Elan8

VERIFICATION AND VALIDATION PLAN

Autonomous Floor Cleaning Robot

Document number	RVC-VVP-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 System under verification **4**
3 Verification and validation approach **6**
4 Test articles, facilities and equipment **6**
5 System verification **7**
5.1 Verification cases 7
5.2 Requirements verification matrix 9
6 Module verification **10**
7 Validation **11**
7.1 Validation cases 11
7.2 Validation matrix 12
8 Status and open points **12**

1 Introduction

1.1 Purpose

This plan states how Elan8 will show that the robot meets its requirements and that it is the product a household needs. Verification answers the first question against RVC-SRS-001 and the module requirements of RVC-SDS-001; validation answers the second against RVC-CRS-001. The plan defines the methods, the cases with their pass criteria, and the matrices that show every requirement is covered. It contains no results.

1.2 Scope

The plan covers the robot: its mechanics, electronics and firmware, at three levels.

- **Module verification** against the module requirements of RVC-SDS-001.
- **System verification** against the system requirements of RVC-SRS-001.
- **Validation** against the customer requirements of RVC-CRS-001.

The docking station and the mobile application take part as test equipment. Their own verification, production acceptance testing of each manufactured unit, regulatory approval and reliability growth testing are outside this plan.

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 System under verification

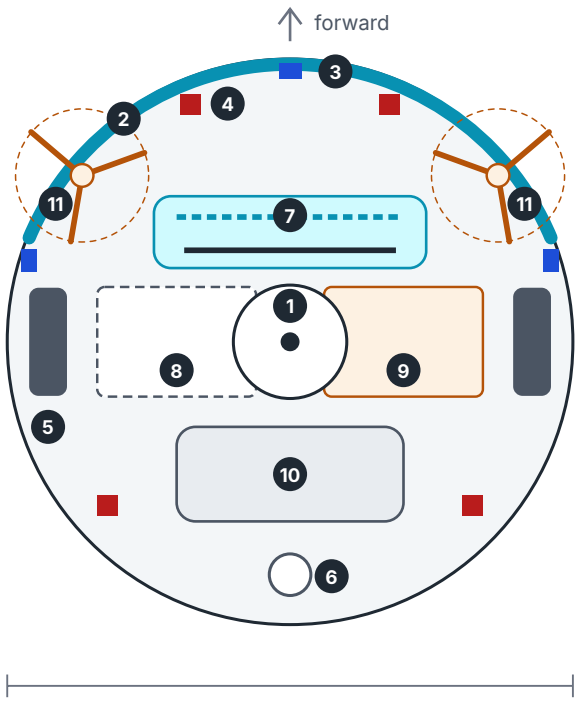
The system under verification is the robot described in RVC-SDS-001: six modules and the firmware on the main control board.

Requirements flow down in two steps. Each customer requirement is derived into system requirements, and each system requirement that no single module can meet alone is split into module budgets. Verification runs the other way: a module is shown to be inside its budget, the robot is shown to meet its system requirements, and the product is shown to meet the needs of the household.

Level	Requirements	Number	Shown by
Customer	USR, in RVC-CRS-001	11	5 validation cases
System	SYS, in RVC-SRS-001	21	12 verification cases
Module	BASE, PCB, FW, TOP, BIN, HAR, in RVC-SDS-001	13	The same 12 cases, with the module quantity measured separately

Plan view (shell removed)

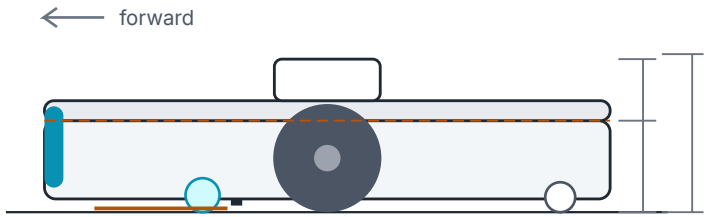
Underside cleaning parts shown through the chassis



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 1: The robot and its modules, the units verification is planned against

3 Verification and validation approach

Methods

Four methods are used, as defined in the NASA Systems Engineering Handbook. The tables of this plan name them with the terms of the SysML v2 standard library.

Method	In the tables	Used when
Test	`test`	The requirement is shown by operating the robot or its firmware under controlled conditions and measuring the result against the limit.
Analysis	`analyze`	The requirement is shown by calculation or simulation from design data, where a test is impractical or to extend a test result to conditions that were not tested.
Inspection	`inspect`	The requirement is shown by examining or measuring the product or its records without operating it.
Demonstration	`demo`	The requirement is shown by operating the product and observing the result, without measurement against a numeric limit.

