Safety analysis

Michal Sojka

Czech Technical University in Prague,
FEE and CIIRC

December 20, 2023

Outline

Outline

Common analysis methods

- Should be conducted early in the development process (step 2 in generic safety process from MIL-STD-882E)
- Serves as input for defining safety integrity level (SIL)
- Common techniques:
  - What-if analysis
  - Interaction analysis
  - Zonal analysis
  - Fault modes and effect analysis (FMEA)
  - Hazard and operability study (HAZOP)

Common analysis methods

- Should be conducted early in the development process (step 2 in generic safety process from MIL-STD-882E)
- Serves as input for defining safety integrity level (SIL)
- Common techniques:
  - What-if analysis
  - Interaction analysis
  - Zonal analysis
  - Fault modes and effect analysis (FMEA)
  - Hazard and operability study (HAZOP)

Outline

HAZOP study

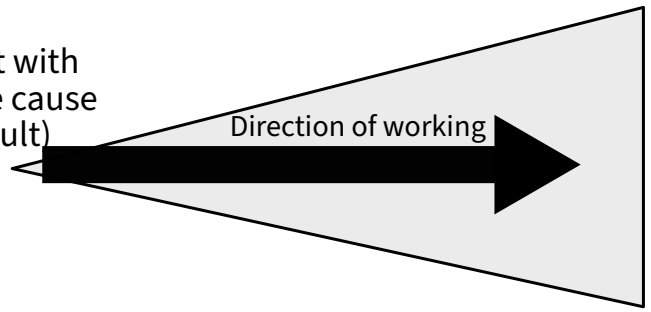
Hazard and operability study

Methodical investigation of the hazards and operational problems to which the plant or system being studied could give rise.

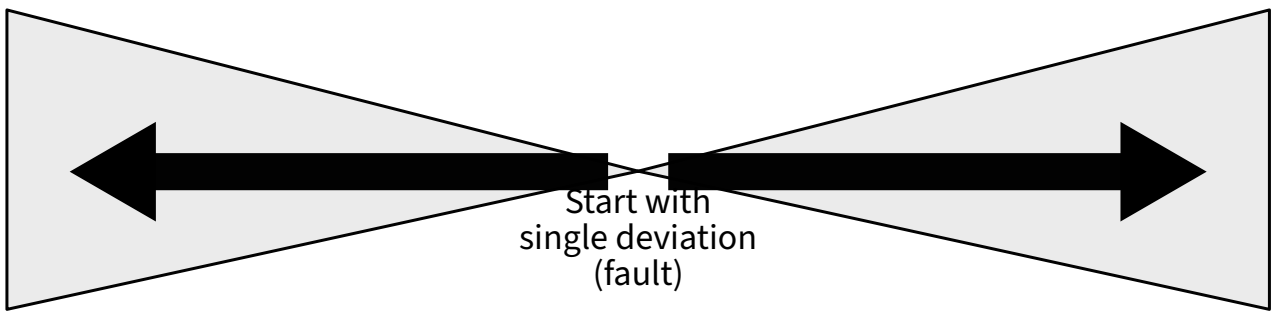
- Goals:
  1. Identify possible deviations from design intent (the intention of the designer)
  2. Investigate deviation's possible causes and consequences.
- Deviations can occur in either a component of the system or an interaction between components of the system.
- Always carried out by a team!

HAZOP compared to other safety analysis methods

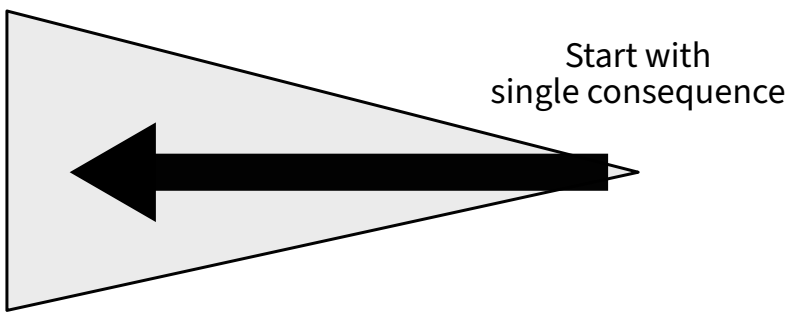
FMEA



HAZOP



FTA



Fault Tree Analysis

Team structure

Roles involved in the study:

