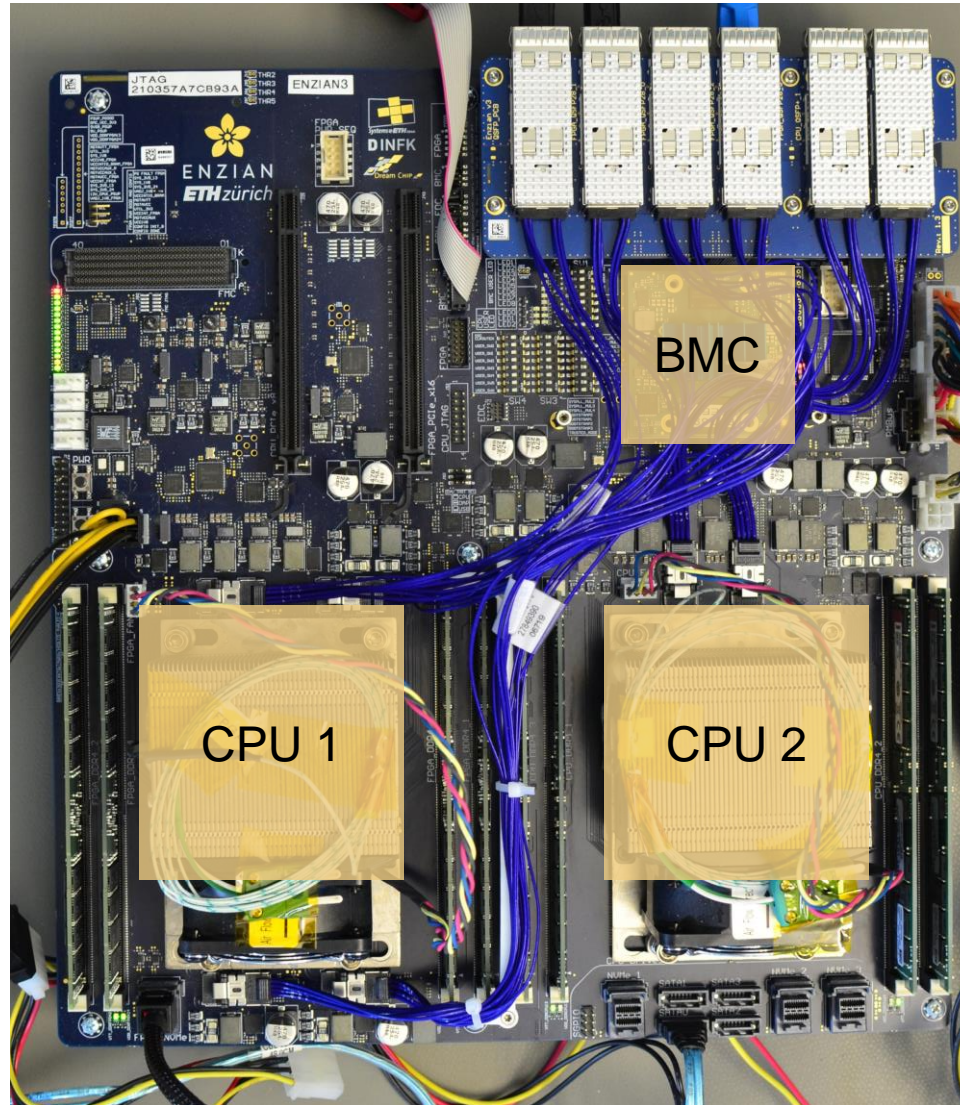


# Trustworthy Board Management Software

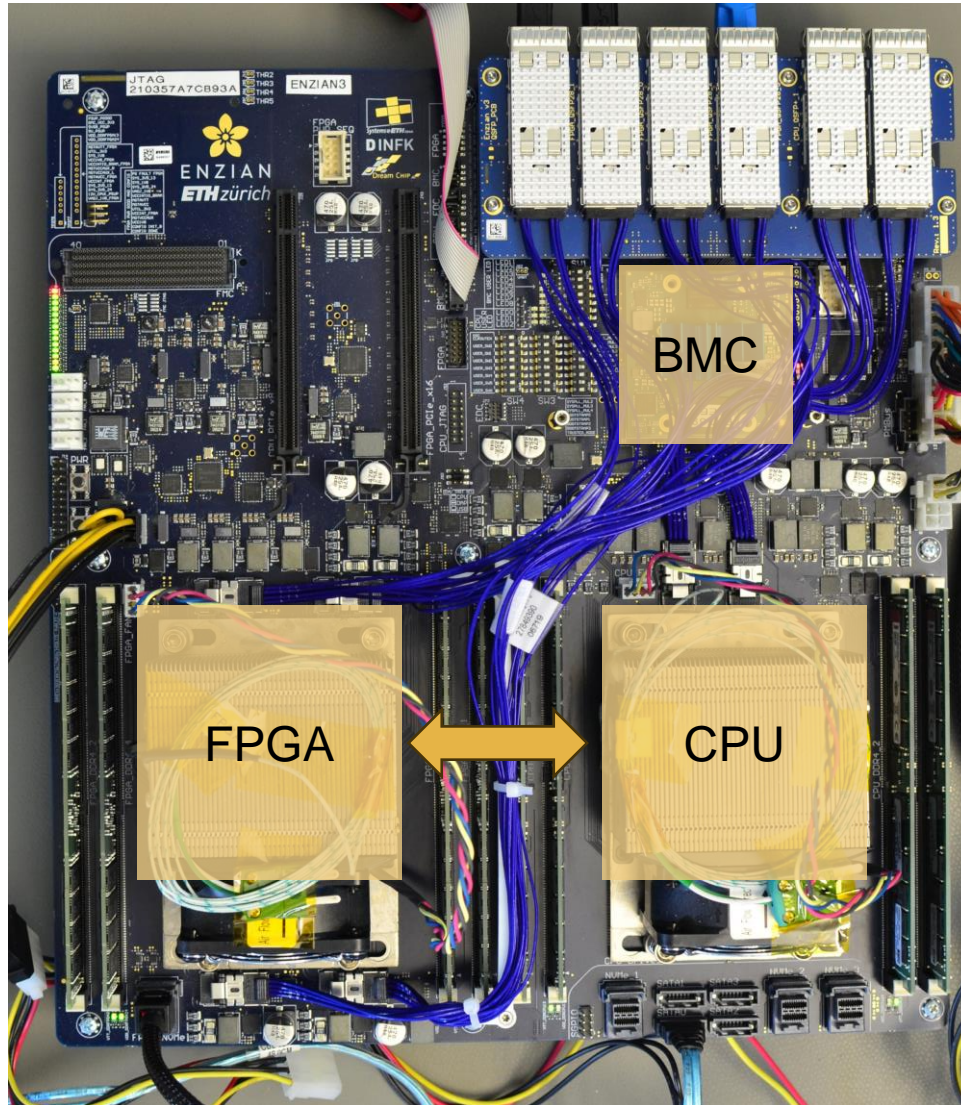
Daniel Schwyn, Ben Fiedler, David Cock, Michael Giardino, Timothy Roscoe, et al.  
Systems Group @ ETH Zürich



# The Computer in the Computer



# The Computer in the Computer



# State of the Art – Closed source



?

BMC Hardware

... and buggy

**NIST** ☰ NVD MENU

Information Technology Laboratory

**NATIONAL VULNERABILITY DATABASE**

**NIST** ☰ NVD MENU

**NIST** ☰ NVD MENU

Information Technology Laboratory

**NATIONAL VULNERABILITY DATABASE**

**NVD**

**NVD**

☰ NVD MENU

**NVD**

VULNERABILITIES

**NIST**

Information Technology Laboratory

**NATIONAL VULNERABILITY DATABASE**

VULNERABILITIES

### CVE-2022-22374

#### Current Description

BMC firmware (IBM Power 9 AC922 OP910, OP920, OP930, and OP940) may be subject to a firmware downgrade attack which may affect its ability to operate its host. IBM X-Force ID: 221442.

VULNERABILITIES

[+View Analysis Description](#)

#### Severity

CVSS 3.x Severity



Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H



Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H

### CVE-2021-2025

#### Current Description

A flaw was found in Red Hat Satellite password through the API to an aut view\_hosts permission. The highest confidentiality and integrity as well

[+View Analysis Description](#)

#### Severity

CVSS Version



NIST: NVD

Base Score: 5.3 MEDIUM

Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L

### CVE-2022-22374 Detail

#### Current Description

The BMC (IBM Power 9 AC922 OP910, OP920, OP930, and OP940) may be subject to a firmware downgrade attack which may affect its ability to operate its host. IBM X-Force ID: 221442.

[+View Analysis Description](#)

#### Severity

CVSS Version 3.x

CVSS Version 2.0

##### CVSS 3.x Severity and Metrics:



NIST: NVD

Base Score: 9.1 CRITICAL

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H



CNA: IBM Corporation

Base Score: 6.5 MEDIUM

Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:H

#### QUICK INFO

##### CVE Dictionary Entry:

CVE-2022-22374

##### NVD Published Date:

03/24/2022

##### NVD Last Modified:

04/05/2022

##### Source:

IBM Corporation

#### QUICK INFO

##### CVE Dictionary Entry:

CVE-2020-8573

##### NVD Published Date:

06/29/2020

##### NVD Last Modified:

07/17/2020

##### Source:

NetApp, Inc.

ent  
int and  
During  
ndle 12.2.92  
tforms is  
e attackers

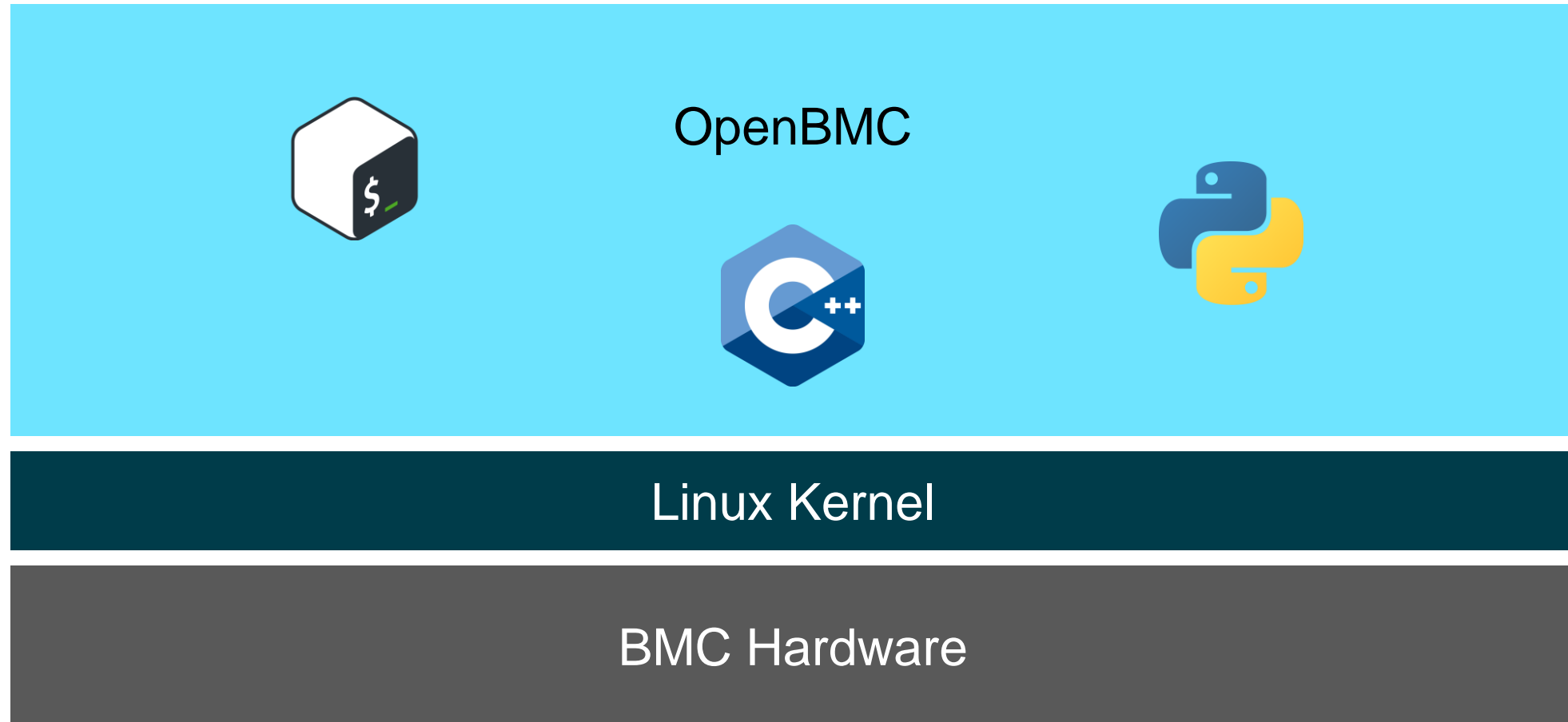
##### CVSS 3.x Severity and Metrics:



