ES-SHC5300

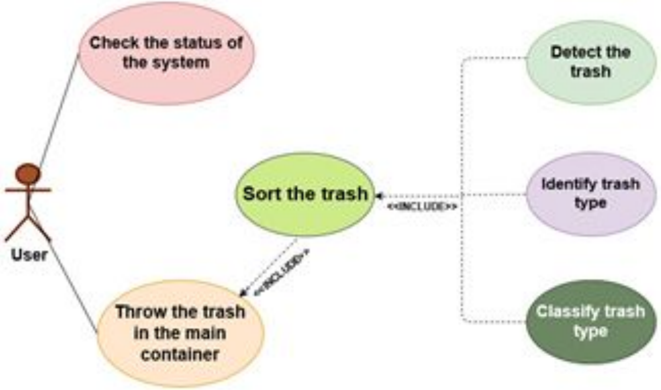
Safety Critical systems

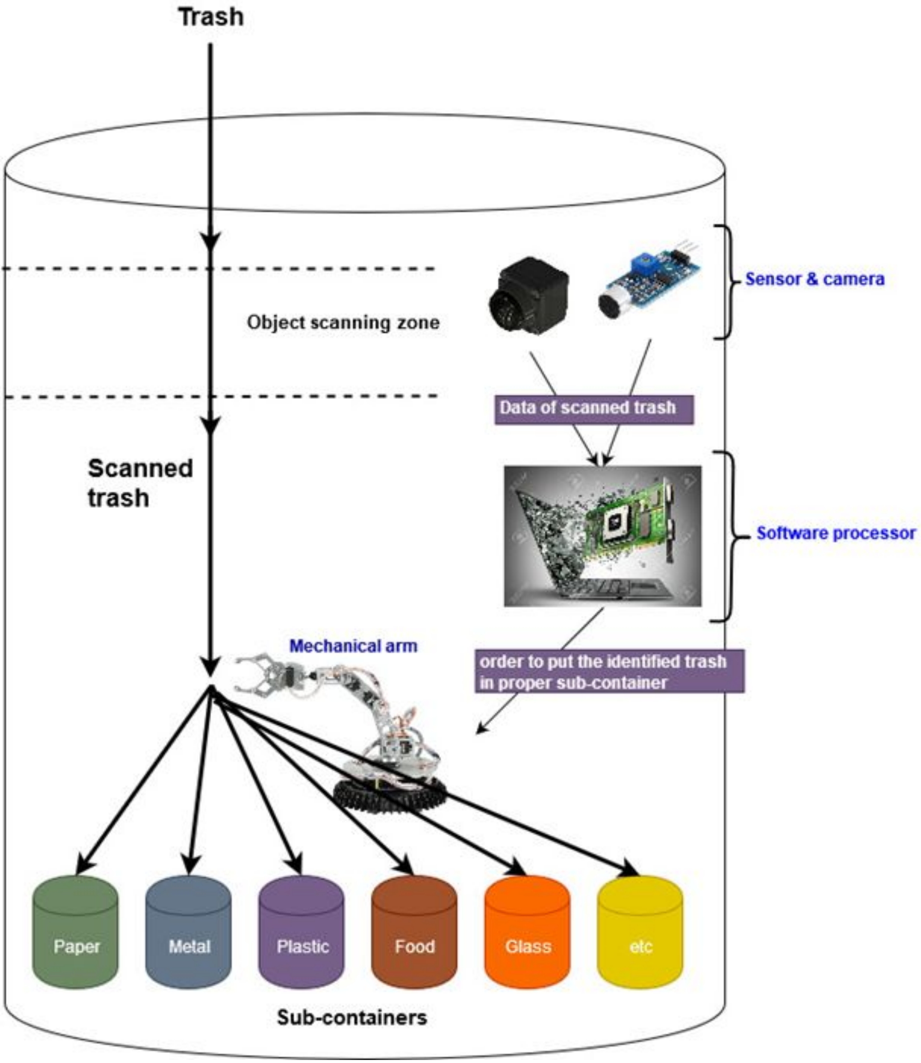
Autonomous waste sorter

Yasin Yari

2019/20

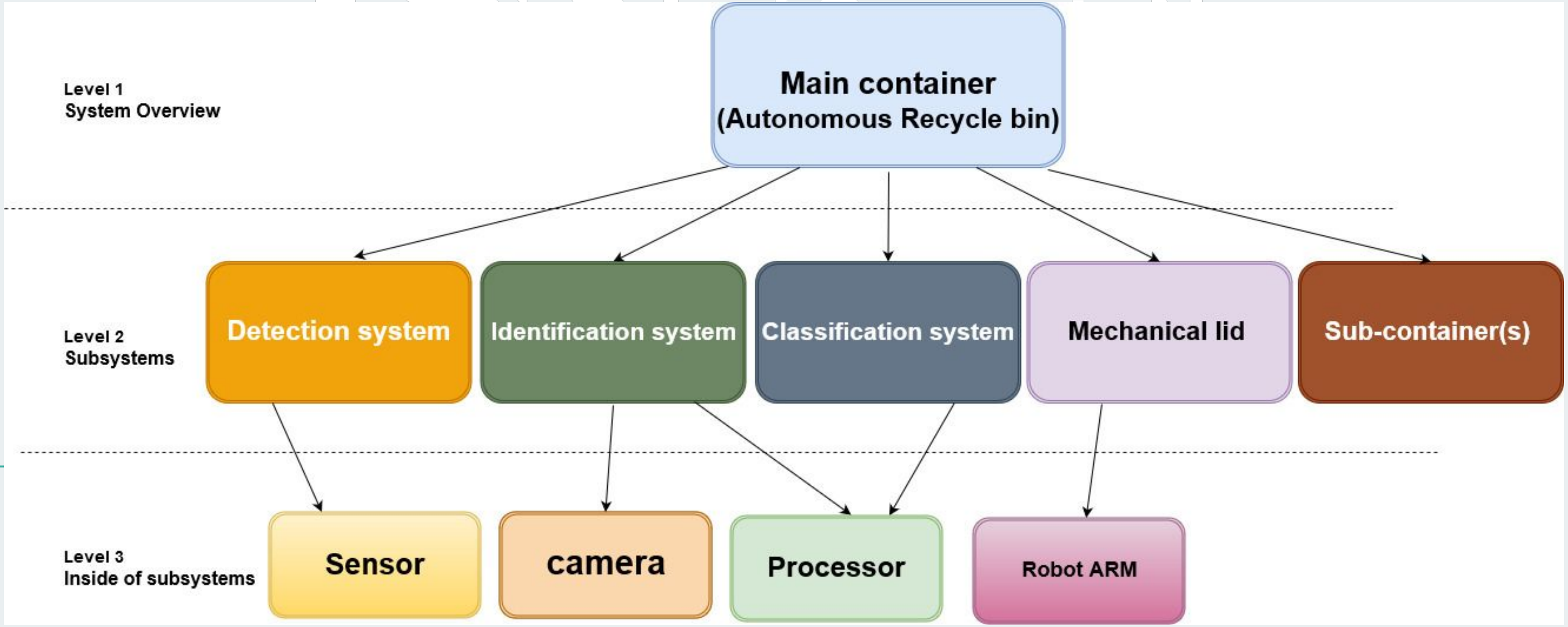
System Overview



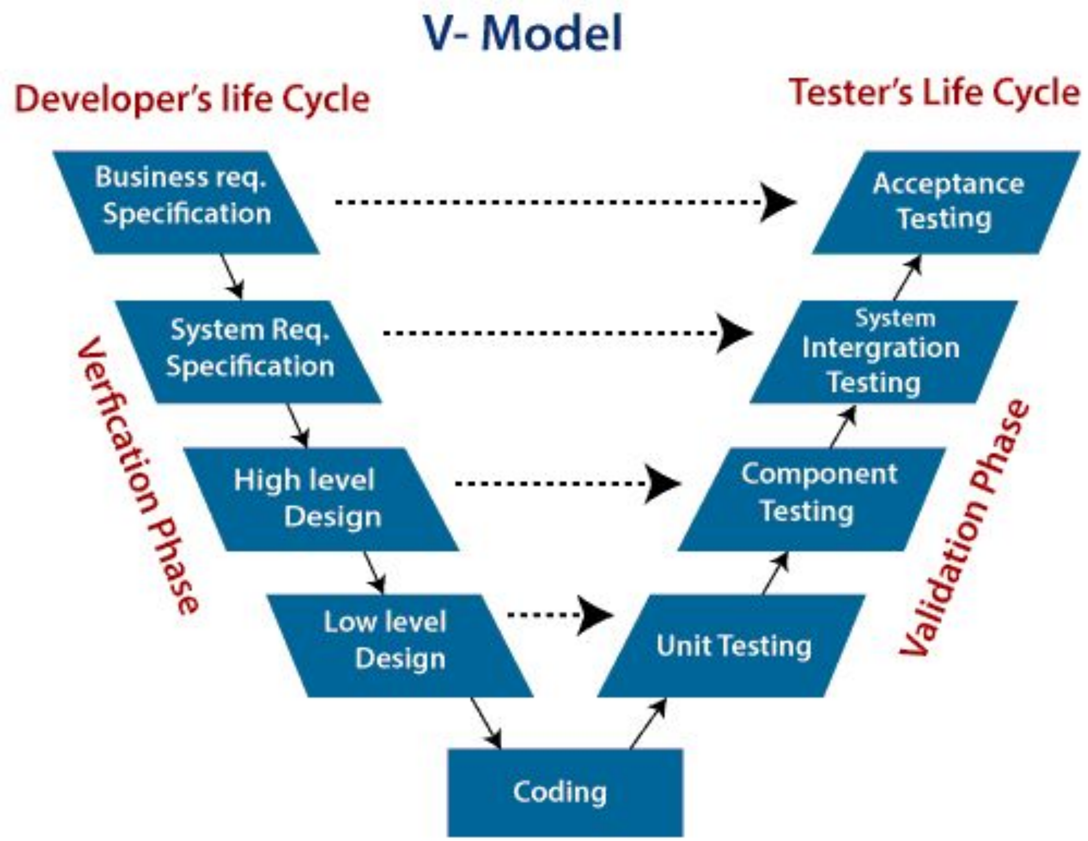


Universitetet i Sørøst-Norge

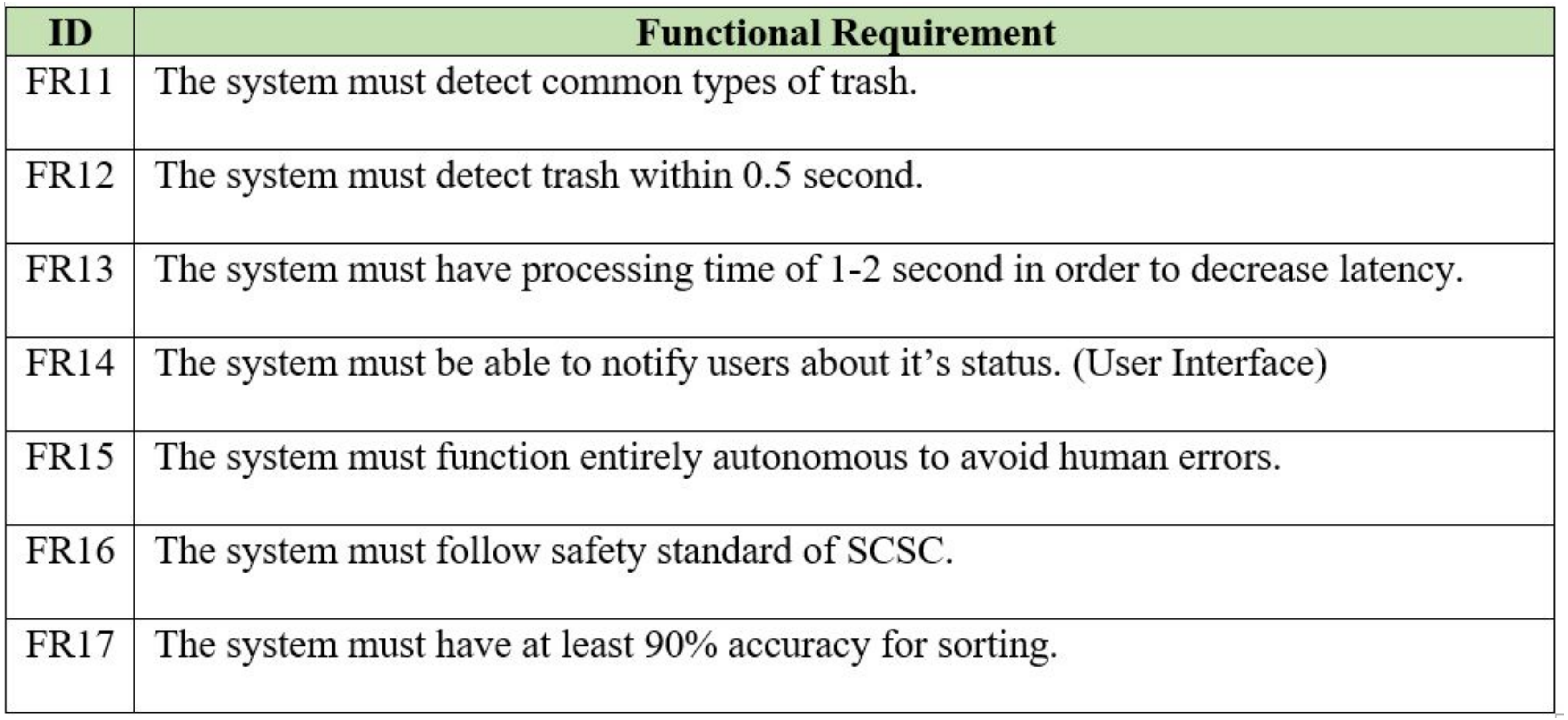
System Overview



- Top-down
- Buttom-up
- Verification
- Integration
- Validation
- Testing

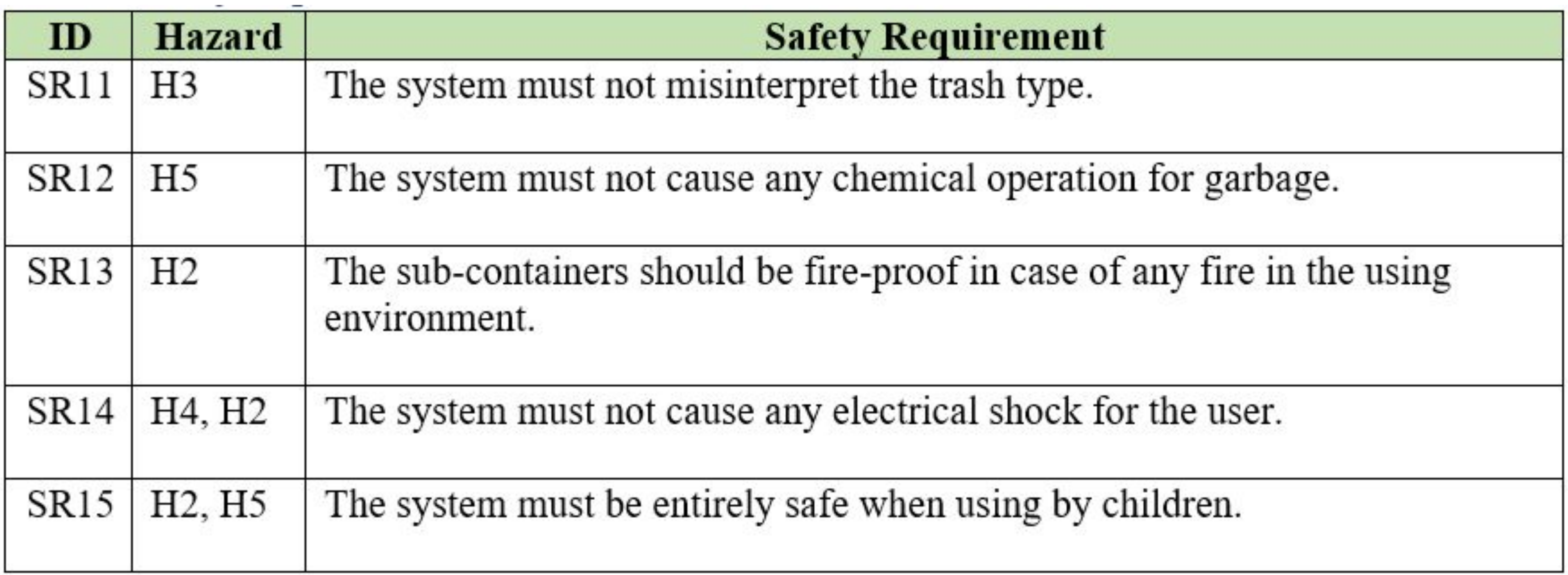


Requirement specifications



ID	Functional Requirement
FR11	The system must detect common types of trash.
FR12	The system must detect trash within 0.5 second.
FR13	The system must have processing time of 1-2 second in order to decrease latency.