- Study leader
- Designer
- User or intended user
- Expert/Experts from different domains
- Recorder

Optimal team size: 4 – 10 persons

Study process

- Input: – Design representation with elements and their attributes.
  – Interpretation of guide word for different attributes.
- Process:

```
Explain design intent;
foreach entity e in design representation do
    foreach attribute a of element e do
        foreach guide word w do
            Investigate deviation of (e, a) suggested by w;
            if deviation is credible then
                Investigate causes and consequences and document;
            end
        end
    end
end
Sign-off the documentation
```

- Output: – Identified hazards
  – Questions
  – Recommendations

Guide words

and their generic meaning

No	no part of the intention is achieved
More	a quantitative increase
Less	a quantitative decrease
As well as	all design intent but with additional results
Part of	only some of the intention is achieved
Reverse	the logical opposite of the intention
Other than	result other than original intention is achieved
Early	relative to clock time
Late	relative to clock time
Before	related to order or sequence
After	related to order or sequence

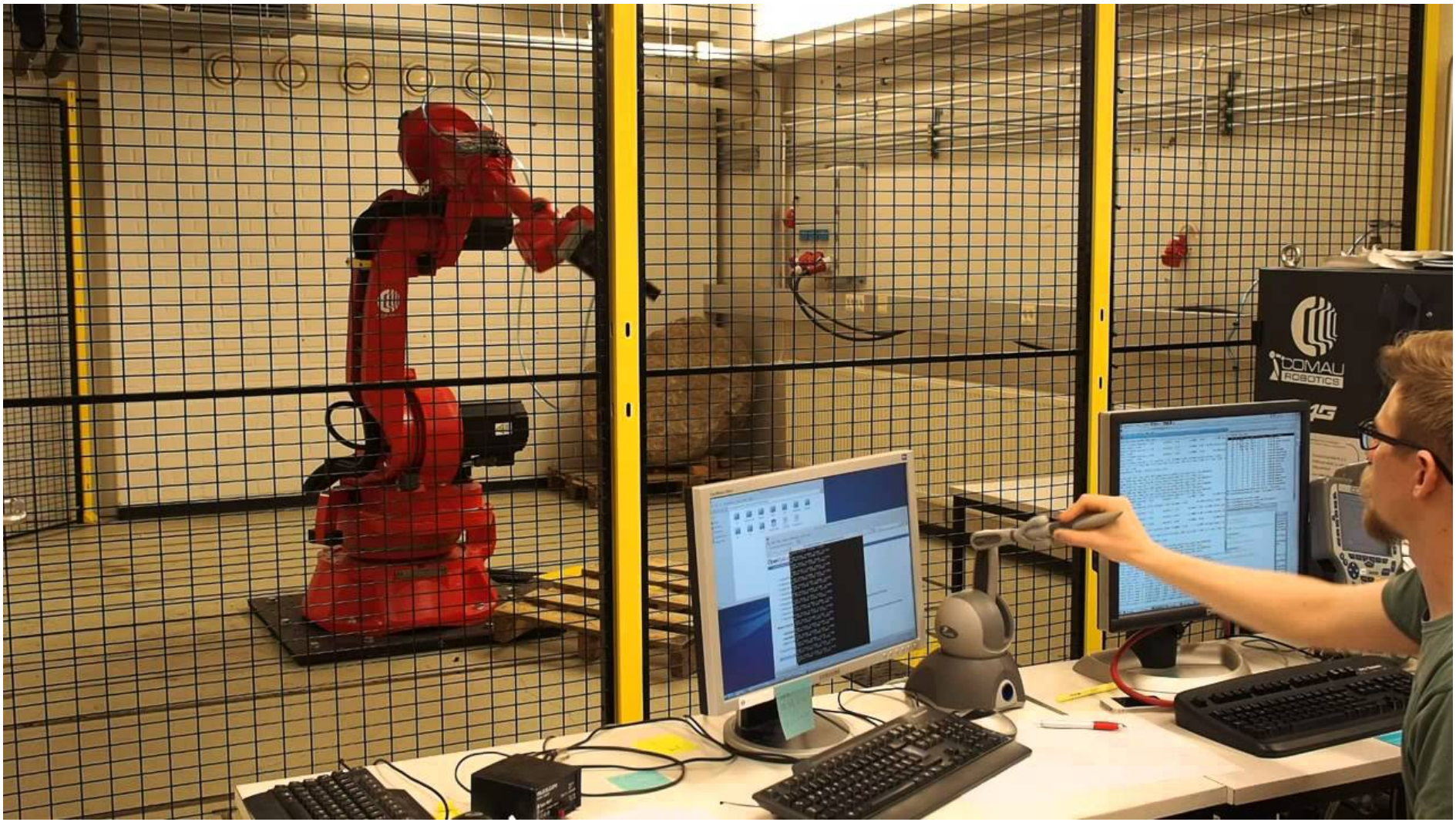
Guide word interpretation

Guide word	Wire	UDP message	Code execution
No	Missing or broken	No message received	Not executed
More	Too high voltage	Duplicate reception	Executed more often
Less	Too low voltage	Lost message	Executed less often
As well as	Noisy signal or EMI	More data in the message	Something else runs in parallel (e.g. IRQ)
Part of	N/A	Partial message received	Only part of code is executed
Reverse	Negative voltage	N/A	N/A
Other than	Other wire	Unexpected message received	Other code is executed instead
Early	N/A	Message received earlier than expected	Executed too early
Late	N/A	Message received later than expected	Executed too late
Before	N/A	Two messages swapped	Before other code
After	N/A	Two messages swapped	After other code