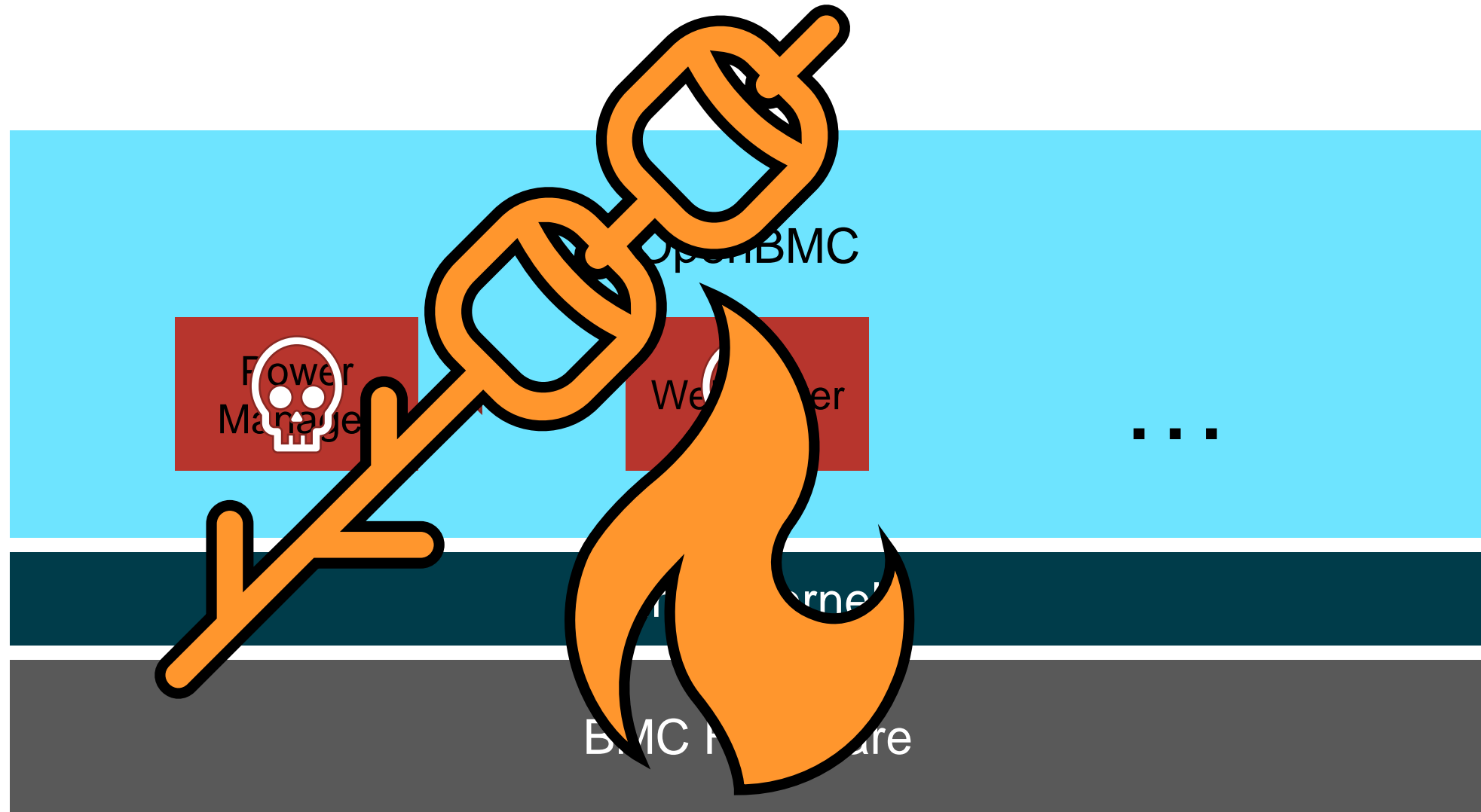
NIST: NVD

Base Score: 6.5 MEDIUM

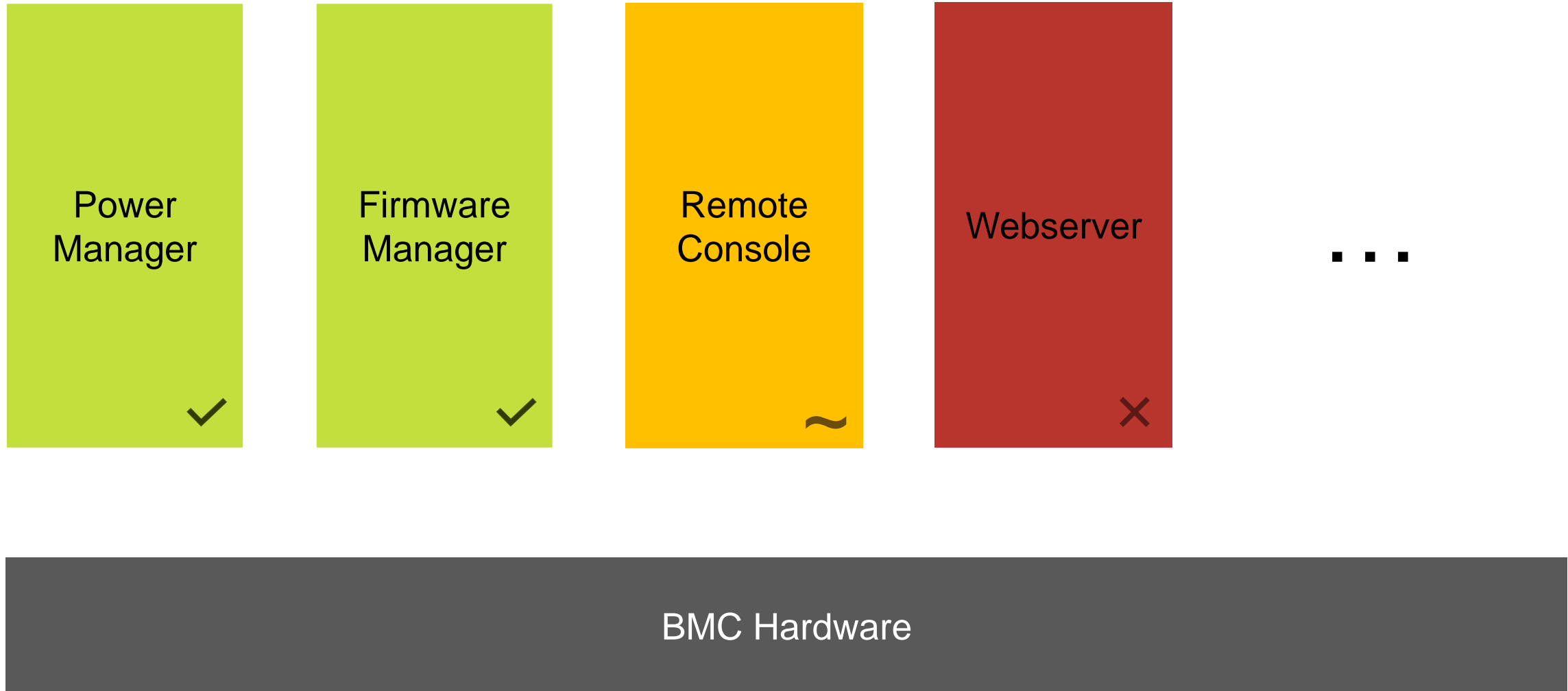
Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H



# State of the Art – Open Source

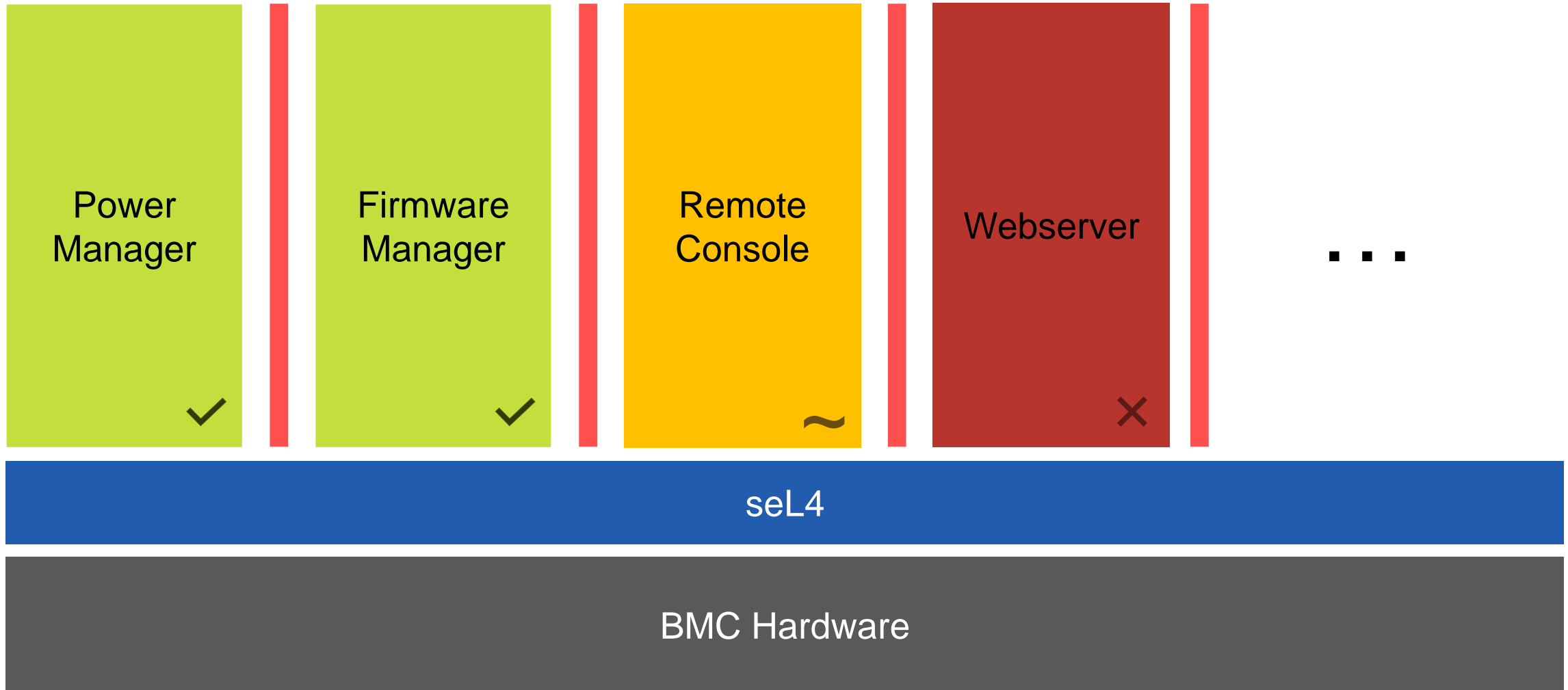


# Trust & Threat Model

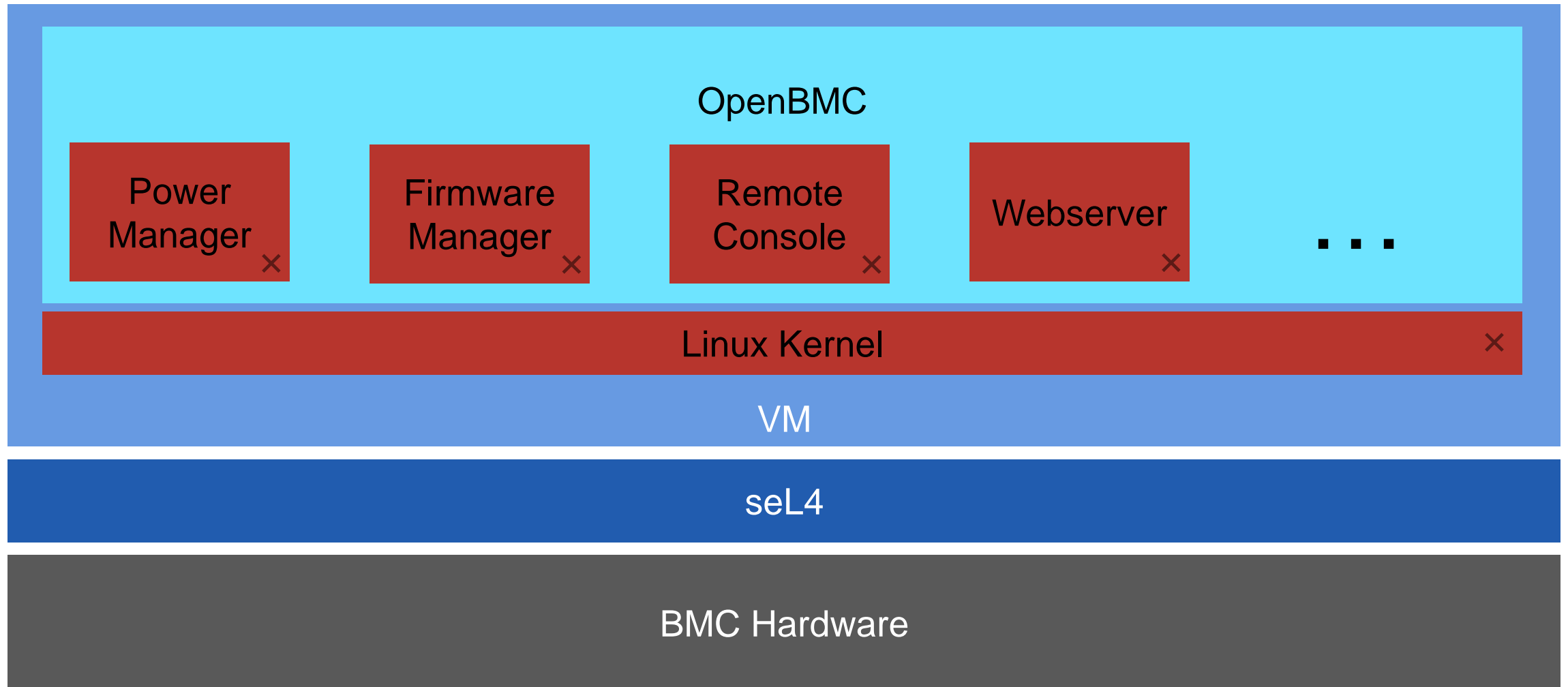




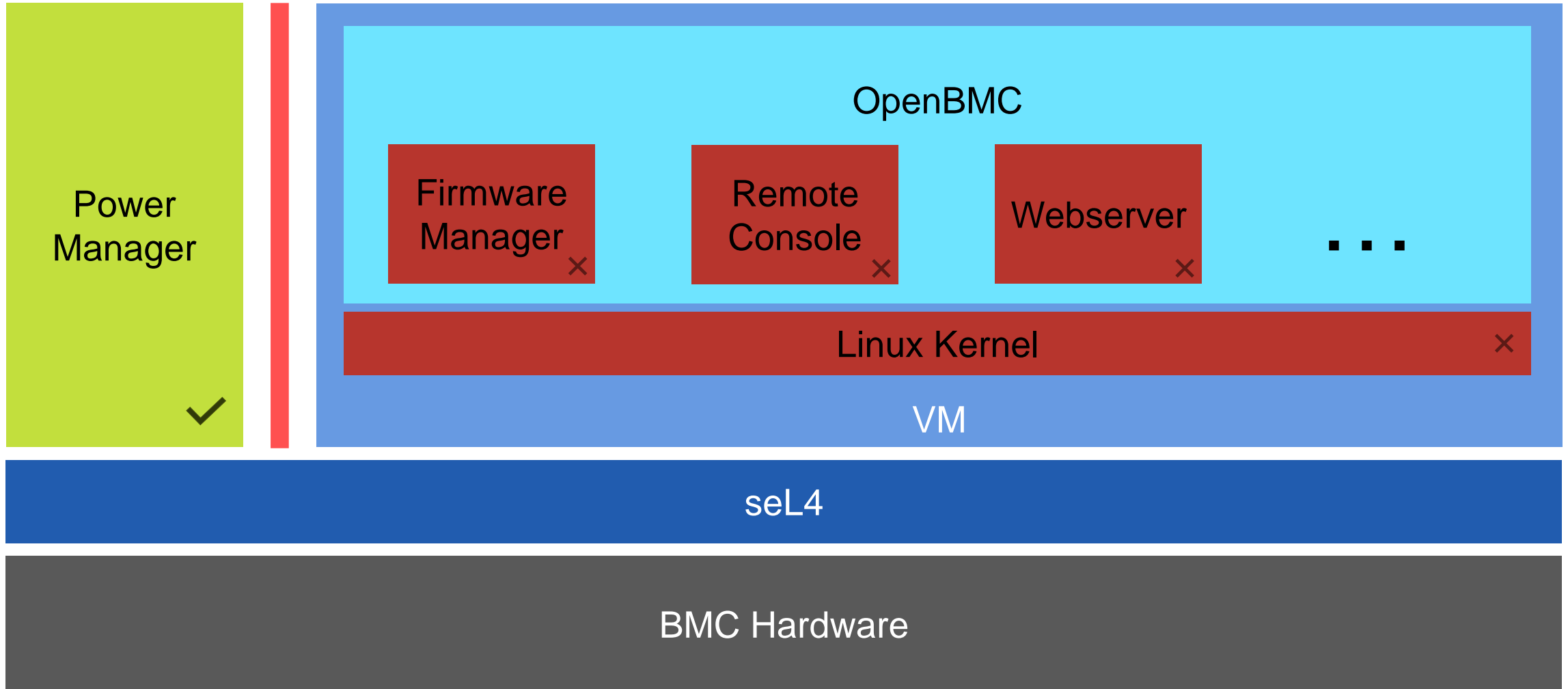
# Isolation: Confidentiality, Integrity, Availability



