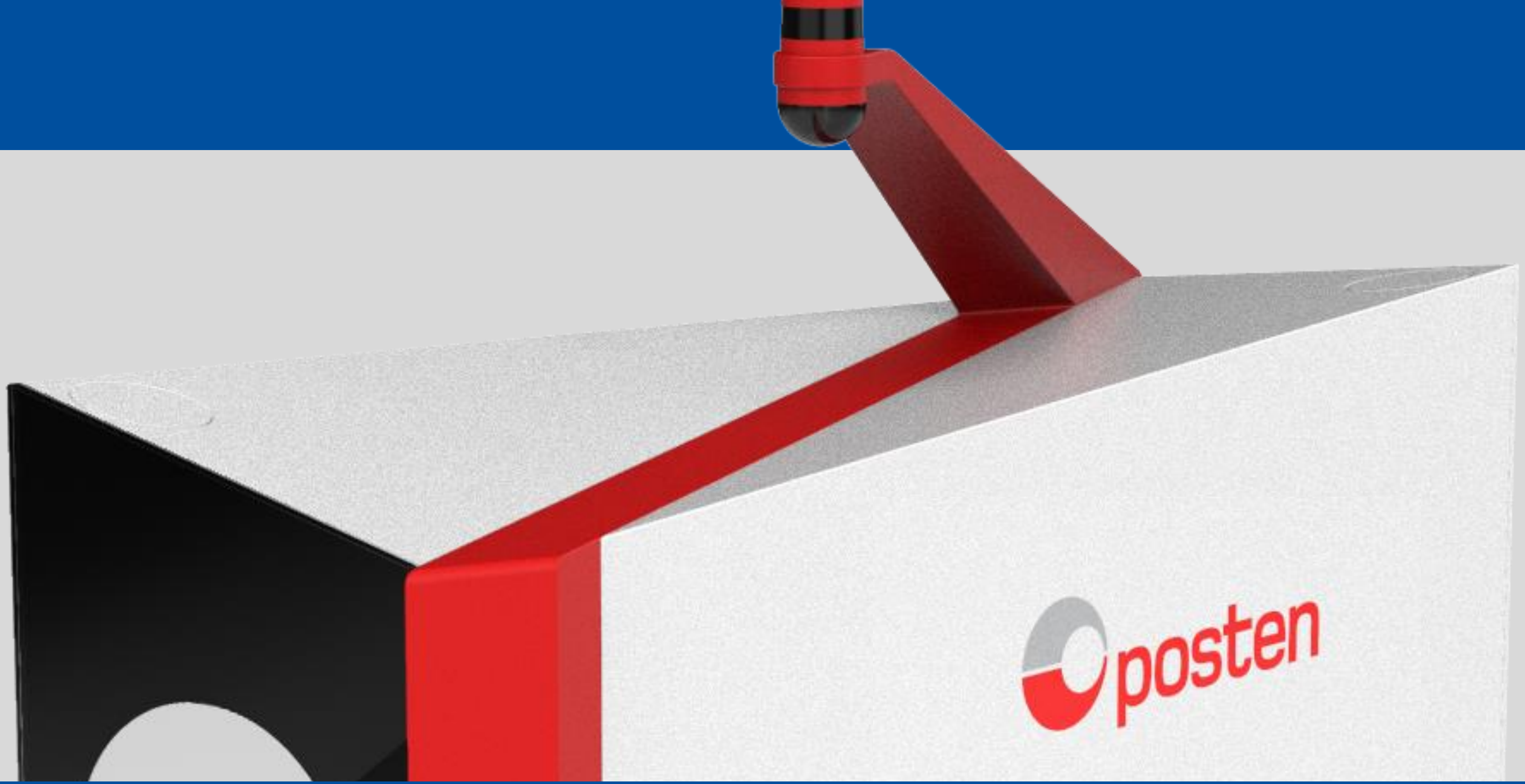


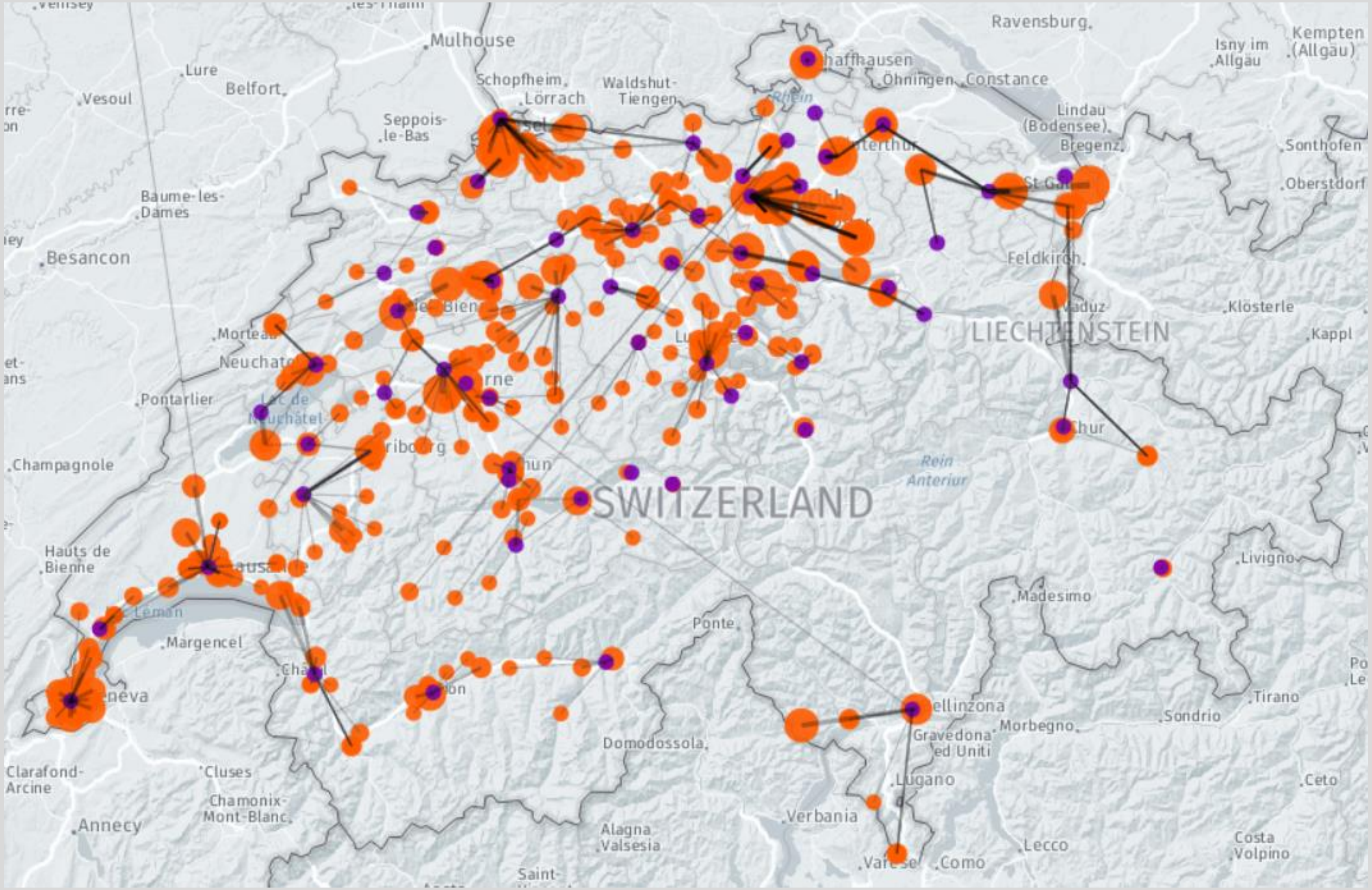
Accelerating Deployment of Autonomous Delivery Robots using Model Based Design

Dr. Erik Wilhelm

KYBURZ Switzerland

02.06.2020

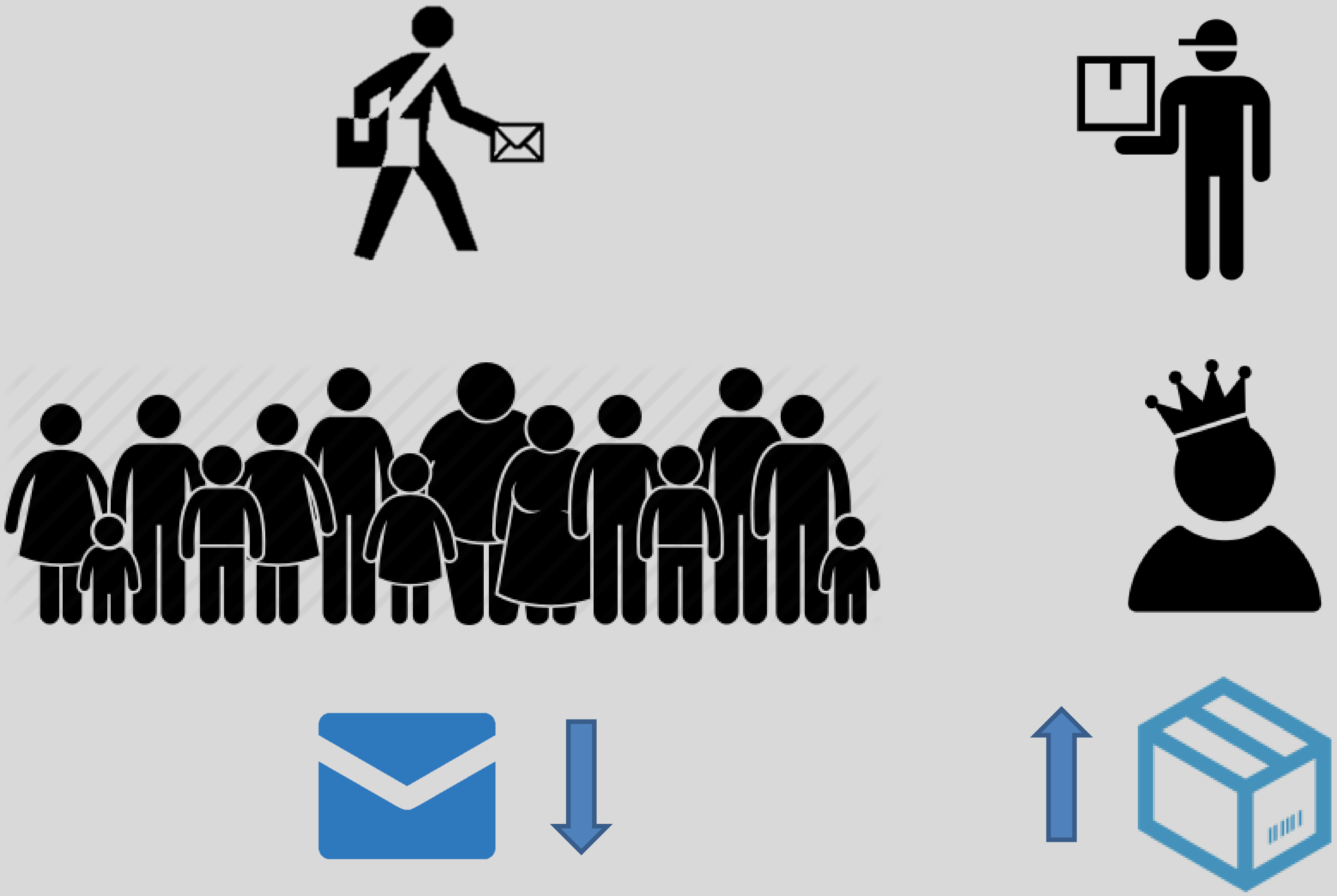
A well-established brand

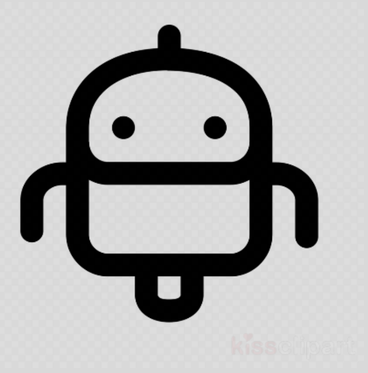


MathWorks AUTOMOTIVE CONFERENCE 2020 EUROPE

KYBURZ

Why Autonomous Delivery?





