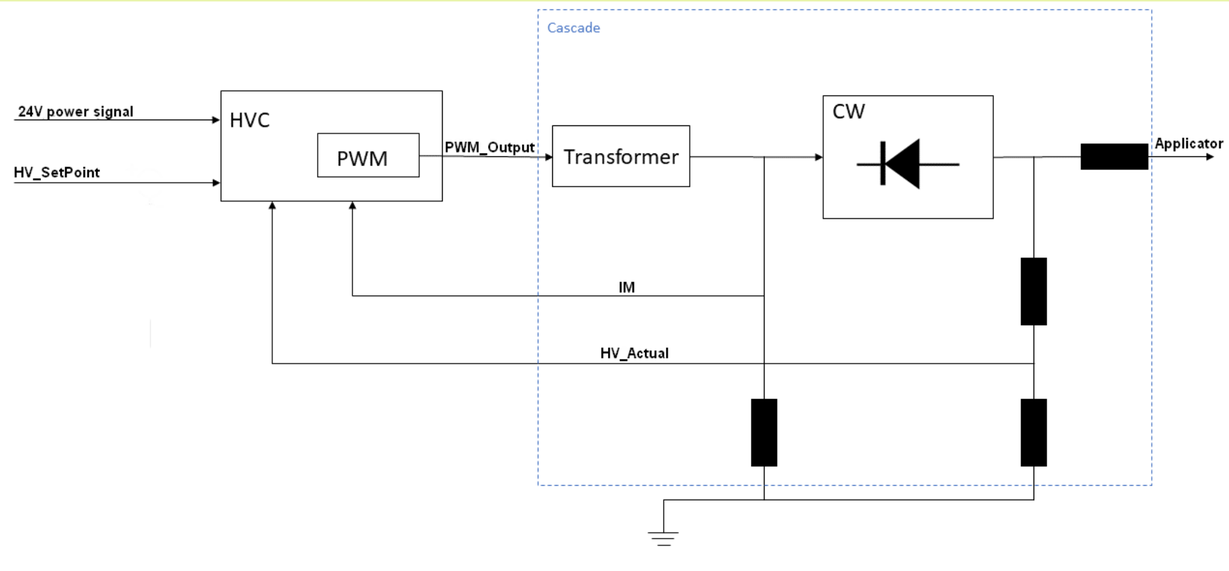
Yvonne Murray, Pedro Ribeiro, David A. Anisi,
Martin Sirevåg and Morten Mossige

Safety Assurance of an Industrial Robotic Control System Using Hardware/Software Co-Verification

Background

As a general trend in industrial robotics, an increasing number of safety functions are being developed or re-engineered to be handled in software rather than by physical hardware. This trend reinforces the importance of supplementing traditional, input-based testing with formal verification and model-checking methods. To this end, our use-case focuses on safety assurance of a high voltage controller (HVC) used in an industrial painting robot from ABB, by the use of hardware/software co-verification.



Block diagram of one part of the paint robot, containing the HVC.

Properties of Interest

- P1: **HV_Actual** should converge to the reference value **HV_SetPoint**
- P2: **PWM_Output** is set to 0 whenever the 24V power signal is off
- P3: **mSetPoint**, an internal representation of the setpoint, is set to 0 when the 24V power signal is switched off
- P4: The software is deadlock free

Properties **P2-P4** are properties of the software, while **P1** is a system property.

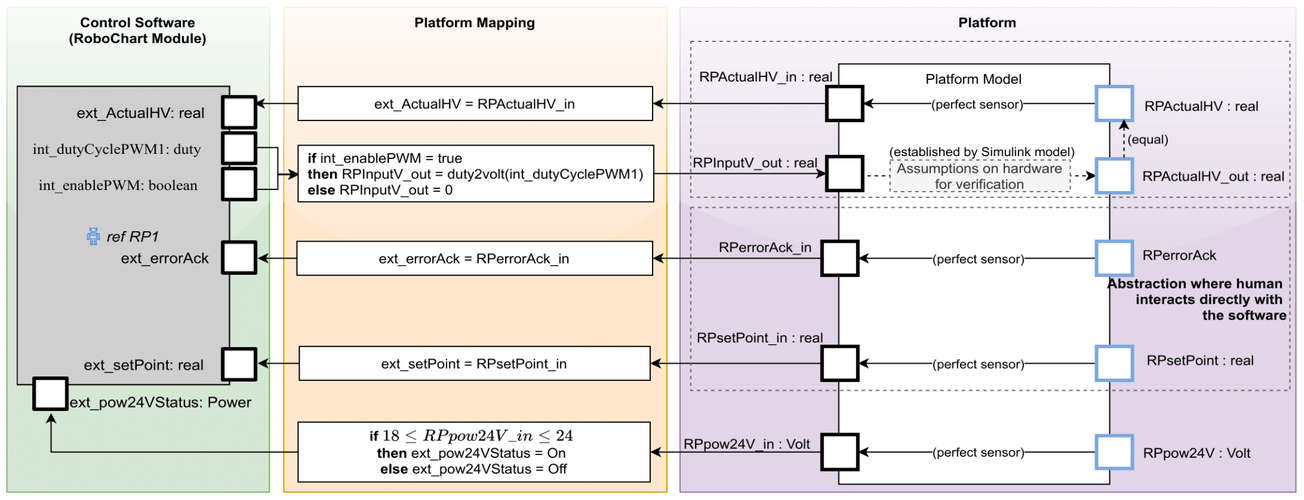
Verification Approach

Verification of **P1** requires:

