Elan8

SYSTEM DESIGN SPECIFICATION

Autonomous Floor Cleaning Robot

Document number	RVC-SDS-001
Revision	A
Status	Draft for review
Prepared by	Elan8

Generated from the SysML v2 model of the product with Doc42. Tables, values and diagrams are read from the model at this revision; change the model, not this document.

Contents

1 Introduction 3
1.1 Purpose 3
1.2 Scope 3
1.3 Document conventions 3
1.4 Applicable and reference documents 3
2 Design overview 4
3 Functional design 6
3.1 Operating states 6
3.2 Cliff safe-stop sequence 8
4 Physical architecture 10
4.1 Module interconnection 10
4.2 Base module 12
4.3 Power module 14
4.4 Main control board 16
4.5 Top module 18
5 Requirement allocation to modules 20
5.1 Safe-stop time budget 20
5.2 Base module requirements 21
5.3 Main control board requirements 21
5.4 Firmware requirements 22
5.5 Top module, dust bin and harness requirements 22
5.6 Module requirement summary 22
6 Firmware architecture 23
7 Bill of materials 23
7.1 Design-determining components 25
8 Design analyses 25
9 Requirement satisfaction 26
10 Limitations and open design points 26

1 Introduction

1.1 Purpose

This specification describes how the robot is built to meet RVC-SRS-001: its functions, its physical and firmware architecture, the purchased components it relies on, and the reasoning that links the design to the requirements.

1.2 Scope

The design described here is the single selected baseline of the robot. It covers the functional design, the physical architecture down to module level, the firmware task architecture and the purchased components that determine the design.

It also allocates the system requirements to the modules, and lists the bill of materials at the level of the model. Detailed mechanical drawings, circuit schematics and source code are outside this document. Product variants and the trade studies that led to the baseline are not recorded.

1.3 Document conventions

This document is generated from the SysML v2 model of the robot. Tables, values and diagrams are read from the model at the revision stated on the title page, so they agree with it by construction; the surrounding text is written by the engineering team.

Requirements are identified by a stable number. The word *shall* marks a binding requirement.

Prefix	Identifies	Specified in
USR	Customer requirement	RVC-CRS-001
SYS	System requirement	RVC-SRS-001
BASE, PCB, FW, TOP, BIN, HAR	Module requirement	RVC-SDS-001
VER	Verification case	RVC-VVP-001
VAL	Validation case	RVC-VVP-001

1.4 Applicable and reference documents

The four documents of the robot form one set. Each holds one kind of information and refers to the others for the rest.

Number	Document	Answers
RVC-CRS-001	Customer Requirements Specification	What does the household need?
RVC-SRS-001	System Requirements Specification	What shall the robot do, and how well?
RVC-SDS-001	System Design Specification	How is the robot built to do it?
RVC-VVP-001	Verification and Validation Plan	How will we know that it does?

The structure and content of the set follow these guides, tailored to a product of this size:

- ISO/IEC/IEEE 29148:2018, *Systems and software engineering — Life cycle processes — Requirements engineering*, for the stakeholder and system requirements specifications.
- NASA/SP-2016-6105 Rev 2, *NASA Systems Engineering Handbook*, for the verification and validation plan and the requirements verification matrix.
- INCOSE, *Systems Engineering Handbook*, fifth edition, and INCOSE, *Guide to Writing Requirements*, for the separation of needs, requirements, design and verification, and for the wording of requirements.

2 Design overview

The system of interest, *robotSystem*, has one physical realisation (*AutonomousFloorCleaningRobot*) and one operating behaviour (*OperateCleaningRobot*). The design links the two: every function is allocated to the hardware module and the firmware task that carry it out, and every system requirement is claimed by the function or the part that meets it.

The first figure shows the architecture as a block diagram, the second where the parts sit in the product.

Four decisions shape the design:

- **Safety is supervised independently of mission control.** Hazard signals reach a dedicated, highest-priority firmware task that can stop the motors without the mission controller's cooperation.
- **All loads are fed through the battery management system.** No module is connected to the battery directly, so over-current and over-temperature protection applies to every load.
- **The battery protects itself.** Over-current, over-voltage, under-voltage and over-temperature disconnect the pack in the gauge and protection circuit, without the application firmware.
- **Purchased components are selected, not specialised.** The robot's own part definitions state what the design needs; a named dependency selects the catalogue part that provides it. Replacing a component changes one dependency.

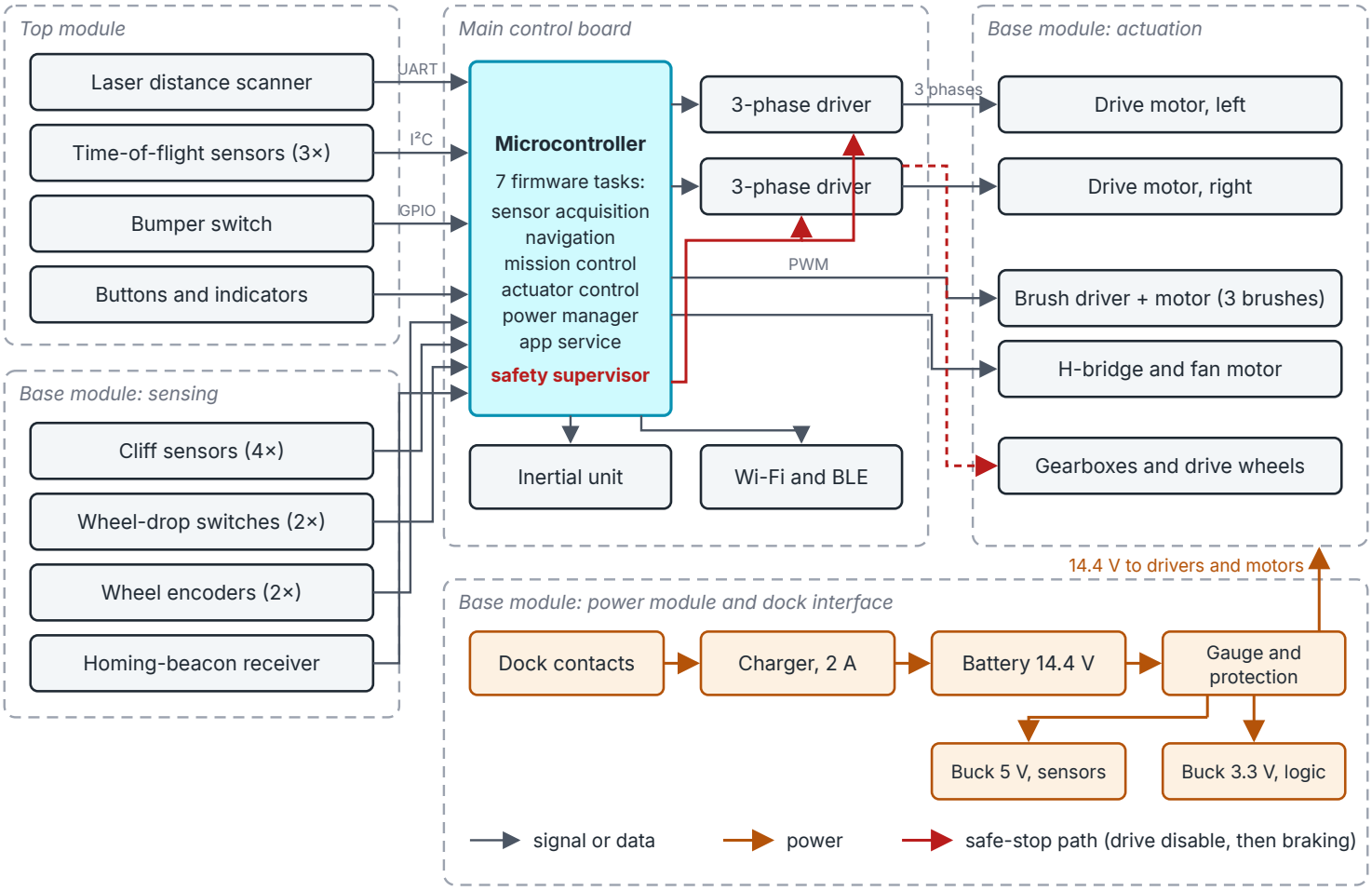
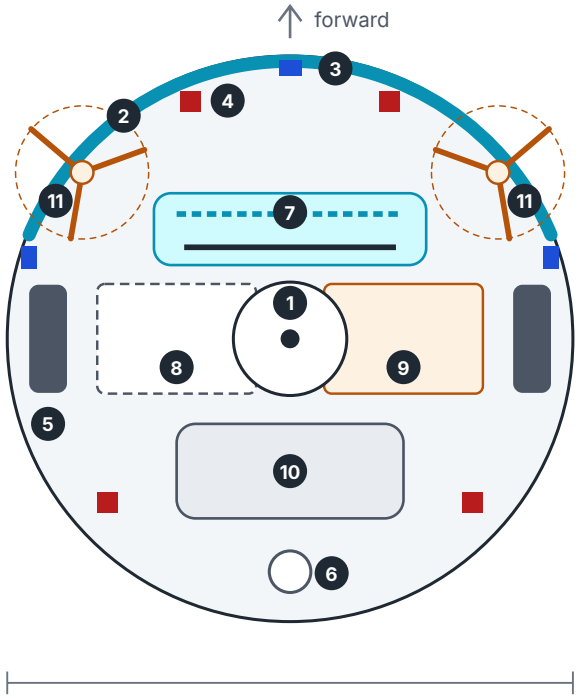