FR14	The system must be able to notify users about it's status. (User Interface)
FR15	The system must function entirely autonomous to avoid human errors.
FR16	The system must follow safety standard of SCSC.
FR17	The system must have at least 90% accuracy for sorting.

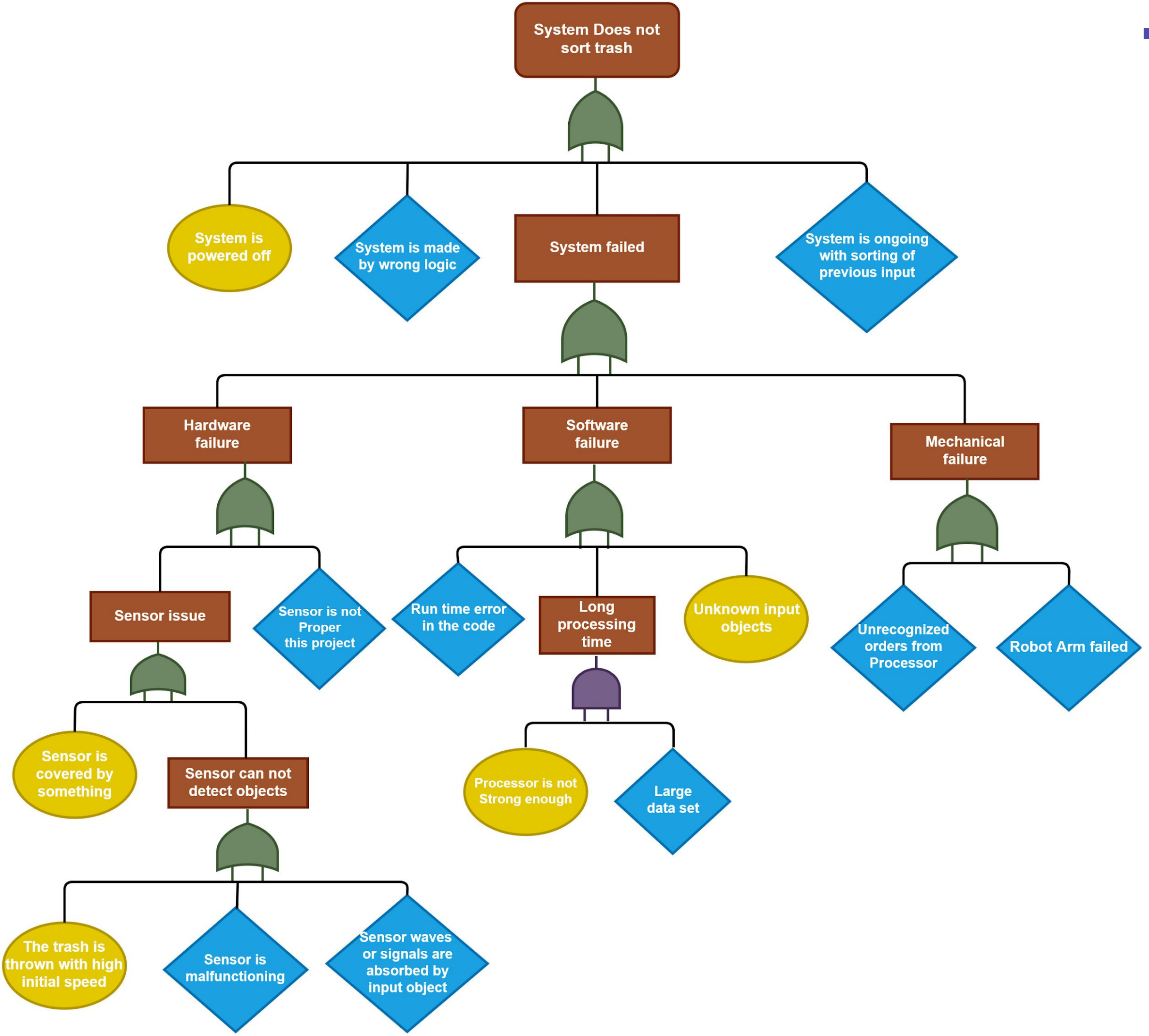
Safety requirements



ID	Hazard	Safety Requirement
SR11	H3	The system must not misinterpret the trash type.
SR12	H5	The system must not cause any chemical operation for garbage.
SR13	H2	The sub-containers should be fire-proof in case of any fire in the using environment.
SR14	H4, H2	The system must not cause any electrical shock for the user.
SR15	H2, H5	The system must be entirely safe when using by children.