- Models of the software and hardware
- A formal specification for **P1**

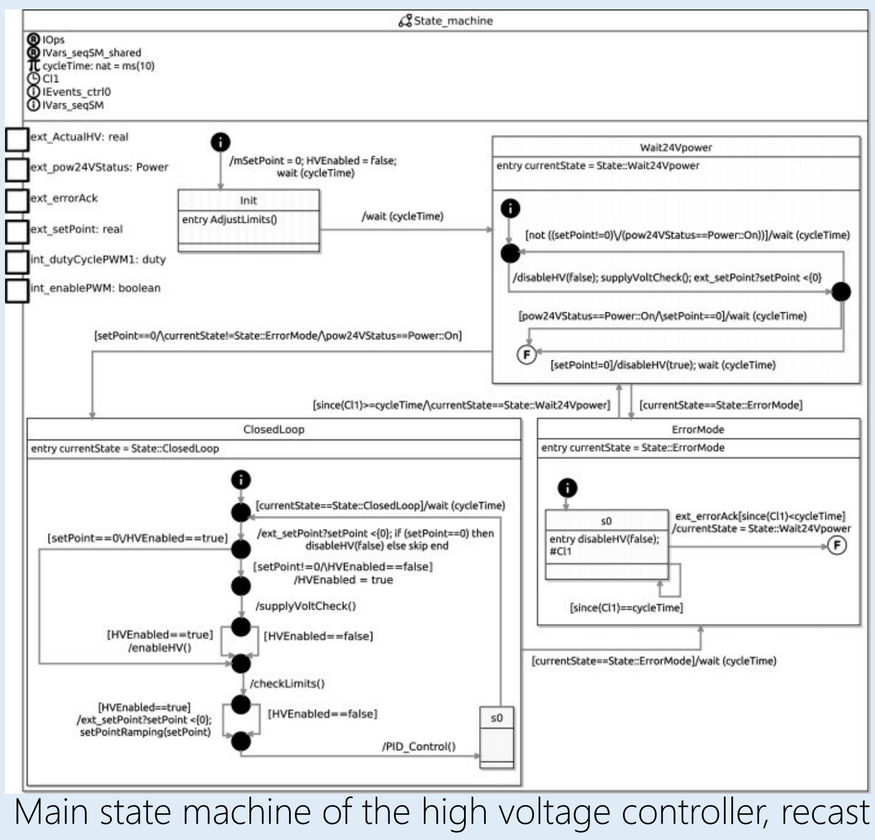
Our co-verification approach is as follows:

1. Software is modelled in RoboChart and hardware in Simulink.
2. Connection between models is defined via platform mapping.
3. Property **P1** is stated over inputs/outputs of system in tock-CSP.
4. Property **P1**$_{HW}$ of the hardware, needed to establish **P1**, is verified in Simulink.
5. Then, using the above construction, **P1** is checked in FDR

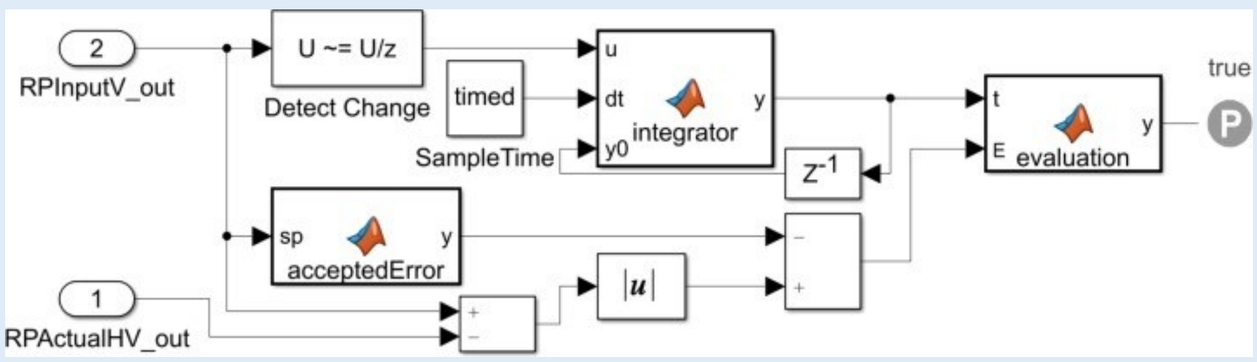


Co-verification framework, with arrows indicating the direction of the information flow between inputs and outputs, of the software and hard-

Modelling and Results



Main state machine of the high voltage controller, recast in RoboChart



SDV implementation of the PWM hardware convergence property, **P1**$_{HW}$

Property	Result	Elapsed Time			Complexity	
		Compilation	Verification	Total	States	Transitions
P1	PASS	1456s	1394s	2850s	126,481,225	517,333,656
P2	PASS	1456s	247s	1703s	1,460,749	3,855,659
P3	PASS	1539s	248s	1787s	1,452,829	3,831,246
P4	PASS	1253s	334s	1587s	1,920,070	5,795,521

Verification results using FDR model checker.

robostar.cs.york.ac.uk
University of York
UiA
Norwegian University of Life Sciences
ABB
UKRI Engineering and Physical Sciences Research Council