Figure 1: System architecture: sensing, control, actuation and power, with the safe-stop path

Plan view (shell removed)

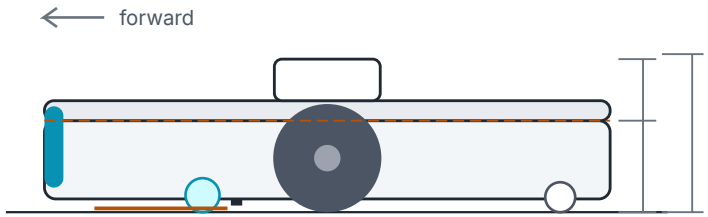
Underside cleaning parts shown through the chassis



Dashed brush circles: 80 mm swept diameter.
Both side brushes sweep inward to the cleaning head.
Rear caster trails the main roller and suction intake.

Left side elevation

92 mm design; 95 mm maximum (SYS-011)



Drive wheels: 65 mm diameter

Top: 37 mm design / 38 mm budget (TOP-001)

Base: 55 mm design / 57 mm budget (BASE-004)

Dashed horizontal line: module parting line

1 360° laser distance scanner

2 Front bumper with switch

3 Time-of-flight sensors (3×, blue)

4 Cliff sensors (4×, red)

5 Drive trains with wheel-drop switch (2×)

6 Rear caster wheel

7 Main roller and suction intake

8 Main control board (above chassis)

9 Power module with 14.4 V battery pack

10 Removable dust bin with filter

11 Side brushes (2×, shared mechanical drive)

Figure 2: Product layout and envelope

3 Functional design

The operating behaviour is decomposed into nine functions that exchange typed items: maps and obstacles from perception to navigation, drive commands from navigation through mission control to locomotion, and hazards from every source to safety supervision.

Each function is allocated to the elements that perform it:

- **Locomotion:** the base module and the actuator-control task.
- **Cleaning:** the cleaning head and the actuator-control task.
- **Perception:** the sensors of the base and top modules and the sensor-acquisition task.
- **Navigation:** the navigation task.
- **Power management:** the power module and the power-manager task.
- **Docking:** the dock interface.
- **Mission control:** the mission-controller task.
- **Safety supervision:** the safety-supervisor task.
- **User interaction:** the human-machine interface and the application-service task.

3.1 Operating states

Mission control is a state machine. Every hazard leads to the safe stop, from which only an explicit clearance returns the robot to service.

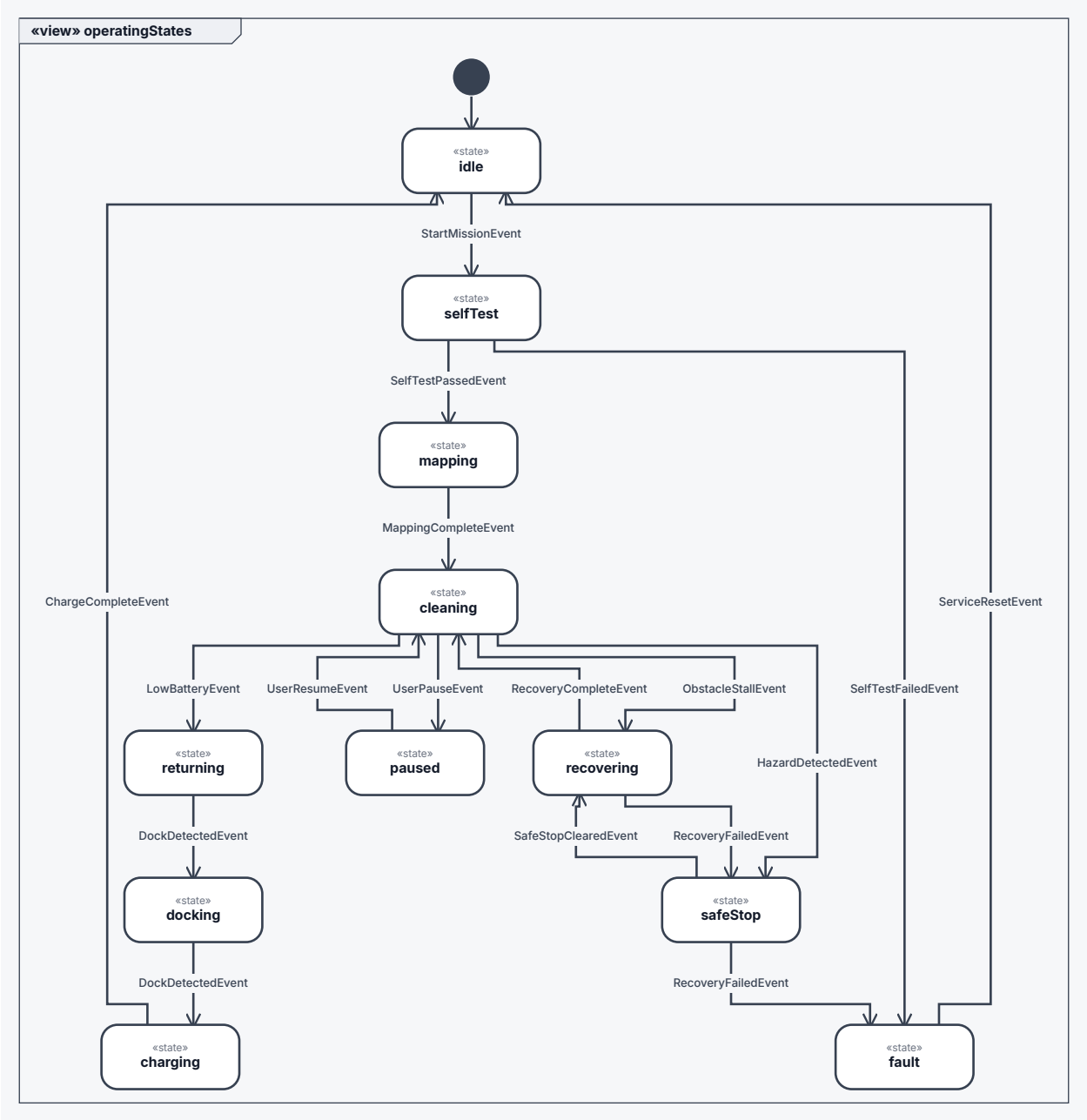


Figure 3: Operating states

3.2 Cliff safe-stop sequence

The safety-critical path from a cliff observation to stopped motors and a reported safe-stop state.