Hazard Analysis

FTA



System Does not sort trash

System is powered off

System is made by wrong logic

System failed

System is ongoing with sorting of previous input

Hardware failure

Software failure

Mechanical failure

Sensor issue

Sensor is not Proper this project

Sensor is covered by something

Sensor can not detect objects

The trash is thrown with high initial speed

Sensor is malfunctioning

Sensor waves or signals are absorbed by input object

Run time error in the code

Long processing time

Unknown input objects

Processor is not Strong enough

Large data set

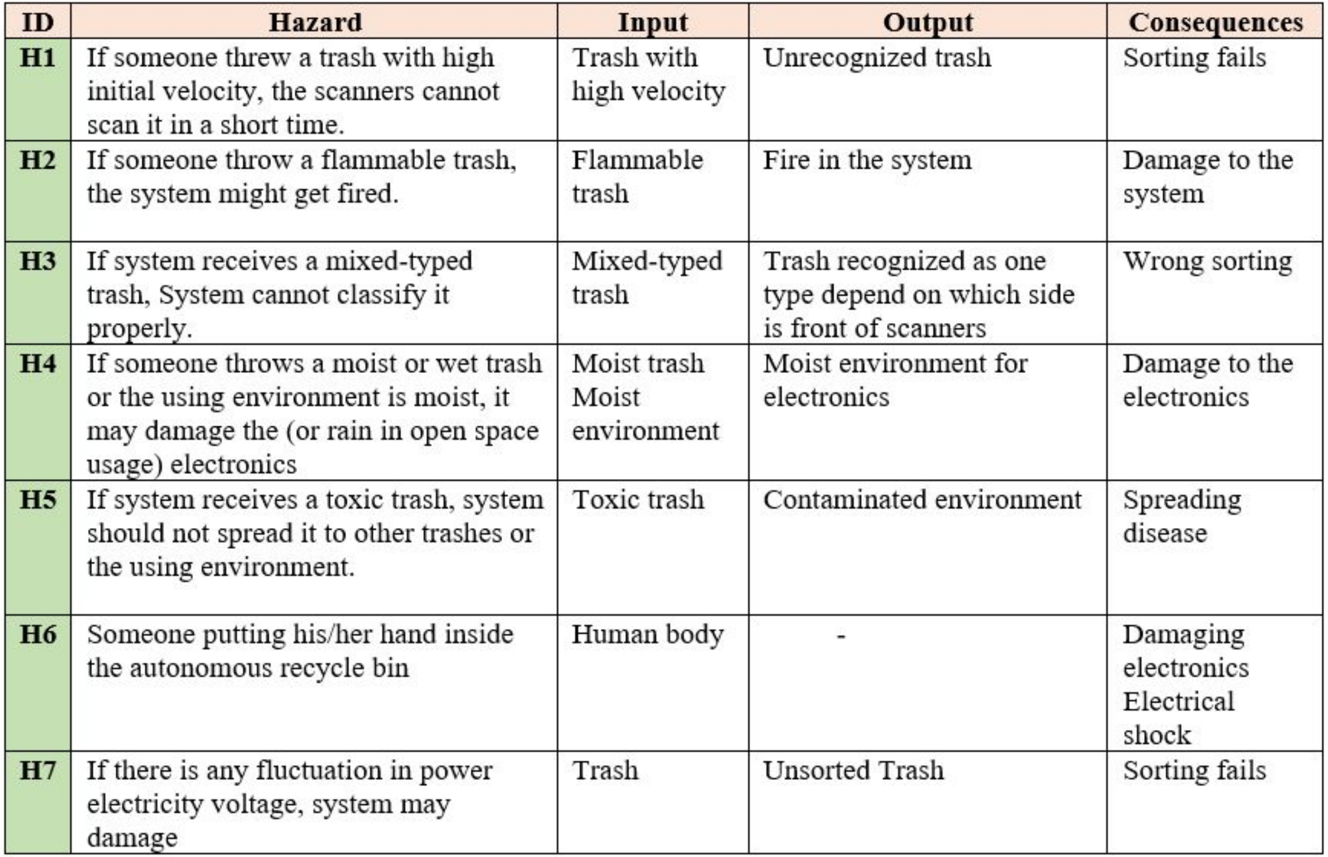
Unrecognized orders from Processor

Robot Arm failed

Universitetet i Sørøst-Norge

Hazards

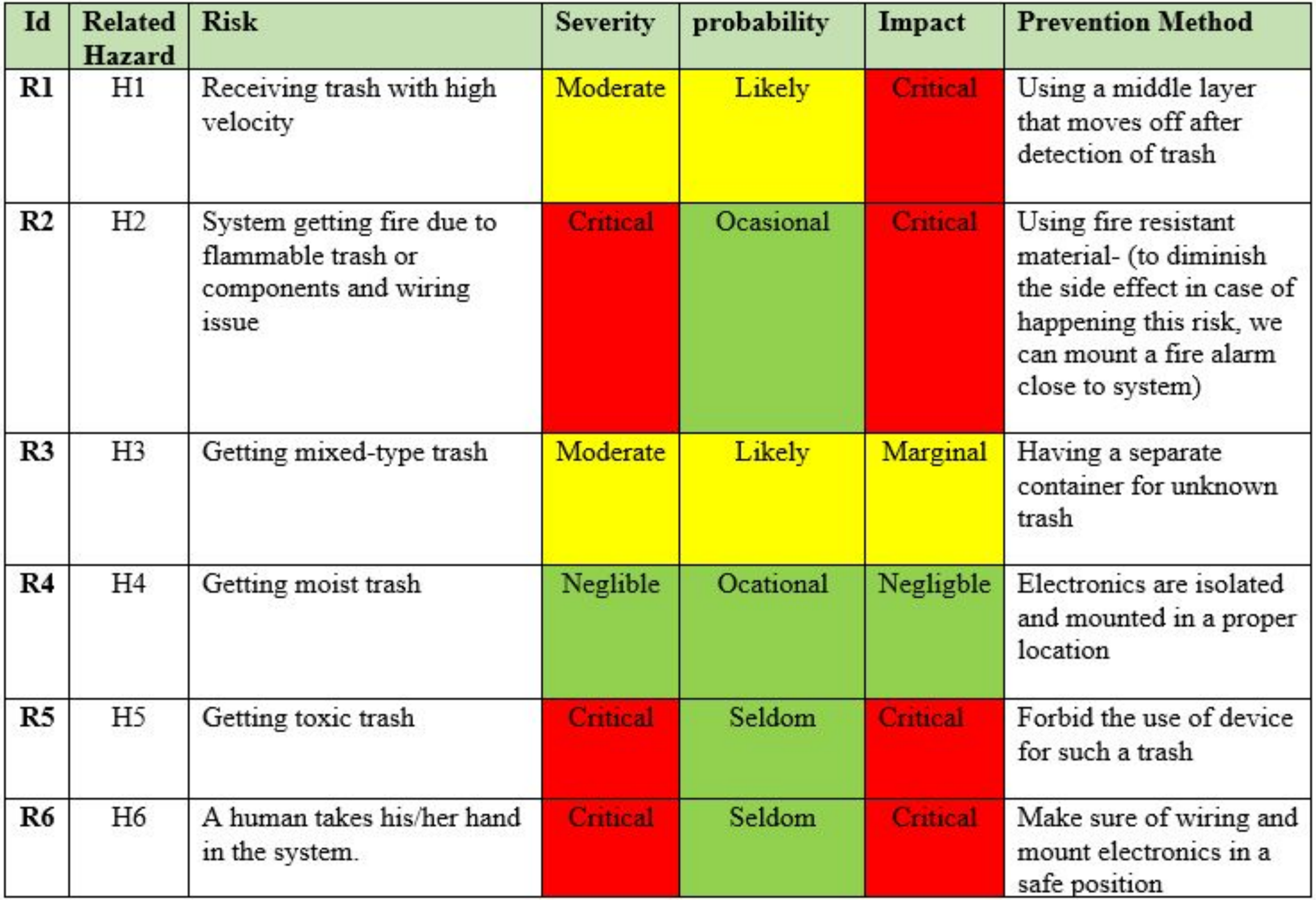
- ❑ System
- ❑ Environment



ID	Hazard	Input	Output	Consequences
H1	If someone threw a trash with high initial velocity, the scanners cannot scan it in a short time.	Trash with high velocity	Unrecognized trash	Sorting fails
H2	If someone throw a flammable trash, the system might get fired.	Flammable trash	Fire in the system	Damage to the system
H3	If system receives a mixed-typed trash, System cannot classify it properly.	Mixed-typed trash	Trash recognized as one type depend on which side is front of scanners	Wrong sorting
H4	If someone throws a moist or wet trash or the using environment is moist, it may damage the (or rain in open space usage) electronics	Moist trash Moist environment	Moist environment for electronics	Damage to the electronics
H5	If system receives a toxic trash, system should not spread it to other trashes or the using environment.	Toxic trash	Contaminated environment	Spreading disease
H6	Someone putting his/her hand inside the autonomous recycle bin	Human body	-	Damaging electronics Electrical shock
H7	If there is any fluctuation in power electricity voltage, system may damage	Trash	Unsorted Trash	Sorting fails