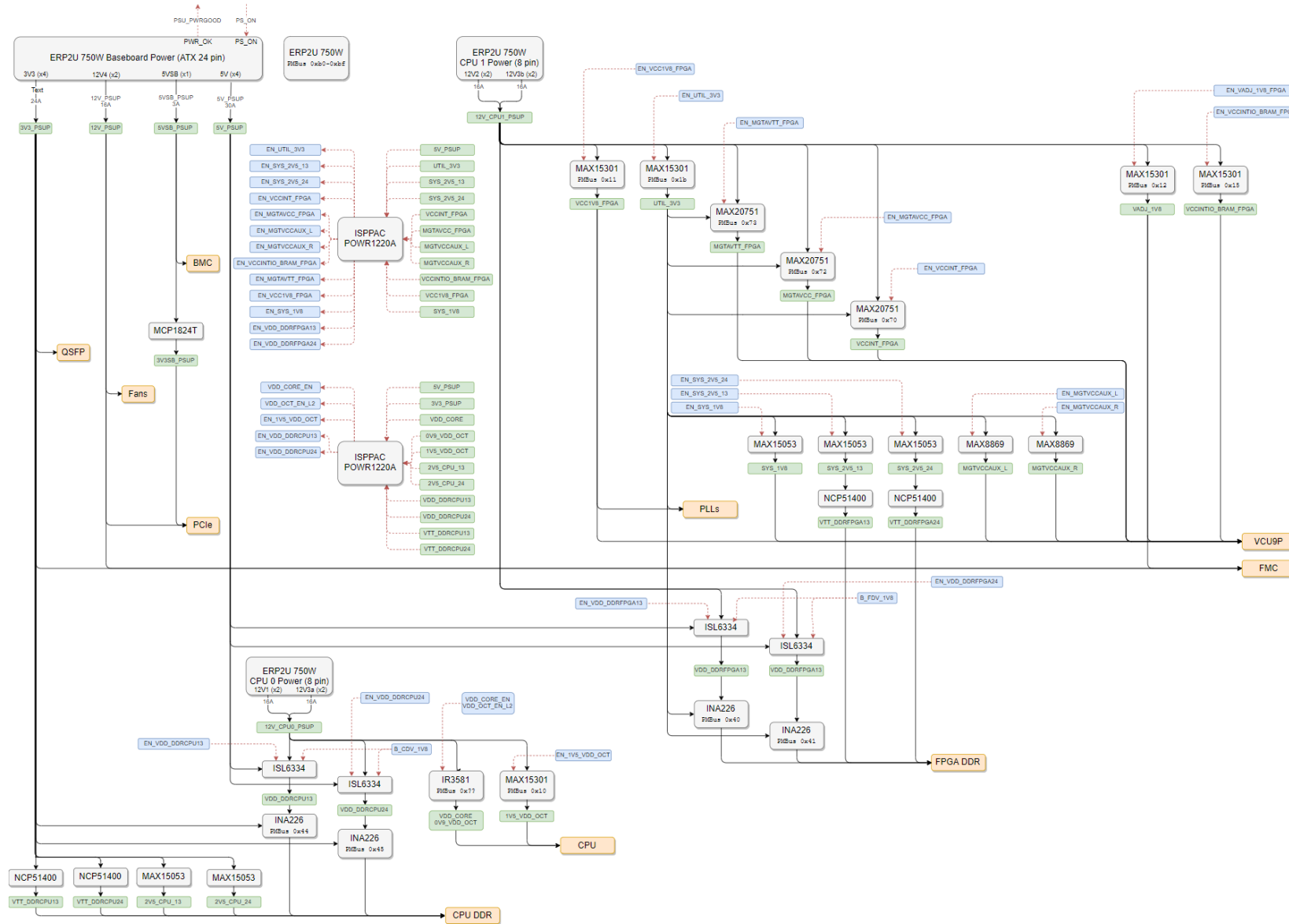
# Cyber Retrofit – Step 1



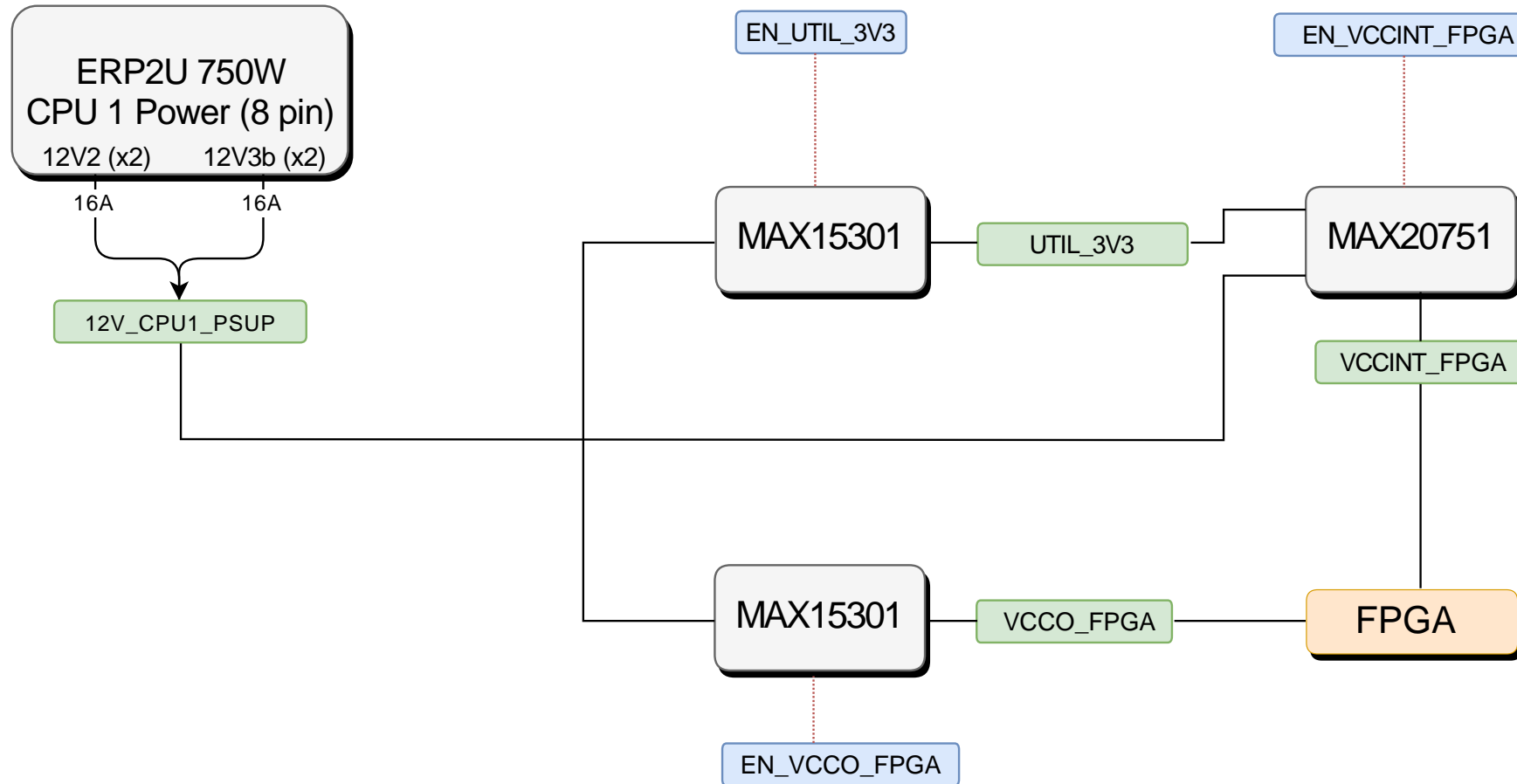
# Cyber Retrofit – Step 2



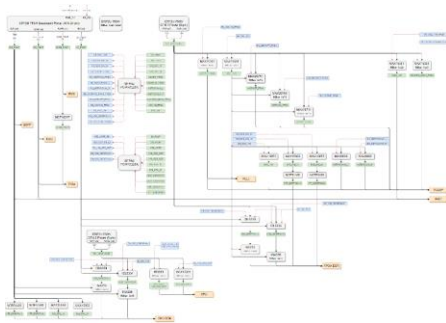
# Turning on computers is hard...



# Turning on computers is hard...



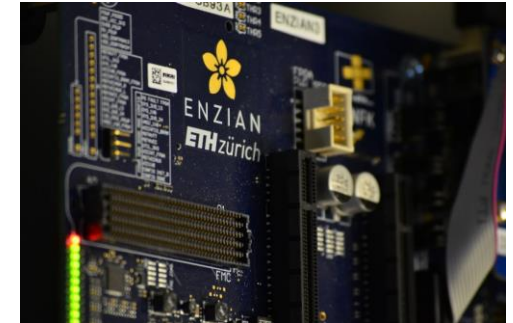
... and we need a more systematic approach!



SMT  
Solver



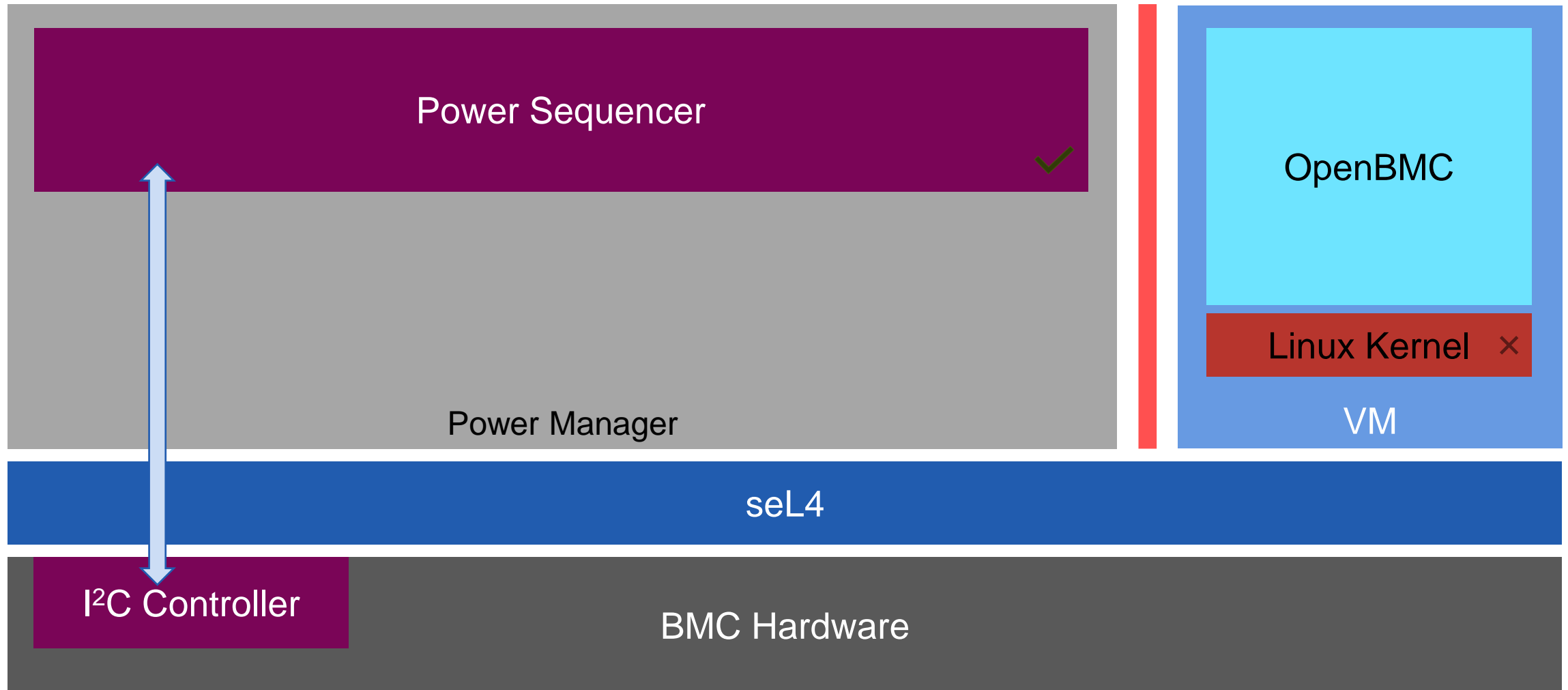
1. \_\_\_\_\_
2. \_\_\_\_\_
3. \_\_\_\_\_
4. \_\_\_\_\_
5. \_\_\_\_\_



- We can derive sequences efficiently (< 10s)
- Works on real hardware
- More confidence in power-up sequences
- Basis for rigorous specification of correct behavior

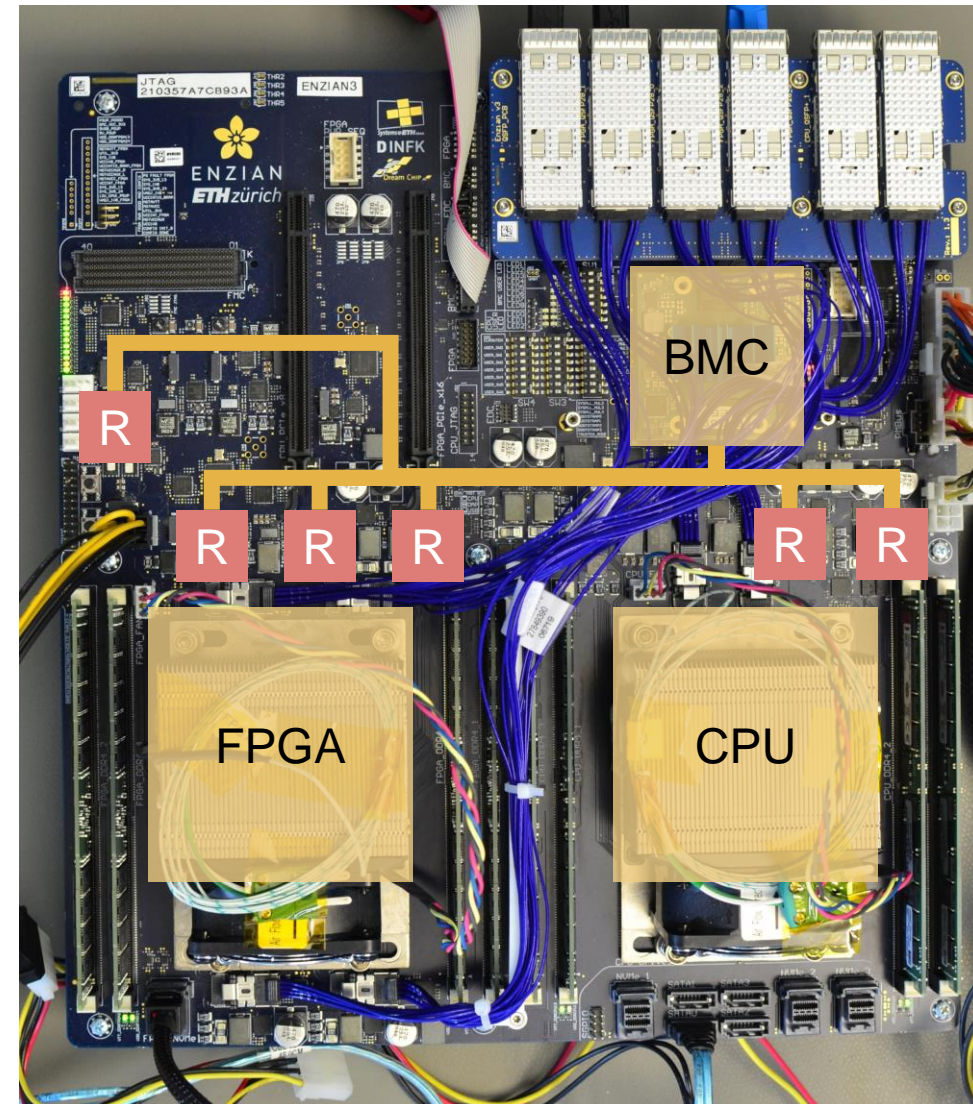
Jasmin Schult, Daniel Schwyn, Michael Giardino, David Cock, Reto Achermann, and Timothy Roscoe. 2021. Declarative Power Sequencing. ACM Trans. Embed. Comput. Syst. 20, 5s, Article 84

