RESafety

Requirements Engineering for Safety

PhD Student: Moniky Ribeiro
Advisor: Prof. Jaelson Castro
Co-advisor: Prof. Ricardo Argenton

Context

A Safety-Critical System (SCS) is defined as:

A system which, if it fails or behaves unexpectedly, can cause accidents resulting in injury or death, damage to property or the environment, or significant financial loss (Leveson, 1995; Leveson, 2011).

Context

- Developing SCS involves some additional activities not common in non-critical contexts
  - Define high-level safety requirements
  - Identify accidents and hazards
  - Investigate if the combined behavior of system's components and stakeholders may lead to hazards
  - Refine safety requirements towards system's design
  - Assure system's safety
- Hazard elimination or mitigation impacts system's requirements:
  - It may derive new functional requirements
  - It may derive new non-functional requirements
  - It may derive new architectural decisions
  - Or it may impact existing ones

RESafety

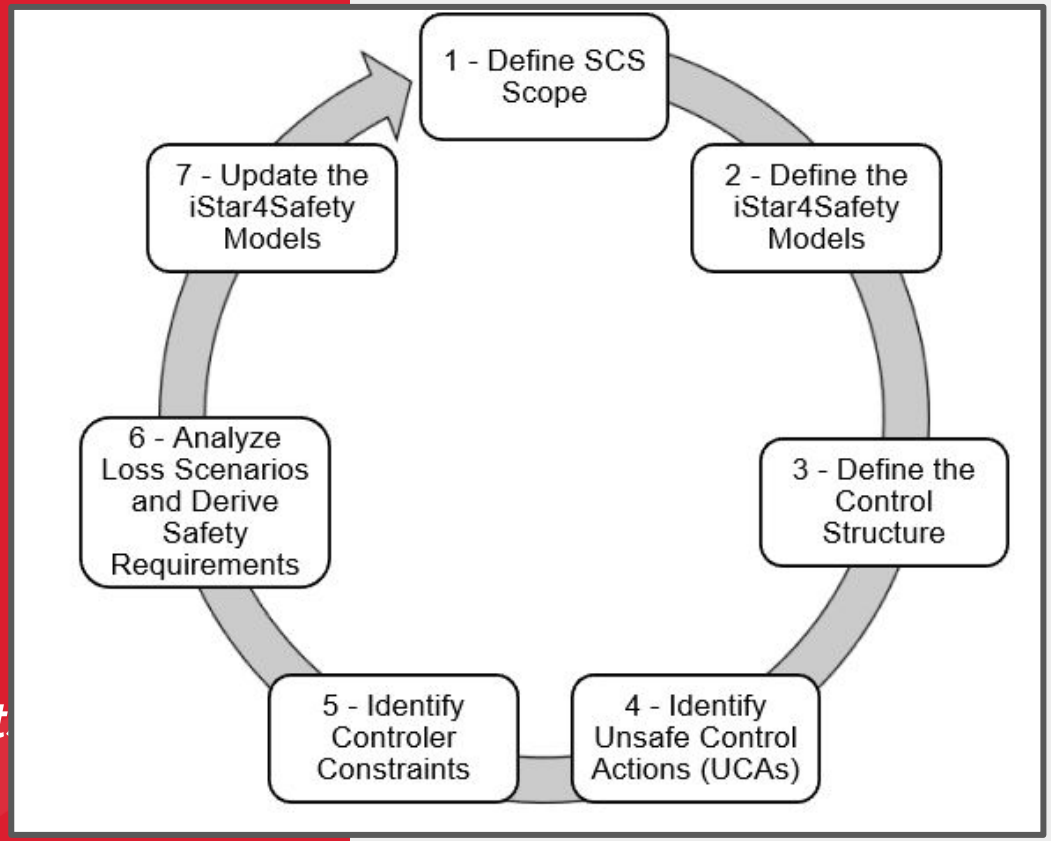
IStar4Safety
- Safety goals
- Hazards
- Mitigation strategies (Safety Tasks/ Safety Resources)