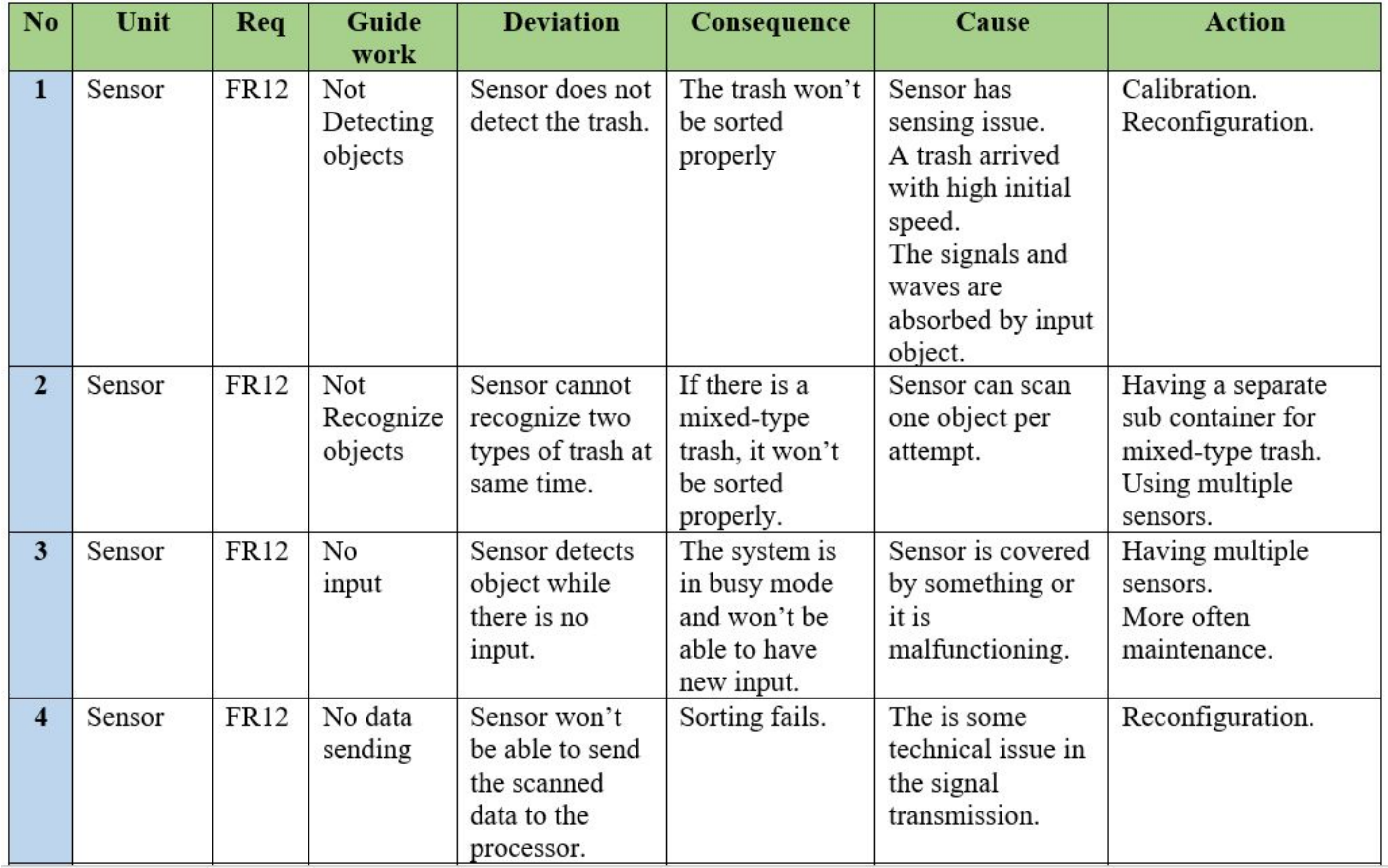
Risk

Exposures on hazards



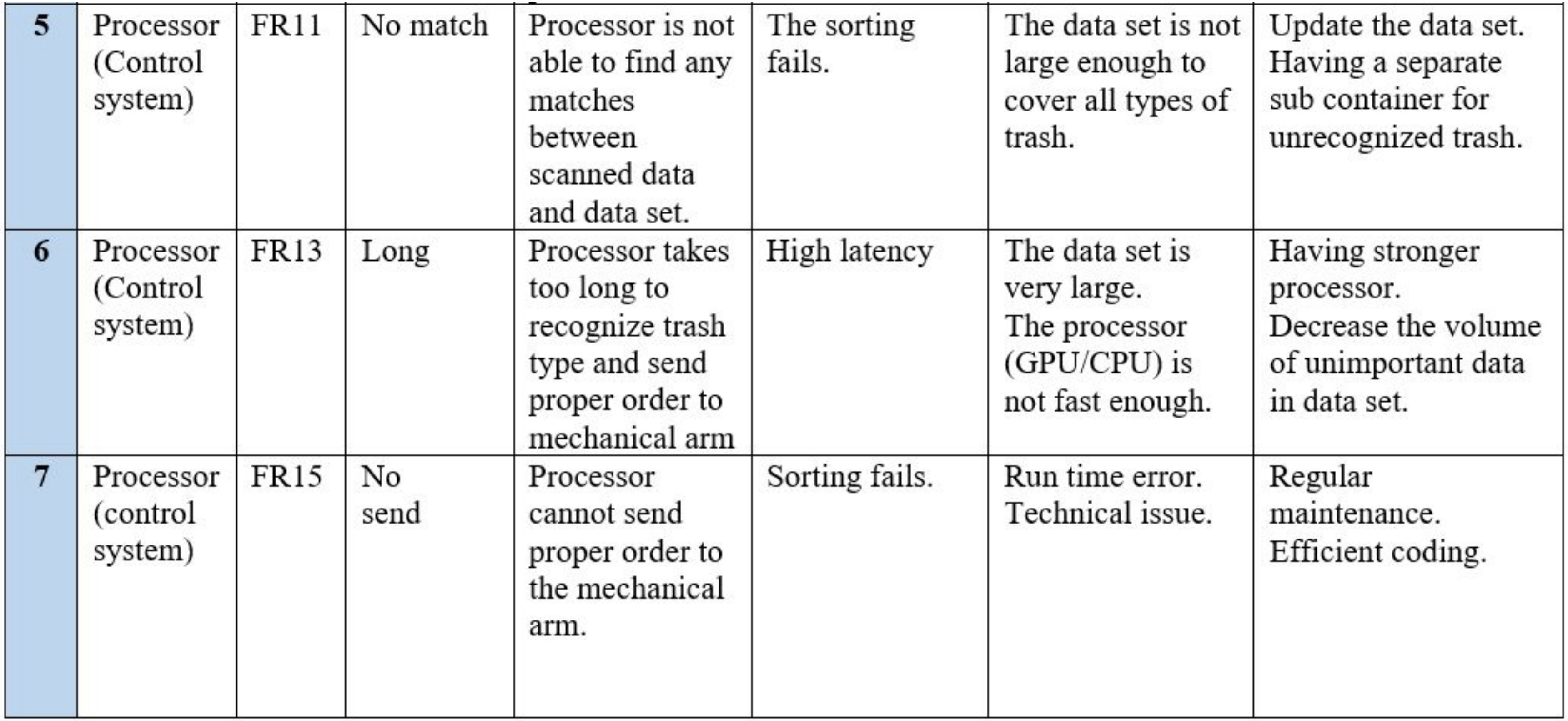
Id	Related Hazard	Risk	Severity	probability	Impact	Prevention Method
R1	H1	Receiving trash with high velocity	Moderate	Likely	Critical	Using a middle layer that moves off after detection of trash
R2	H2	System getting fire due to flammable trash or components and wiring issue	Critical	Ocasional	Critical	Using fire resistant material- (to diminish the side effect in case of happening this risk, we can mount a fire alarm close to system)
R3	H3	Getting mixed-type trash	Moderate	Likely	Marginal	Having a separate container for unknown trash
R4	H4	Getting moist trash	Neglible	Ocational	Negligble	Electronics are isolated and mounted in a proper location
R5	H5	Getting toxic trash	Critical	Seldom	Critical	Forbid the use of device for such a trash
R6	H6	A human takes his/her hand in the system.	Critical	Seldom	Critical	Make sure of wiring and mount electronics in a safe position

HAZOP



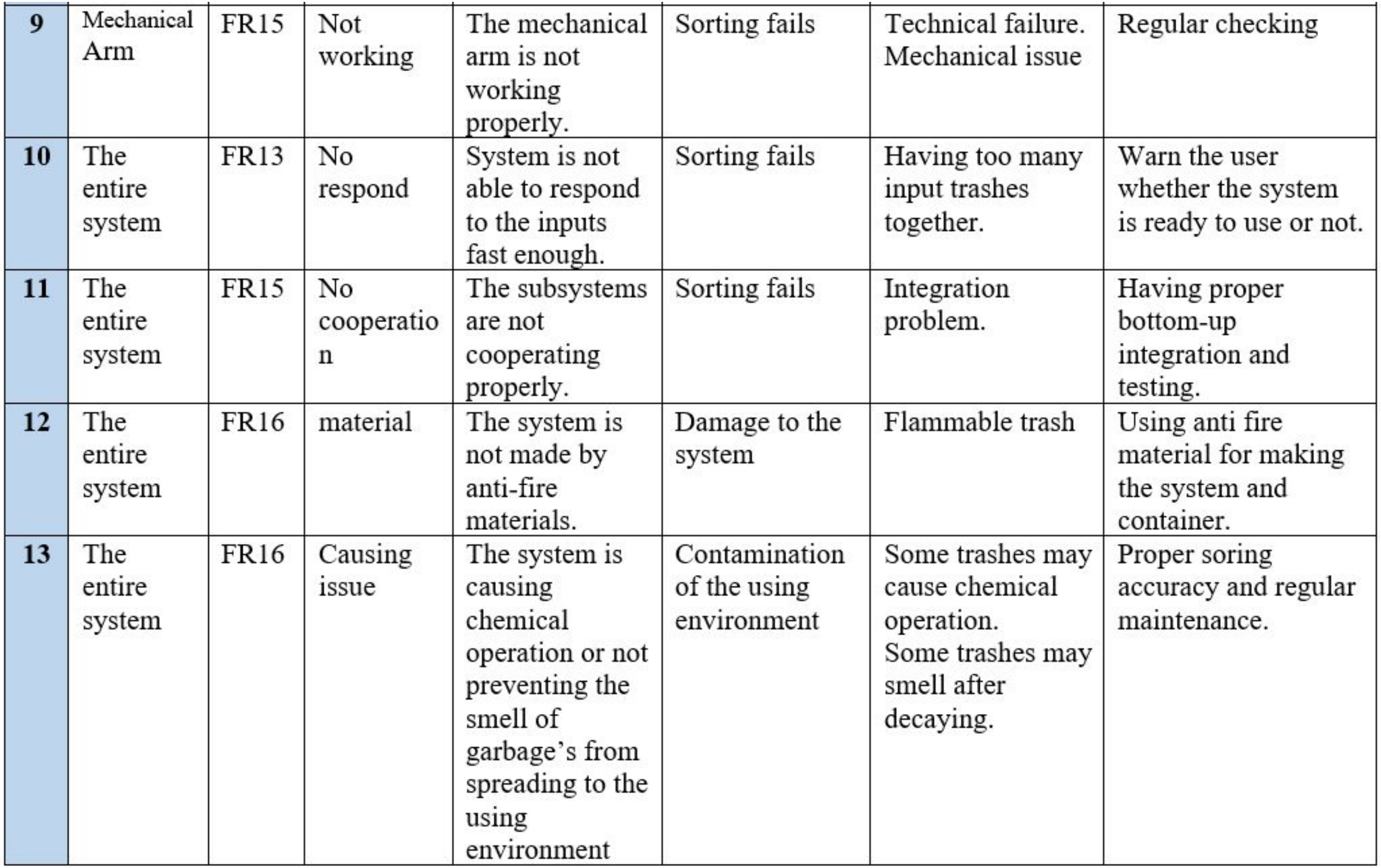
No	Unit	Req	Guide work	Deviation	Consequence	Cause	Action
1	Sensor	FR12	Not Detecting objects	Sensor does not detect the trash.	The trash won't be sorted properly	Sensor has sensing issue. A trash arrived with high initial speed. The signals and waves are absorbed by input object.	Calibration. Reconfiguration.
2	Sensor	FR12	Not Recognize objects	Sensor cannot recognize two types of trash at same time.	If there is a mixed-type trash, it won't be sorted properly.	Sensor can scan one object per attempt.	Having a separate sub container for mixed-type trash. Using multiple sensors.
3	Sensor	FR12	No input	Sensor detects object while there is no input.	The system is in busy mode and won't be able to have new input.	Sensor is covered by something or it is malfunctioning.	Having multiple sensors. More often maintenance.
4	Sensor	FR12	No data sending	Sensor won't be able to send the scanned data to the processor.	Sorting fails.	The is some technical issue in the signal transmission.	Reconfiguration.