- Must be:
  - Cheaper
  - Faster
  - More reliable
  - ... More personal?

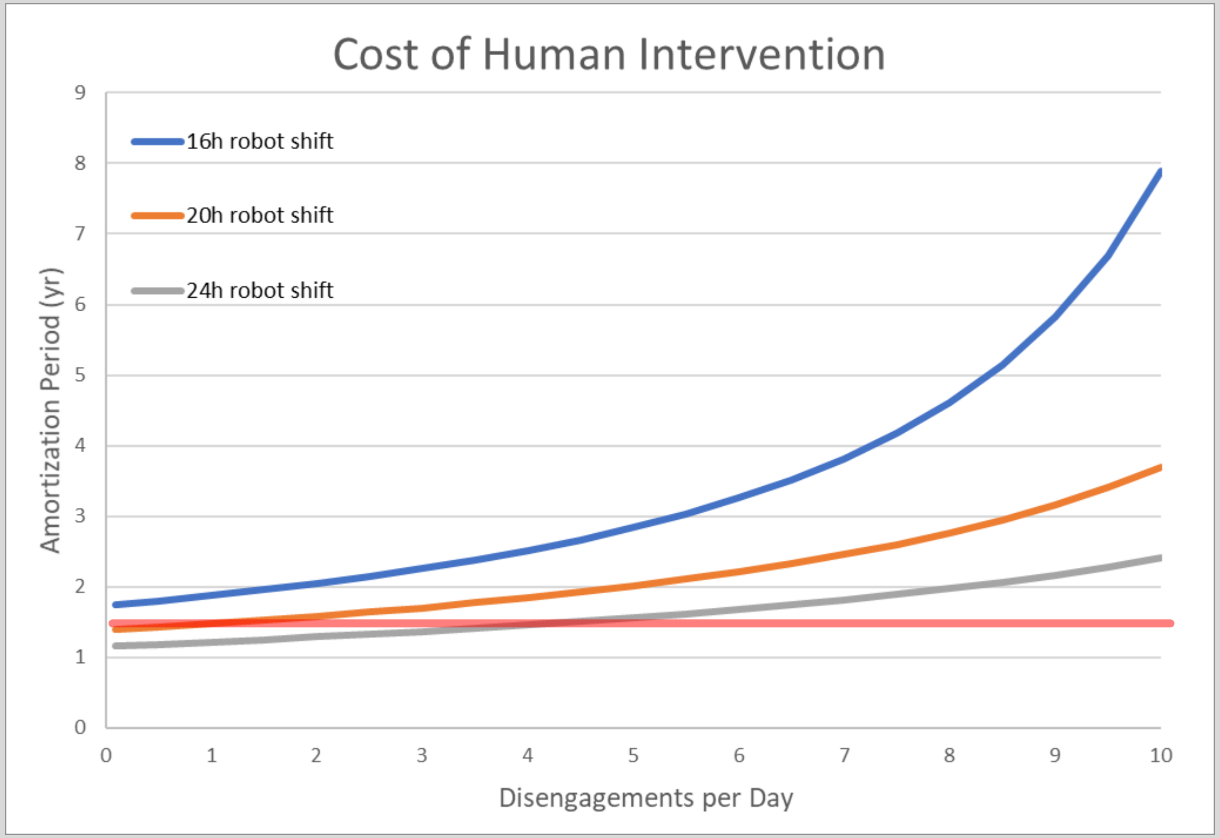
Four functional prototypes in 24 Months

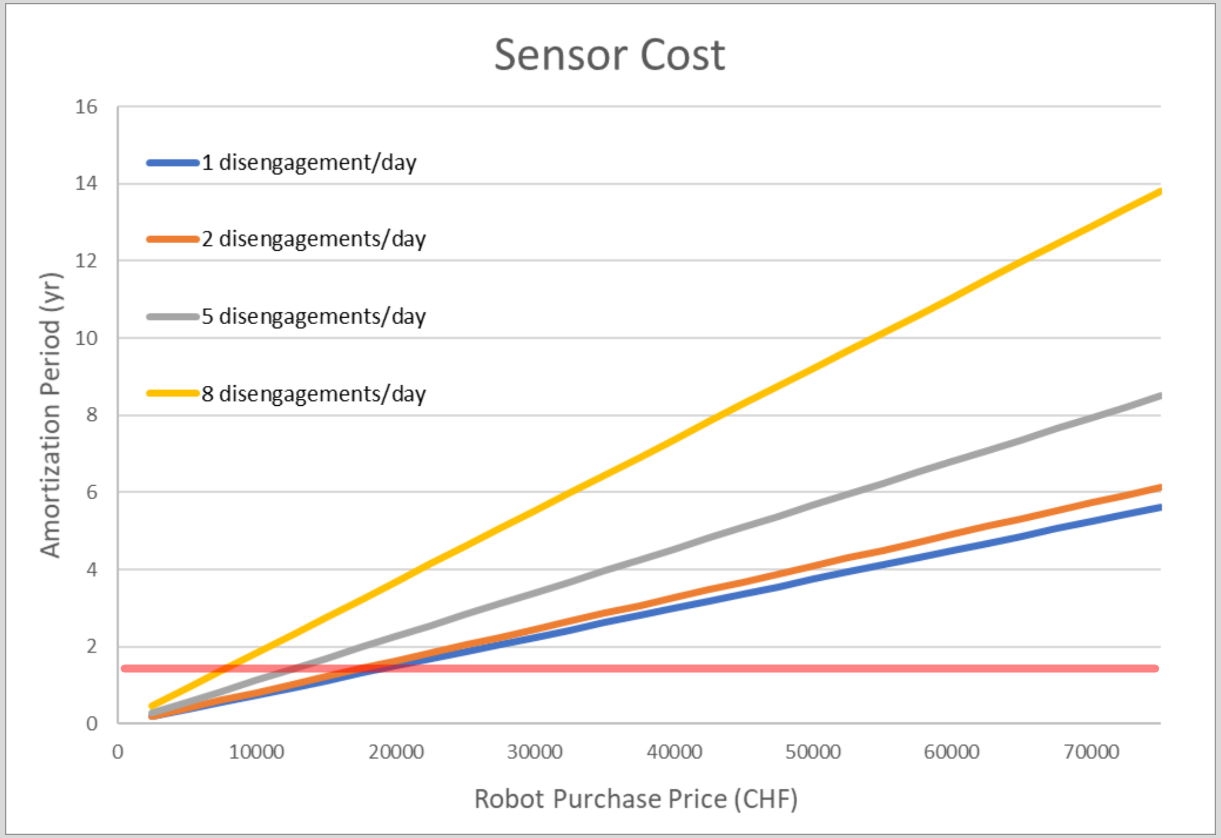
- Mobile depot box (eT1 / eT2)
- Sensors
  - 2D Lidar
  - Ultrasonic
  - 360 camera
  - GPS
  - Bump-stop

- Autonomous delivery agent (eT3)
- Sensors
  - 3D Lidar
  - Ultrasonic
  - Infraded
  - INS
  - Bump-stop

- Flexible delivery system (eT4)
- Sensors
  - 3D Lidar (2x)
  - Ultrasonic (12x)
  - Infrared (12x)
  - Radar
  - GPS (INS)
  - 360 Cameras (localization)
  - 360 Cameras (comprehension)
  - Time-of-flight camera
  - Bump-stop

Economics of Delivery Robots





- Robots should be operated for long shifts without disengagement with cheap sensors