Test is preferred for every requirement with a numeric limit. Analysis alone is not accepted for a safety requirement.

Pass criteria

Each case states its own criterion. A requirement is verified when every case that names it has passed on the configuration under test. A case that is run again after a change to the robot is run in full.

Order of work

Firmware cases run first, on the target board, because they need no assembled robot. Module quantities are measured next, so that a module outside its budget is found before system tests. System cases follow on the assembled robot, and validation comes last, with production-representative units.

Nonconformance

A failed case is recorded with the configuration it was run on. The cause is traced through the model: from the requirement to the module budget, the design element that claims it and the analysis behind it. The case is repeated after the correction.

Independence

The safety cases, VER-002, VER-009 and VER-012, are witnessed by an engineer who did not design the item under test. The household safety walkthrough, VAL-003, is observed by an assessor from outside the project.

4 Test articles, facilities and equipment

Test articles

Article	Number	Used for
Main control board with debug access	3	Firmware cases VER-001 to VER-005 and VER-008
Engineering robot, instrumented	2	System cases VER-006, VER-007 and VER-009 to VER-012
Production-representative robot	10	Validation cases VAL-001 to VAL-005

Facilities and equipment

Facility or equipment	Used in
Reference home: 80 m² of hard floor and low-pile carpet, two rooms, furniture, a threshold and a staircase	VER-006, VER-007, VER-008
Cliff rig: a platform with an adjustable drop, a high-speed camera and a logic analyser	VER-009
External position reference system	VER-008
Surface plate, height gauge, scale and graduated cylinder	VER-010
Low-noise room with a class 1 sound level meter	VER-011
Battery fault injection bench in a fire-safe enclosure	VER-012
Hardware-in-the-loop bench with simulated sensors and a blocked-rotor fixture	VER-001 to VER-005
Network capture on the home network	VER-005
Three occupied homes and a panel of ten households	VAL-001 to VAL-005

5 System verification

Twelve verification cases cover the system requirements. Six are run on the firmware on its target board and six on the assembled robot.

5.1 Verification cases

Each case states its method, what is done, and the criterion for passing. The last column lists the requirements the case verifies, at system and at module level.

ID	Case	Method	Procedure and pass criterion	Verifies
VER-001	Mission control firmware	test	Run the mission controller on the target board against simulated sensor, battery and application inputs. Pass when a stalled wheel is reported and recovered within the limit, the return to the dock starts at the threshold state of charge, the robot is always in exactly one operating mode, and every change of mode is reported.	SYS-006 SYS-007 SYS-009 SYS-017
VER-002	Safety supervisor firmware	test	Inject every hazard event on the target board under worst-case load of the other tasks and measure the time to the safe-stop command with a logic analyser. Pass when the command is issued within the deadline for every hazard in 1000 consecutive injections, and no drive command is passed on until the hazard is removed and a user confirmation is received.	SYS-SAFE-011 SYS-SAFE-010 SYS-008 FW-001 SYS-SAFE-013
VER-003	Sensor acquisition firmware	test	Replay recorded sensor data with obstacles and drops of known size through the acquisition task. Pass when every obstacle of at least the minimum	SYS-003 SYS-SAFE-010

ID	Case	Method	Procedure and pass criterion	Verifies
			height and every drop of at least the minimum depth produces its event.	
VER-004	Actuator control firmware	test	Drive the motor outputs on the target board into a blocked rotor and command a safe stop at cleaning speed. Pass when the stall is detected within the limit and the drive outputs are disabled on the safe-stop command.	SYS-006 SYS-SAFE-011
VER-005	Application service and map privacy	test inspect	Exercise the application interface on the home network and capture all traffic leaving the robot, then inspect where map data is stored. Pass when status is reported for every mission event and no map data leaves the robot without recorded consent.	SYS-009 SYS-010
VER-006	Cleaning coverage mission	test analyze	Run a full mission in the reference home from a full charge and compare the cleaned area with the surveyed reachable floor; confirm the energy margin with the mission energy analysis. Pass when the cleaned area and the coverage meet their limits in three consecutive missions.	SYS-001 SYS-002
VER-007	Docking and charging	test	Let the robot run down to the return threshold in the reference home, return, dock and recharge, while logging charge current, cell temperature and time. Pass when the robot docks without help in ten of ten runs, charging stays inside the battery safe operating area and the recharge time is within the limit.	SYS-007 SYS-008 SYS-016 BASE-005 BASE-006
VER-008	Navigation performance	test analyze	Track the robot with an external reference system during the reference mission and compare its estimated pose with the reference; support the result with the localization performance analysis. Pass when the localization error stays within the limit and the coverage map matches the floor actually cleaned.	SYS-004 SYS-005
VER-009	Cliff safe stop	test analyze	Drive the robot at cleaning speed towards a drop on the cliff rig from four directions and record sensing, command and wheel motion with a high-speed camera and a logic analyser; compare with the safety reaction analysis. Pass when no wheel crosses the edge, the time from hazard to standstill is within the limit in every run, each step is within its module budget, the safe stop is	SYS-SAFE-010 SYS-SAFE-011 SYS-009 BASE-001 BASE-002 PCB-001 SYS-SAFE-013

