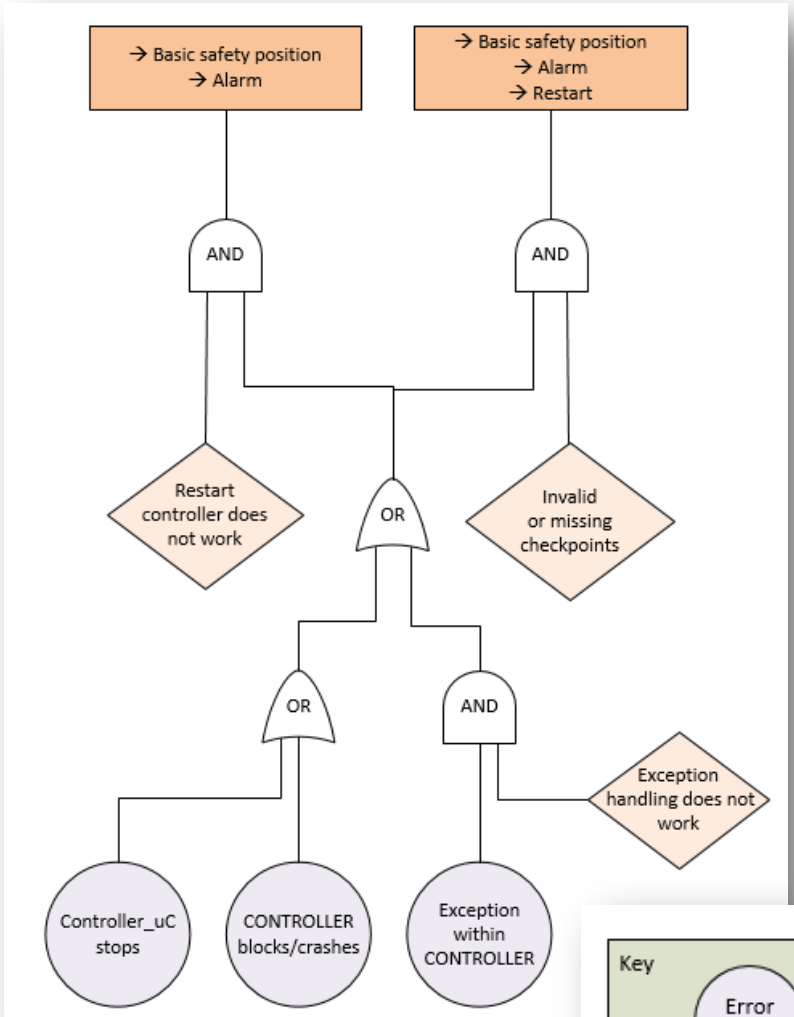
Design tactics:

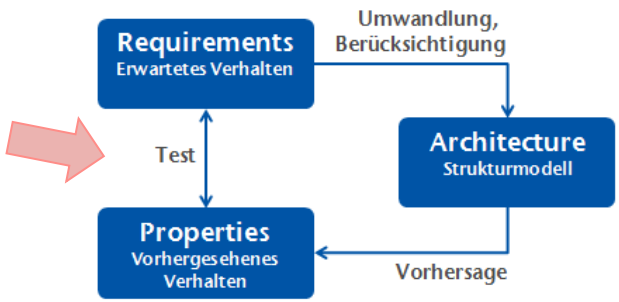
- Fault detection → system monitor
- Fault prevention → removal from service (failsafe)