eT4: Autonomous delivery platform

Autonomous System Design Challenges

High availability

Image: ABC news

Approved safety

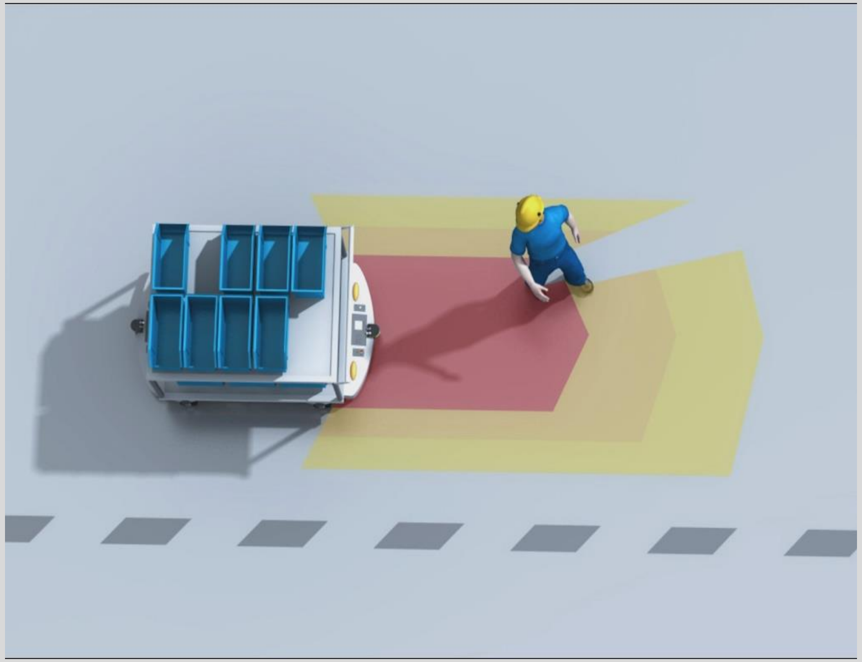


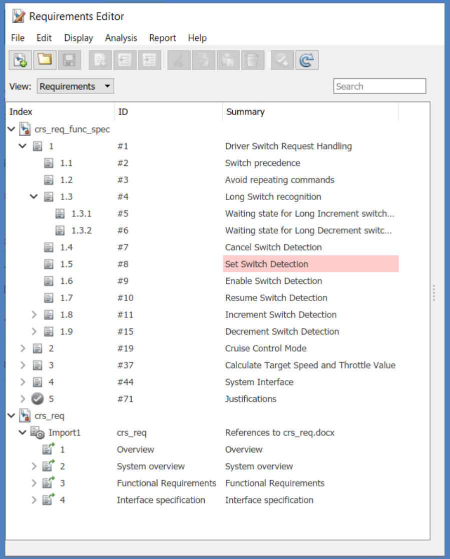
Image: sick.com

Test coverage

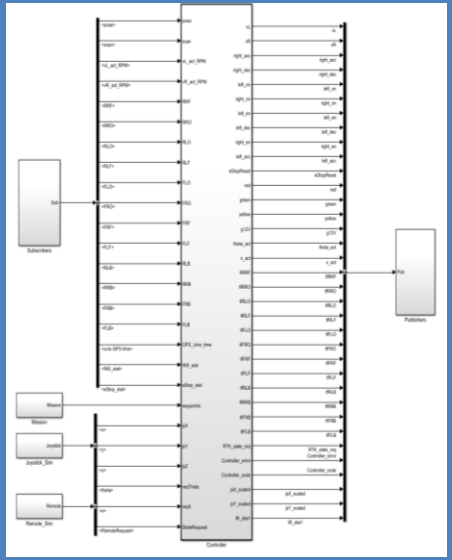
Image: youtube.com

Safety-centered workflow

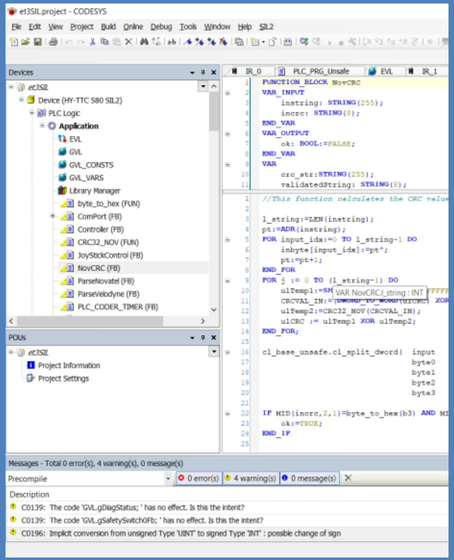
Specifications



Model Based Design



Code Generation

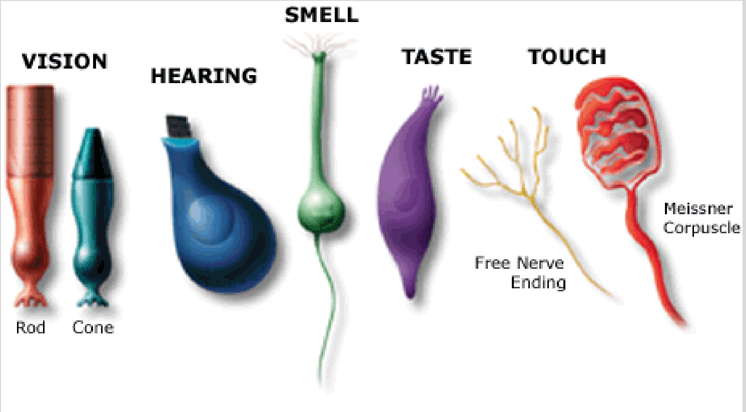


Compilation

- This workflow allows SIL2 certifiable code to be generated using model-based design
- Review and testing occurs within each phase and before each release

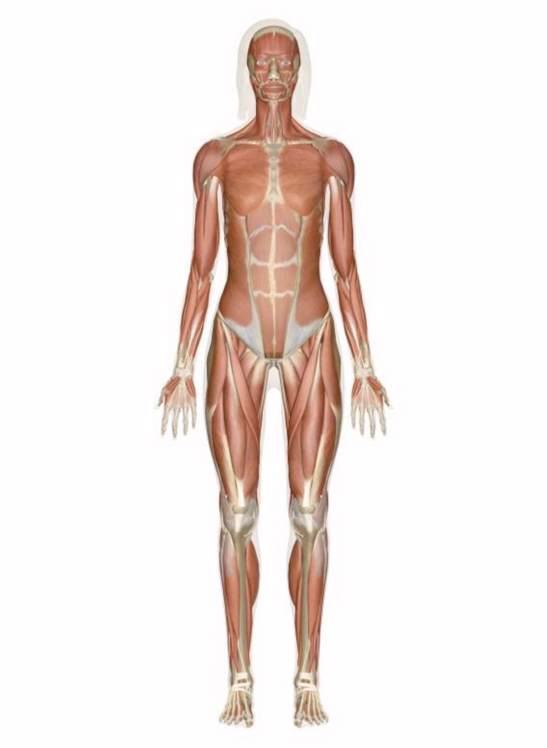
Incumbent

Sense



Infer

Act



100 – 200 ms

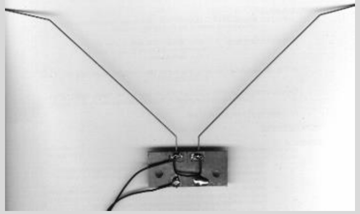
Challenger

Sense

40 ms

20 ms

300 ms



50 - 600 ms

20 ms

Infer

1 ms

300 ms

Act

20– 40 ms

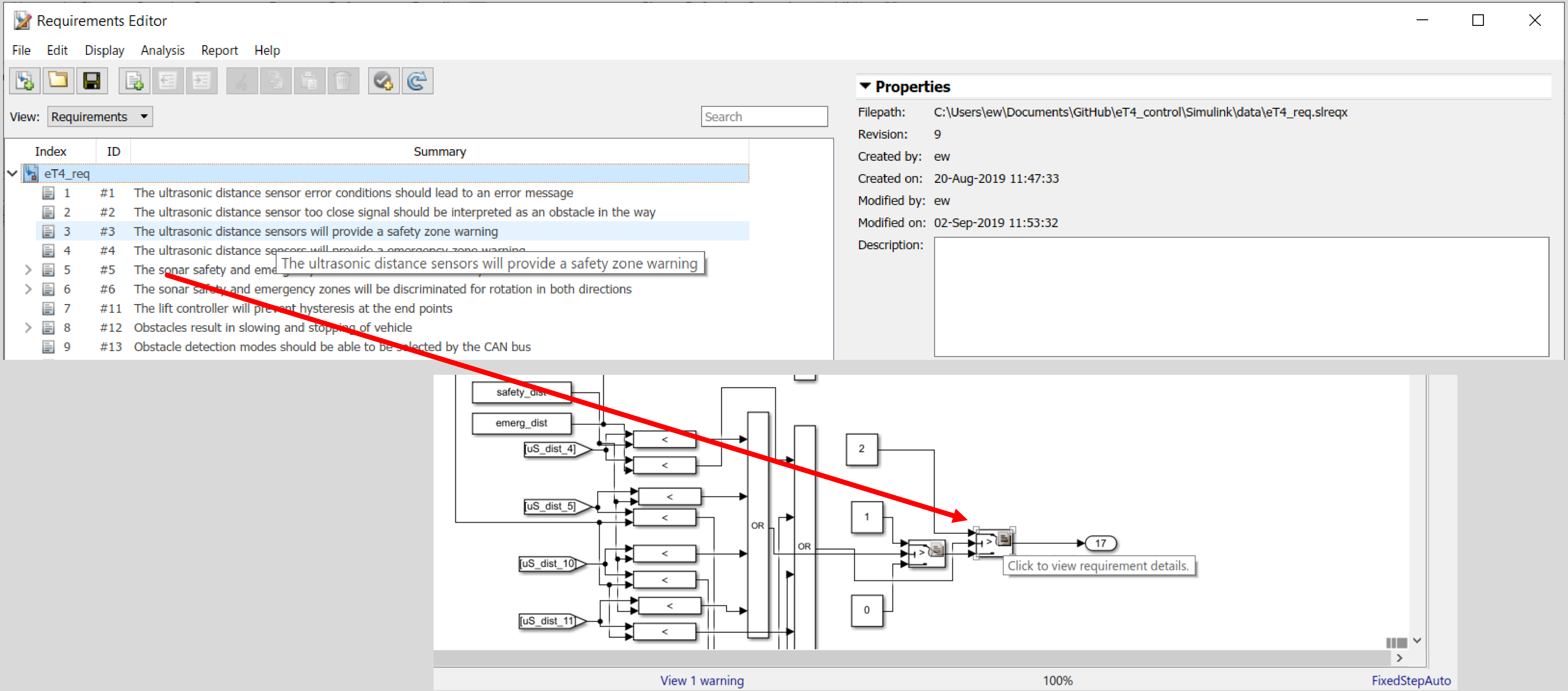
650 – 820 ms

Does it have to be head to head?

Redundancy for sensor systems

Localization	Day	Night	Precipitation	Fog	Tall structures	Tranparent obstacles	Diffuse obstacles
INS (GPS)	✓	✓	✓	✓	!		
Optical	✓	✗	✗	!	✓		
Pointcloud	✓	✓	!	✗	✓	-	-
Obstacle Avoidance							
LiDAR	✓	✓	!	✗	-	✗	!
Optical	✓	✗	✗	!	-	✓	✓
Radar	✓	✓	!	✓	-	✓	✓
Ultrasonic	✓	✓	✓	✓	-	✓	!
Time-of-Flight	!	✓	!	✗	-	!	✗
Infrared	✗	✓	!	✗	-	✗	✗
Bump Stop	✓	✓	✓	✓	-	✓	✓