Outline

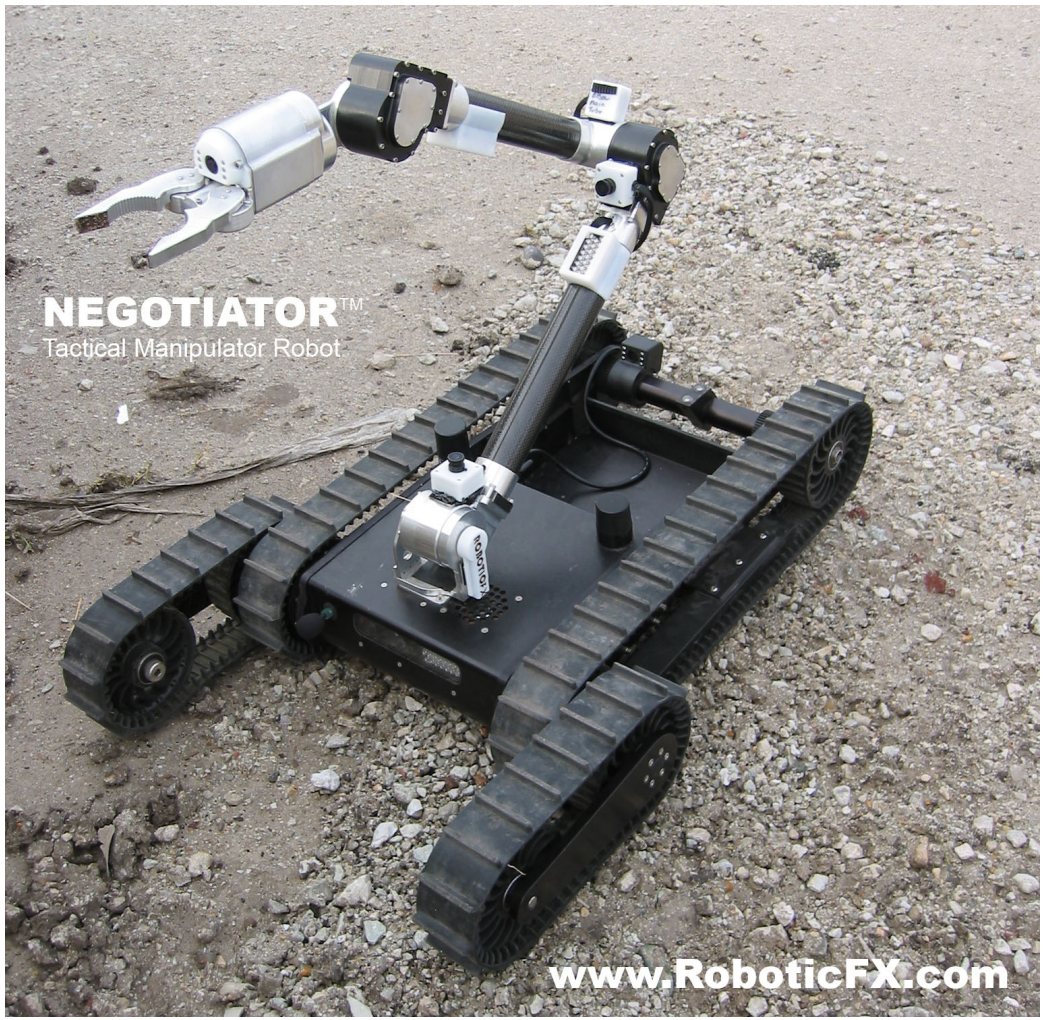
Steer-by-wire for a teleoperated robot

i.e. your semestral work