HAZOP



5	Processor (Control system)	FR11	No match	Processor is not able to find any matches between scanned data and data set.	The sorting fails.	The data set is not large enough to cover all types of trash.	Update the data set. Having a separate sub container for unrecognized trash.
6	Processor (Control system)	FR13	Long	Processor takes too long to recognize trash type and send proper order to mechanical arm	High latency	The data set is very large. The processor (GPU/CPU) is not fast enough.	Having stronger processor. Decrease the volume of unimportant data in data set.
7	Processor (control system)	FR15	No send	Processor cannot send proper order to the mechanical arm.	Sorting fails.	Run time error. Technical issue.	Regular maintenance. Efficient coding.

HAZOP



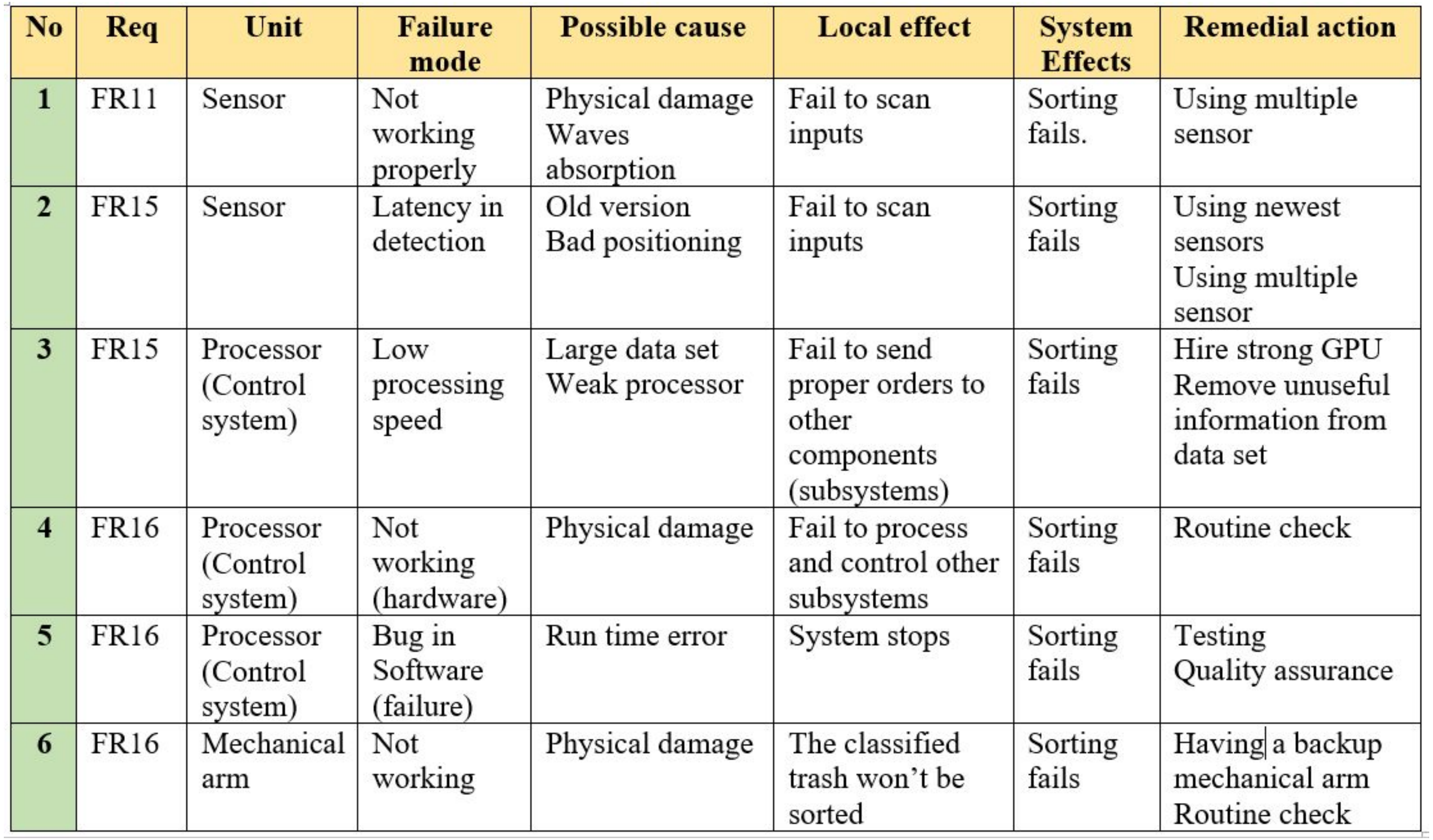
9	Mechanical Arm	FR15	Not working	The mechanical arm is not working properly.	Sorting fails	Technical failure. Mechanical issue	Regular checking
10	The entire system	FR13	No respond	System is not able to respond to the inputs fast enough.	Sorting fails	Having too many input trashes together.	Warn the user whether the system is ready to use or not.
11	The entire system	FR15	No cooperation	The subsystems are not cooperating properly.	Sorting fails	Integration problem.	Having proper bottom-up integration and testing.
12	The entire system	FR16	material	The system is not made by anti-fire materials.	Damage to the system	Flammable trash	Using anti fire material for making the system and container.
13	The entire system	FR16	Causing issue	The system is causing chemical operation or not preventing the smell of garbage's from spreading to the using environment	Contamination of the using environment	Some trashes may cause chemical operation. Some trashes may smell after decaying.	Proper soring accuracy and regular maintenance.

FMEA

A methodology to identify and analyze:

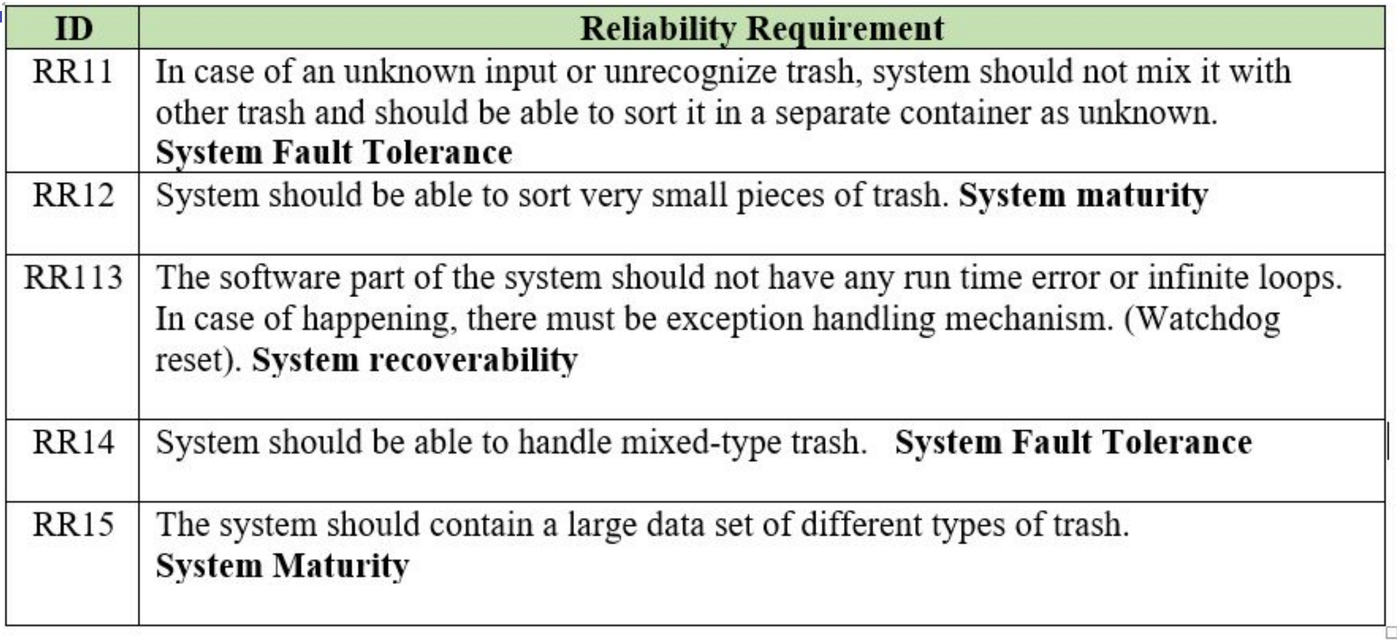
❑ all potential failure
❑ how to avoid or mitigate effects of the failures.
❑ Systematic procedure
❑ “Bottom-up” technique
❑ One subsystem at a time
❑ Risk/consequence matrix