Integrated code-level functional specification



Corner Cases

ROSAS Center Fribourg	Document N°:	R18_025_025_072_88043
	Page:	12 of 21

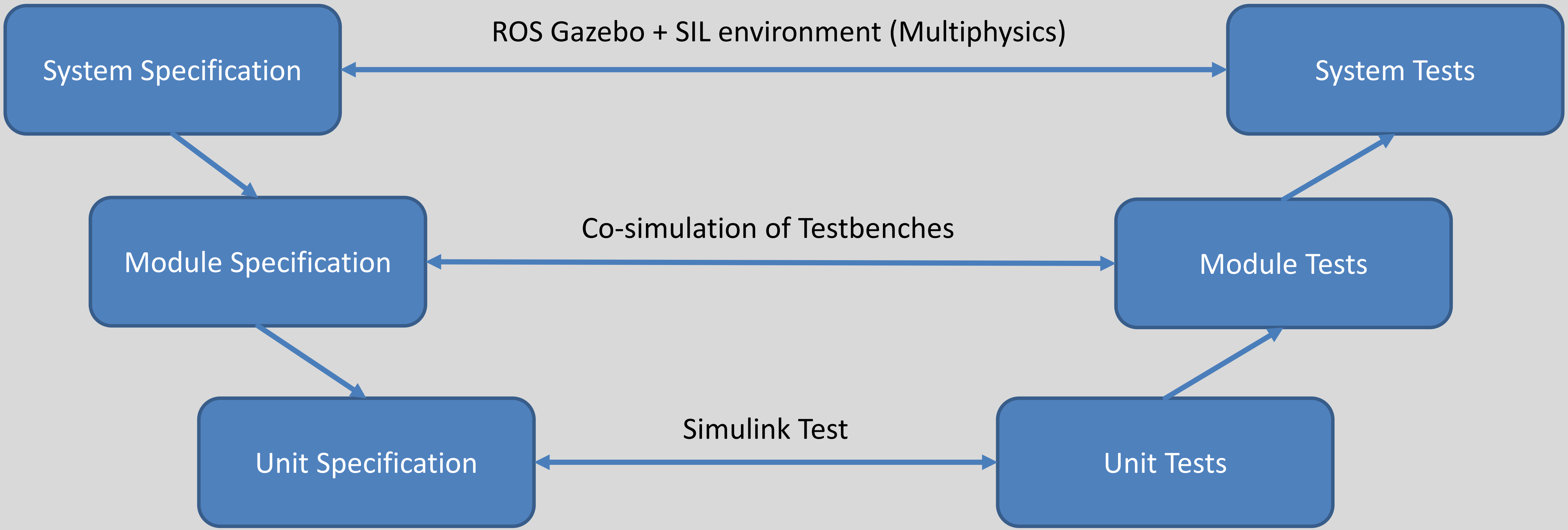
Field of Study: Hazard and Risk Analysis eT4

Item Defintion - Functional Description			Hazard and Risk Analysis			ASIL Determination							Safety Goal			Allocation		
Operating Mode	ID	Function	Malfunction	Situation	Hazard	Severity	S-Comment	Exposure	E-comment	Controlability	C-Comment	ASIL	Safety Goal		Safe State	ID	Requirement	Elem[illegible]
Driving Mode	F.01	Moving forward	Unintended moving forward	Downhill slope / Curvy Road	Crushing, impact with humans/kids	S3	Life-threatening injuries (survival uncertain),fatal injuries	E4	High probability	C3	Difficult to control or uncontrollable	D	SG.01	Unintended moving shall be prevented	Stopped	FSR.01	Motion command shall be provided correctly	VCU
																FSR.02	Freewheeling motor shall be prevented	Motor controller Motor
																FSR.03	Emergency stop signal shall be transmitted correctly	PDU
																FSR.04	Motion command shall be properly interpreted	Motor controller Motor
			Not moving forward	Train crossing / Crossover	Impact with others rolling vehicles, part ejected	S3	Life-threatening injuries (survival uncertain),fatal injuries	E2	High probability	C2	Difficult to control or uncontrollable	A	SG.02	Unintended stop shall be prevented	Safe movement operation	FSR.01	Motion command shall be provided correctly	VCU
				High-speed Road	Impact with others rolling vehicles, part ejected	S3	Life-threatening injuries (survival uncertain),fatal injuries	E4	High probability	C1	Simply controllable	B				FSR.03	Emergency stop signal shall be transmitted correctly	PDU
																FSR.05	Power [illegible] shall be normally available in driving mode	PDU [illegible] System (Power provider)
																FSR.06	Traction shall be available in driving mode	Motor controller Motor
			Incorrect moving	Falling down the stairs / Pedestrian area	Crushing, impact with humans/kids	S3	Life-threatening injuries (survival uncertain),fatal injuries	E3	Medium probability	C3	Difficult to control or uncontrollable	C	SG.03	Incorrect movement shall be prevented	Stopped	FSR.01	Motion command shall be provided correctly	VCU

Image: drivingtests.co.nz

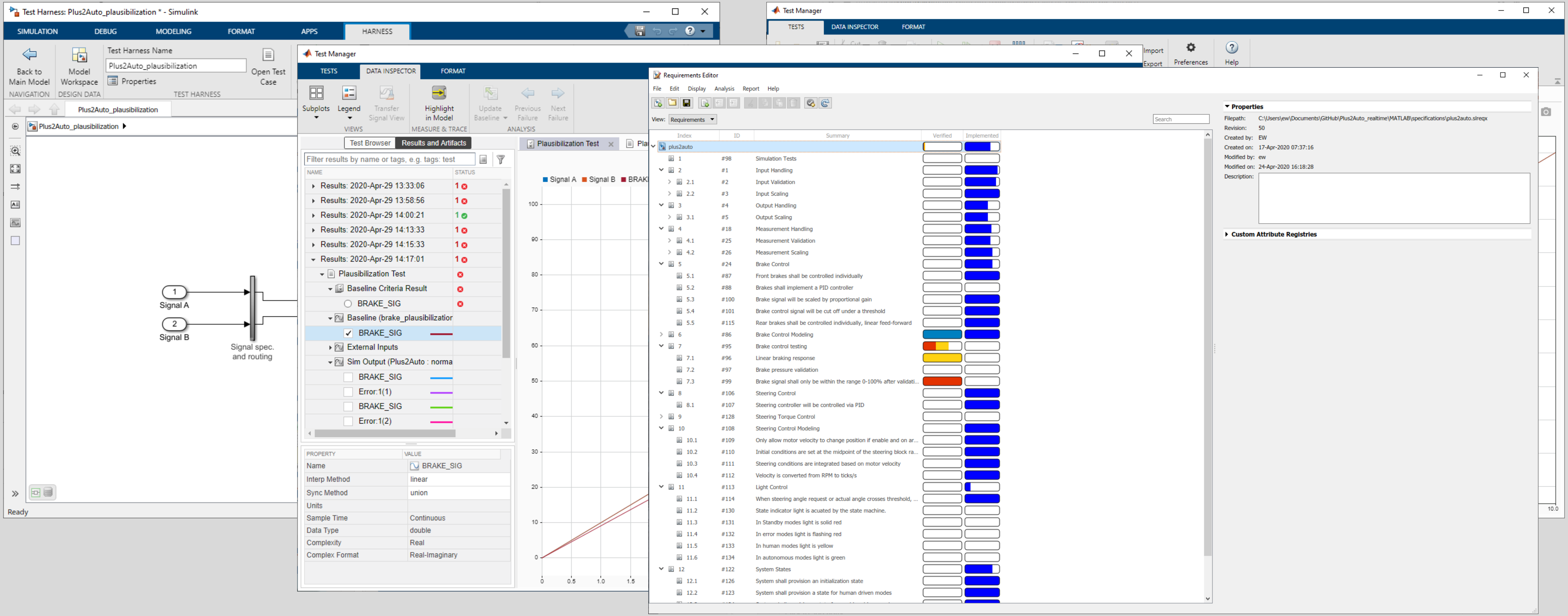
Image: arstechnica.com

Safety Solution



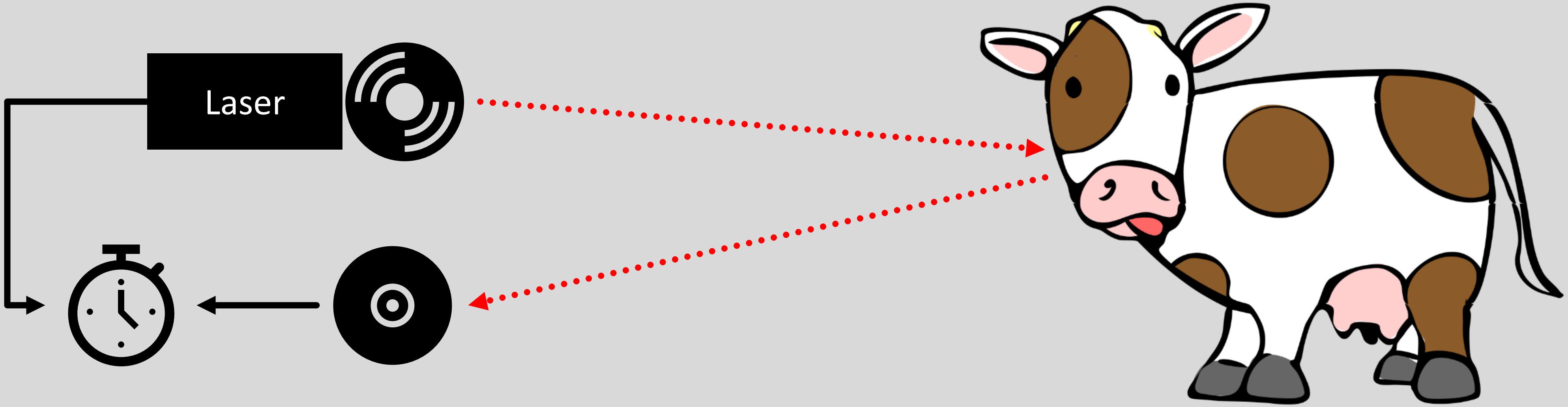
- Kyburz toolchain uses layered verification techniques and model-based design
- All requirements are easily documented for traceability