ID	Case	Method	Procedure and pass criterion	Verifies
			reported, and the robot stays stationary until the drop is covered and the user confirms.	
VER-010	Physical envelope	inspect analyze	Measure the height of the assembled robot on a surface plate, weigh the robot and each module, and measure the dust bin volume by filling; compare the masses with the mass budget analysis. Pass when every measured value is within its limit or budget.	SYS-011 SYS-015 SYS-013 BASE-003 BASE-004 PCB-002 TOP-001 TOP-002 BIN-001 HAR-001
VER-011	Mobility and acoustics	test	Cross a rigid threshold of the limit height in both directions ten times, and measure the sound pressure level at 1 m while cleaning a hard floor in a low-noise room. Pass when every crossing succeeds and the A-weighted level is within the limit.	SYS-014 SYS-012
VER-012	Battery protection	test	Apply over-current, over-voltage, under-voltage and over-temperature to the battery pack on the fault injection bench with the application firmware halted. Pass when the pack disconnects for every fault without firmware action.	SYS-SAFE-012 SYS-008

5.2 Requirements verification matrix

Every system requirement of RVC-SRS-001 with the methods and the cases that verify it. The build of the model fails for a requirement without a case, so a requirement cannot be missing from this matrix or be left without verification.

ID	System requirement	Method	Verified by
SYS-001	Cleaning area per charge	test analyze	*VER-006 Cleaning coverage mission*
SYS-002	Floor coverage	test analyze	*VER-006 Cleaning coverage mission*
SYS-003	Obstacle avoidance	test	*VER-003 Sensor acquisition firmware*
SYS-004	Localization accuracy	test analyze	*VER-008 Navigation performance*
SYS-005	Coverage map maintenance	test analyze	*VER-008 Navigation performance*
SYS-006	Wheel stall detection and recovery	test	*VER-001 Mission control firmware* *VER-004 Actuator control firmware*
SYS-007	Return to dock on low battery	test	*VER-001 Mission control firmware* *VER-007 Docking and charging*
SYS-008	Charging within the battery safe operating area	test	*VER-002 Safety supervisor firmware*

ID	System requirement	Method	Verified by
			VER-007 Docking and charging *VER-012 Battery protection*
SYS-009	Mission status reporting	test inspect analyze	*VER-001 Mission control firmware* *VER-005 Application service and map privacy* *VER-009 Cliff safe stop*
SYS-010	Local storage of map data	test inspect	*VER-005 Application service and map privacy*
SYS-011	Overall height	inspect analyze	*VER-010 Physical envelope*
SYS-012	Acoustic noise	test	*VER-011 Mobility and acoustics*
SYS-013	Dust bin capacity	inspect analyze	*VER-010 Physical envelope*
SYS-014	Threshold climbing	test	*VER-011 Mobility and acoustics*
SYS-015	Robot mass	inspect analyze	*VER-010 Physical envelope*
SYS-016	Recharge time	test	*VER-007 Docking and charging*
SYS-017	Operating modes	test	*VER-001 Mission control firmware*
SYS-SAFE-010	Cliff detection	test analyze	*VER-002 Safety supervisor firmware* *VER-003 Sensor acquisition firmware* *VER-009 Cliff safe stop*
SYS-SAFE-011	Safe stop on hazard	test analyze	*VER-002 Safety supervisor firmware* *VER-004 Actuator control firmware* *VER-009 Cliff safe stop*
SYS-SAFE-012	Battery protection independent of firmware	test	*VER-012 Battery protection*
SYS-SAFE-013	Safe stop held until cleared	test analyze	*VER-002 Safety supervisor firmware* *VER-009 Cliff safe stop*

6 Module verification

Module requirements are the budgets that RVC-SDS-001 allocates to the modules. They are verified in the same cases as the system requirements they come from, with the module quantity measured separately, so that a failure at system level can be traced to the module that exceeded its budget.