FMEA

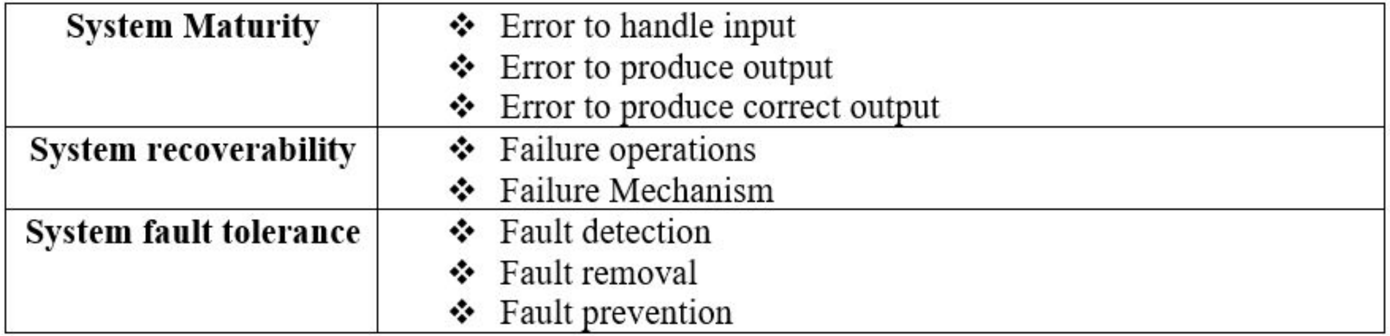


No	Req	Unit	Failure mode	Possible cause	Local effect	System Effects	Remedial action
1	FR11	Sensor	Not working properly	Physical damage Waves absorption	Fail to scan inputs	Sorting fails.	Using multiple sensor
2	FR15	Sensor	Latency in detection	Old version Bad positioning	Fail to scan inputs	Sorting fails	Using newest sensors Using multiple sensor
3	FR15	Processor (Control system)	Low processing speed	Large data set Weak processor	Fail to send proper orders to other components (subsystems)	Sorting fails	Hire strong GPU Remove unuseful information from data set
4	FR16	Processor (Control system)	Not working (hardware)	Physical damage	Fail to process and control other subsystems	Sorting fails	Routine check
5	FR16	Processor (Control system)	Bug in Software (failure)	Run time error	System stops	Sorting fails	Testing Quality assurance
6	FR16	Mechanical arm	Not working	Physical damage	The classified trash won't be sorted	Sorting fails	Having a backup mechanical arm Routine check

Reliability



ID	Reliability Requirement
RR11	In case of an unknown input or unrecognize trash, system should not mix it with other trash and should be able to sort it in a separate container as unknown. **System Fault Tolerance**
RR12	System should be able to sort very small pieces of trash. **System maturity**
RR113	The software part of the system should not have any run time error or infinite loops. In case of happening, there must be exception handling mechanism. (Watchdog reset). **System recoverability**
RR14	System should be able to handle mixed-type trash. **System Fault Tolerance**
RR15	The system should contain a large data set of different types of trash. **System Maturity**



System Maturity	❖ Error to handle input ❖ Error to produce output ❖ Error to produce correct output
System recoverability	❖ Failure operations ❖ Failure Mechanism
System fault tolerance	❖ Fault detection ❖ Fault removal ❖ Fault prevention

Safety critical measure for Software

Software

- Embedded C & C++
  - Watchdog reset
  - converts efficiently into machine code (better than most high-level languages).
  - power on reset
  - low level, faster than C and Python
  - higher abstraction level

- Atmel Studio
  - Assembly language (Instruction per cycle) RISC
  - Machine code
  - Test & Simulate

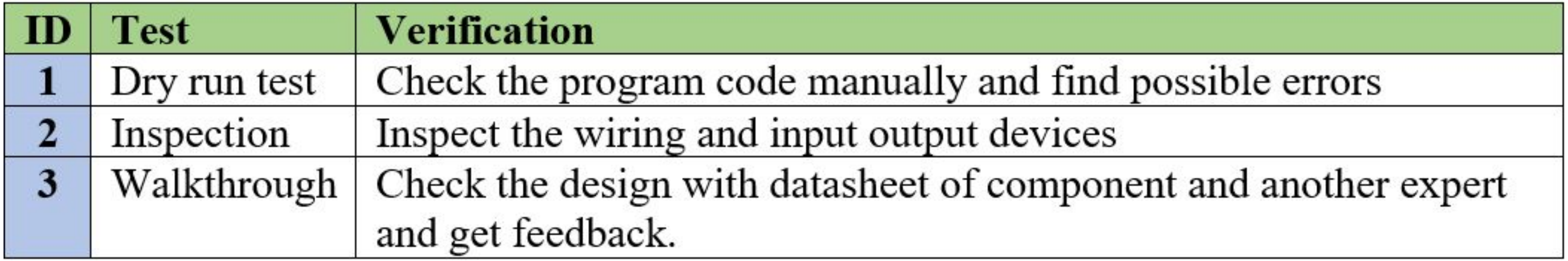
Safety critical measure for hardware

Hardware

- ➢ Sensor (Latency, Accuracy)
- ➢ Hardware timer (very accurate)
- ➢ External event handling (2 threads)
- ➢ Verification and Validation

Testing Methodologies

Static Testing

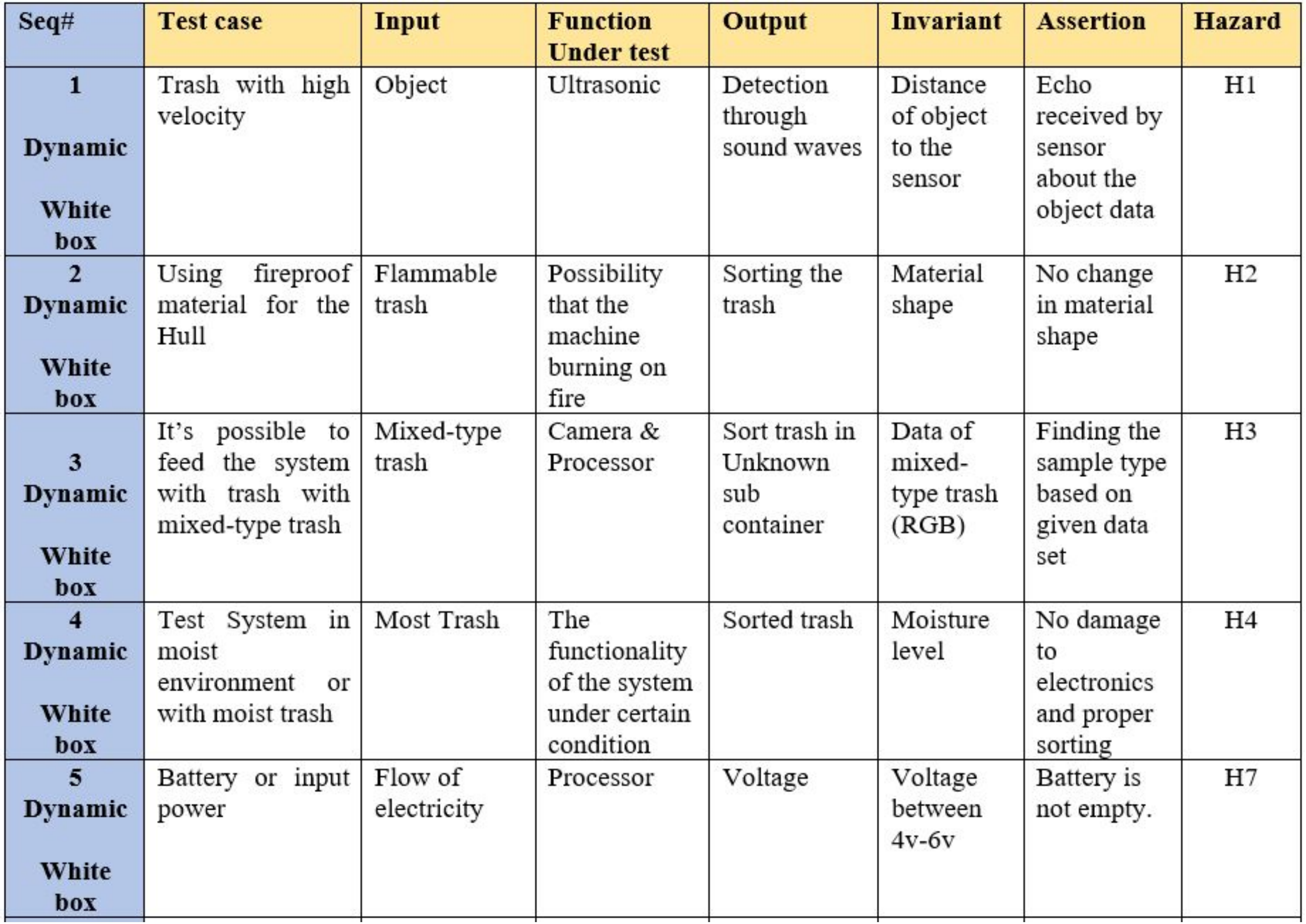


ID	Test	Verification
1	Dry run test	Check the program code manually and find possible errors
2	Inspection	Inspect the wiring and input output devices
3	Walkthrough	Check the design with datasheet of component and another expert and get feedback.