Unit Testing

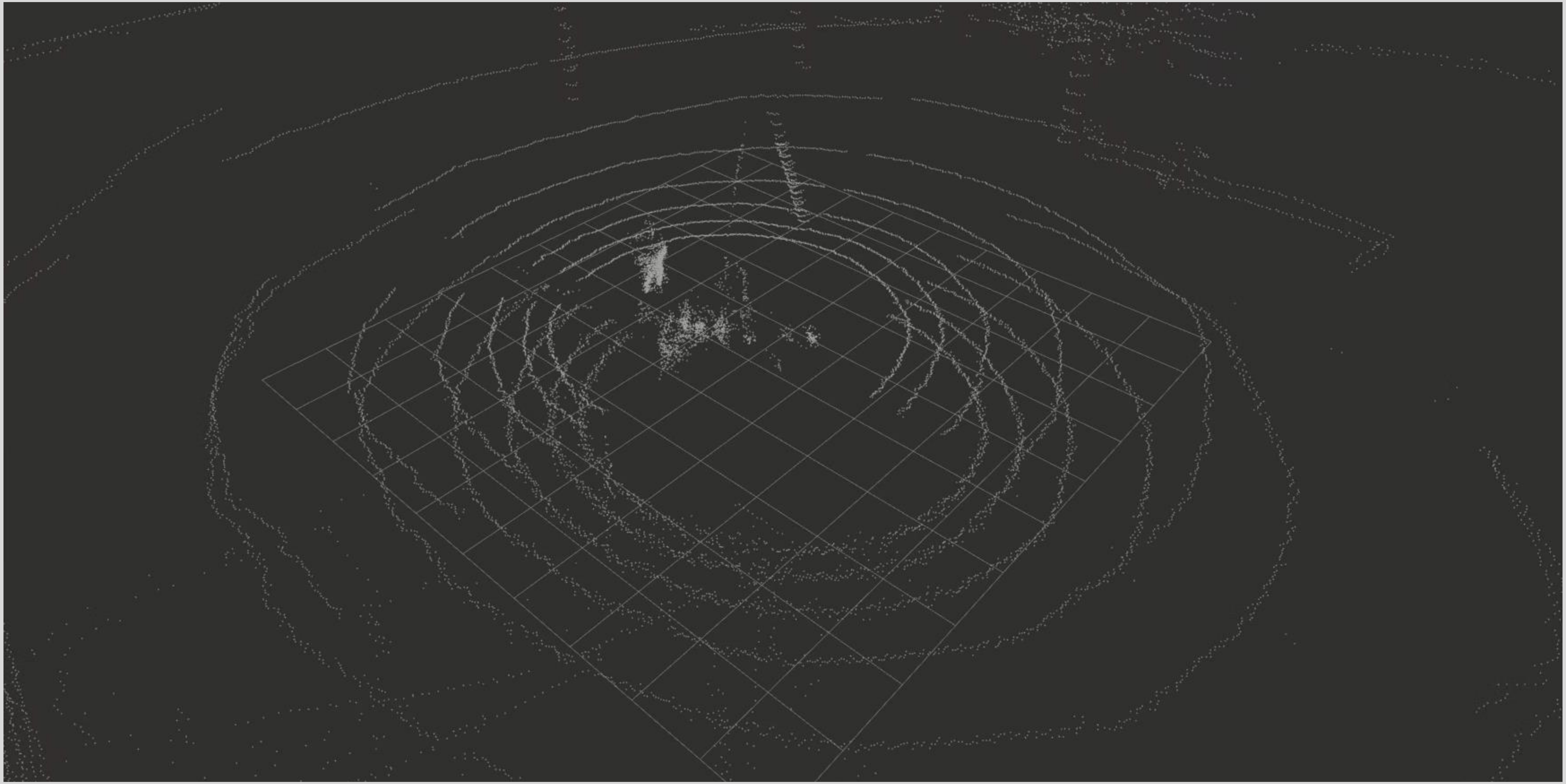


- Unit testing linked with requirements closes the V

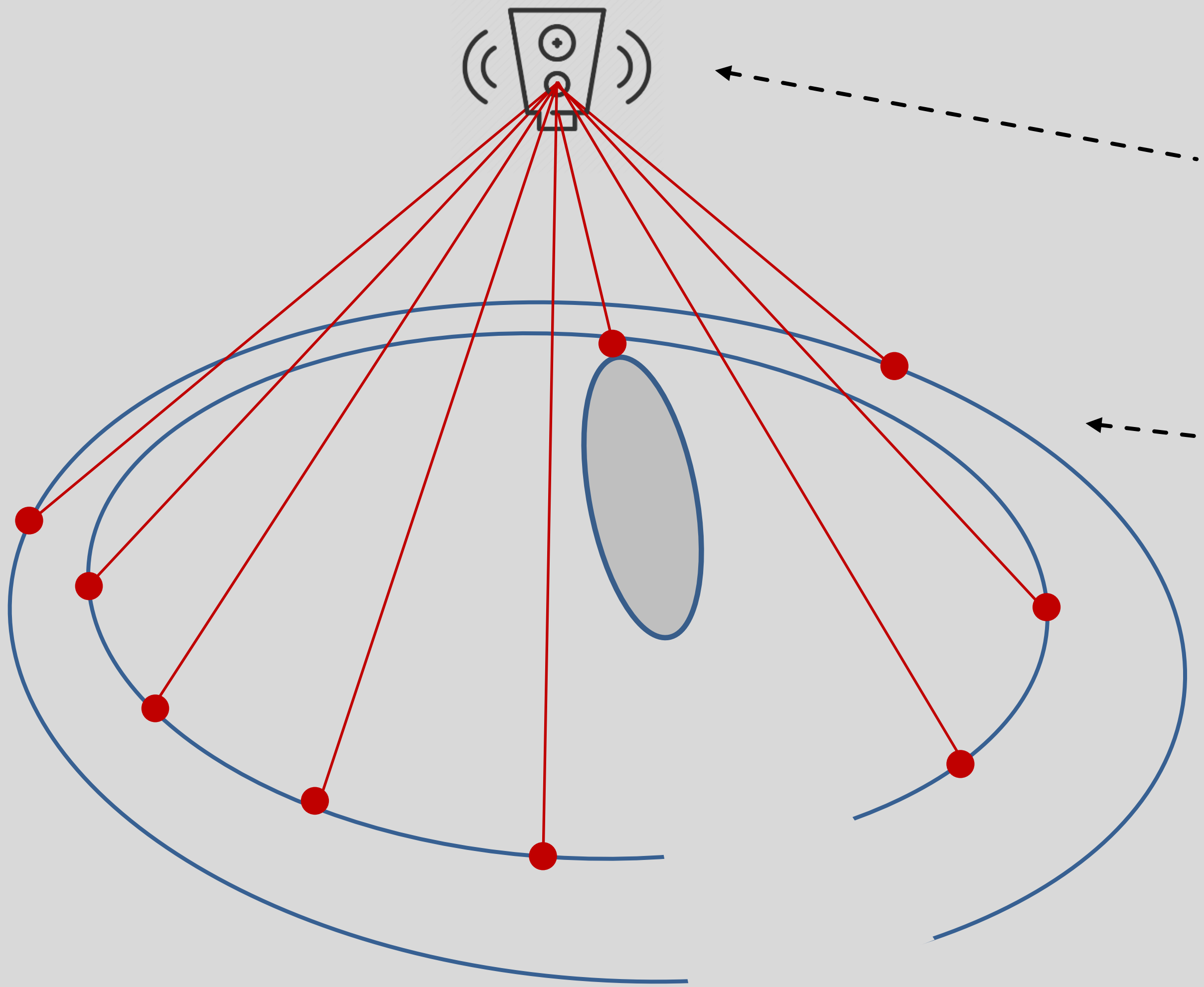
Safety Example: LiDAR (Light Detection and Ranging)



Complexity Management



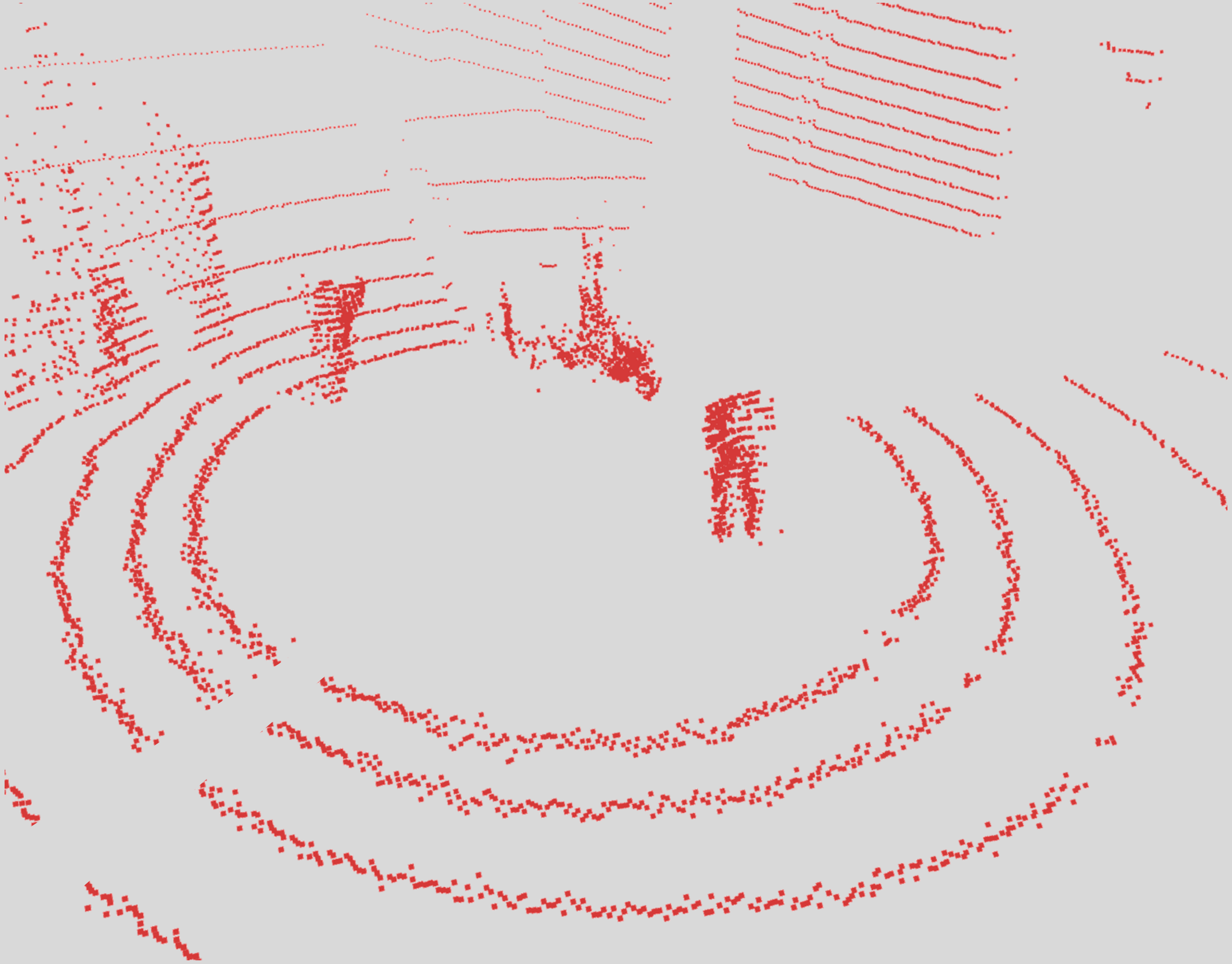
Internal laser reflections



Solution:

1. On even ground predictable rings are formed
2. Detectable obstacles modulate the ring form
3. Undetectable close objects create gaps in the rings

