Save and Secure Robotics based on Open Source Software

„Guidelines“ for specifications of safety critical equipment

- Some hints

Dietmar Reinert, Norbert Jung, Michael Schaefer

Hochschule Bonn-Rhein-Sieg

IFA
Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung

Contents

- Nature & requirements
- Basic properties
- Phases during development
- Examples on methods of specifications
  - E.g. structured analysis

What is a specification?

Attempt of a definition:

- „A specification is a closer description of a primary rather unspecific matter“

- Assembly of different documents
  - What is intended?
  - Which properties it should have?
  - How it will be constructed?
  - How it will be validated/tested?
  - ….
    - ☞ Each on system-, subsystem-, module-, component-level

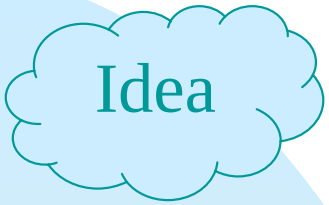
Specification requirements for SILx
(IEC 61508)

Specifications	SIL 4	SIL 3	SIL 2	SIL 1	Applicability: Hardware (H) / Software (S)
Requirements and design specifications	Formal (mathematical)	Semi-formal (e.g. natural language)	Informal (e.g. natural language)	Informal (e.g. natural language)	H/S
Configuration management	Complete (automatic for development & production)	Complete (automatic for development & production)	Yes	Manual	H/S
Prototyping	Yes	Yes	Optional	Optional	H/S
Structured design techniques (e.g. data flowcharts; relation or transfer charts)	Yes	Yes	Preferably	Optional	H/S
Design reviews	Yes (Project team)	Yes (Project team)	Yes (Project team)	Test (Experts)	H/S
Project management	Yes	Yes	Yes	Preferably	H/S

Properties of good specifications

- complete, consistent
- non-ambiguous, free of contradictions
- clear, concise, understandable, readable, …
- refineable, changeable, extendable, …
- testable, measureable
- should not restrict the following design phases
- refers to well recognized (industrial) standards and applicable laws
- …

Phases during development / lifecycle



1. Collecting information, problem analysis

2. Product specification

3a. Requirements Specification

3b. Design Specification

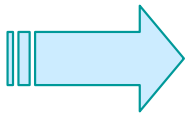
3c. Test Specification

system
subsystems
modules
components

4. Functional design

5. System integration & test

6. Prototyping application



Production

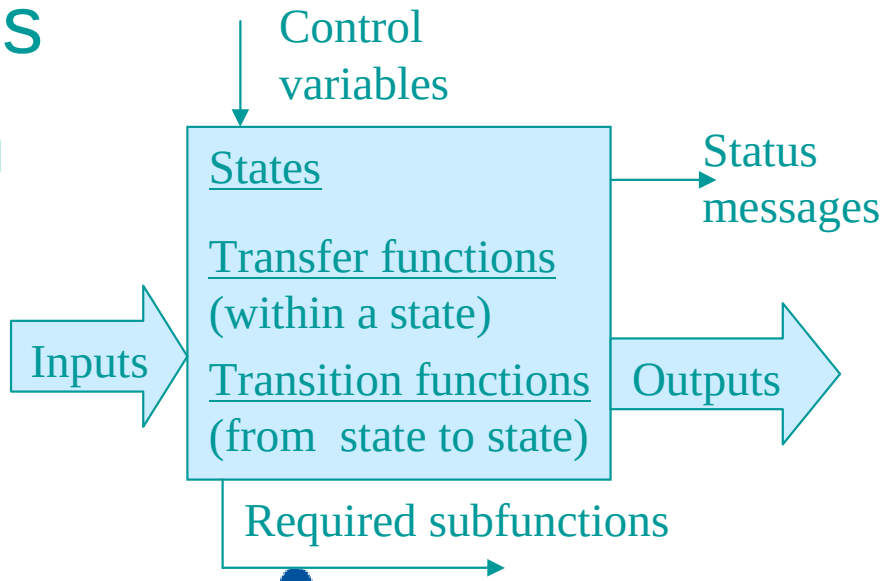
Methods for representation of processes

- Textual: non-formal description in natural language, …
- Graphical: Flow chart, Jackson-diagram, state-diagram, decision tables, sequence diagram, …
- Formal: mathematical expressions, UML