STPA
- Accidents
- Hazards
- Constraints
- Unsafe Control Actions
- Loss Scenarios

RESafety

The 7-Step Process

- *Iterative and incremental*
- *Relies on iStar4Safety models and STPA element*

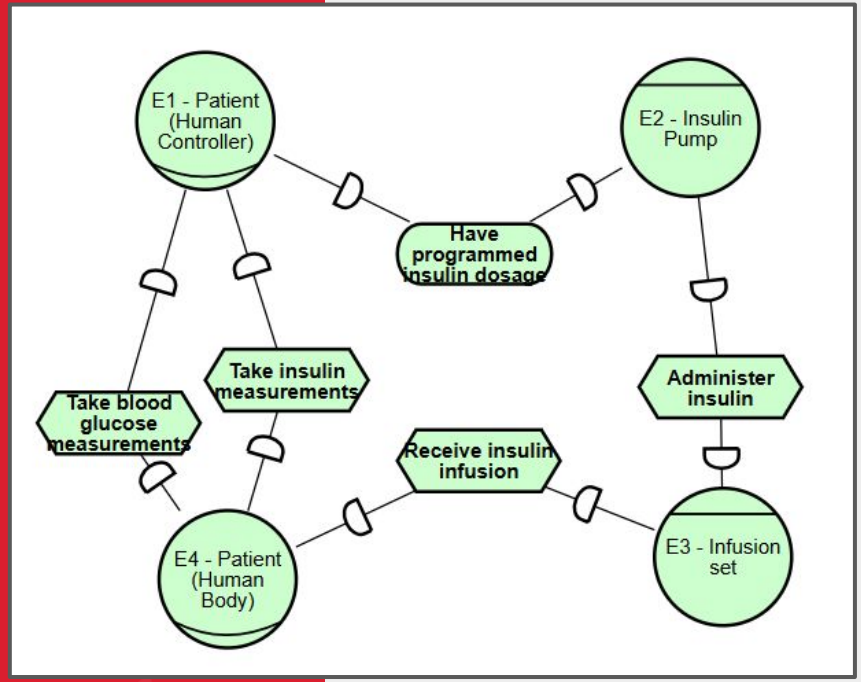


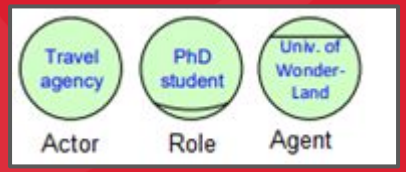
iStar 2.0

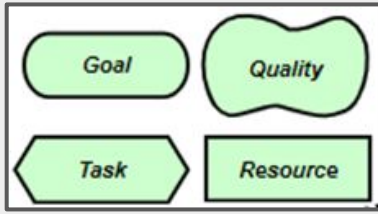
Early requirements Modeling

Overview

(Yu, 1995) and (DALPIAZ; FRANCH; HORKOFF, 2016)