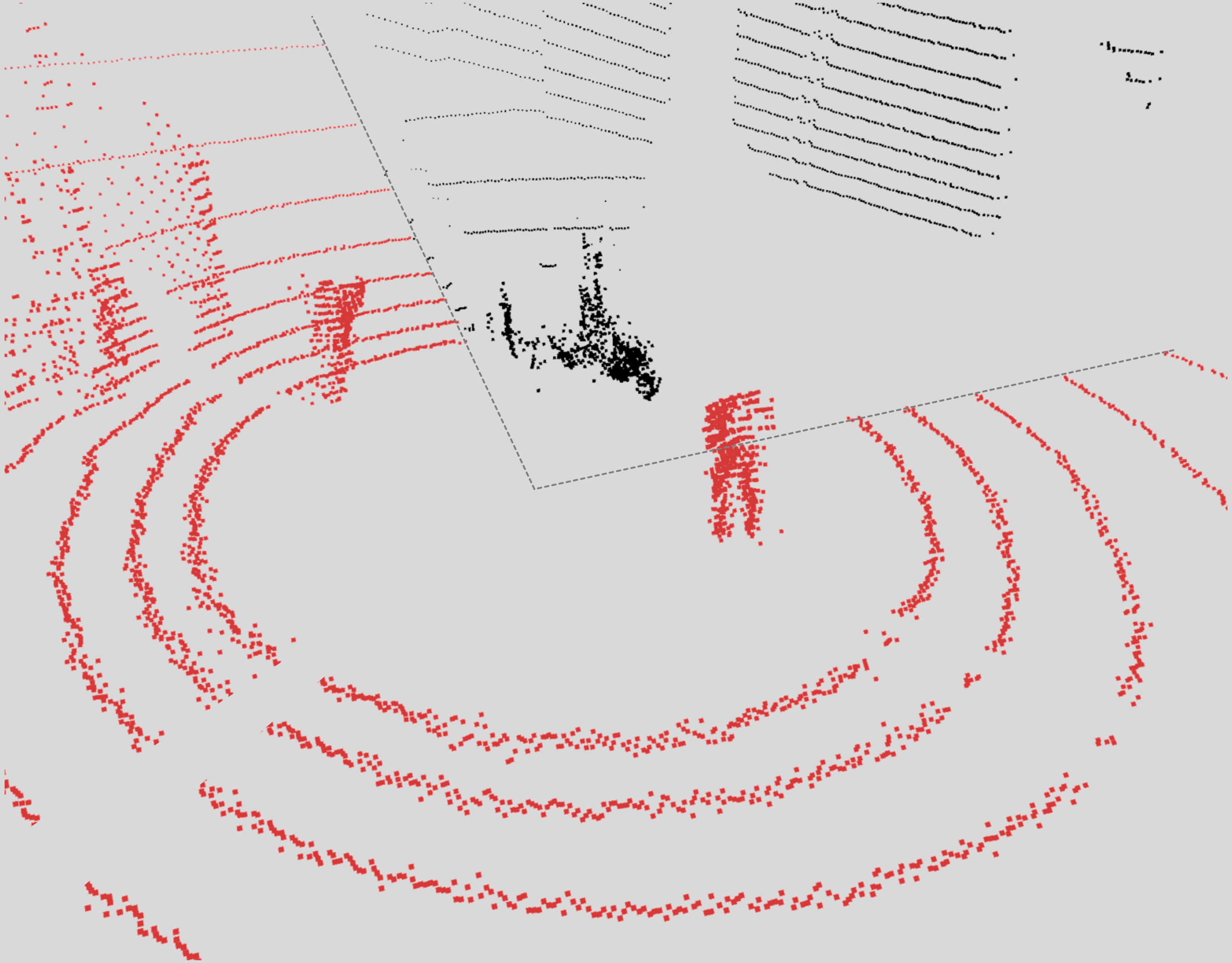
Near-field LiDAR object detection



Algorithm:

1. We receive a 16x1024 point cloud in 3 dimensions

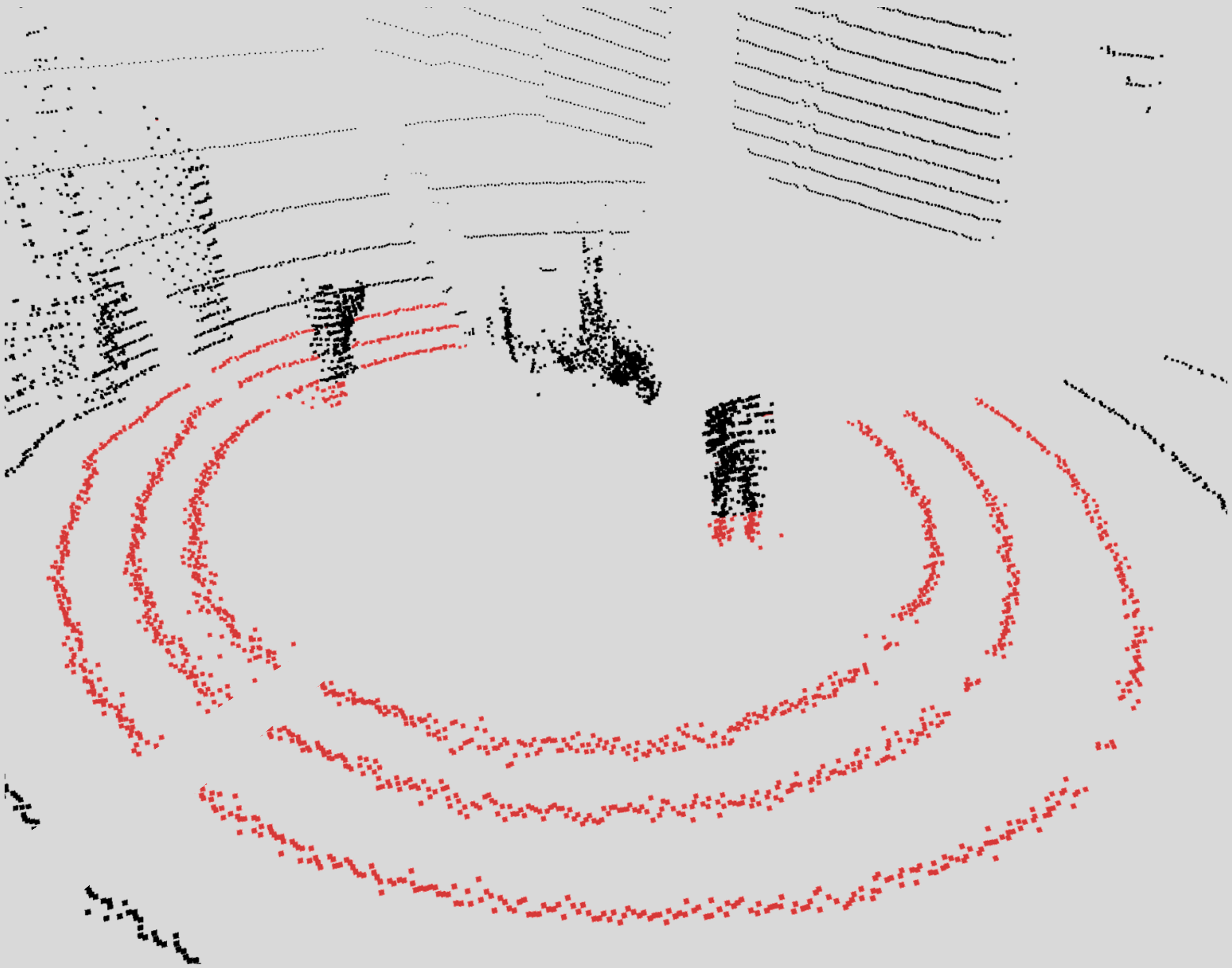
Objekterkennung mit LIDAR



Algorithm:

1. We receive a 16x1024 point cloud in 3 dimensions
2. We remove points which are echoed by the robot itself

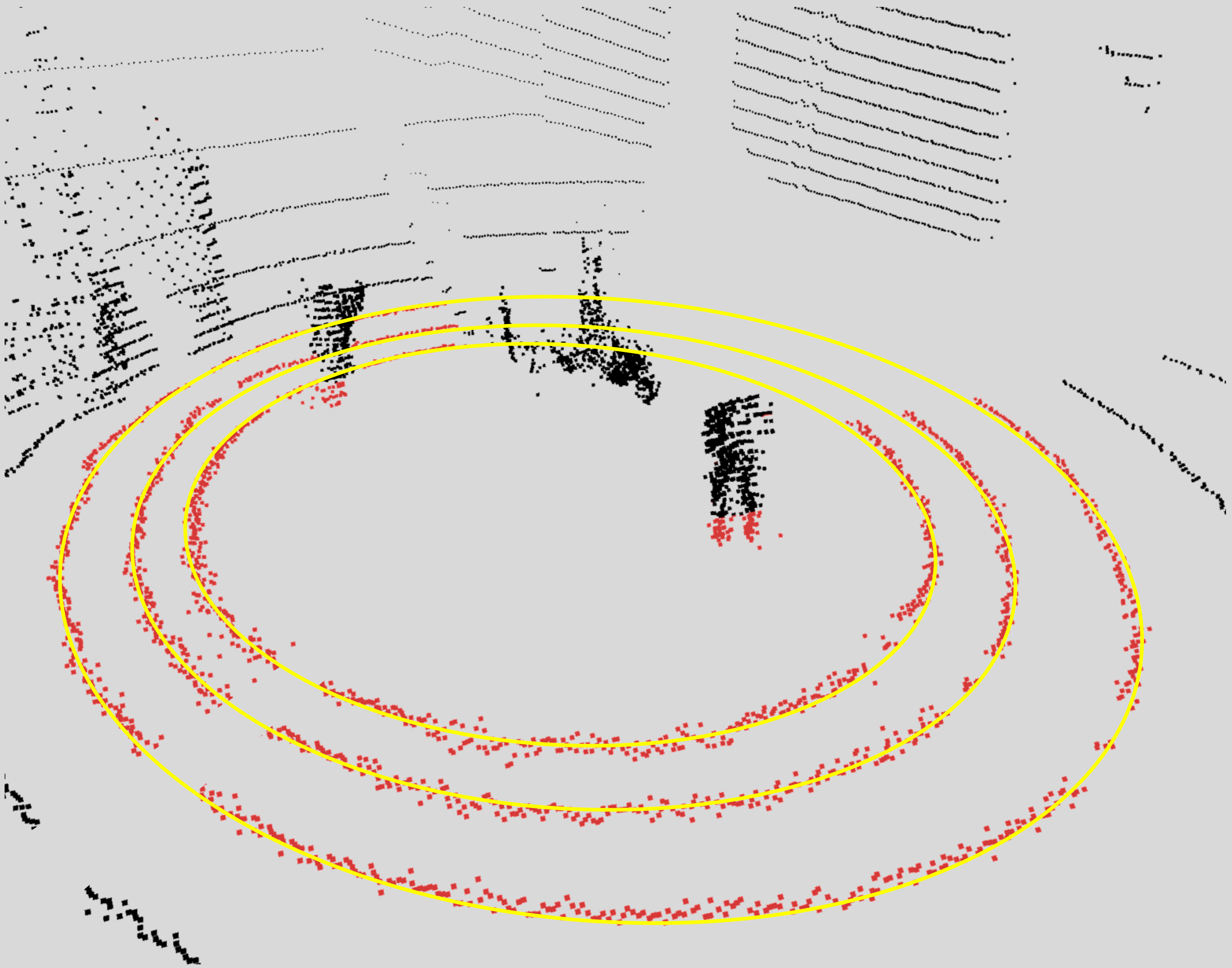
Objekterkennung mit LIDAR



Algorithm:

1. We receive a 16x1024 point cloud in 3 dimensions
2. We remove points which are echoed by the robot itself
3. We extract the lowest three rings