- Usually starting textual; finally combination of different methods

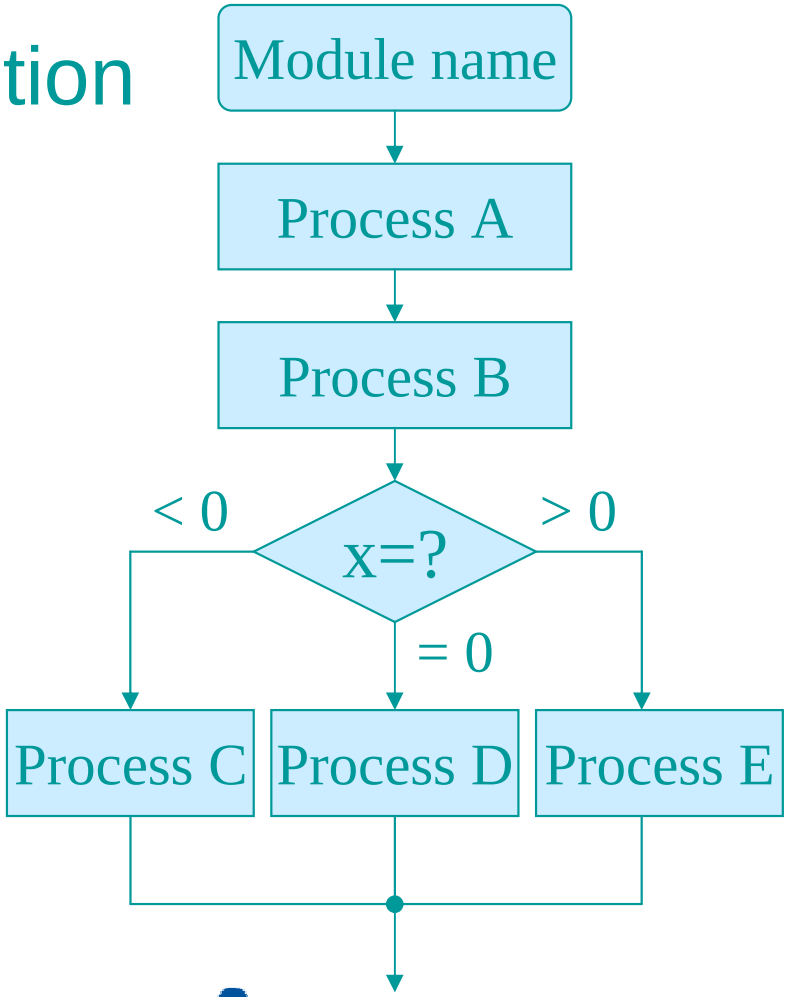
Example: Structured analysis

- Graphical analysis method (known since long)
- Splitting complex function into simple elements
  - iterative top-down approach
  - Data flow, control flow, …
- Result: hierachical document specifying system behavior and its properties
- Advantage: clear notation
- Replaced by UML etc.