# Trustworthy Power Manager



# I<sup>2</sup>C

- Widespread, low-speed configuration bus
- Controls critical hardware components
- Devices implement the standard only partially or violate it



— I<sup>2</sup>C bus  
R regulator / sensor



# I<sup>2</sup>C Modelling Framework

Voltage Set Request



Controller

Voltage Set Action



Voltage  
Regulator

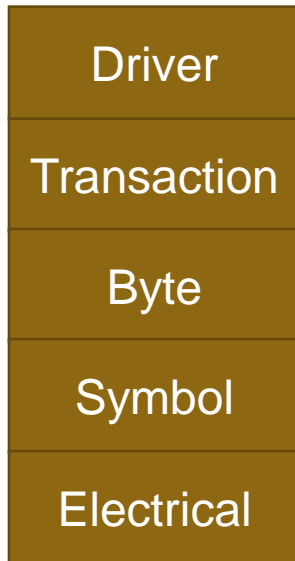


Other  
devices

Lukas Humbel, Daniel Schwyn, Nora Hossle, Roni Haecki, Melissa Licciardello, Jan Schaer, David Cock, Michael Giardino, Timothy Roscoe. 2021. A Model Checked I<sup>2</sup>C Specification. 27th International Symposium on Model Checking Software (SPIN 2021)

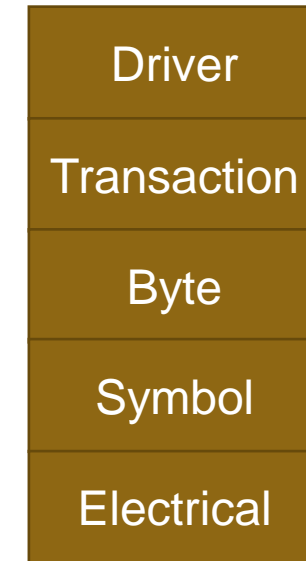
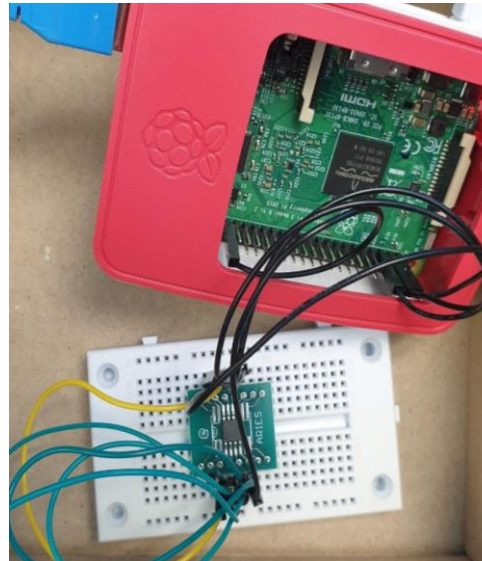
# I<sup>2</sup>C Modelling Framework

Voltage Set Request



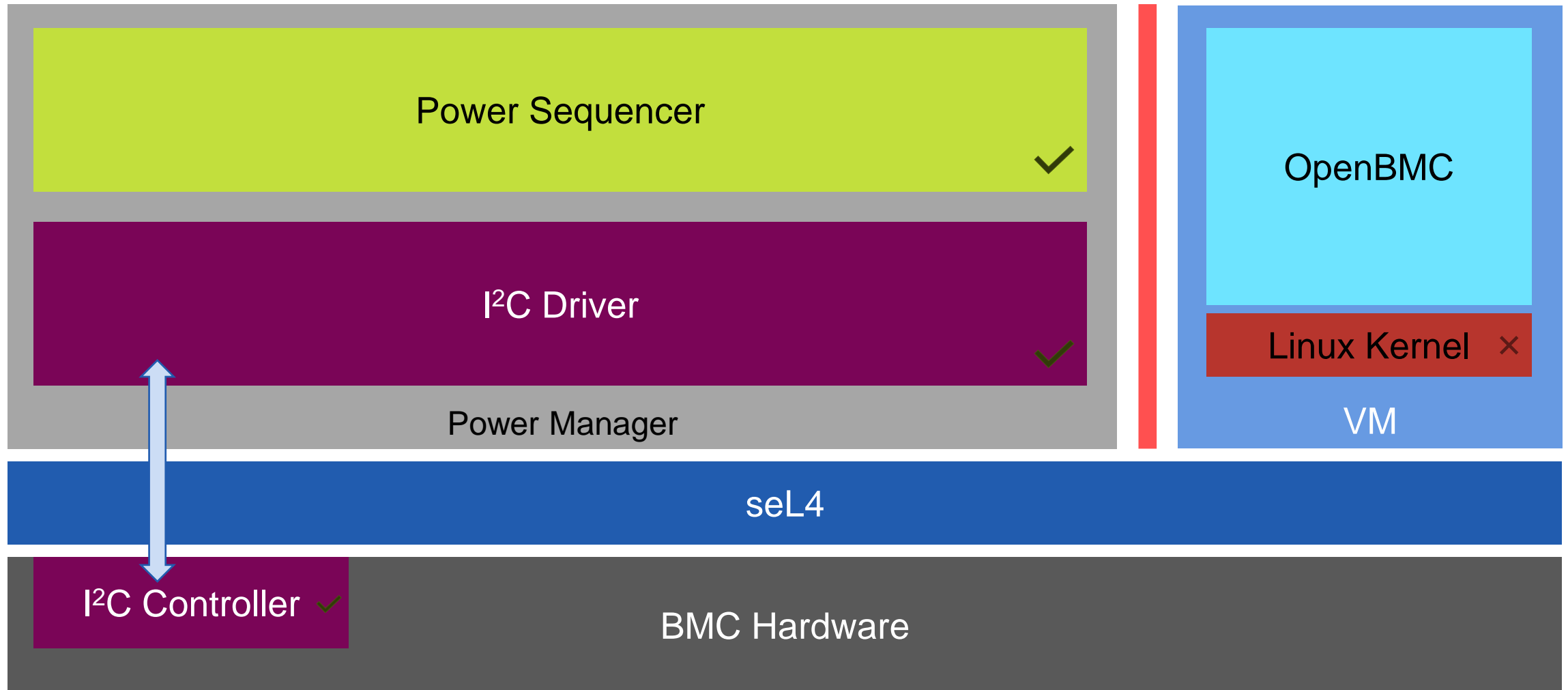
Voltage Set Action

Generated C Code running on actual hardware

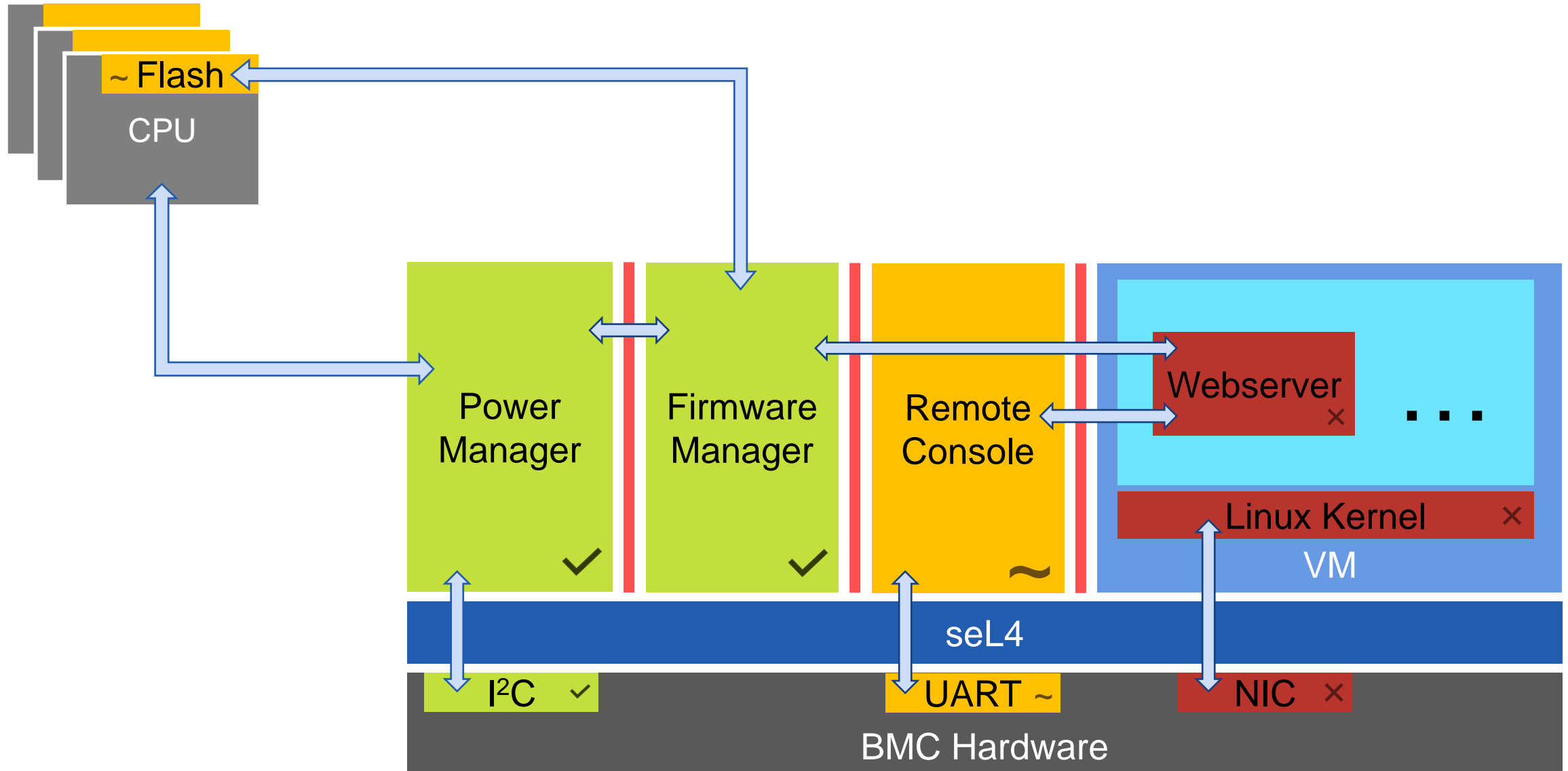


Lukas Humbel, Daniel Schwyn, Nora Hossle, Roni Haecki, Melissa Licciardello, Jan Schaer, David Cock, Michael Giardino, Timothy Roscoe. 2021. A Model Checked I<sup>2</sup>C Specification. 27th International Symposium on Model Checking Software (SPIN 2021)