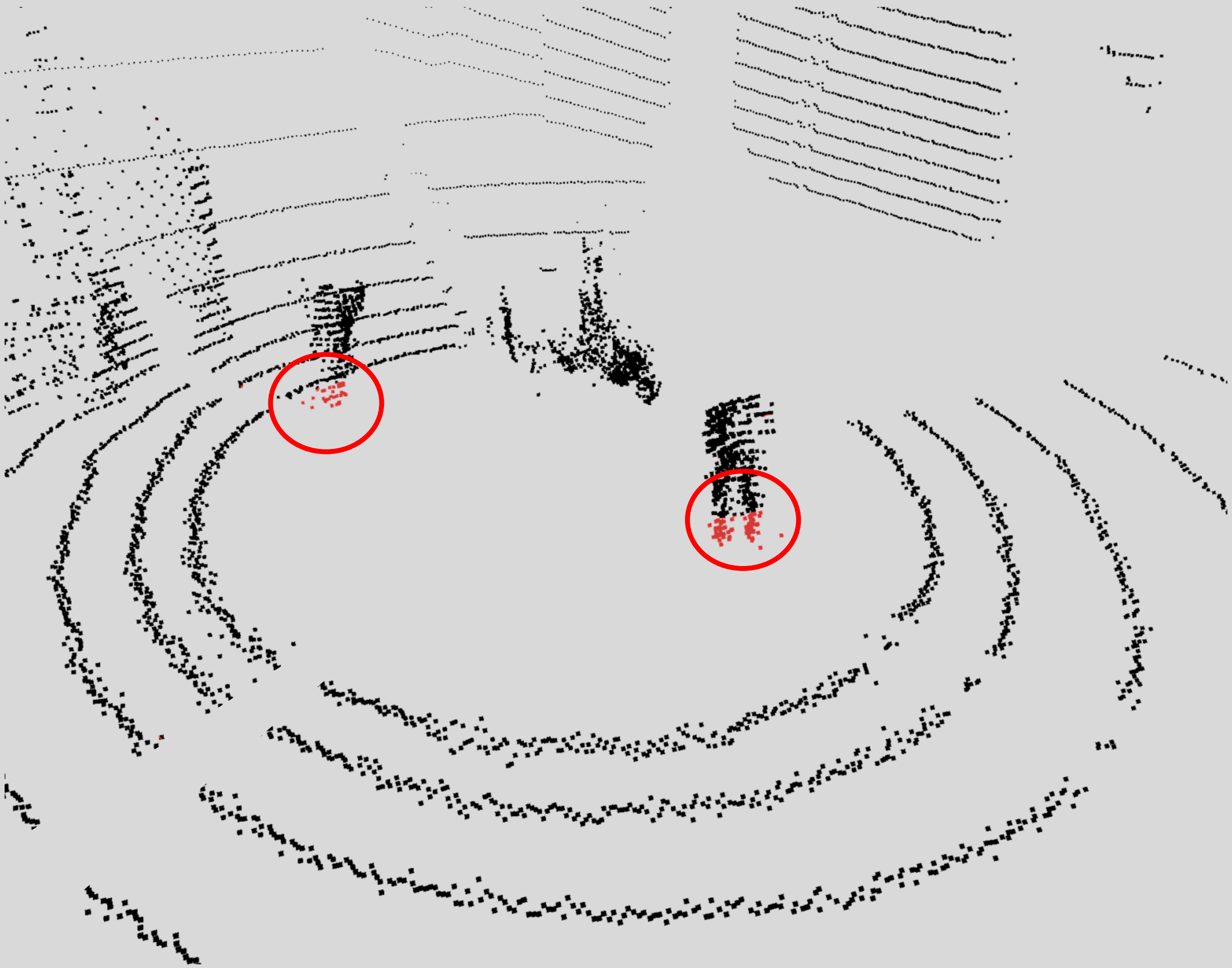
Objekterkennung mit LIDAR



Algorithm:

1. We receive a 16x1024 point cloud in 3 dimensions
2. We remove points which are echoed by the robot itself
3. We extract the lowest three rings
4. And search for ring shapes

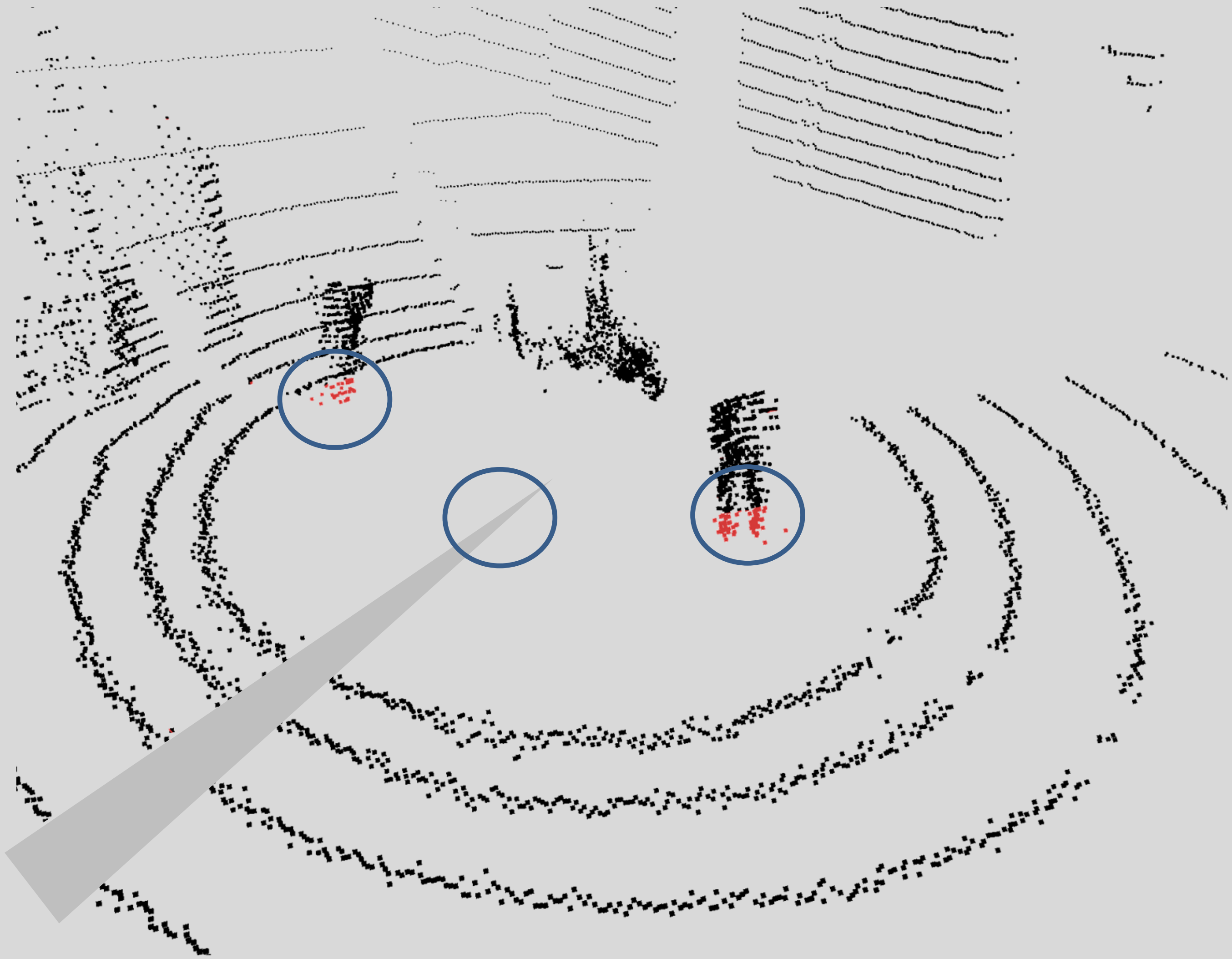
Objekterkennung mit LIDAR



Algorithm:

1. We receive a 16x1024 point cloud in 3 dimensions
2. We remove points which are echoed by the robot itself
3. We extract the lowest three rings
4. And search for ring shapes
5. Everything which is not part of a ring is classified as an obstacle