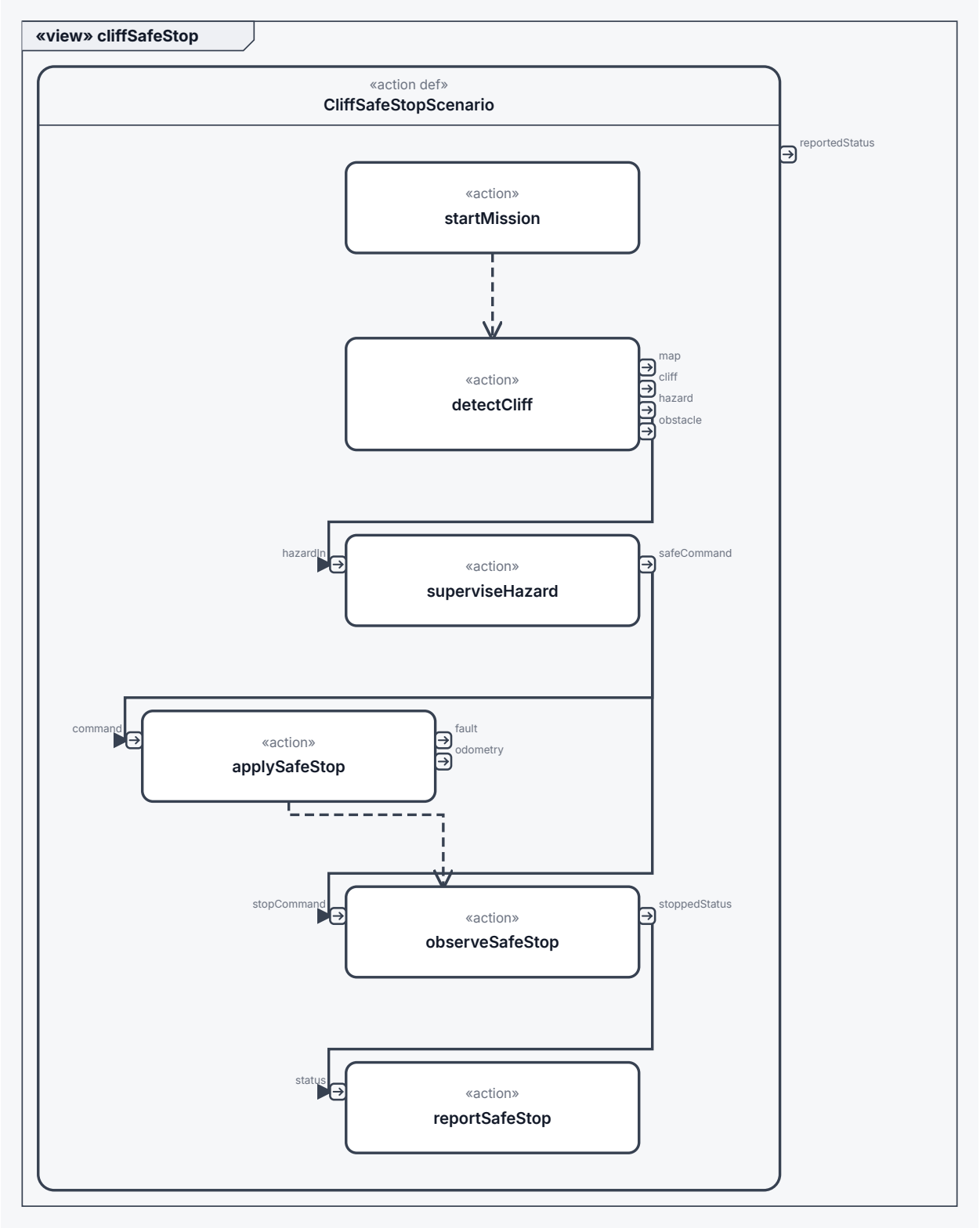


Figure 4: Cliff safe-stop sequence

4 Physical architecture

The robot consists of six line-replaceable units:

- the **base module**, which carries the chassis, the two drive trains, the cleaning head, four cliff sensors, the power module and the dock interface (*BaseModule*);
- the **main control board**, with the microcontroller, the two motor drivers, the inertial measurement unit and the wireless module (*MainPcbModule*);
- the **top module**, with the LiDAR, three time-of-flight sensors, the bumper and the human-machine interface (*TopModule*);
- the **dust bin**, with its lid and filter (*DustBin*);
- the **base wiring harness** and the **top wiring harness**, which connect the main control board to the two modules (*BaseWiringHarness*, *TopWiringHarness*).

Modules are connected only through typed ports. Power, signal and material paths are modelled explicitly, including dock charging, the protected battery rail and the debris path from the cleaning head to the dust bin. Each wiring harness is a bus: one port at each end that carries its signals as nested ports. The module interconnection therefore shows one connection per harness end, and each module diagram shows where the signals leave the bus for the parts inside. The diagrams in this chapter are drawn from those connections.

The cleaning direction defines the front of the robot. Two forward side brushes sweep inward towards the main roller and suction intake. A belt-and-gear transmission drives all three brushes from the existing 8 W brush motor; there are no separate side-brush motors or control channels. This power rating is an estimate for the complete brush train. The additional brushes and transmission are included in the BOM and mass roll-up.

The caster supports the **rear**, behind both the main roller and suction intake. The model records their longitudinal positions relative to the drive axle and asserts this ordering. The product-layout figure uses the same coordinates. Its body diameter is nominally 340 mm; the modeled height is 55 mm base plus 37 mm top (92 mm total), within the allocated 57 mm and 38 mm budgets and the 95 mm system limit.

4.1 Module interconnection

The six line-replaceable units and the electrical, signal and material connections between them.