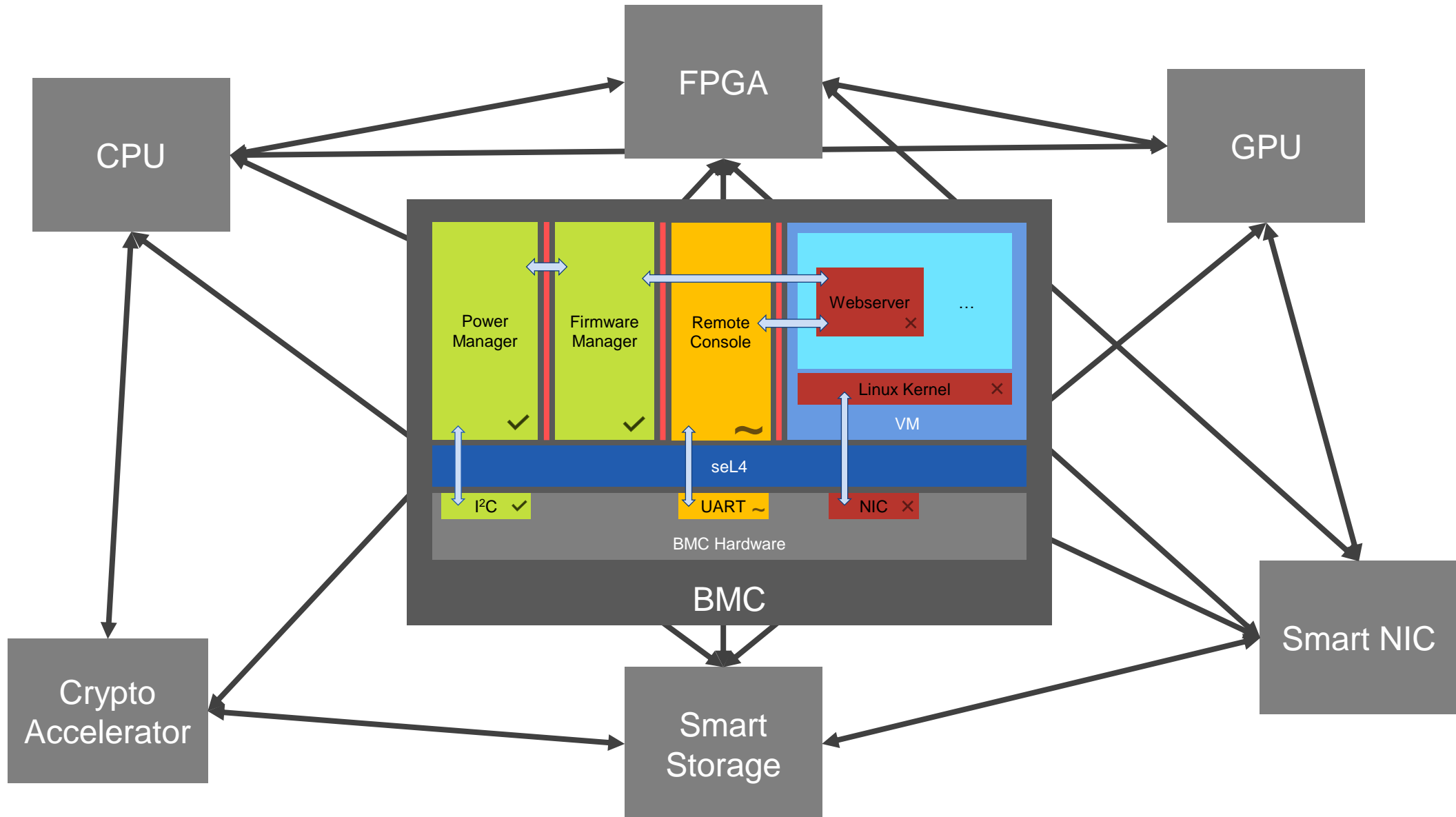
# Trustworthy Power Manager



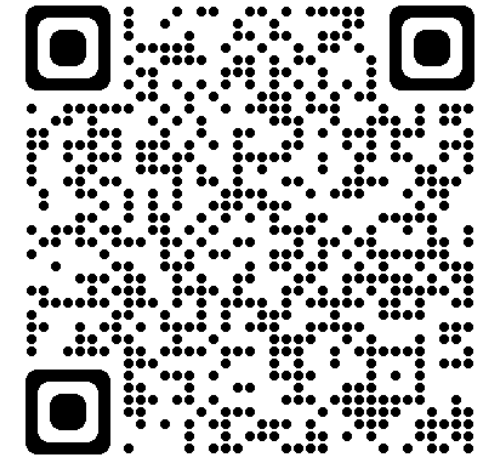
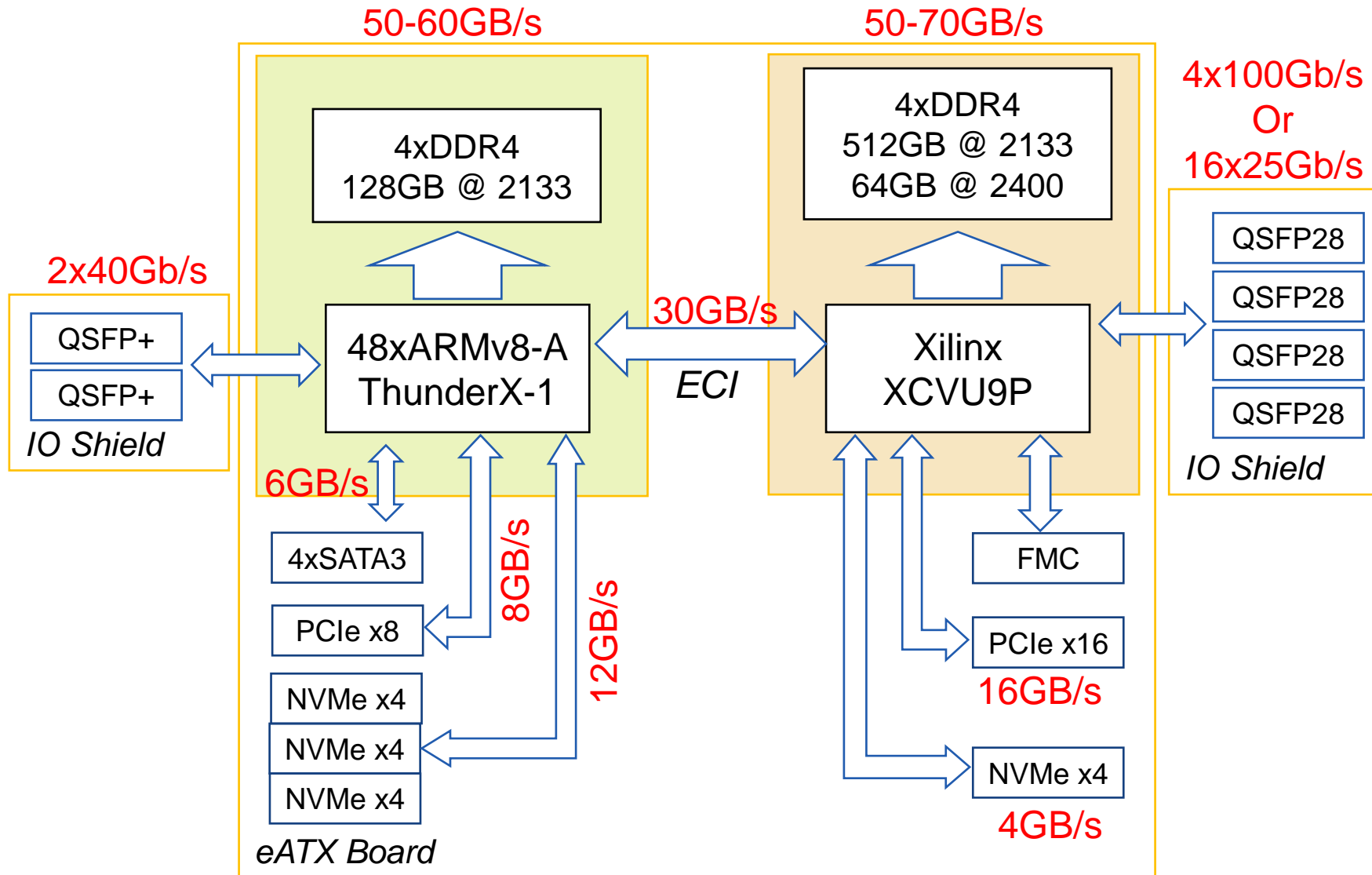
# Beyond Power Management



# Trustworthy BMCs are only the beginning...

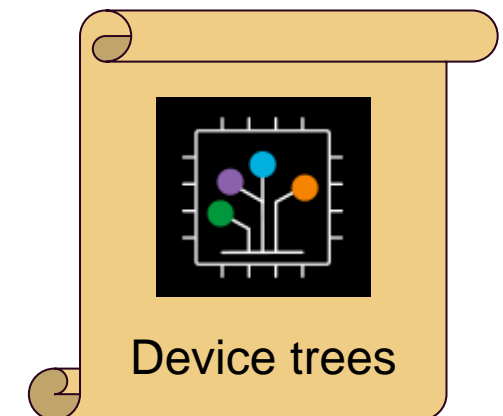
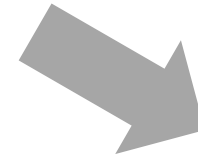
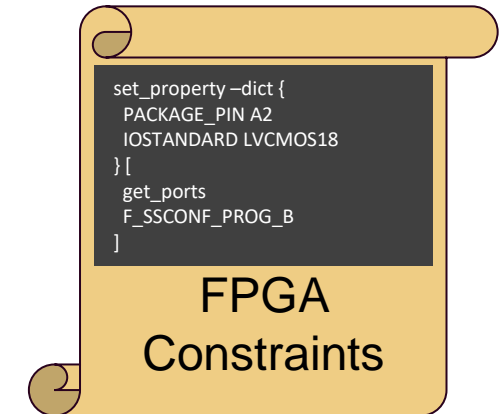
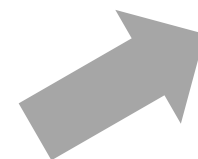
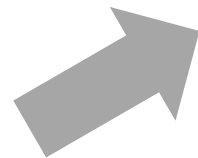
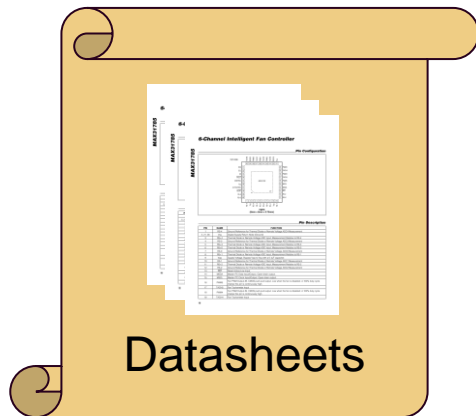
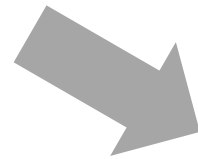
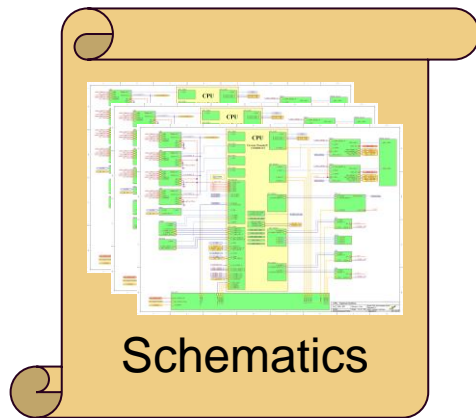