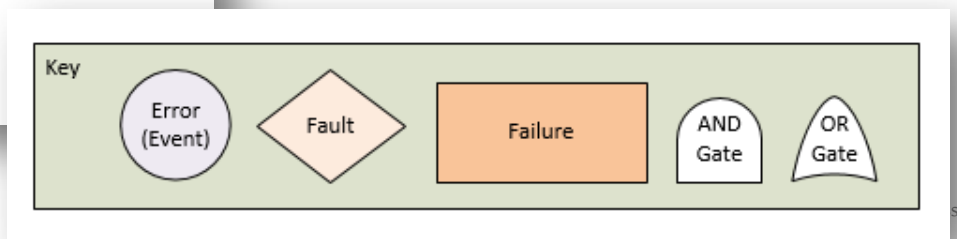
EIN (FAST) REALES BEISPIEL



VERIFIZIERUNG MITTELS FAULT TREE



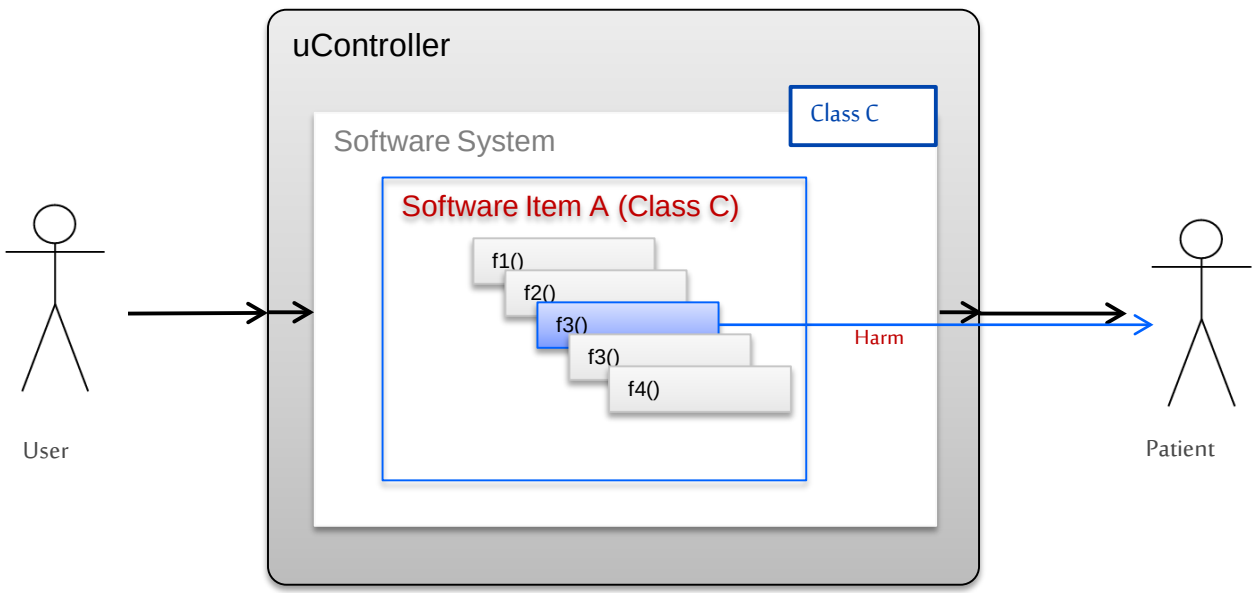




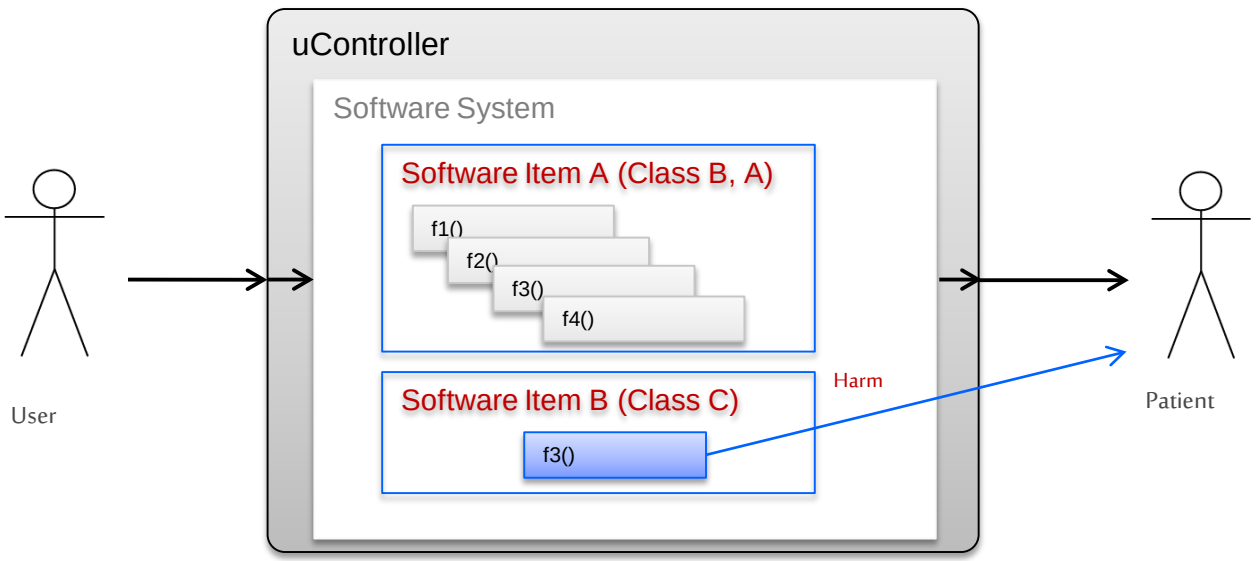
LÖSUNG – ZWEITER TEIL