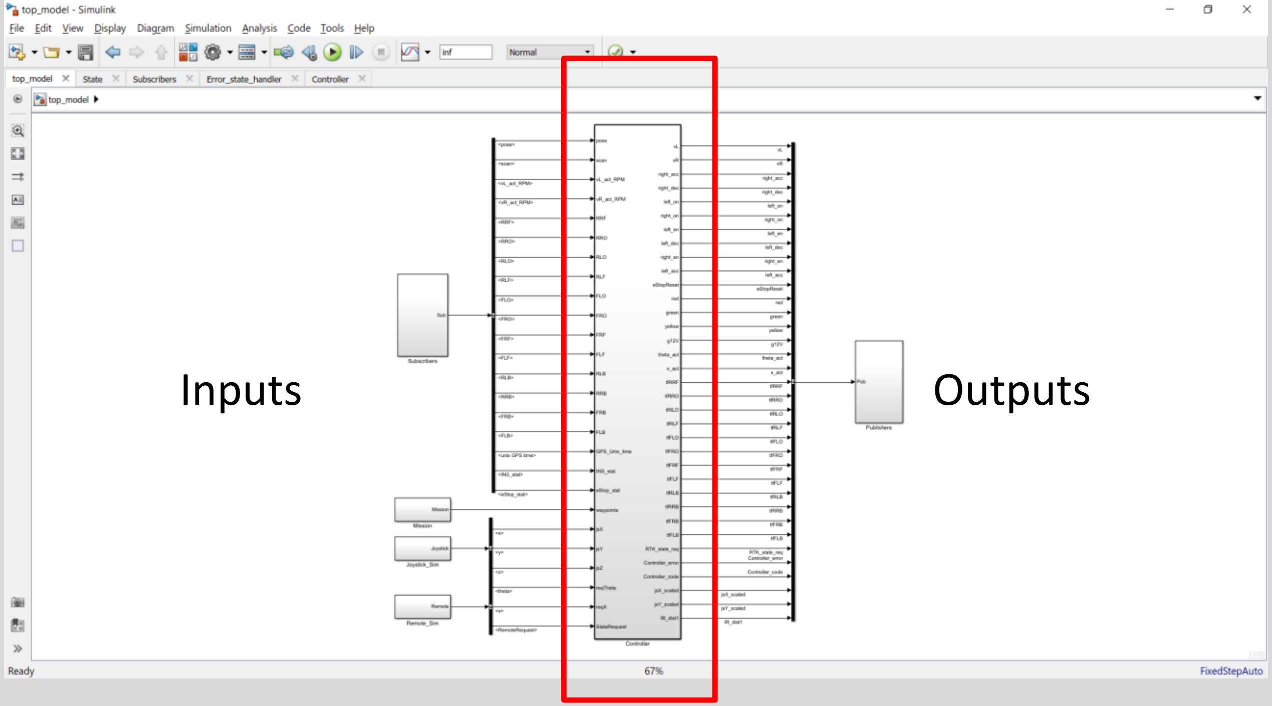
Objekterkennung mit LIDAR



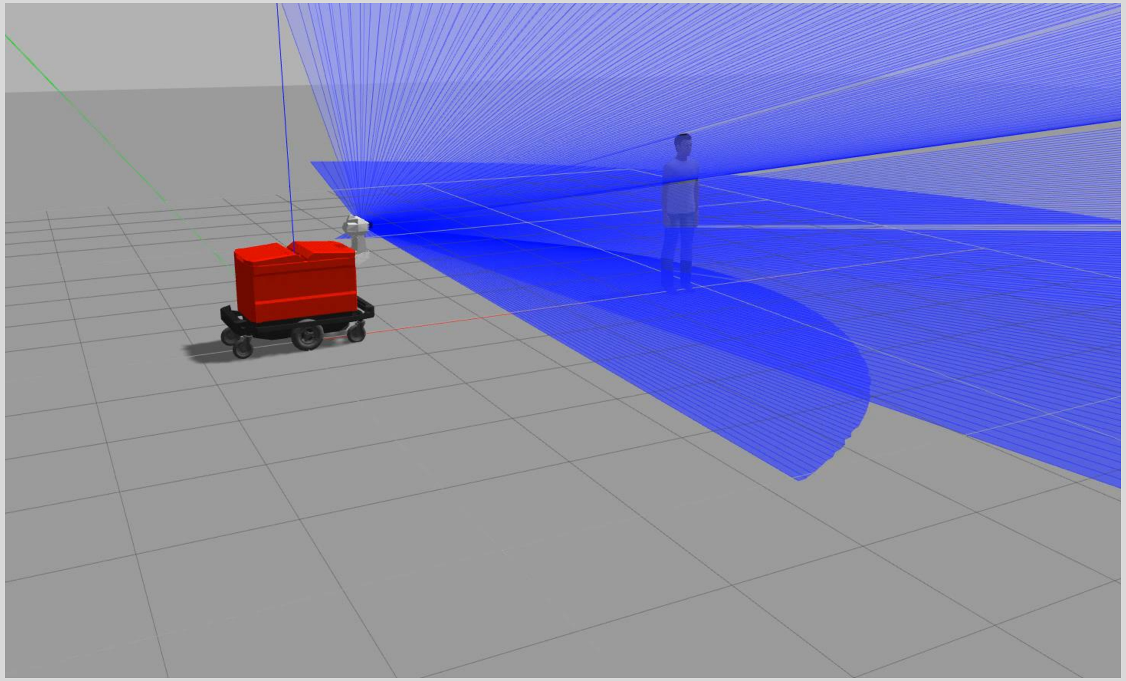
Algorithm:

1. We receive a 16x1024 point cloud in 3 dimensions
2. We remove points which are echoed by the robot itself
3. We extract the lowest three rings
4. And search for ring shapes
5. Everything which is not part of a ring is classified as an obstacle
6. Gaps in the rings are then also classified as obstacles

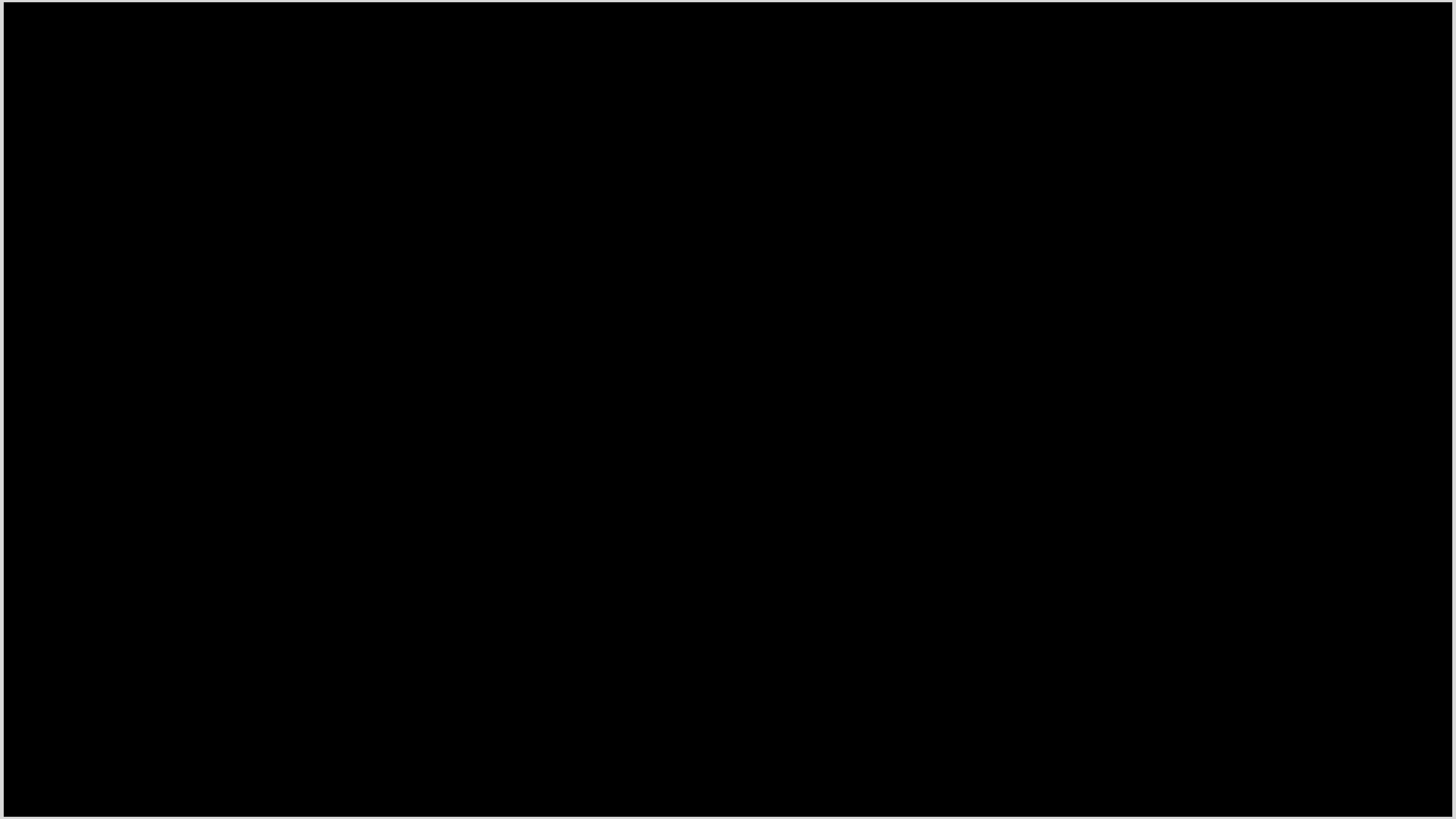
Simulation and Model-based Design



Controller Logic

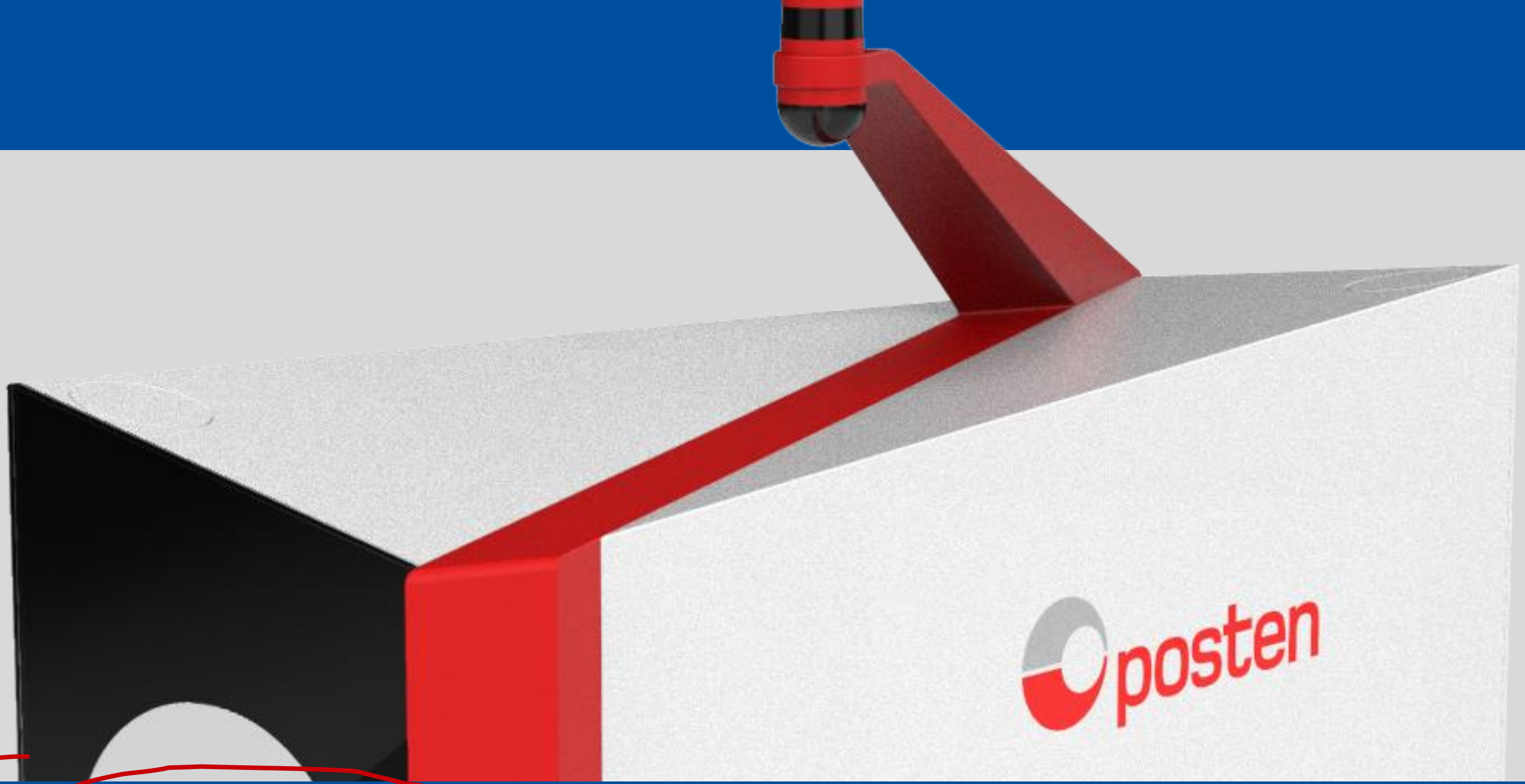


Vehicle in Action



Summary

- Kyburz was able to produce four functional prototypes in a span of 24 months using Model Based Design
- Some of the important lessons from this presentation:
  - Document and ensure adequate process is followed
  - Establish workflow which enables high safety integrity levels to be reached
  - Test at unit, module, and system level
- Success depends on effort multipliers (i.e. tools) as well as structured process
- Stay tuned for further deployments



Accelerating Deployment of Autonomous Delivery Robots using Model Based Design

Dr. Erik Wilhelm

KYBURZ Switzerland

11.04.2019

Q & A - Thank you for your attention