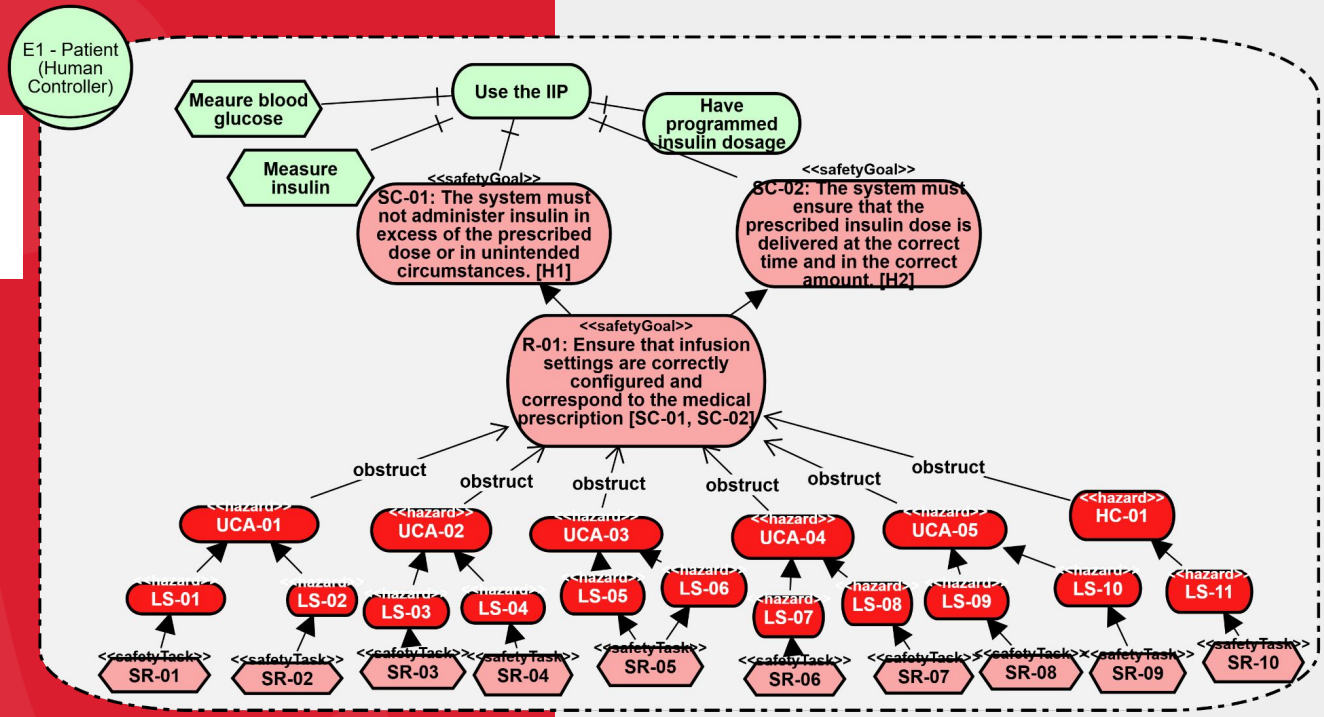


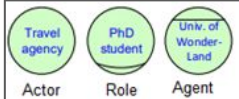
iStar4Safety

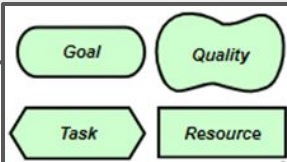
Early Safety Requirements Modeling

Overview

(Ribeiro, 2019)





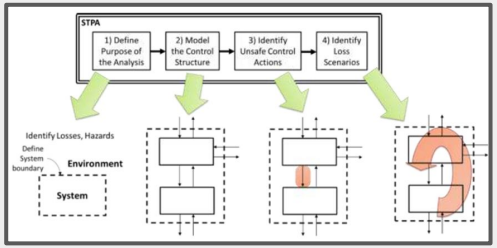


STPA

System-Theoretic Process Analysis

(Leveson, 2011, Leveson & Thomas, 2018)

- Developed by Nancy Leveson (MIT).
- A method for hazard analysis in complex socio-technical systems.
- Based on Systems Theory, not failure-based models like FMEA or FTA.