# The Enzian Research Computer

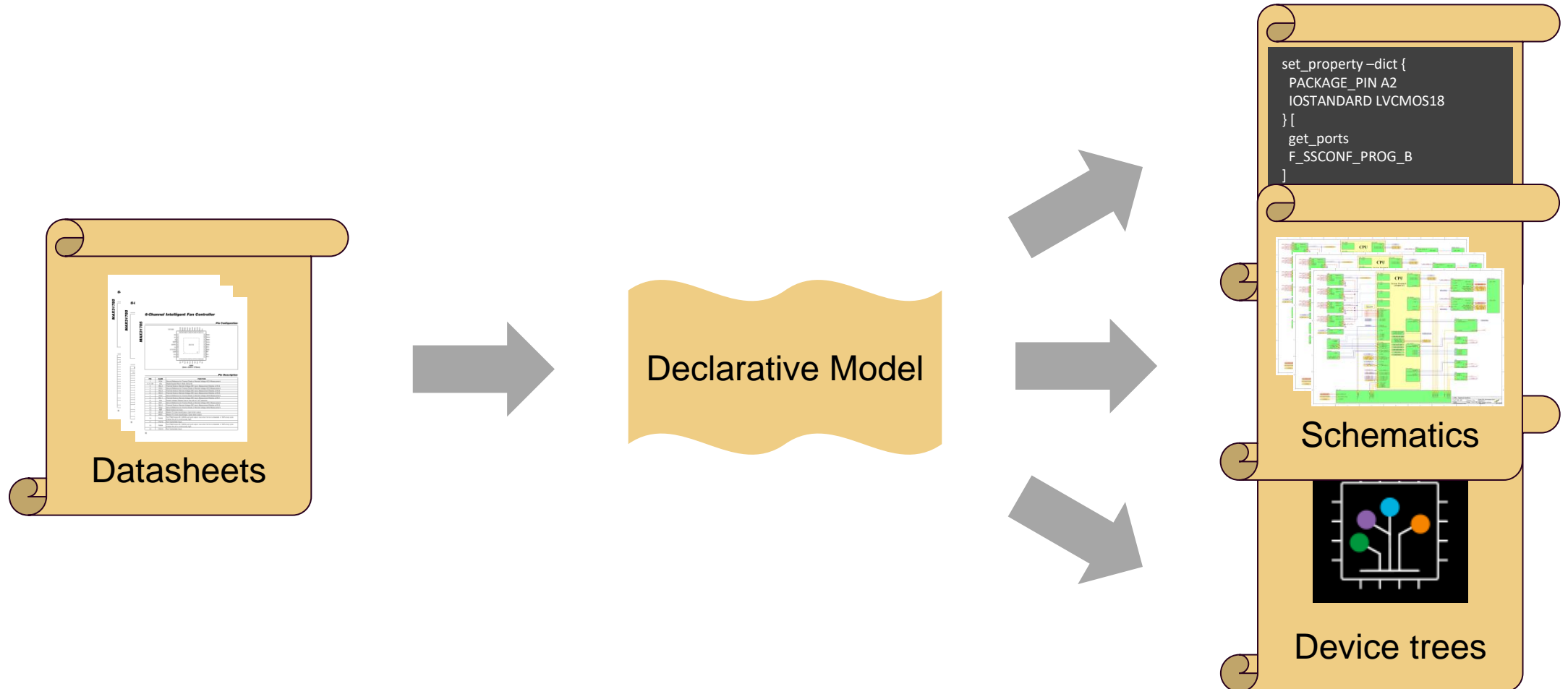


<https://enzian.systems>

# Ongoing Work – Hardware Model Applications

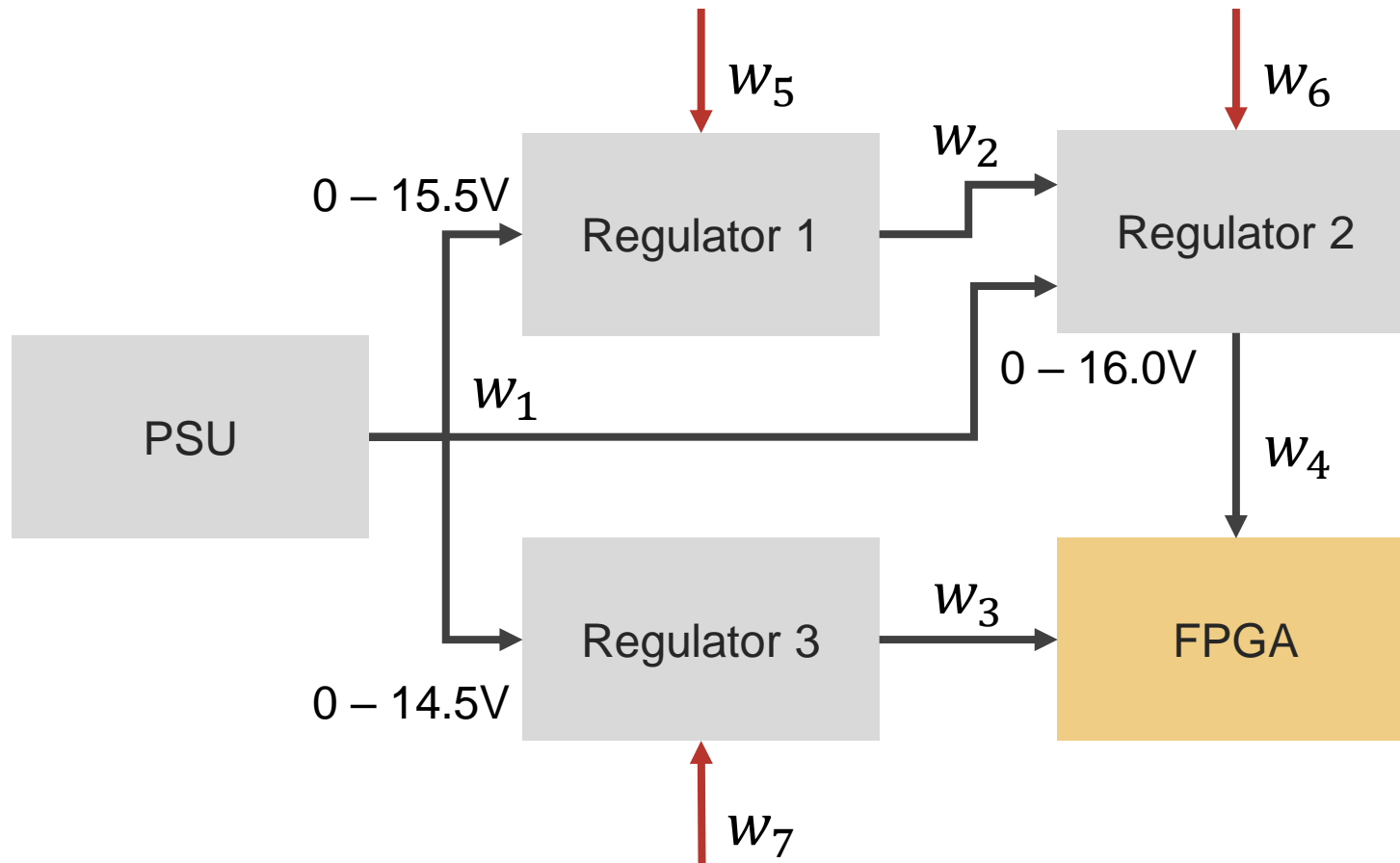


# Ongoing Work – Hardware Model Applications



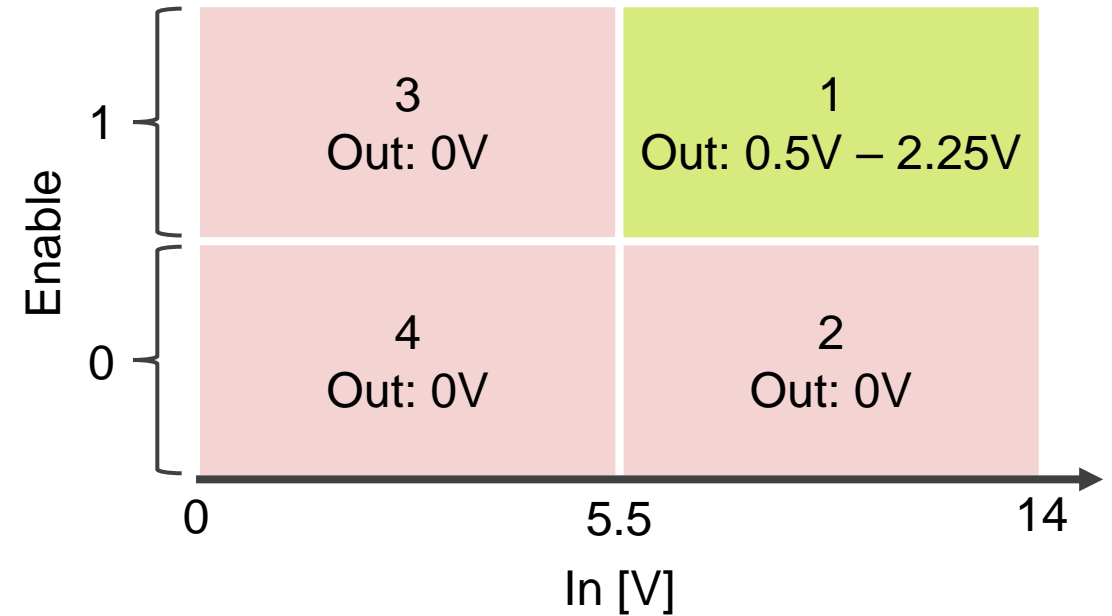
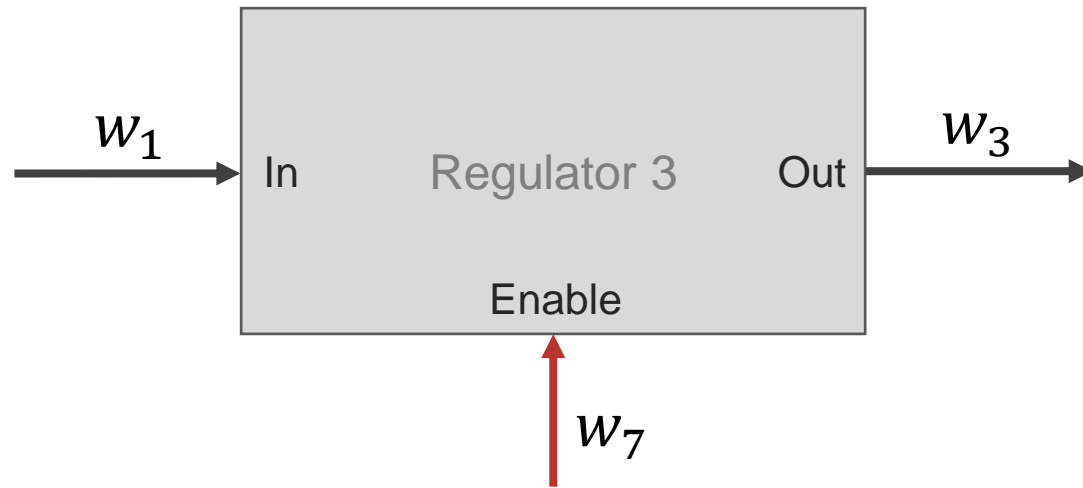


# Modelling the Topology: Directed Graph



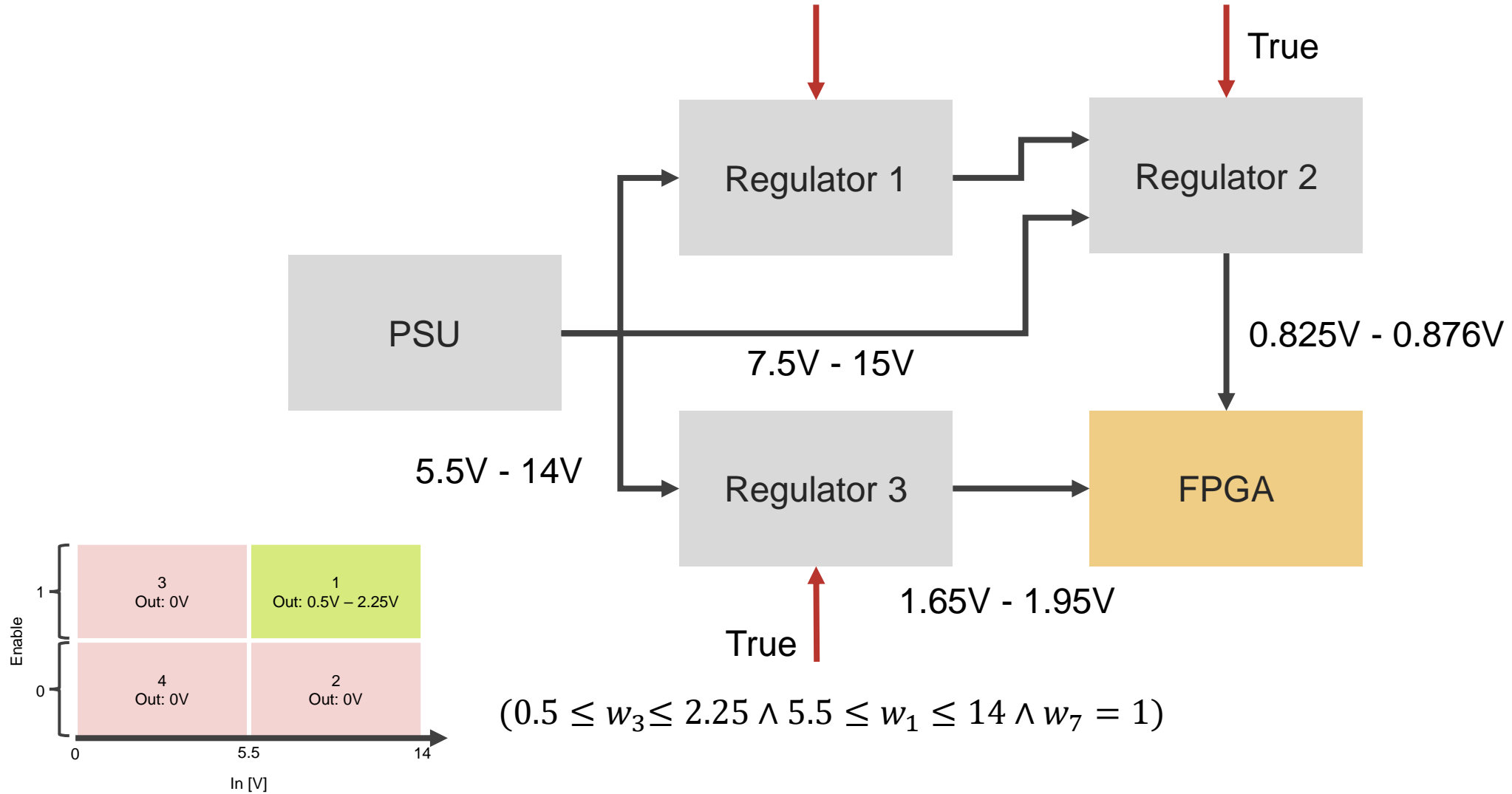
$$0 \leq w_1 \leq 15.5$$
$$0 \leq w_1 \leq 16.0$$
$$0 \leq w_1 \leq 14.5$$

# Modelling the Components: State Diagram

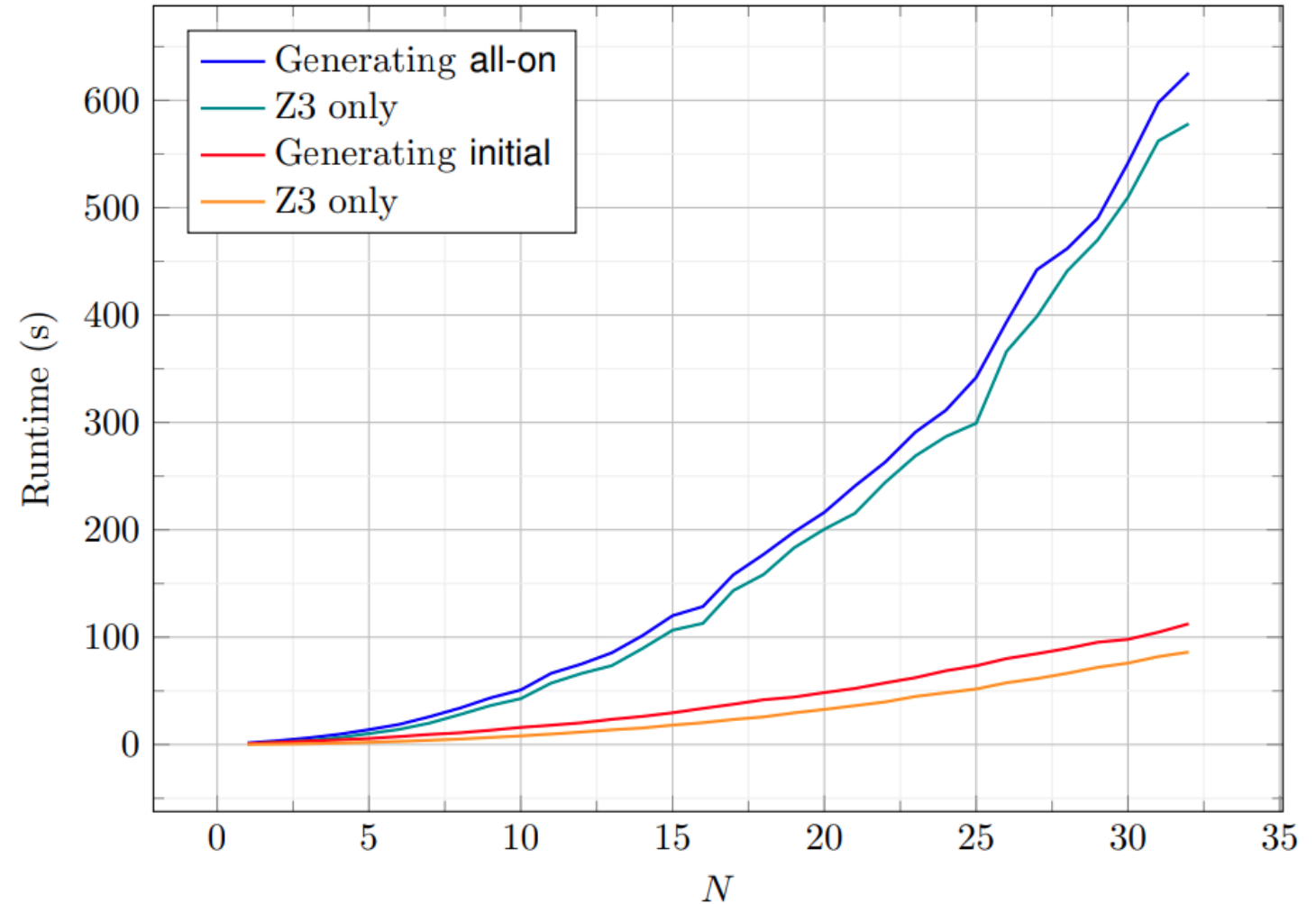
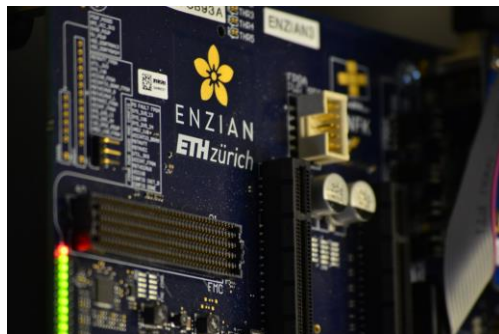


$$(0.5 \leq w_3 \leq 2.25 \wedge 5.5 \leq w_1 \leq 14 \wedge w_7 = 1)$$
$$\vee (w_3 = 0 \wedge 5.5 \leq w_1 \leq 14 \wedge w_7 = 0)$$
$$\vee (w_3 = 0 \wedge w_1 = 0 \wedge w_7 = 1)$$
$$\vee (w_3 = 0 \wedge w_1 = 0 \wedge w_7 = 0)$$

# Full Platform State: Propagate Constraints to the Root

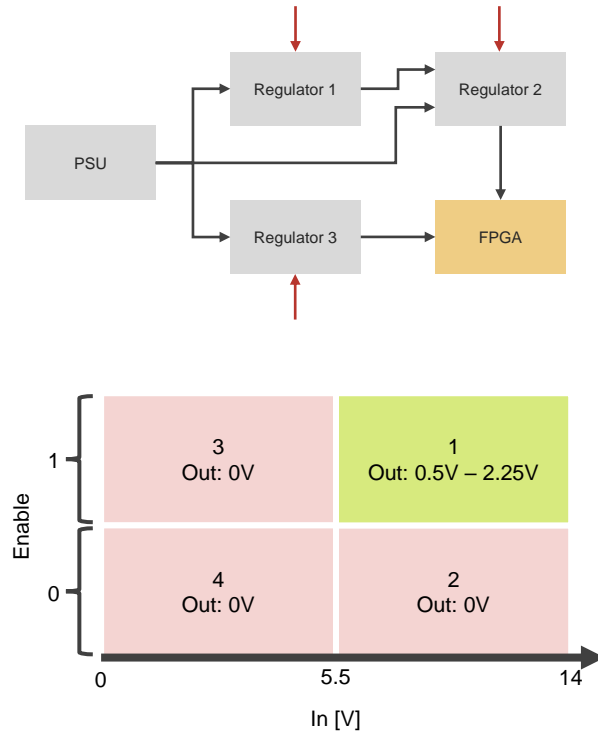


# Synthesizing Configurations from the Model is Practicable



Moritz Knüsel. 2021. Optimizing Declarative Power Sequencing. Master's Thesis, ETH Zürich