ID	Module requirement	Derived from	Method	Verified by
BASE-001	Cliff sensing latency	SYS-SAFE-011	test analyze	*VER-009 Cliff safe stop*
BASE-002	Drive braking time	SYS-SAFE-011	test analyze	*VER-009 Cliff safe stop*
BASE-003	Base module mass	SYS-015	inspect analyze	*VER-010 Physical envelope*
BASE-004	Base module height	SYS-011	inspect analyze	*VER-010 Physical envelope*
BASE-005	Battery capacity	SYS-001	test	*VER-007 Docking and charging*

ID	Module requirement	Derived from	Method	Verified by
BASE-006	Charge current	SYS-016	test	*VER-007 Docking and charging*
BIN-001	Dust bin mass	SYS-015	inspect analyze	*VER-010 Physical envelope*
FW-001	Safety supervisor deadline	SYS-SAFE-011	test	*VER-002 Safety supervisor firmware*
HAR-001	Wiring harness mass	SYS-015	inspect analyze	*VER-010 Physical envelope*
PCB-001	Drive disable latency	SYS-SAFE-011	test analyze	*VER-009 Cliff safe stop*
PCB-002	Main board mass	SYS-015	inspect analyze	*VER-010 Physical envelope*
TOP-001	Top module height	SYS-011	inspect analyze	*VER-010 Physical envelope*
TOP-002	Top module mass	SYS-015	inspect analyze	*VER-010 Physical envelope*

7 Validation

Validation asks whether the robot is the product a household needs. It is planned against the customer requirements, not the system requirements: a robot can meet every system requirement and still disappoint, if a requirement was derived wrongly or a need was missed.

Validation cases are therefore run by households in homes, with production-representative robots and without the development team steering the outcome. Most are demonstrations: the acceptance criterion is what the household experienced, not a measured limit.

7.1 Validation cases

ID	Case	Method	Activity and acceptance criterion	Validates
VAL-001	Whole-home mission	demo	A household starts a mission from the application in each of three reference homes and lets the robot finish. Accepted when the whole reachable floor is cleaned in one run in every home, including under furniture and across thresholds, and the household could follow progress in the application.	USR-001 USR-003 USR-004 USR-006 USR-009
VAL-002	Two weeks unattended	demo	The robot runs a daily scheduled mission for two weeks in an occupied home without the development team present. Accepted when it was ready for every mission without help, and the household emptied the dust bin at most once per run and without tools.	USR-002 USR-008
VAL-003	Household safety walkthrough	demo inspect	The robot runs in a home with stairs, pets, cables and children's toys while an independent safety assessor observes, and the assessor reviews the hazard analysis. Accepted when no fall, harmful collision or entanglement occurs and the assessor has no open finding.	USR-SAFE-001

ID	Case	Method	Activity and acceptance criterion	Validates
VAL-004	Privacy review	inspect	A privacy reviewer inspects the data the robot and the application store and transmit during normal use. Accepted when the home map stays on the robot unless the household gave consent in the application.	USR-005
VAL-005	Living with the robot	demo	A panel of ten households uses the robot for a week and answers a structured questionnaire. Accepted when at least eight can hold a conversation in the room while it cleans and can carry it between floors in one hand.	USR-007 USR-010

7.2 Validation matrix

Every customer requirement of RVC-CRS-001 with the validation case that covers it.

ID	Customer requirement	Method	Validated by
USR-001	Whole-home cleaning in one run	demo	*VAL-001 Whole-home mission*
USR-002	Unattended docking and charging	demo	*VAL-002 Two weeks unattended*
USR-003	Reliable navigation at home	demo	*VAL-001 Whole-home mission*
USR-004	Mission progress and fault feedback	demo	*VAL-001 Whole-home mission*
USR-005	Privacy of the home map	inspect	*VAL-004 Privacy review*
USR-006	Cleaning under furniture	demo	*VAL-001 Whole-home mission*
USR-007	Quiet operation	demo	*VAL-005 Living with the robot*
USR-008	Easy routine maintenance	demo	*VAL-002 Two weeks unattended*
USR-009	Thresholds between rooms	demo	*VAL-001 Whole-home mission*
USR-010	Carrying between floors	demo	*VAL-005 Living with the robot*
USR-SAFE-001	Safe operation in the household	demo inspect	*VAL-003 Household safety walkthrough*

8 Status and open points

No verification or validation case has been run for this revision. No requirement is claimed as verified, and no customer requirement as validated.

The model holds the plan: cases, methods, subjects and the requirements each case covers. It does not hold results. When cases are run, their results are to be recorded against the case and the configuration under test, and reported in a verification report, which is not part of this revision.

Open points:

- The reference home and the cliff rig are to be built; their designs are not part of this revision.
- The pass criteria for coverage and docking use repeated runs; the number of runs is a first estimate and is to be confirmed with a statistical argument.
- The analysis inputs of RVC-SDS-001 are estimates. A case that uses analysis is not passed until its inputs are measured values.
- The household panel for VAL-005 is to be recruited, and its questionnaire to be written.