- Design eines sicheren Systems, welches die Anforderungen der EN 62304 erfüllt und den Entwicklungsaufwand minimiert

SAFETY CLASSIFICATION



REDUKTION DER SAFETY CASSIFICATION MITTELS EXTRAKTION DER KRITISCHEN TEILE

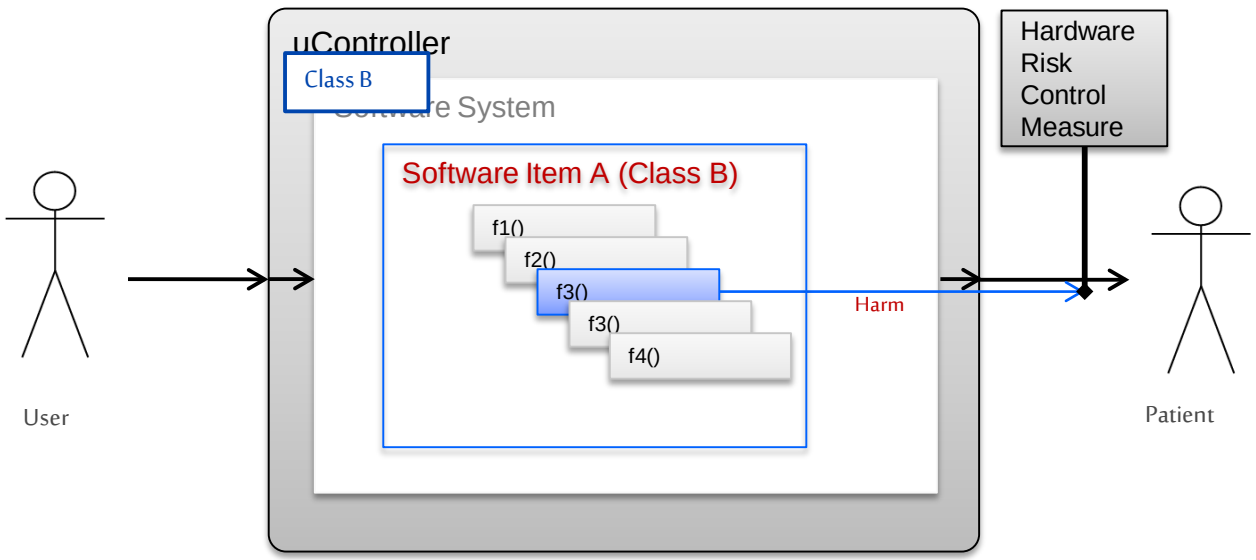


Segregation:

- Software Item A darf Software Item B nicht direkt oder indirekt negativ beeinflussen
- Software Item A darf den Patienten nicht gefährden
- Die Laufzeit Umgebung, in denen Software Item A und B laufen, darf die Sicherheit nicht beeinflussen

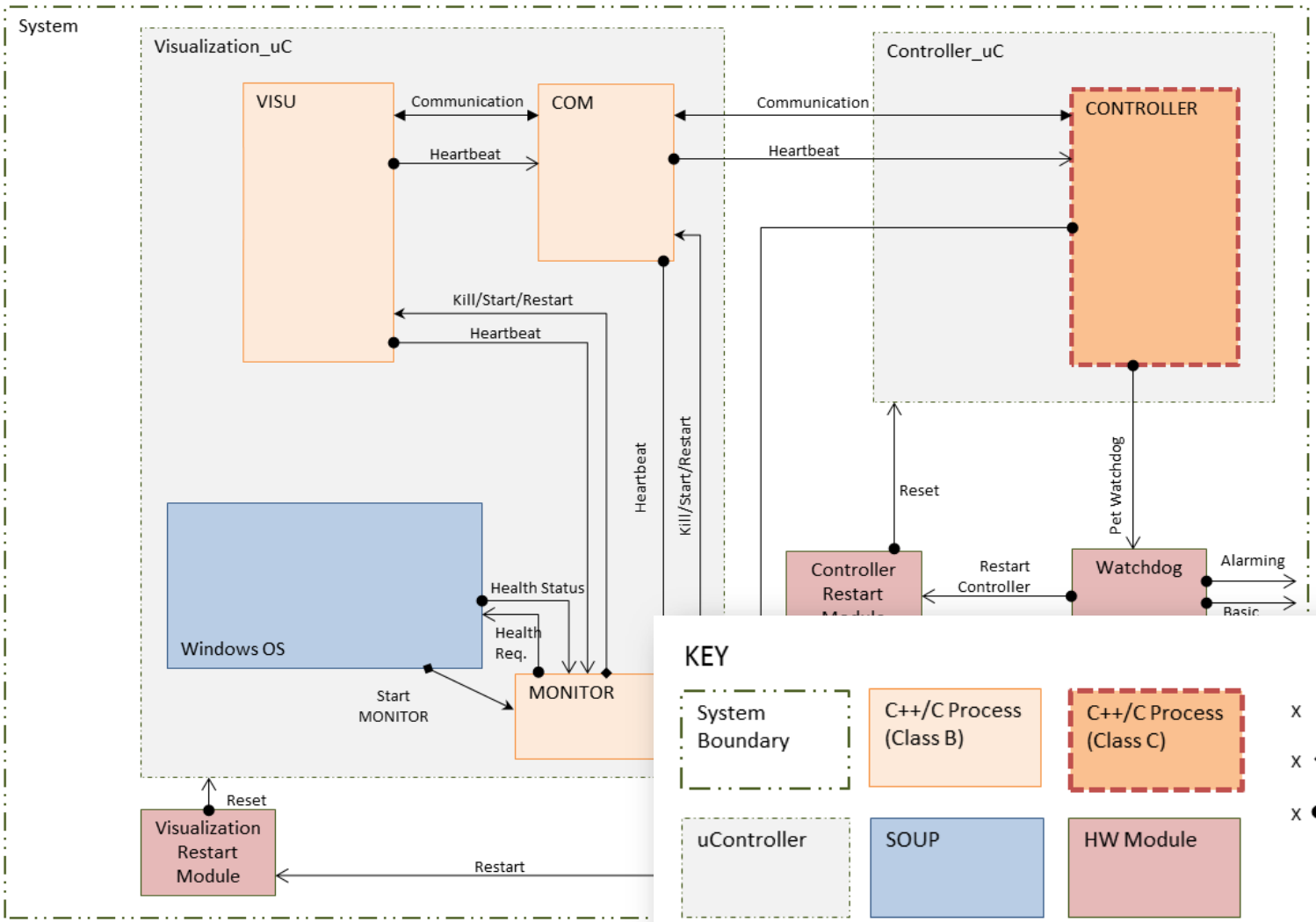
(→ IEC/TR 80002-1)