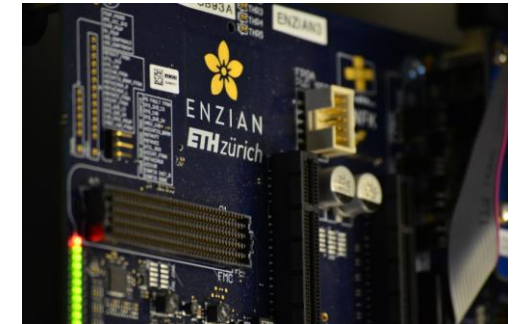
# Our work so far



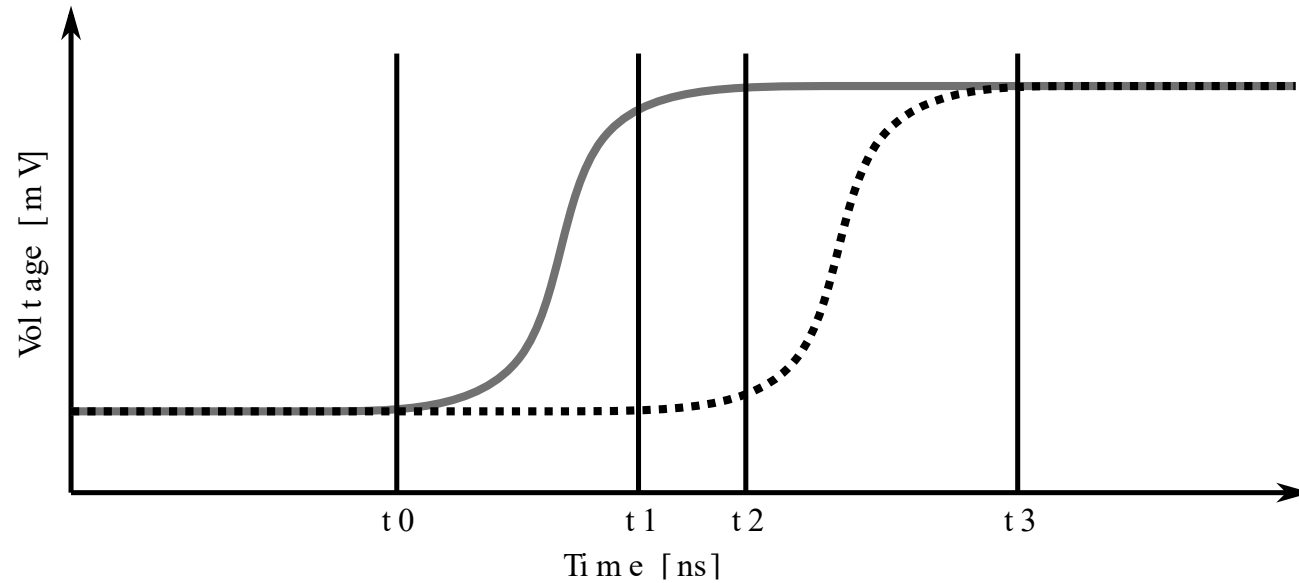
CSP Solver



1. \_\_\_\_\_
2. \_\_\_\_\_
3. \_\_\_\_\_
4. \_\_\_\_\_
5. \_\_\_\_\_



- More confidence in power sequences
- Better automation & maintainability
- Basis for rigorous specification

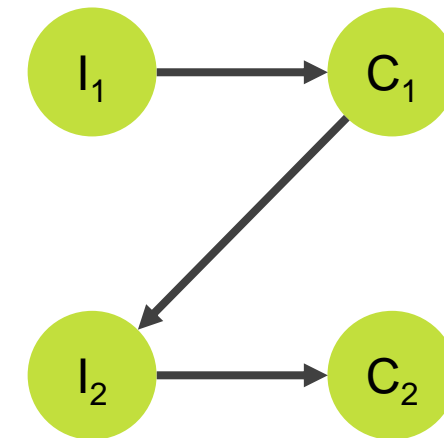


**Initiate event:**

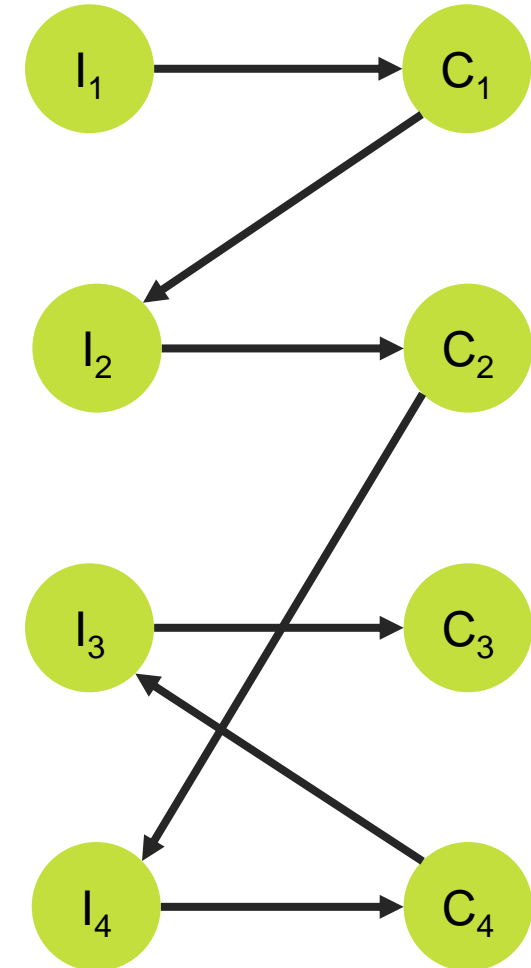
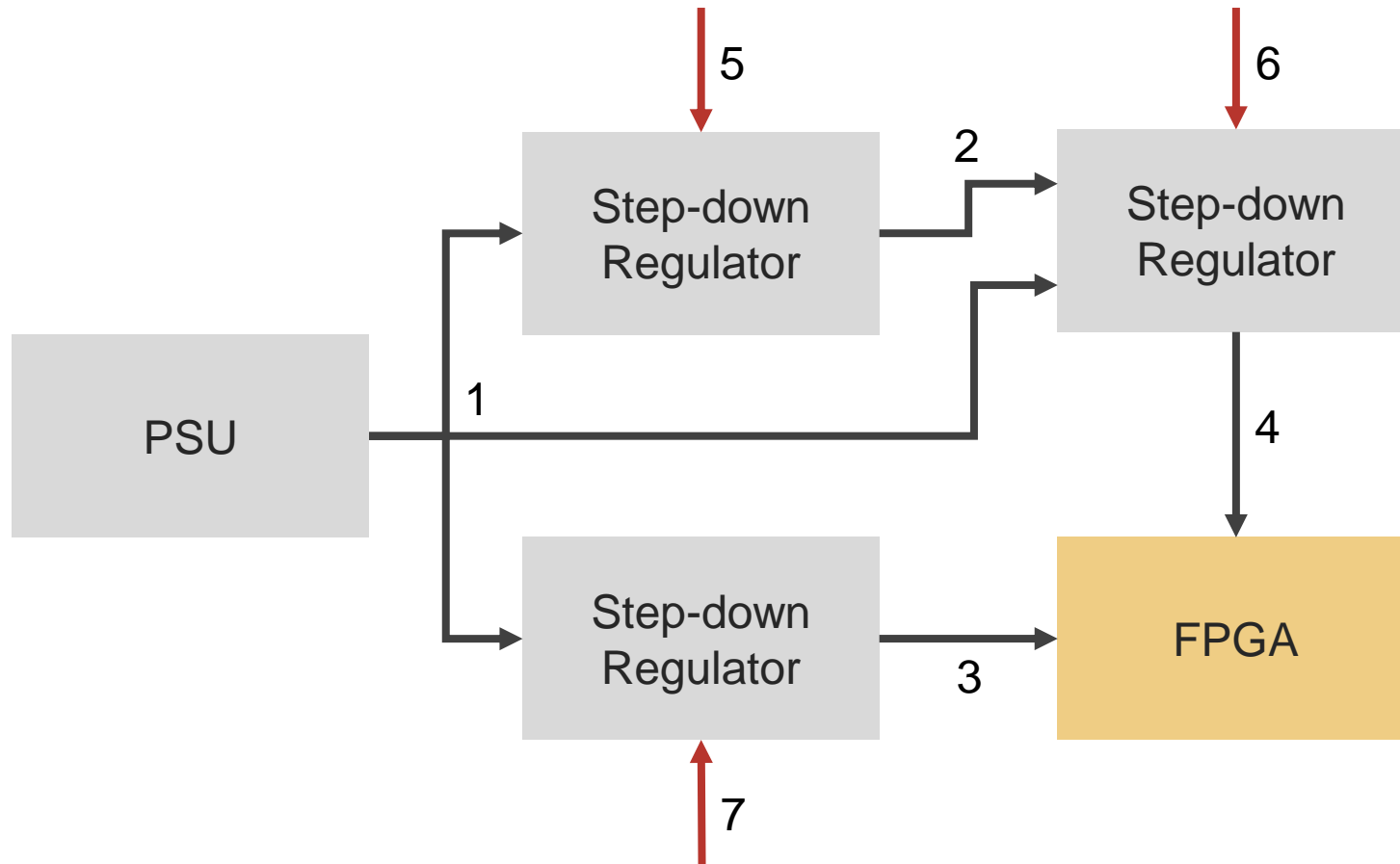
Action that triggers change

**Complete event:**

Measurement that confirms change



# Sequence Constraints

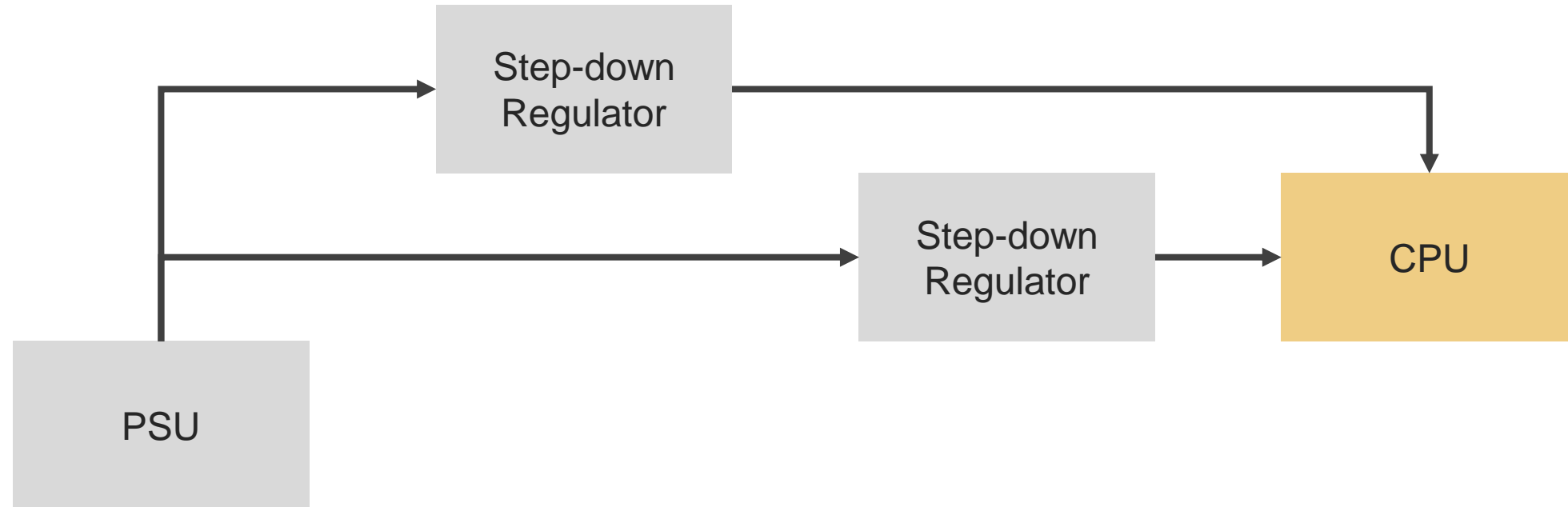


# Power Distribution networks became complex

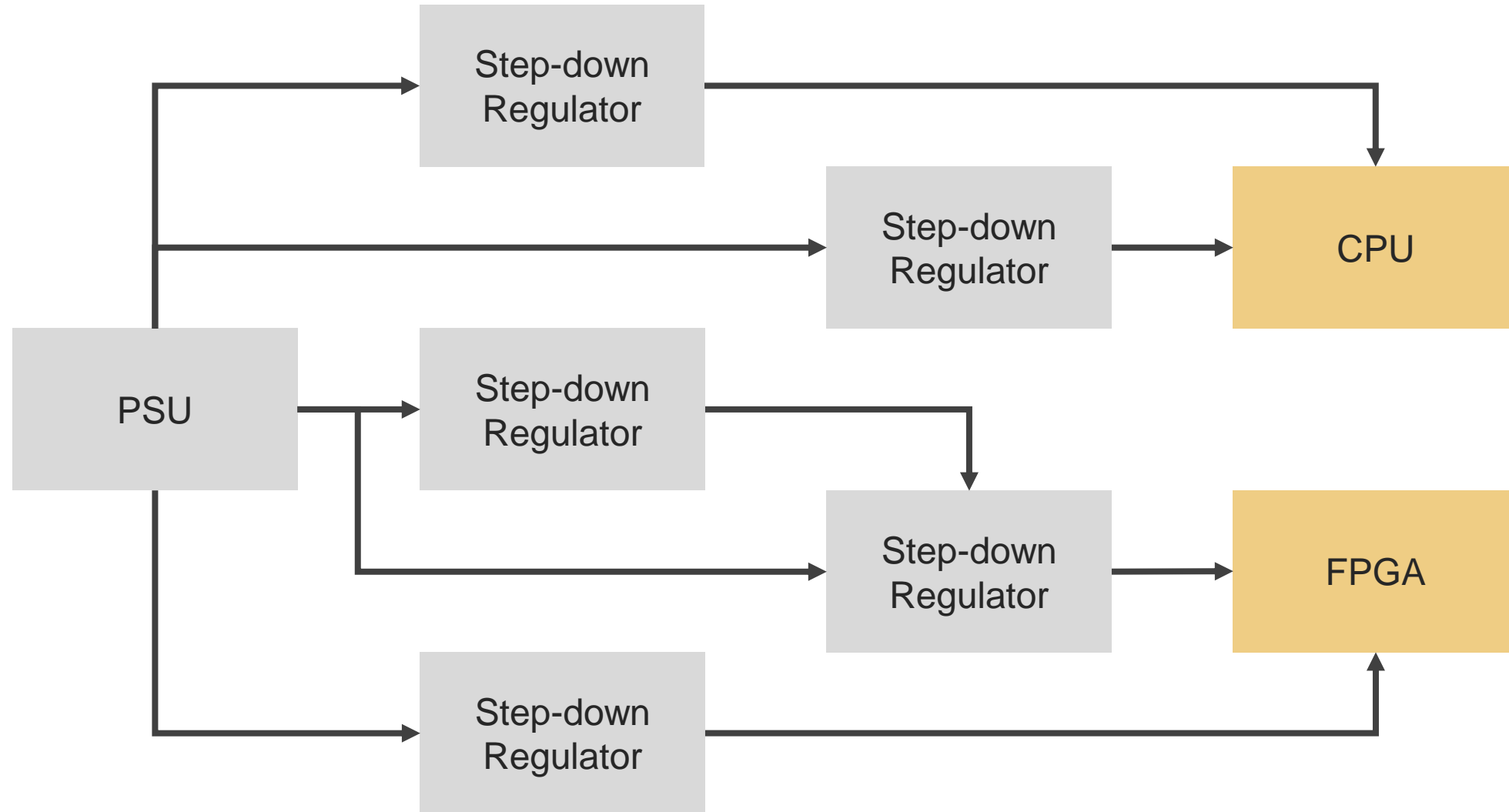




# Power Distribution networks became complex



# Power Distribution networks became complex



# Maximum Ratings

Table 1: Absolute Maximum Ratings (cont'd)