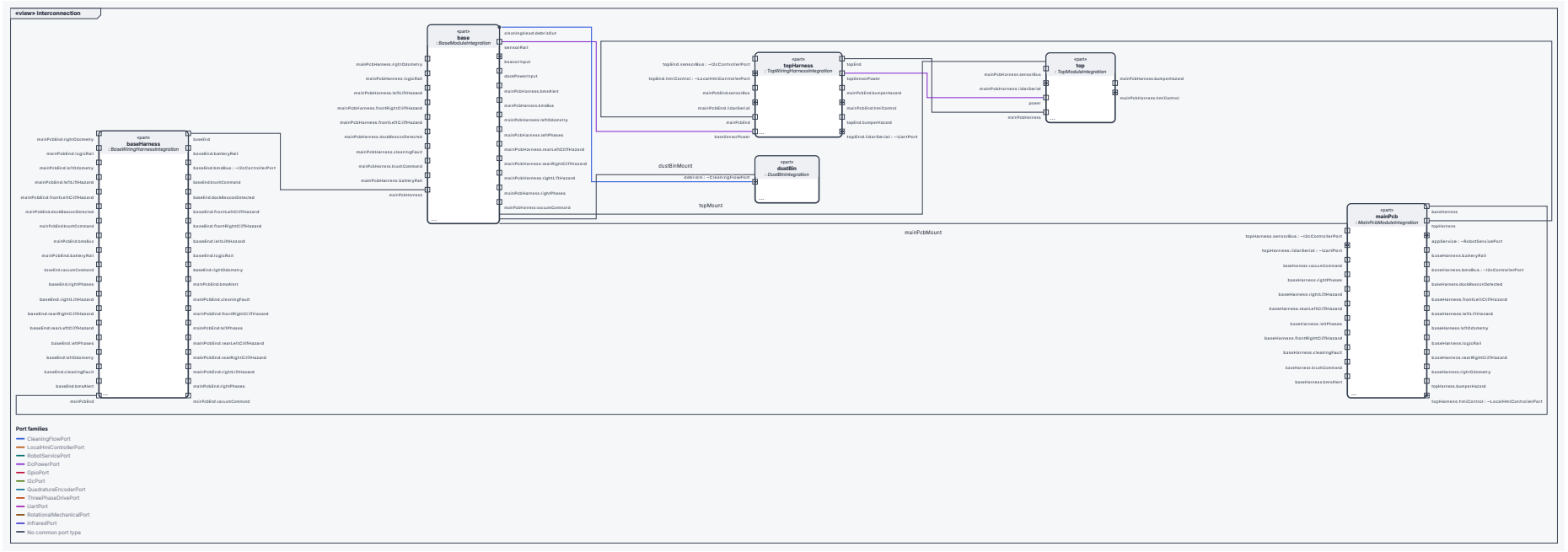


Figure 5: Module interconnection

4.2 Base module

Chassis, both drive trains, the cleaning head, the four cliff sensors, the power module and the dock interface.

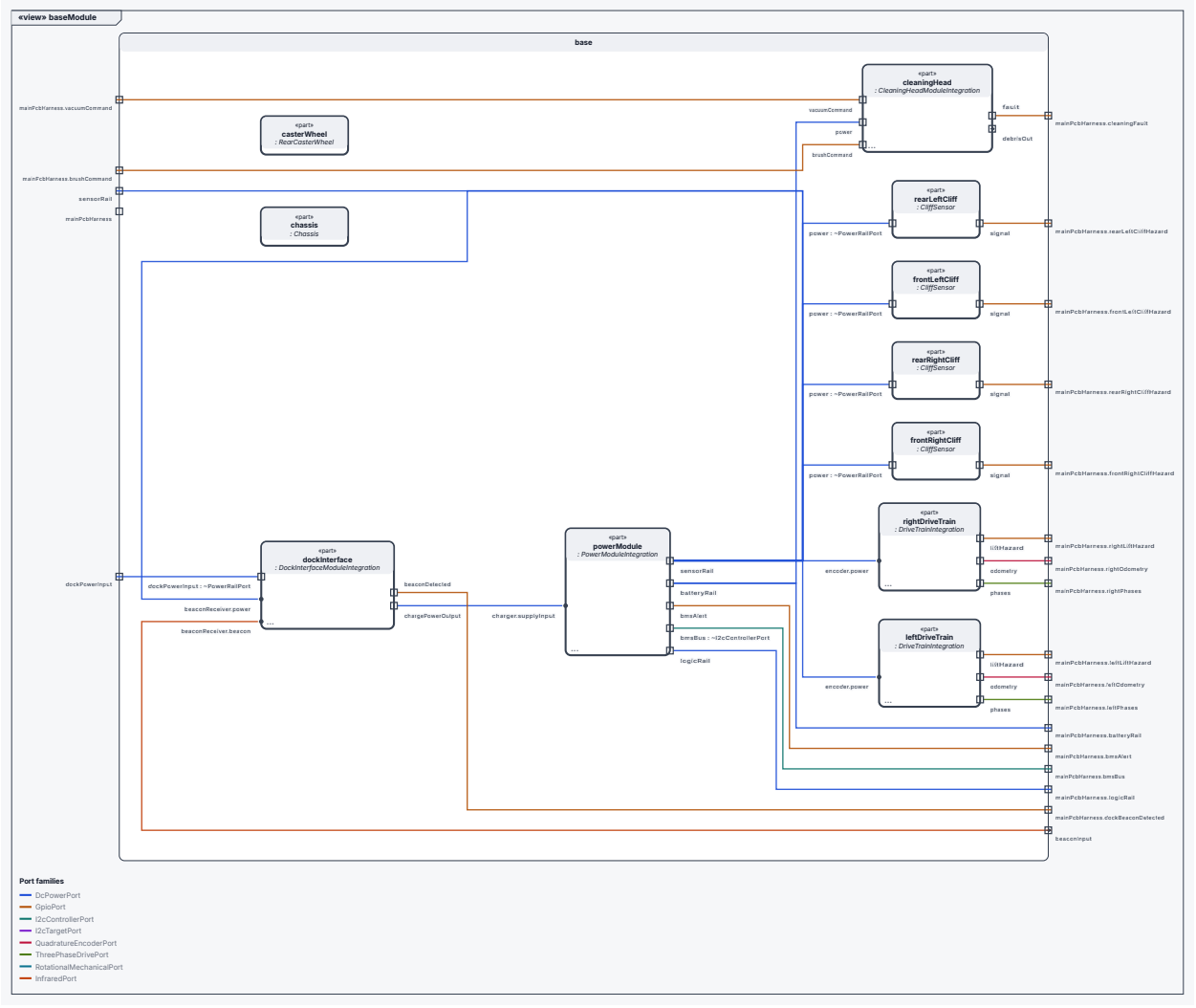


Figure 6: Base module

4.3 Power module

Battery, battery management, charger and the two regulated rails. All loads are fed through the protected output of the battery management system.