Dynamic Testing

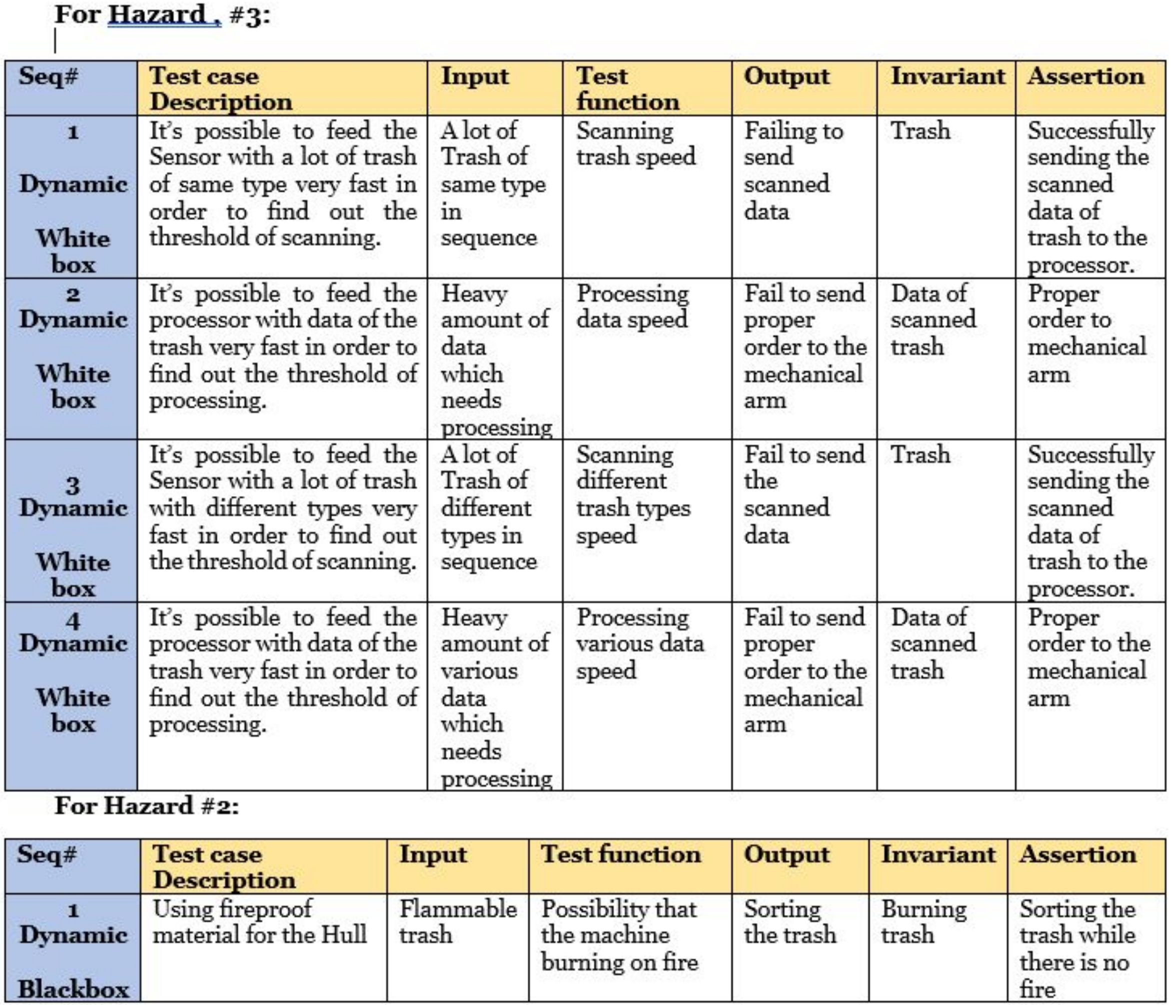
invariant, also known as the pre-condition, by which the component will accept the input,

assertion, also known as the post-condition, which allows the output to be generated by the component.



Seq#	Test case	Input	Function Under test	Output	Invariant	Assertion	Hazard
1 **Dynamic** **White box**	Trash with high velocity	Object	Ultrasonic	Detection through sound waves	Distance of object to the sensor	Echo received by sensor about the object data	H1
2 **Dynamic** **White box**	Using fireproof material for the Hull	Flammable trash	Possibility that the machine burning on fire	Sorting the trash	Material shape	No change in material shape	H2
3 **Dynamic** **White box**	It's possible to feed the system with trash with mixed-type trash	Mixed-type trash	Camera & Processor	Sort trash in Unknown sub container	Data of mixed-type trash (RGB)	Finding the sample type based on given data set	H3
4 **Dynamic** **White box**	Test System in moist environment or with moist trash	Most Trash	The functionality of the system under certain condition	Sorted trash	Moisture level	No damage to electronics and proper sorting	H4
5 **Dynamic** **White box**	Battery or input power	Flow of electricity	Processor	Voltage	Voltage between 4v-6v	Battery is not empty.	H7

Test case sequence



For Hazard , #3:

Seq#	Test case Description	Input	Test function	Output	Invariant	Assertion
1 Dynamic White box	It's possible to feed the Sensor with a lot of trash of same type very fast in order to find out the threshold of scanning.	A lot of Trash of same type in sequence	Scanning trash speed	Failing to send scanned data	Trash	Successfully sending the scanned data of trash to the processor.
2 Dynamic White box	It's possible to feed the processor with data of the trash very fast in order to find out the threshold of processing.	Heavy amount of data which needs processing	Processing data speed	Fail to send proper order to the mechanical arm	Data of scanned trash	Proper order to mechanical arm
3 Dynamic White box	It's possible to feed the Sensor with a lot of trash with different types very fast in order to find out the threshold of scanning.	A lot of Trash of different types in sequence	Scanning different trash types speed	Fail to send the scanned data	Trash	Successfully sending the scanned data of trash to the processor.
4 Dynamic White box	It's possible to feed the processor with data of the trash very fast in order to find out the threshold of processing.	Heavy amount of various data which needs processing	Processing various data speed	Fail to send proper order to the mechanical arm	Data of scanned trash	Proper order to the mechanical arm

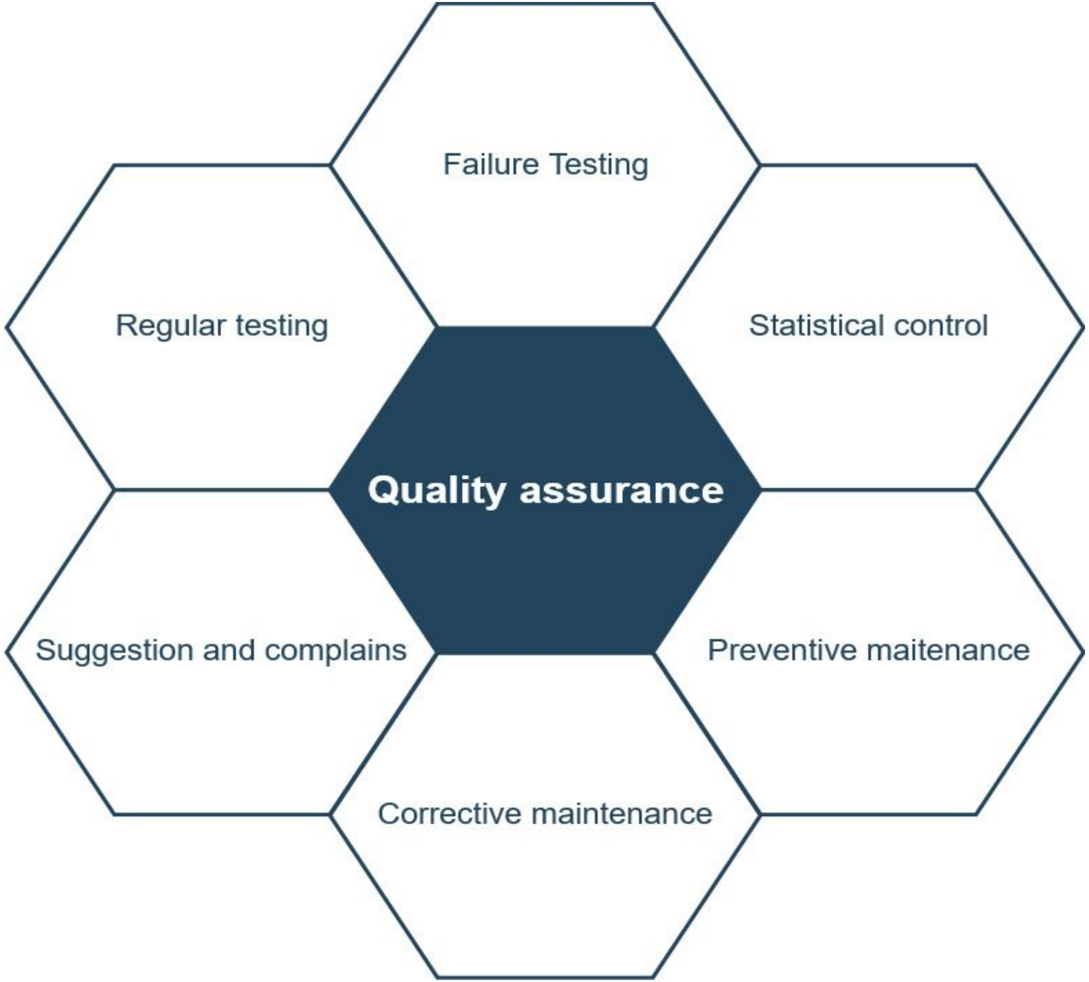
For Hazard #2:

Seq#	Test case Description	Input	Test function	Output	Invariant	Assertion
1 Dynamic Blackbox	Using fireproof material for the Hull	Flammable trash	Possibility that the machine burning on fire	Sorting the trash	Burning trash	Sorting the trash while there is no fire

Verification and Validation

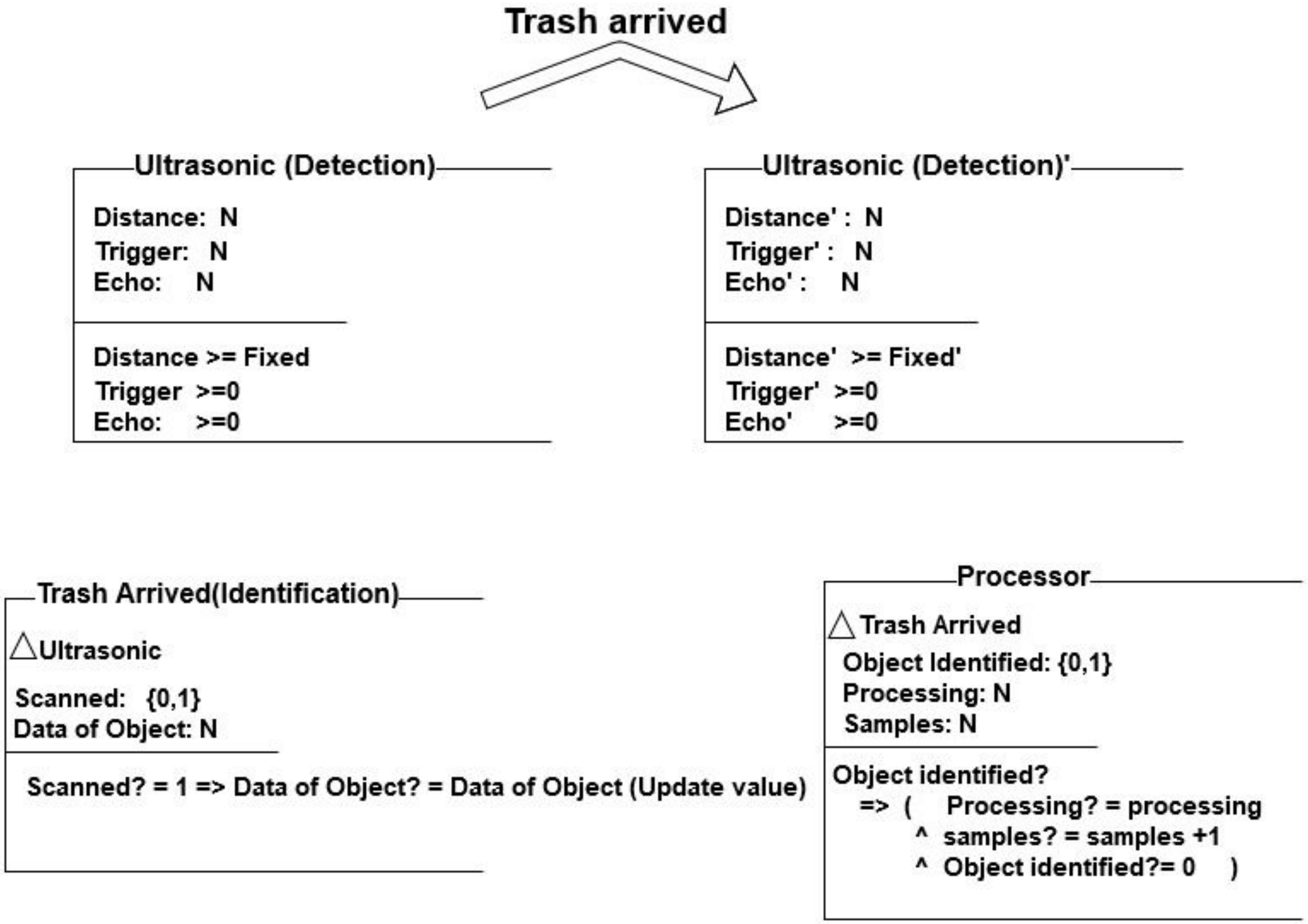
- Dragon board (JTAG)
- Embedded system workbench
- Analysis- WCET (Ultrasonic 0.5 sec)
- Inspection
- Test
- demonstration