Steer-by-wire for a teleoperated robot

i.e. your semestral work

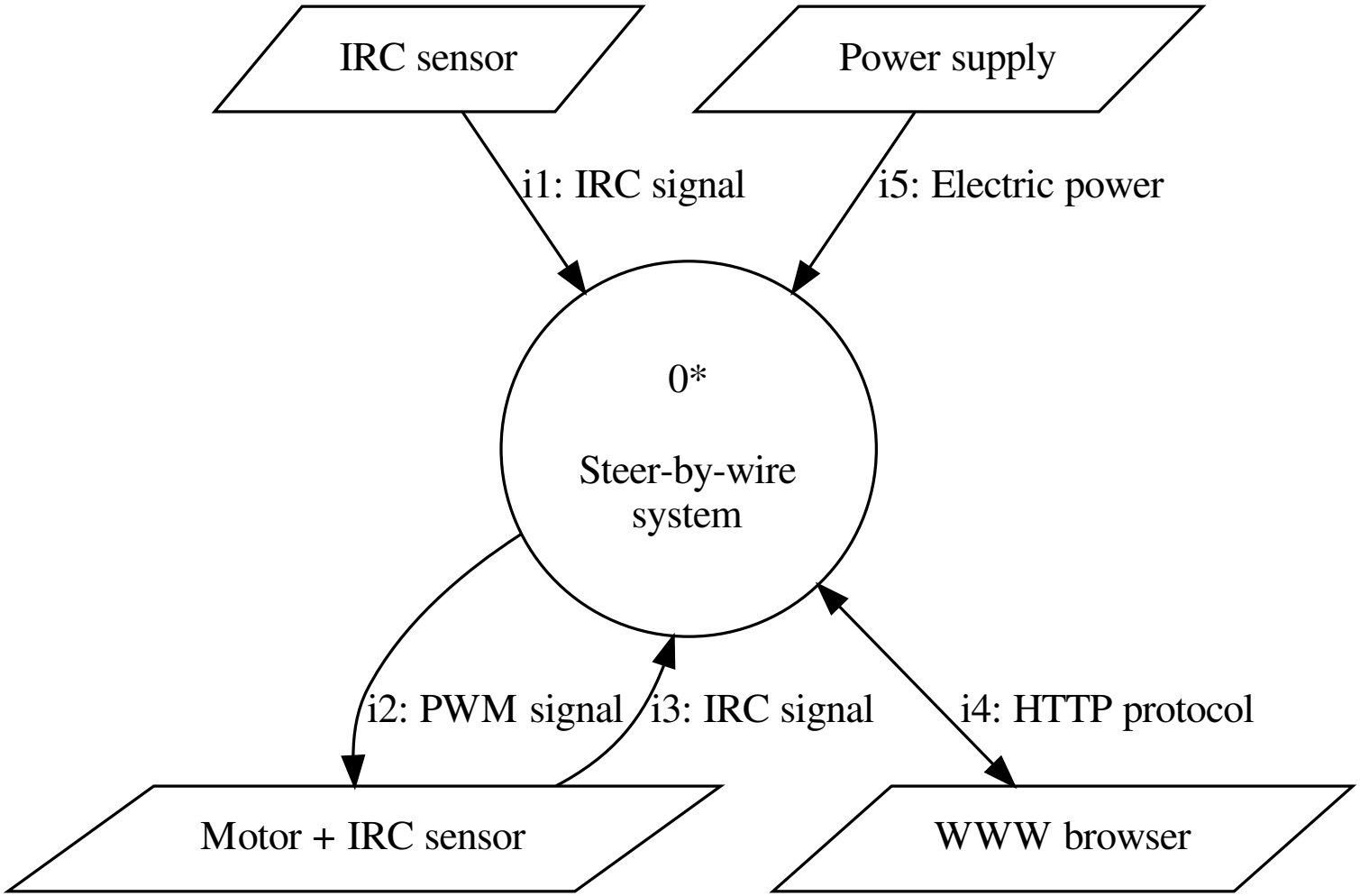


Steer-by-wire for a teleoperated robot