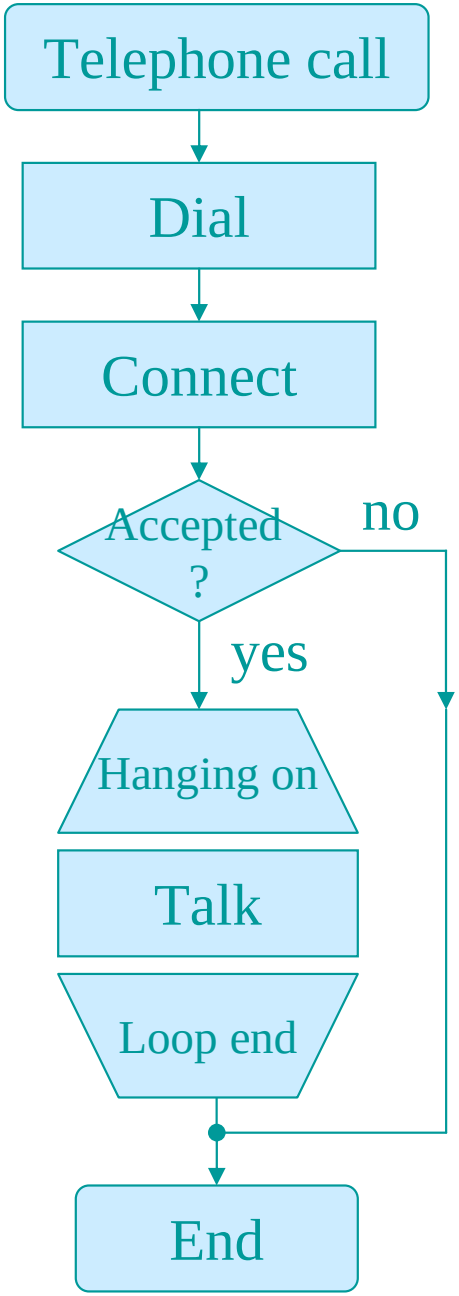


Flowchart

- Standard e.g. DIN 66001
- Sequence, selection, repetition
- Only for small structures
- Alternative: structogram



Flowchart example „telephone call“

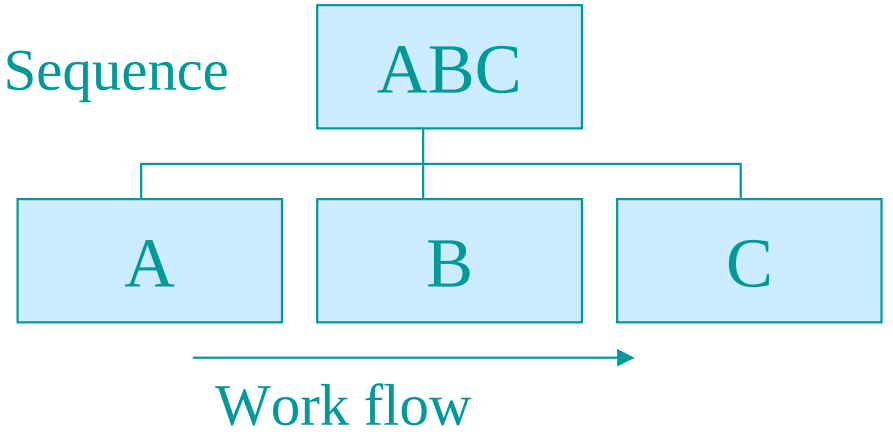


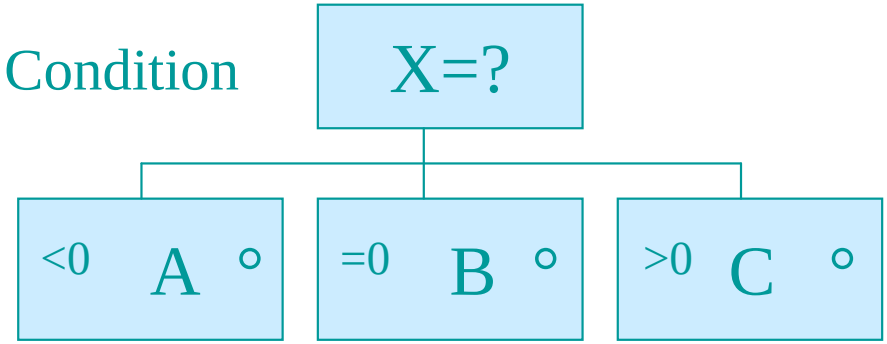
Hochschule Bonn-Rhein-Sieg

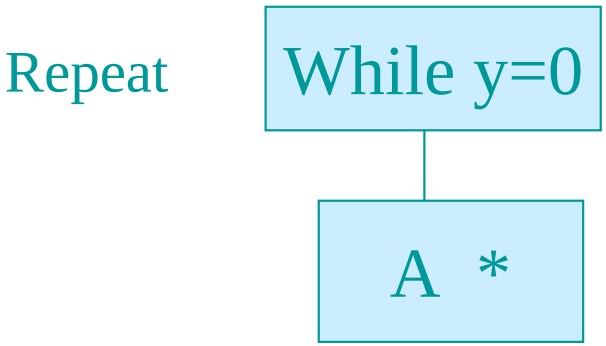
IFA Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung

Jackson diagram

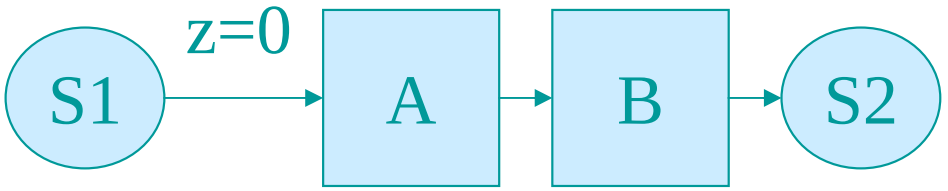
- Hierachical tree diagram
- Refineable
- Flow top-down, left-right
- Separate trees for each task or interrupt



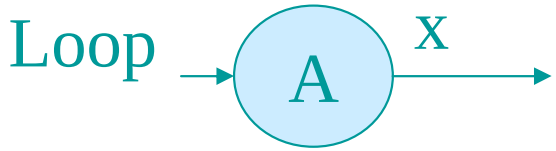


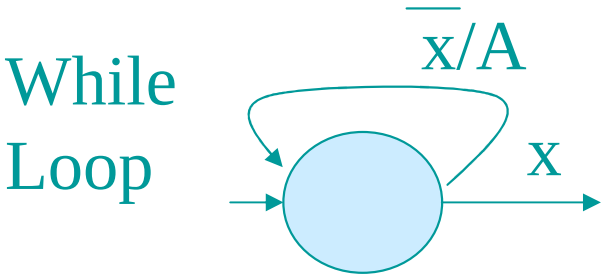


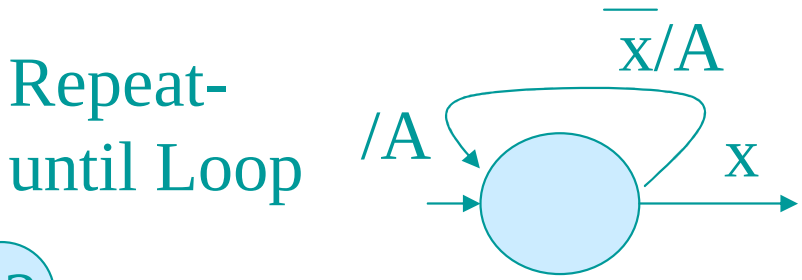
Sequence diagram

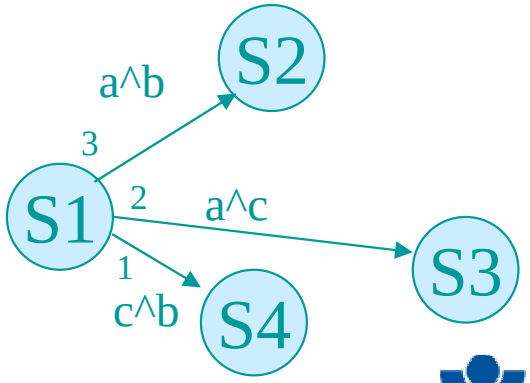


- Description of processes
  - dynamic, parallel
- State transition due to event
- State=interruptable process
- Events= non-interruptable
- State transition if condition = true









Hochschule Bonn-Rhein-Sieg

IFA Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung

Recommendation

- Make your own choice, but be clear
  - What where the criteria of a good specification?
- Structured apporach required
  - (short) orientation phase
  - Specifications of
    - requirements, (What)
    - design and test (How)
  - prior any implementation!
  - Finally validation (and refinement iteration)