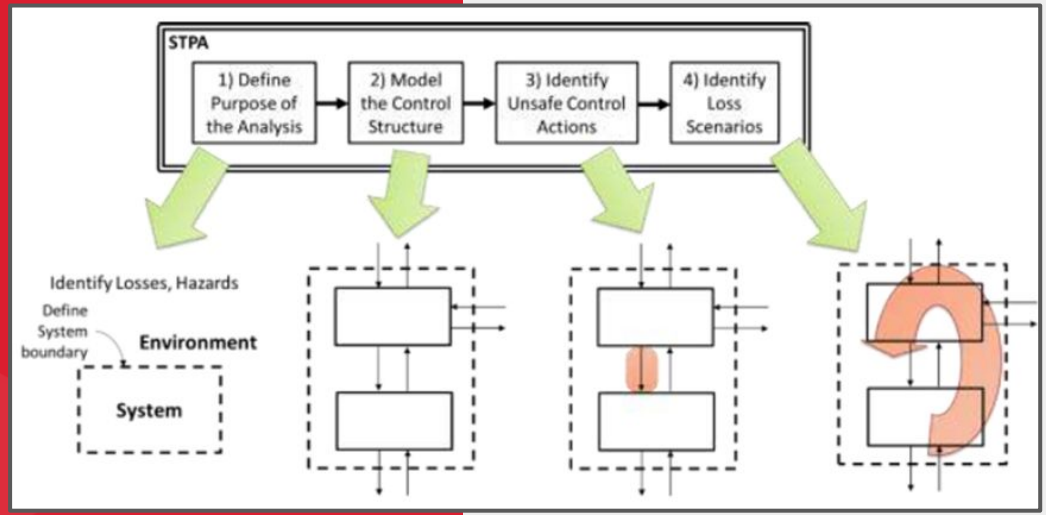


STPA

System-Theoretic Process Analysis

(Leveson, 2011, Leveson & Thomas, 2018)

- Definition of the purpose of the analysis
- Control structure modeling
- Identification of UCAs - Unsafe Control Actions
- Identification of Loss Scenarios

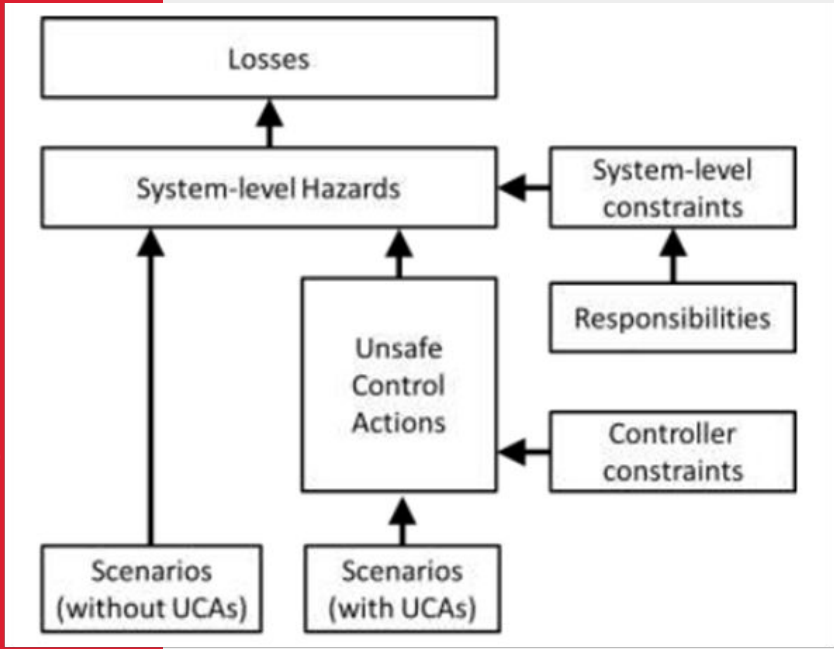


STPA

System-Theoretic Process Analysis

(Leveson, 2011, Leveson & Thomas, 2018)

Outputs and Traceability in STPA



Leveson & Thomas, 2018.

References

1. Leveson, N. G. (2011). Engineering a Safer World: Systems Thinking Applied to Safety. Mit Press, Massachusetts, London, England.
2. Leveson, N. G. & Thomas, J. P. (2018). STPA Handbook. first edition.
3. Ribeiro, M. (2019). Desenvolvimento de uma extensão da linguagem de modelagem istar para sistemas críticos de segurança - istar4safety. Master's thesis, Universidade Federal de Recife.
4. Yu, E. S.-K. (1995). Modelling Strategic Relationships for Process Reengineering. PhD thesis, Toronto, Ont., Canada, Canada. AAINN02887.

Thanks!

Contacts:

Moniky Ribeiro-> monikyr@gmail.com **or**
smsr@cin.ufpe.br

Jaelson Castro-> jbc@cin.ufpe.br

Centro de Informática

UFPE