i.e. your semestral work

System context

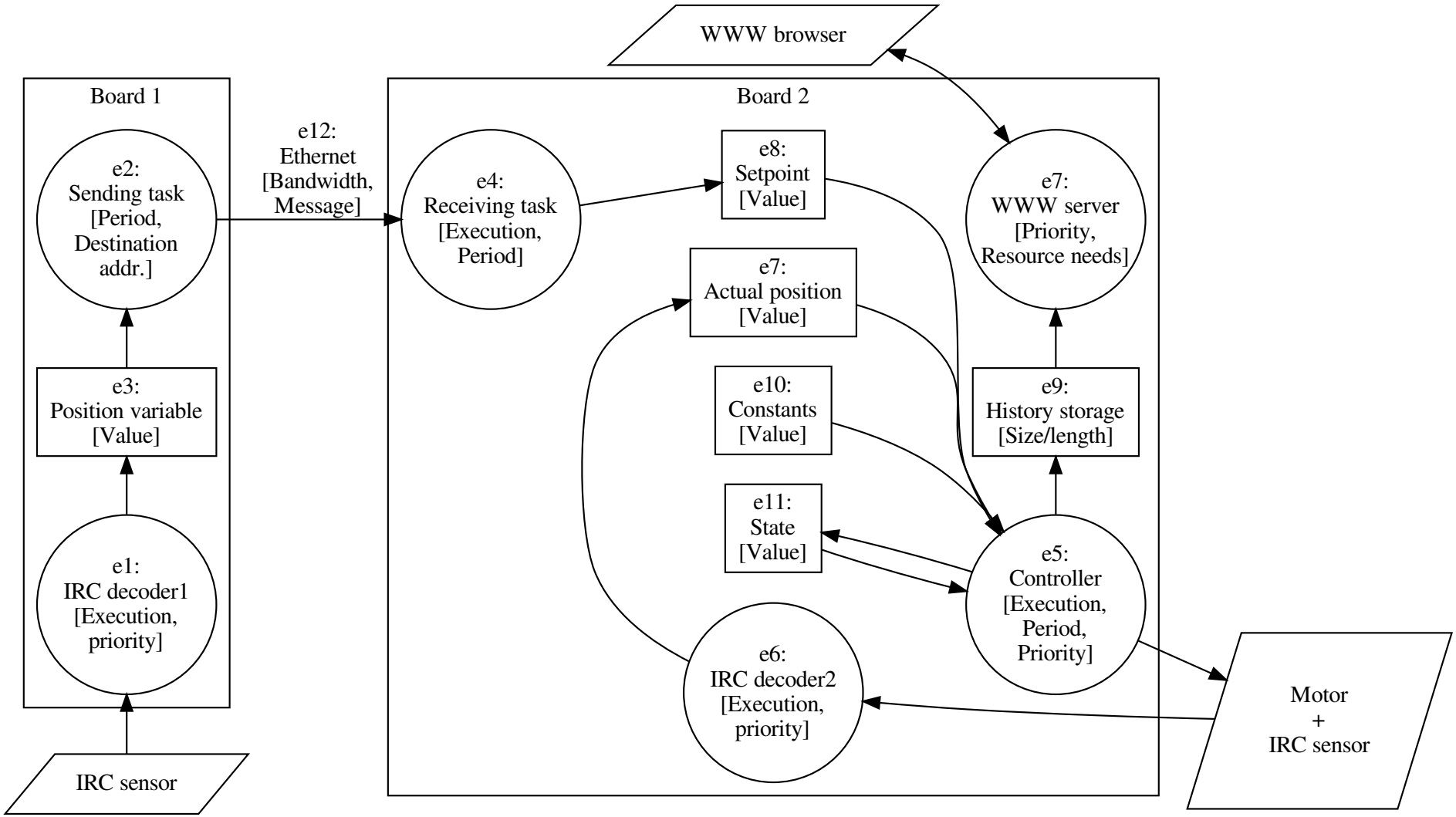
With external interfaces (i)