Quality Management



Formal method

Z notation



Trash arrived

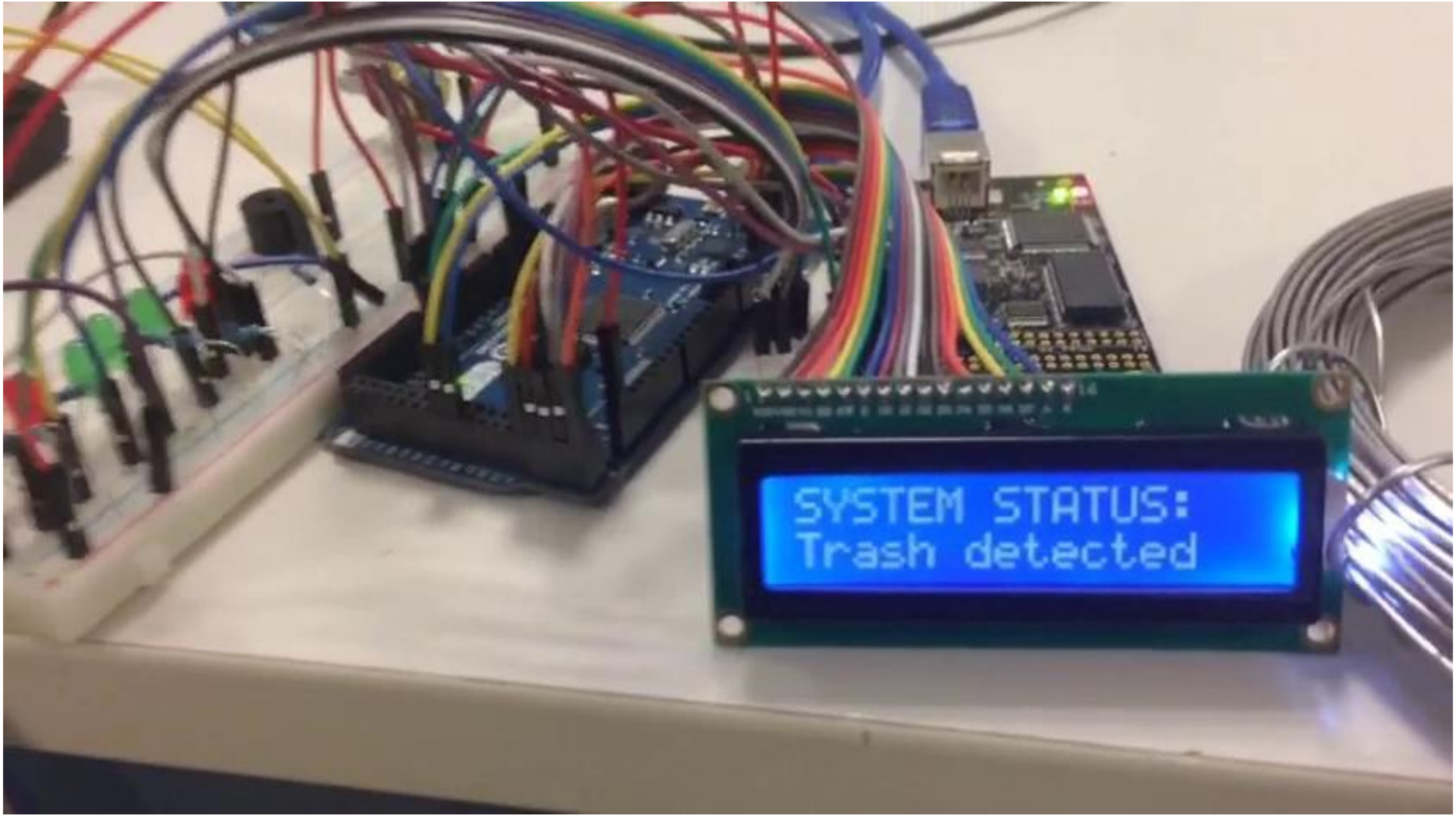
```
Ultrasonic (Detection)
Distance:  N
Trigger:   N
Echo:      N
----------------------
Distance >= Fixed
Trigger  >=0
Echo:    >=0
```

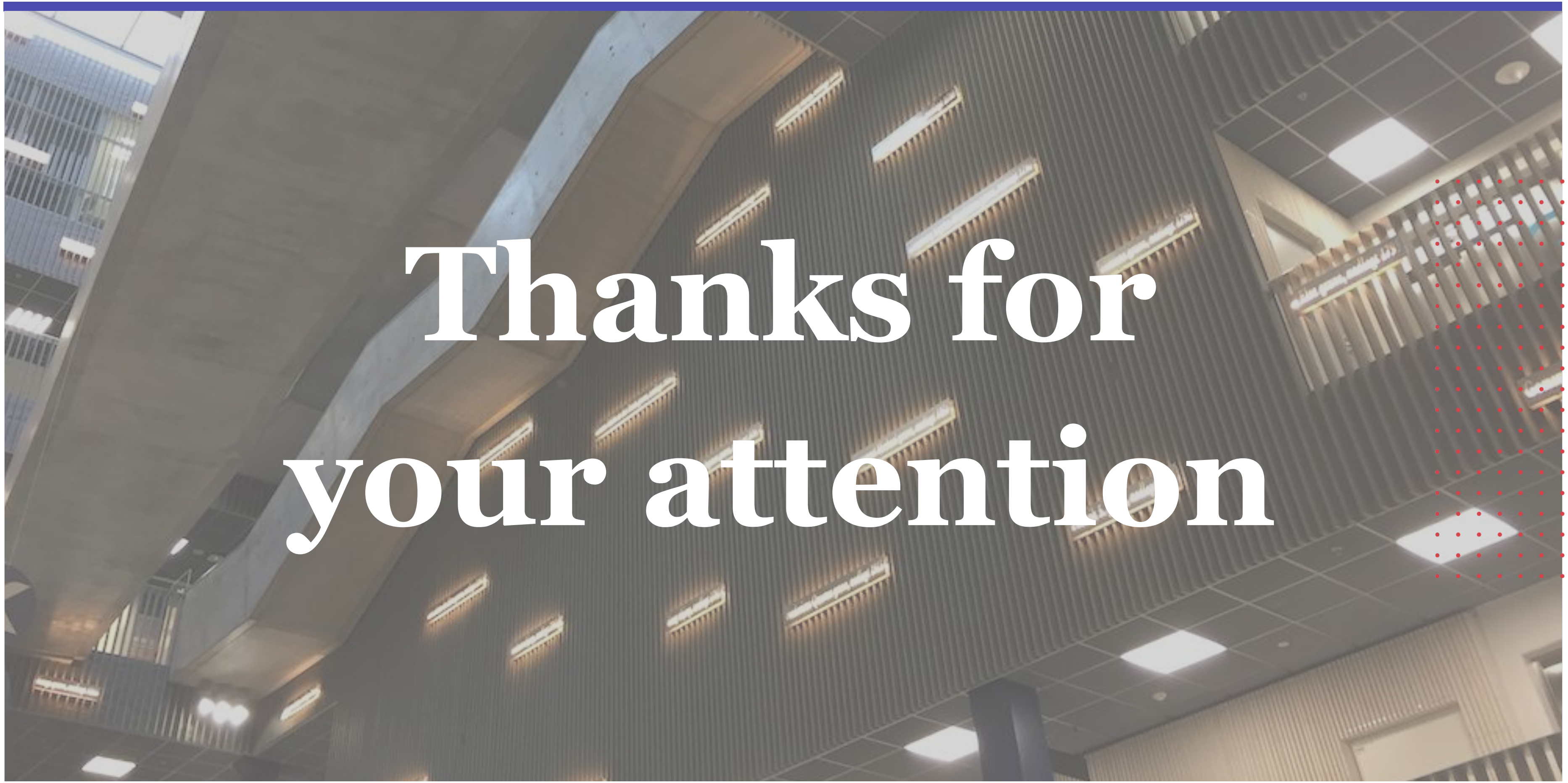
```
Ultrasonic (Detection)'
Distance' :  N
Trigger' :   N
Echo' :      N
----------------------
Distance'  >= Fixed'
Trigger'  >=0
Echo'     >=0
```

```
Trash Arrived(Identification)
△Ultrasonic
Scanned:   {0,1}
Data of Object: N
----------------------
Scanned? = 1 => Data of Object? = Data of Object (Update value)
```

```
Processor
△Trash Arrived
Object Identified: {0,1}
Processing: N
Samples: N
----------------------
Object identified?
  => (     Processing? = processing
         ^  samples? = samples +1
         ^  Object identified?= 0     )
```

Demo


SYSTEM STATUS:
Trash detected



Thanks for your attention

Universitetet i Sørøst-Norge