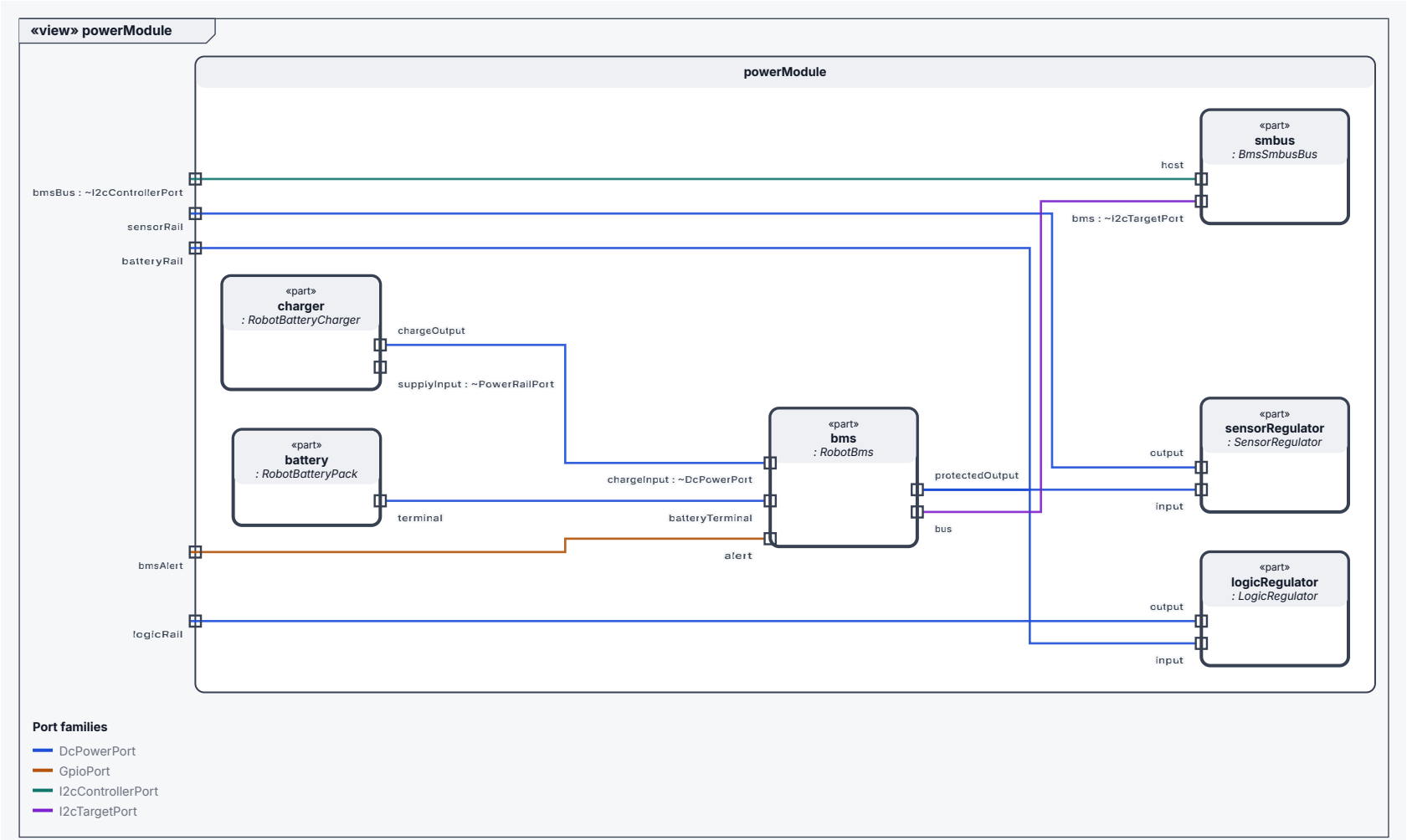


Figure 7: Power module

4.4 Main control board

Microcontroller, motor drivers, inertial measurement unit and wireless module.

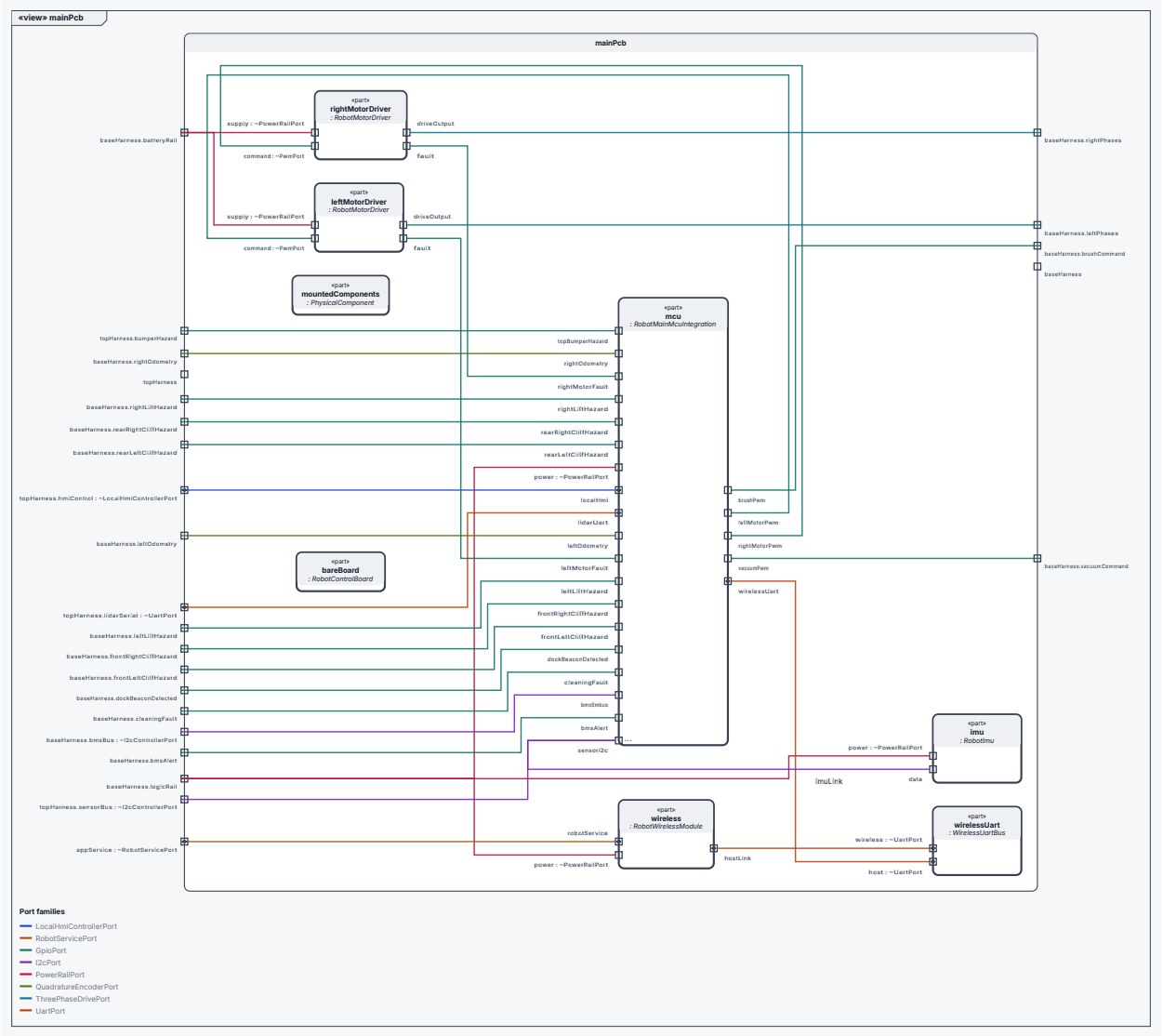


Figure 8: Main control board

4.5 Top module

LiDAR, the three time-of-flight sensors, the bumper and the human-machine interface.