- "*" means that this level can be expanded

Detailed design

Entities: e, attributes: [...]



Doing HAZOP in a spreadsheet

ID	Item	Attribute	Guide word	Cause	Consequence/ Implication	Indication/ protection	Question/ recommendation		Probability	Severity	Mitigation	Risk	SIL
i1	IRC signal	Dig. Signal	No	Broken wire	Safe state maintained								
			More	Elmag. Interference	CPU overload								
			Less	Elmag. Interference	Imprecise positioning								
			As well as	Elmag. Interference	Imprecise positioning								
			Part of	Elmag. Interference	Imprecise positioning								
			Reverse	Switched wired	Opposite movement								
			Other than	Wrong connector	Uncontrolled movement								
			Late	Digital circuit delay	Imprecise positioning								
i2	PWM	PWM signal	No	El. failure, sw. failure	Robot falls down		Q1: Is motor braked without PWM?						
			More	El. failure, sw. failure	Faster movement, unintentional move								
			Less	El. failure, sw. failure	Degraded/slower movement								
		PWM frequency	No	See above									
			More	Hw. failure, sw. failure	Overheat		Q2: What happens?						
					Motor not controlled		Q3: What is the exact behaviour?						
i3	IRC motor	IRC signal2	See above										
			Reverse	Wrong wiring	Uncontrolled fast movement								
i5	Power	Voltage	No	Blackout	Motor not controlled								
			More		Control system destroyd, motor not controlled								
			Less				Q4: It there undervoltage protection?						
i4	HTTP protocol	Messages	No	No browser connectd	No								

Doing HAZOP in a spreadsheet

ID	Item	Attribute	Guide word	Cause	Consequence/ Implication	Indication/ protection	Question/ recommendation		Probability	Severity	Mitigation	Risk	SIL
			More	Computer ifected by virus	CPU overload	HTTP handler should have low priority, request rate limiting							
			Less	Bad network	NO								
		Connections	No										
			More	DoS	Out of memory	Do not use dynamic memory allocation in real-time part							
e7	Actual position variable	Value	No		N/A								
			More	HW failure, buffer overflos, SW failure	Fast motor movement	Plausability checks			Improbable	Critical	Plausability checks	Medium	SIL1
			Less						z2				
			Reverse	SW error, HW connection error	Positive feedback, oncontrolled motor movement				Occational	Critical	Initial identification	Serios	SIL2

References

- F. Redmill, M. Chudleigh, J. Catmur; System Safety: HAZOP and Software HAZOP, Wiley, 1999.