REDUKTION DER SAFETY CASSIFICATION MITTELS EINER HARDWARE RISIKO-KONTROLL MASSNAHME

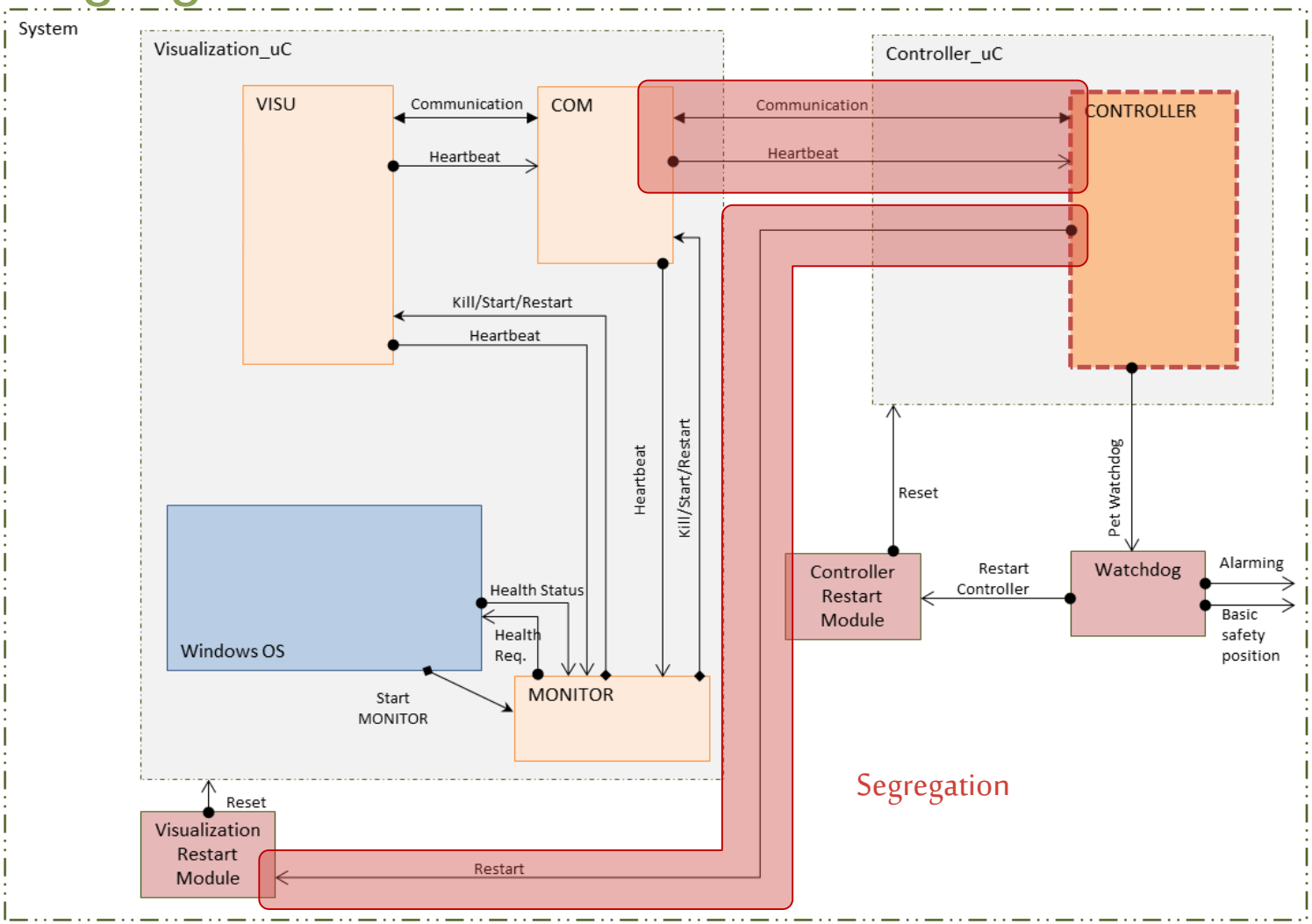


- Die «hardware risk control measure» muss die Auswirkung oder die Wahrscheinlichkeit einer Gefährdung des Patienten reduzieren
- Eine «hardware risk control measure» kann auch ein separater Microkontroller oder ein Mikroprozessor mit Software sein

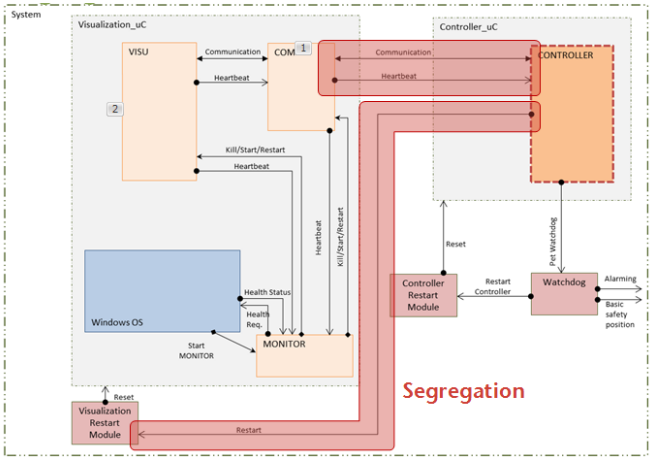
Dokumentation der Safety Classification



Segregation?



SEGREGATION



Kommunikation zwischen "CONTROLLER" und "COM"

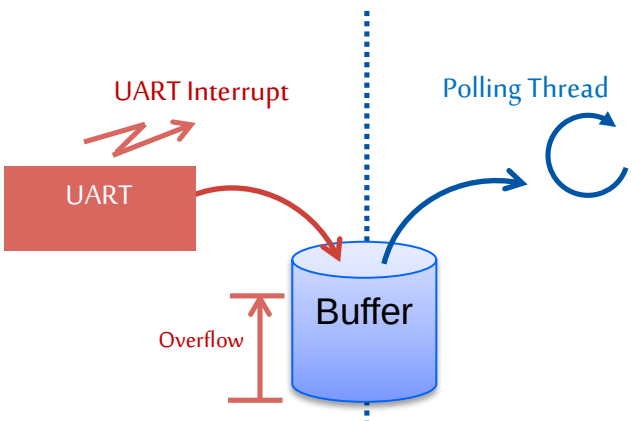
- "Kein" Interrupt auf Seite "CONTROLLER" (→ Polling)
- Verwenden einer gepufferten Kommunikation
- Achtung: Serielle Kommunikation mit Hardware Handshaking

Restart Signal

- Nur Hardware Signal (kein Interrupt)

Heartbeat

- Unidirektional von CONTROLLER zur Visualisierung



ZUSAMMENFASSUNG

- Lessons learned…

LESSONS LEARNED

- Sämtliche Anforderungen, funktional und nicht-funktional (Qualitätseigenschaften) sollten vor dem System Design explizit definiert und beschrieben werden
- Design und Architektur ist «Design & Test»
- Entwurfshilfen können «Design Tactics» und «Design Pattern» sein
- Fehlertoleranz, Robustheit,.. sollten explizit in den Entwurf einbezogen werden
- Die Safety Classification und die daraus resultierende Segregation-Betrachtung sollte von Anfang an in den Entwurf der Software (des Systems) einbezogen werden

ERNI

enables & delivers

www.erni-consultants.com

matthias.kuenzi@erni.ch