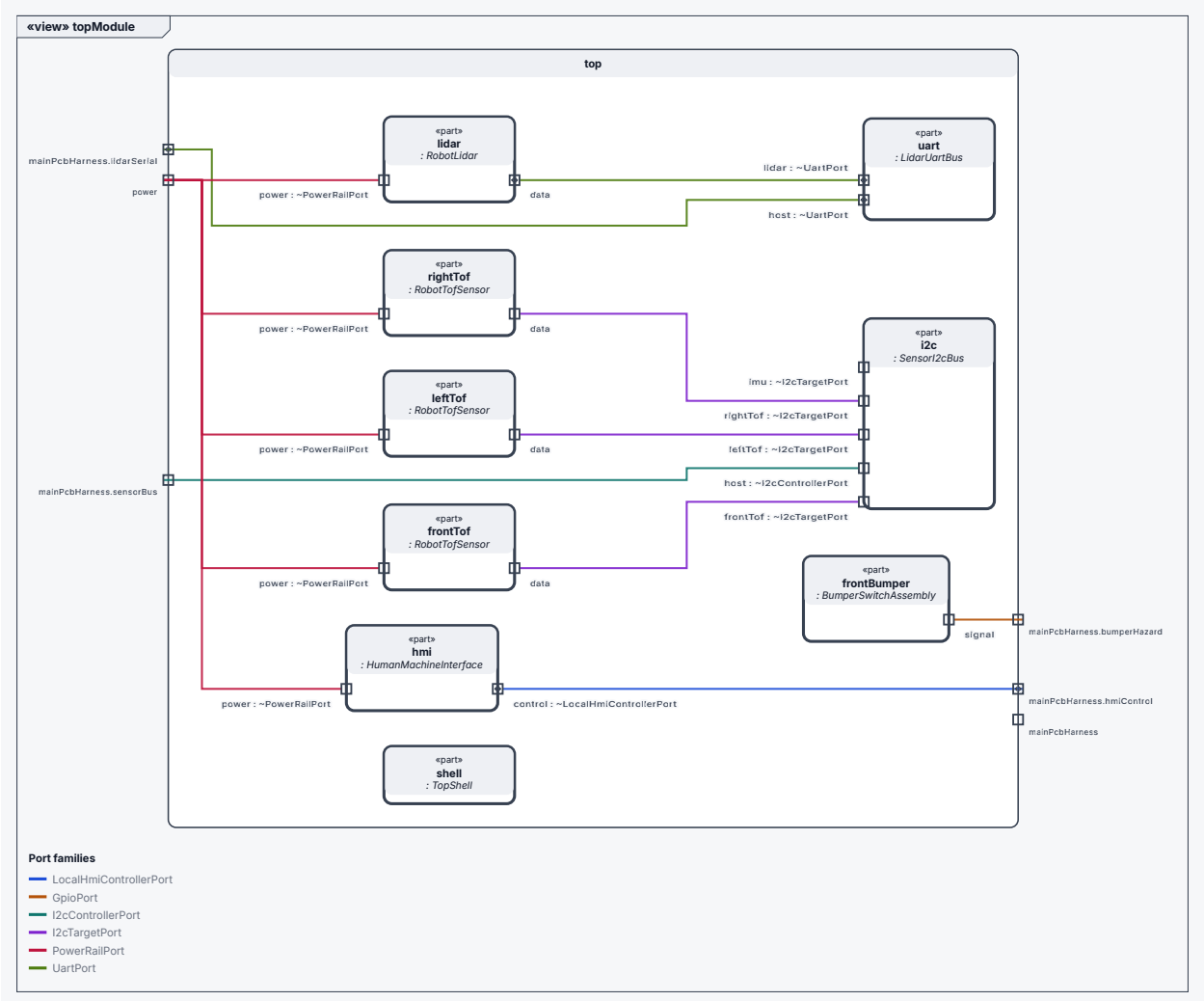


Figure 9: Top module

5 Requirement allocation to modules

A system requirement that no single module can meet alone is split into budgets, one for each module on the path. Each budget is a requirement on that module, so a module team can design and verify against its own specification, and a change to one budget is visible to the others.

Five system requirements are split this way. Each split is a derivation in the model that records why the budgets close. The module requirements constrain design values that are attributes of the module in the model, so the model shows at any time whether the current design is inside its budget.

System requirement	Module requirements	How the budget closes
SYS-001 Cleaning area per charge	*BASE-005 Battery capacity*	The mission energy analysis shows that 80 m² at an average of 2.6 A takes 4875 mAh. With a 15 % reserve for the return to the dock this needs a 6400 mAh pack.
SYS-011 Overall height	*BASE-004 Base module height* *TOP-001 Top module height*	The overall height is the base module up to the parting line plus the top module above it. The split at 57 mm follows the drive wheel diameter and the battery pack; the remaining 38 mm is for the shell and the scanner turret.
SYS-015 Robot mass	*BASE-003 Base module mass* *TOP-002 Top module mass* *PCB-002 Main board mass* *BIN-001 Dust bin mass* *HAR-001 Wiring harness mass*	Every gram of the robot belongs to one of five budgets, and the budgets add up to the 4.0 kg limit. Margin is held inside each module budget, so a module that grows has to renegotiate with the others rather than use up a common reserve unnoticed.
SYS-016 Recharge time	*BASE-006 Charge current*	Recharging 85 % of 6400 mAh within 4 hours, including the constant-voltage tail, needs at least 2 A in the constant-current phase.
SYS-SAFE-011 Safe stop on hazard	*BASE-001 Cliff sensing latency* *FW-001 Safety supervisor deadline* *PCB-001 Drive disable latency* *BASE-002 Drive braking time*	The 100 ms from hazard to standstill is a chain of four steps in three modules: sensing 25 ms, supervisor decision 10 ms, drive disable 5 ms and braking 50 ms. The budgets add up to 90 ms, which leaves 10 ms unallocated margin.

5.1 Safe-stop time budget

The safe stop is the tightest chain in the design. From the moment a hazard appears, the base module has to sense it, the safety supervisor has to decide, the main board has to remove drive, and the drive trains have to come to standstill. Three modules and four steps share 100 ms.

The budgets are 25 ms for sensing, 10 ms for the supervisor, 5 ms for removing drive and 50 ms for braking. They add up to 90 ms; the remaining 10 ms is unallocated margin.

The current design is inside every budget. Sensing at 100 Hz with a two-sample debounce takes 20 ms, the supervisor has a deadline of 10 ms, the gate-driver disable input acts within 2 ms, and active braking from cleaning speed takes 40 ms. The design values are estimates until they are measured on hardware; braking dominates and is to be measured first.

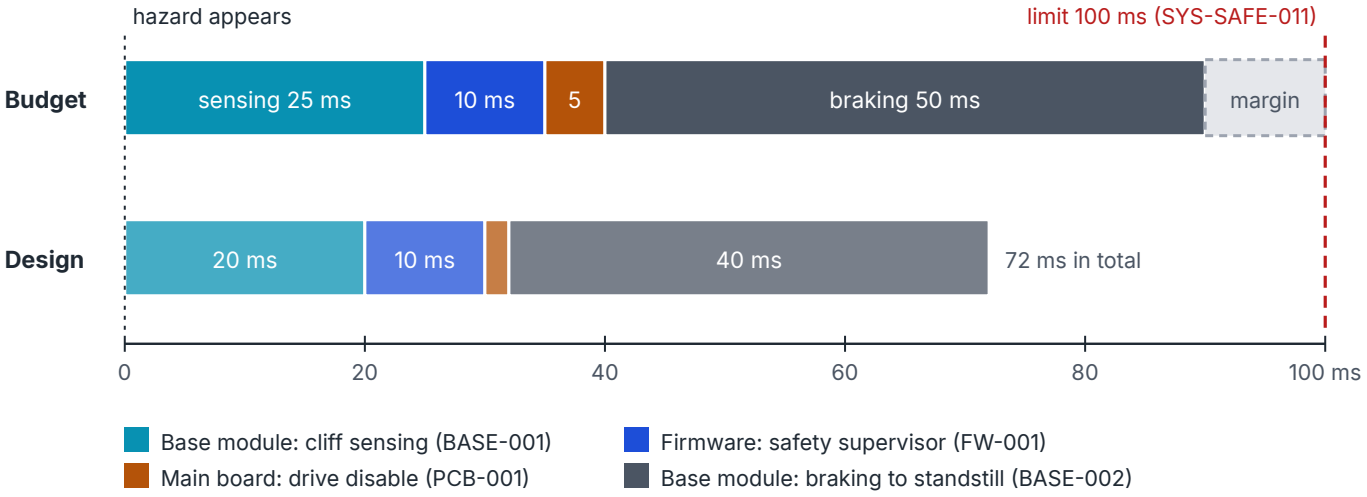


Figure 10: Safe-stop time: module budgets and current design values against the 100 ms limit

5.2 Base module requirements

ID	Requirement	Text	Satisfied by
BASE-001	Cliff sensing latency	The base module shall assert a cliff or wheel-drop hazard signal within 25 ms of the hazard appearing under a sensor.	robotSystem::physical::base
BASE-002	Drive braking time	The base module shall bring both drive wheels to standstill within 50 ms of the drive outputs being disabled at cleaning speed.	robotSystem::physical::base
BASE-003	Base module mass	The base module shall have a mass of at most 2.75 kg including the battery pack.	robotSystem::physical::base
BASE-004	Base module height	The base module shall be at most 57 mm high from the floor to the parting line with the top module.	robotSystem::physical::base
BASE-005	Battery capacity	The power module shall hold a battery pack with a rated capacity of at least 6400 mAh.	robotSystem::physical::base::powerModule
BASE-006	Charge current	The power module shall charge the battery pack with at least 2 A in the constant-current phase.	robotSystem::physical::base::powerModule

5.3 Main control board requirements

ID	Requirement	Text	Satisfied by
PCB-001	Drive disable latency	The main board shall remove drive from both motors within 5 ms of the safe-stop command, through a disable line that does not depend on the motion-control loop.	robotSystem::physical::mainPcb
PCB-002	Main board mass	The assembled main board shall have a mass of at most 0.25 kg.	robotSystem::physical::mainPcb

5.4 Firmware requirements

ID	Requirement	Text	Satisfied by
FW-001	Safety supervisor deadline	The safety supervisor task shall issue the safe-stop command within 10 ms of a hazard event entering its queue, under worst-case load of all other tasks.	robotSystem::physical::firmwareTasks::safetySupervisor

5.5 Top module, dust bin and harness requirements

ID	Requirement	Text	Satisfied by
BIN-001	Dust bin mass	The empty dust bin with its filter shall have a mass of at most 0.22 kg.	robotSystem::physical::dustBin
HAR-001	Wiring harness mass	The base and top wiring harnesses together shall have a mass of at most 0.18 kg.	robotSystem::physical
TOP-001	Top module height	The top module shall rise at most 38 mm above the parting line, including the laser scanner turret.	robotSystem::physical::top
TOP-002	Top module mass	The top module shall have a mass of at most 0.6 kg.	robotSystem::physical::top

5.6 Module requirement summary

Every module requirement with the system requirement it was derived from and the part that claims it. How each one is verified is in RVC-VVP-001.

ID	Module requirement	Derived from	Satisfied by
BASE-001	Cliff sensing latency	*SYS-SAFE-011 Safe stop on hazard*	robotSystem::physical::base
BASE-002	Drive braking time	*SYS-SAFE-011 Safe stop on hazard*	robotSystem::physical::base
BASE-003	Base module mass	*SYS-015 Robot mass*	robotSystem::physical::base
BASE-004	Base module height	*SYS-011 Overall height*	robotSystem::physical::base
BASE-005	Battery capacity	*SYS-001 Cleaning area per charge*	robotSystem::physical::base::powerModule
BASE-006	Charge current	*SYS-016 Recharge time*	robotSystem::physical::base::powerModule
BIN-001	Dust bin mass	*SYS-015 Robot mass*	robotSystem::physical::dustBin
FW-001	Safety supervisor deadline	*SYS-SAFE-011 Safe stop on hazard*	robotSystem::physical::firmwareTasks::safetySupervisor
HAR-001	Wiring harness mass	*SYS-015 Robot mass*	robotSystem::physical
PCB-001	Drive disable latency	*SYS-SAFE-011 Safe stop on hazard*	robotSystem::physical::mainPcb
PCB-002	Main board mass	*SYS-015 Robot mass*	robotSystem::physical::mainPcb
TOP-001	Top module height	*SYS-011 Overall height*	robotSystem::physical::top
TOP-002	Top module mass	*SYS-015 Robot mass*	robotSystem::physical::top

6 Firmware architecture

The firmware runs on the microcontroller of the main control board as seven tasks under a fixed-priority real-time scheduler. The seven tasks are allocated to the scheduler execution platform, which is allocated to the microcontroller. Tasks communicate only through typed message queues.

- **Safety supervisor**, event-driven, deadline 10 ms, highest priority. Receives every hazard and issues the safe command.
- **Actuator control**, every 20 ms. Drives the wheel and cleaning motors and detects stalls.
- **Sensor acquisition**, every 20 ms. Reads the cliff, time-of-flight, bumper and inertial sensors and the LiDAR.
- **Mission controller**, event-driven, deadline 50 ms. Sequences the mission and arbitrates between planner and safety commands.
- **Power manager**, every 100 ms. Monitors the battery and controls charging.
- **Navigation**, every 50 ms. Maintains the map and pose and plans the path.
- **Application service**, event-driven, deadline 100 ms, lowest priority. Serves the mobile application.

Hazards travel on their own queue from sensor acquisition to the safety supervisor, and the safe command travels on its own queue to mission control. Neither shares a queue with planner or user traffic, so a busy planner cannot delay a stop.

7 Bill of materials

The bill of materials is generated from the physical architecture. Every part that is bought or made carries a classification in the model with its description, whether it is bought or made, and a unit cost; its mass is the attribute the mass budget uses. Quantities follow from the part usages, so four cliff sensors in the model are four on the list. Where the design has selected a catalogue part, the manufacturer and part number come from that part. The build fails for a physical part without a classification or a mass.

Costs are budgetary estimates at a volume of 10 000 units, in euro, for comparison between design options. They are not quotations. Fasteners, labels, packaging and the docking station are not in the model and not on the list. The same lines are written to `generated/bom.csv` for use in a spreadsheet.

Item	Qty	Source	Manufacturer and part number	Unit cost (EUR)	Cost (EUR)	Mass (g)
Base						
Chassis tub, injection moulded	1	Make		3.50	3.50	300
Left drive train						
Drive motor, brushless DC, 14 W	1	Buy		4.80	4.80	140
Planetary gearbox, 30:1	1	Buy		1.60	1.60	150
Drive wheel with tyre, 65 mm	1	Make		0.90	0.90	80
Quadrature encoder, magnetic	1	Buy		0.70	0.70	5
Wheel-drop switch	1	Buy		0.15	0.15	10
Right drive train						
Drive motor, brushless DC, 14 W	1	Buy		4.80	4.80	140
Planetary gearbox, 30:1	1	Buy		1.60	1.60	150
Drive wheel with tyre, 65 mm	1	Make		0.90	0.90	80

Item	Qty	Source	Manufacturer and part number	Unit cost (EUR)	Cost (EUR)	Mass (g)
Quadrature encoder, magnetic	1	Buy		0.70	0.70	5
Wheel-drop switch	1	Buy		0.15	0.15	10
Rear caster wheel	1	Buy		0.60	0.60	30
Cliff sensor, infrared reflective	4	Buy		0.45	1.80	80
Cleaning head						
Brush belt and gear transmission	1	Make		0.60	0.60	30
Side brush, three-arm	2	Make		0.30	0.60	30
Cleaning head housing with main brush and duct	1	Make		2.60	2.60	400
Brush motor, brushed DC, 8 W	1	Buy		1.80	1.80	70
H-bridge motor driver	2	Buy		0.55	1.10	4
Vacuum fan motor, brushed DC, 10 W	1	Buy		3.20	3.20	160
Power module						
Lithium-ion battery pack, 4S2P, 14.4 V	1	Buy		16.00	16.00	500
Battery charger stage, 2 A	1	Buy		1.20	1.20	40
Battery gauge and protection circuit	1	Buy	Texas Instruments BQ40Z50-R2	2.90	2.90	30
Buck regulator, 3.3 V	1	Buy		0.40	0.40	20
Buck regulator, 5 V	1	Buy		0.40	0.40	20
Dock interface						
Charging contact assembly	1	Make		0.80	0.80	50
Infrared homing-beacon receiver	1	Buy		0.35	0.35	30
Main PCB						
Main control board, bare PCB with passives and connectors	1	Make		3.40	3.40	155
Main microcontroller	1	Buy	STMicroelectronics STM32U575VGT6	4.60	4.60	10
Three-phase motor driver	2	Buy	Texas Instruments DRV8316RRGFR	2.30	4.60	10
Wi-Fi and Bluetooth LE module	1	Buy	Espressif Systems ESP32-C3-MINI-1-N4	1.50	1.50	5
Inertial measurement unit, 6-axis	1	Buy		1.40	1.40	30
Top						

Item	Qty	Source	Manufacturer and part number	Unit cost (EUR)	Cost (EUR)	Mass (g)
Top shell with bumper carrier, moulded	1	Make		2.80	2.80	200
360° laser distance scanner	1	Buy	Slamtec RPLIDAR C1M1	35.00	35.00	150
Time-of-flight distance sensor module	3	Buy	STMicroelectronics VL53L1CXV0FY/1	2.60	7.80	90
Bumper switch assembly	1	Buy		0.20	0.20	20
Button and indicator board	1	Make		1.10	1.10	80
Dust bin						
Dust bin body, moulded	1	Make		0.70	0.70	150
Dust bin lid, moulded	1	Make		0.30	0.30	30
Pleated dust filter	1	Buy		0.55	0.55	20
Base wiring harness with connectors	1	Make		1.90	1.90	120
Top wiring harness with connectors	1	Make		1.10	1.10	60
Total	49				**121.10**	**3694**

7.1 Design-determining components

Six purchased components determine the design. Each is a catalogue part in the model with its manufacturer, part number and datasheet reference; the robot's own part definition selects it through a named dependency.

- **Microcontroller:** STMicroelectronics STM32U575VGT6 (*STM32U575VGT6*).
- **Motor driver:** Texas Instruments DRV8316R, one per drive motor (*DRV8316R*).
- **Time-of-flight sensor:** STMicroelectronics VL53L1CX, three fitted (*VL53L1CX*).
- **LiDAR:** Slamtec RPLIDAR C1 (*RPLIDARC1*).
- **Wireless module:** Espressif ESP32-C3-MINI-1 (*ESP32C3MINI1*).
- **Battery management:** Texas Instruments BQ40Z50-R2 (*BQ40Z50R2*).

Lifecycle status and availability were checked against the manufacturers' published data when the parts were entered and must be checked again before procurement.

8 Design analyses

Four analyses in the model support the design. Each compares a calculated value with a design limit of RVC-SRS-001. The input values are design estimates, not measurements.

Mission energy (*MissionEnergyAnalysis*). An average current of 2.6 A over a mission of 1.875 hours draws 4 875 mAh. The budget of 6 400 mAh less a 15 percent reserve leaves 5 440 mAh, so the mission fits with a margin of 565 mAh.

Safety reaction (*SafetyReactionAnalysis*). The analysis adds the design values of the four steps of the safe stop, taken from the modules: 20 ms, 10 ms, 2 ms and 40 ms, together 72 ms against the 100 ms limit.

Localization performance (*LocalizationPerformanceAnalysis*). The selected combination of time-of-flight sensors, laser scanner, inertial measurement and odometry gives an estimated error of 95 mm against a limit of 150 mm.

Mass budget (*MassBudgetAnalysis*). The module masses are rolled up from the parts of the bill of materials and compared with the mass limit. The table below is generated from the same values.

Module	Mass (kg)	Share
Base	2.56	69 %
Top	0.54	15 %
Main PCB	0.21	6 %
Dust bin	0.20	5 %
Base harness	0.12	3 %
Top harness	0.06	2 %
Total	**3.69**	100 %
Limit (SYS-015)	4.00	
Margin	0.31	8 % of the limit

9 Requirement satisfaction

The design element that claims each system requirement. A claim is a design intent recorded in the model, not evidence; evidence comes from the verification cases of RVC-VVP-001.

ID	System requirement	Satisfied by
SYS-001	Cleaning area per charge	robotSystem::operate::cleaning
SYS-002	Floor coverage	robotSystem::operate::navigation
SYS-003	Obstacle avoidance	robotSystem::operate::perception
SYS-004	Localization accuracy	robotSystem::operate::navigation
SYS-005	Coverage map maintenance	robotSystem::operate::navigation
SYS-006	Wheel stall detection and recovery	robotSystem::operate::missionControl
SYS-007	Return to dock on low battery	robotSystem::operate::docking
SYS-008	Charging within the battery safe operating area	robotSystem::operate::powerManagement
SYS-009	Mission status reporting	cliffSafeStop::reportSafeStop, robotSystem::operate::userInteraction
SYS-010	Local storage of map data	robotSystem::operate::userInteraction
SYS-011	Overall height	robotSystem::physical::top
SYS-012	Acoustic noise	robotSystem::physical::base::cleaningHead
SYS-013	Dust bin capacity	robotSystem::physical::dustBin
SYS-014	Threshold climbing	robotSystem::operate::locomotion
SYS-015	Robot mass	robotSystem::physical
SYS-016	Recharge time	robotSystem::operate::powerManagement
SYS-017	Operating modes	robotSystem::operate::missionControl
SYS-SAFE-010	Cliff detection	cliffSafeStop::detectCliff, robotSystem::operate::perception
SYS-SAFE-011	Safe stop on hazard	cliffSafeStop::superviseHazard, robotSystem::operate::safetySupervision
SYS-SAFE-012	Battery protection independent of firmware	robotSystem::physical::base::powerModule::bms
SYS-SAFE-013	Safe stop held until cleared	robotSystem::operate::safetySupervision

10 Limitations and open design points

This design is a teaching and tool-validation baseline. It is not a certified product design, and its bill of materials is not released for production.

- The analysis inputs are estimates. They must be replaced by measured values before the analyses are used as verification evidence.
- The safe-stop design values add up to 72 ms against a 100 ms limit; the braking time dominates and should be confirmed on hardware first.
- Costs in the bill of materials are budgetary estimates, and several purchased parts do not yet have a selected manufacturer part.
- The mass margin is 8 percent of the limit, which is small for this stage of a design.
- The shared 8 W brush motor drives the main roller and both side brushes through a belt-and-gear transmission. Its starting torque, debris-jam load and full-train power draw need hardware confirmation.
- The firmware architecture defines tasks, queues and timing, not their internal design.
- Component lifecycle status is recorded as checked on a date and is not monitored.