Symbol	Description <sup>1</sup>	Min	Max	Units
V <sub>CCBRAM</sub>	Supply voltage for the block RAM memories	-0.500	1.000	V
V <sub>CCO</sub>	Output drivers supply voltage for HD I/O banks (VU19P and VU23P only)	-0.500	3.400	V
	Output drivers supply voltage for HP I/O banks	-0.500	2.000	V
V <sub>CCAUX_IO</sub> <sup>3</sup>	Auxiliary supply voltage for the I/O banks	-0.500	2.000	V
V <sub>REF</sub>	Input reference voltage	-0.500	2.000	V
V <sub>IN</sub> <sup>4, 5, 6</sup>	I/O input voltage for HD I/O banks (VU19P and VU23P only)	-0.550	V <sub>CCO</sub> + 0.550	V
	I/O input voltage for HP I/O banks	-0.550	V <sub>CCO</sub> + 0.550	V
V <sub>BATT</sub>	Key memory battery backup supply	-0.500	2.000	V
I <sub>DC</sub>	Available output current at the pad	-20	20	mA
I <sub>RMS</sub>	Available RMS output current at the pad	-20	20	mA
<b>High Bandwidth Memory (HBM)</b>				
V <sub>CC_HBM</sub>	Supply voltage for the high-bandwidth memory	-0.300	1.500	V
V <sub>CC_IO_HBM</sub>	I/O supply voltage for the high-bandwidth memory	-0.300	1.500	V
V <sub>CCAUX_HBM</sub>	Auxiliary supply voltage for the high-bandwidth memory	-0.300	3.000	V
<b>GTY or GTM Transceiver<sup>7</sup></b>				
V <sub>CCINT_GT</sub>	Digital supply voltage for select modules in the GTM transceivers	-0.500	1.000	V

Source: Xilinx, Virtex UltraScale+ FPGA Data Sheet: DC and AC Switching Characteristics

## Power-On/Off Power Supply Sequencing

The recommended power-on sequence is  $V_{CCINT}$ ,  $V_{CCINT\_IO}/V_{CCBRAM}$ ,  $V_{CCAUX}/V_{CCAUX\_IO}$ , and  $V_{CCO}$  to achieve minimum current draw and ensure that the I/Os are 3-stated at power-on. The recommended power-off sequence is the reverse of the power-on sequence. If  $V_{CCINT}$  and  $V_{CCINT\_IO}/V_{CCBRAM}$  have the same recommended voltage levels, they can be powered by the same supply and ramped simultaneously.  $V_{CCINT\_IO}$  must be connected to  $V_{CCBRAM}$ . If  $V_{CCAUX}/V_{CCAUX\_IO}$  and  $V_{CCO}$  have the same recommended voltage levels, they can be powered by the same supply and ramped simultaneously.  $V_{CCAUX}$  and  $V_{CCAUX\_IO}$  must be connected together.  $V_{CCADC}$  and  $V_{REF}$  can be powered at any time and have no power-up sequencing requirements.

power-off sequence is the reverse of the power-on sequence to achieve minimum current draw. If these recommended sequences are not met, current drawn from  $V_{MGTAVTT}$  can be higher than specifications during power-up and power-down.

Source: Xilinx, Virtex UltraScale+ FPGA Data Sheet: DC and AC Switching Characteristics

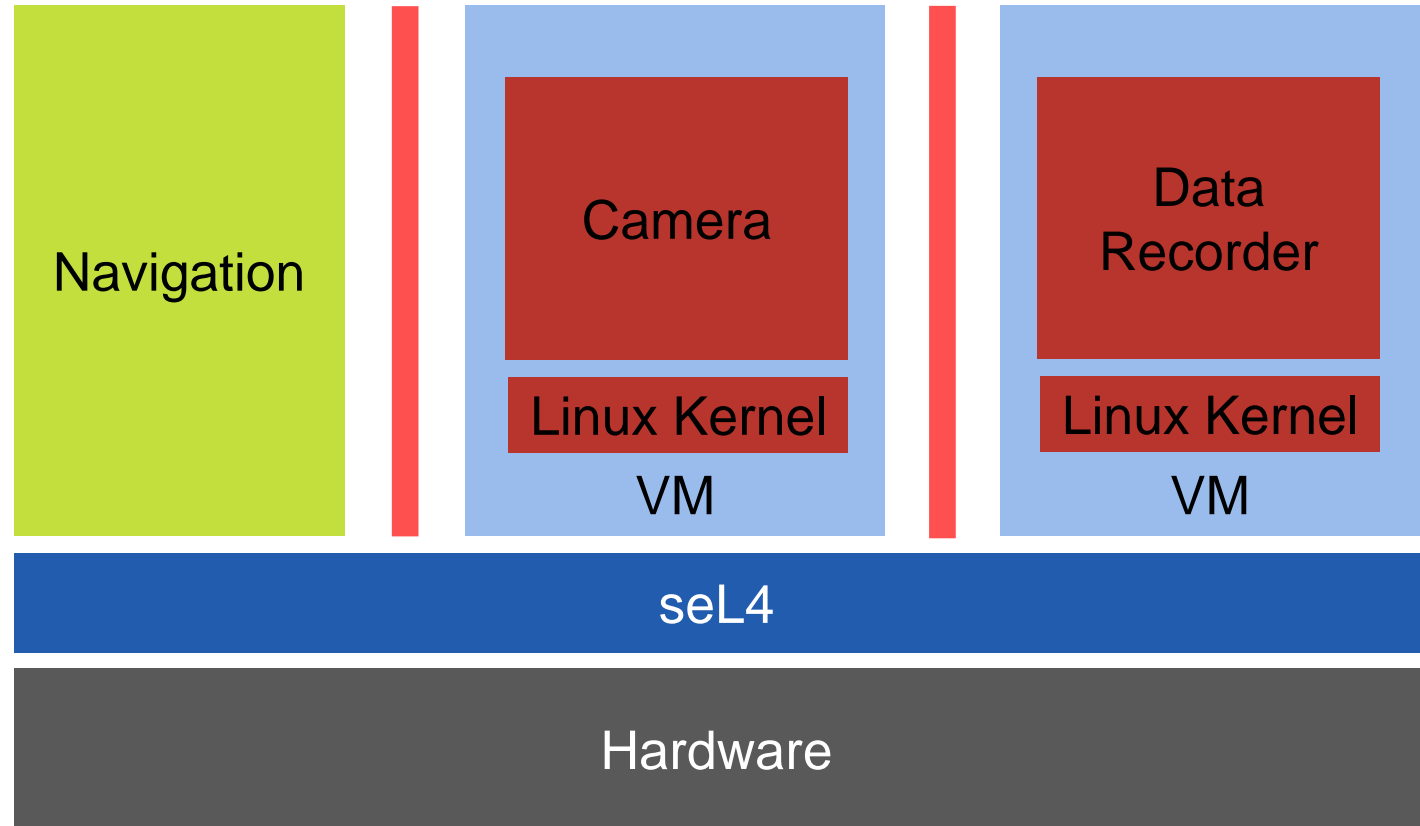
# seL4: Full functional correctness proof & practical



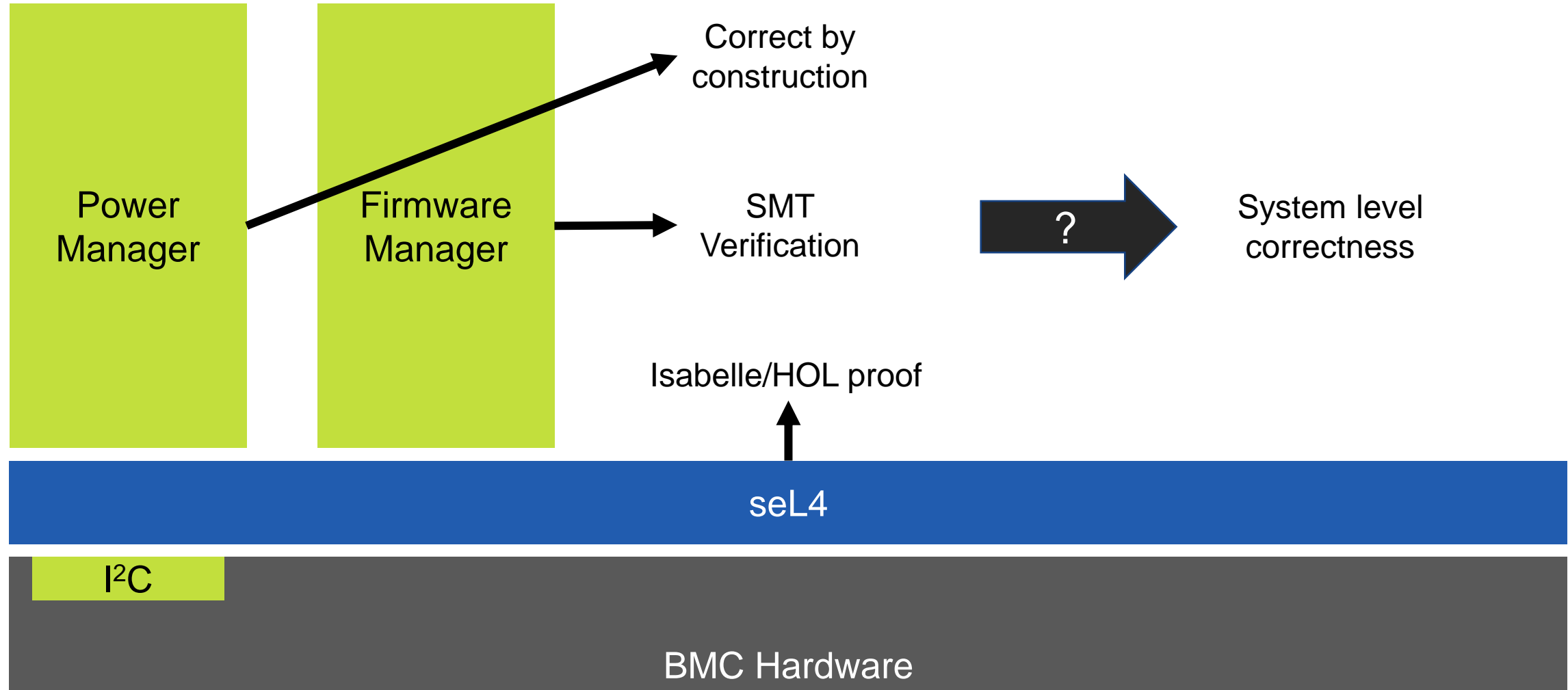
DARPA HACMS Project



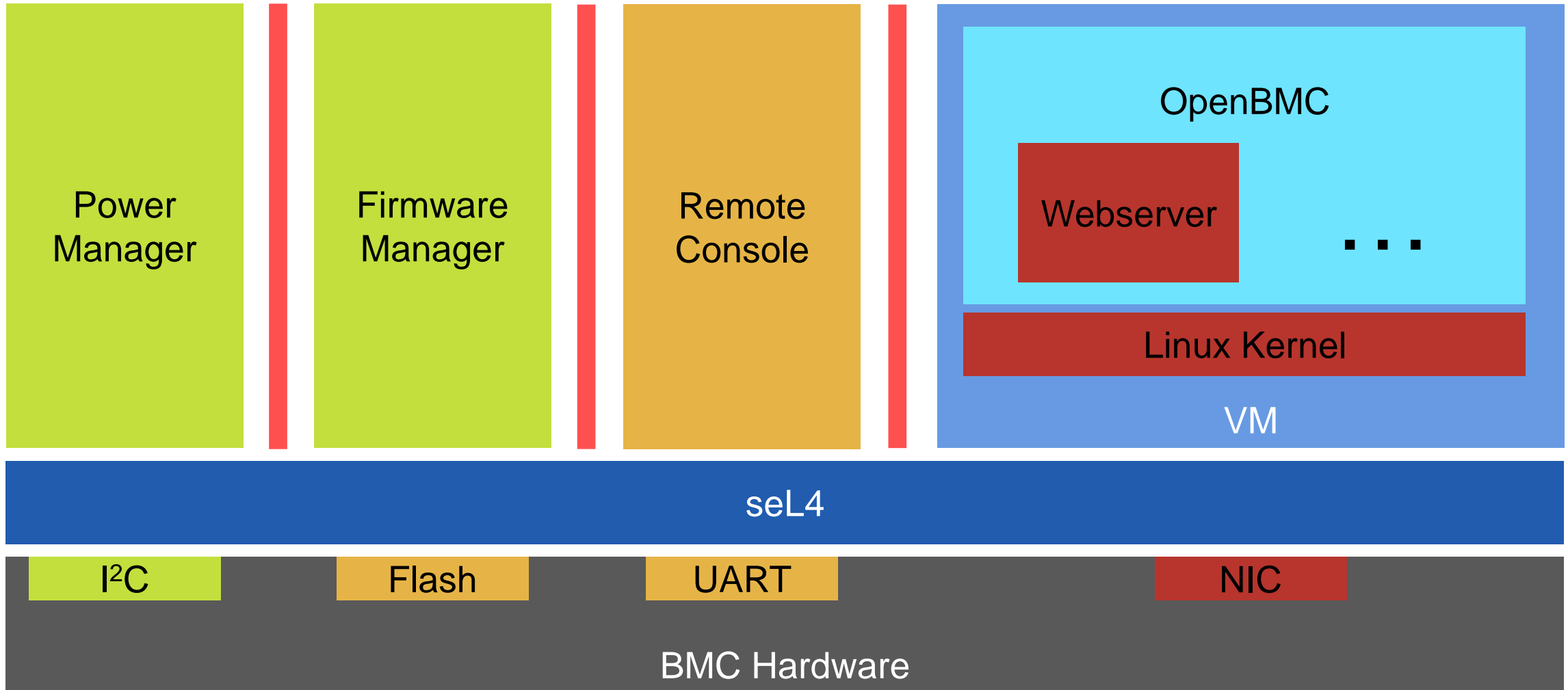
Source:  
<https://trustworthy.systems/projects/TS/SM/ACCM/ulb.png>



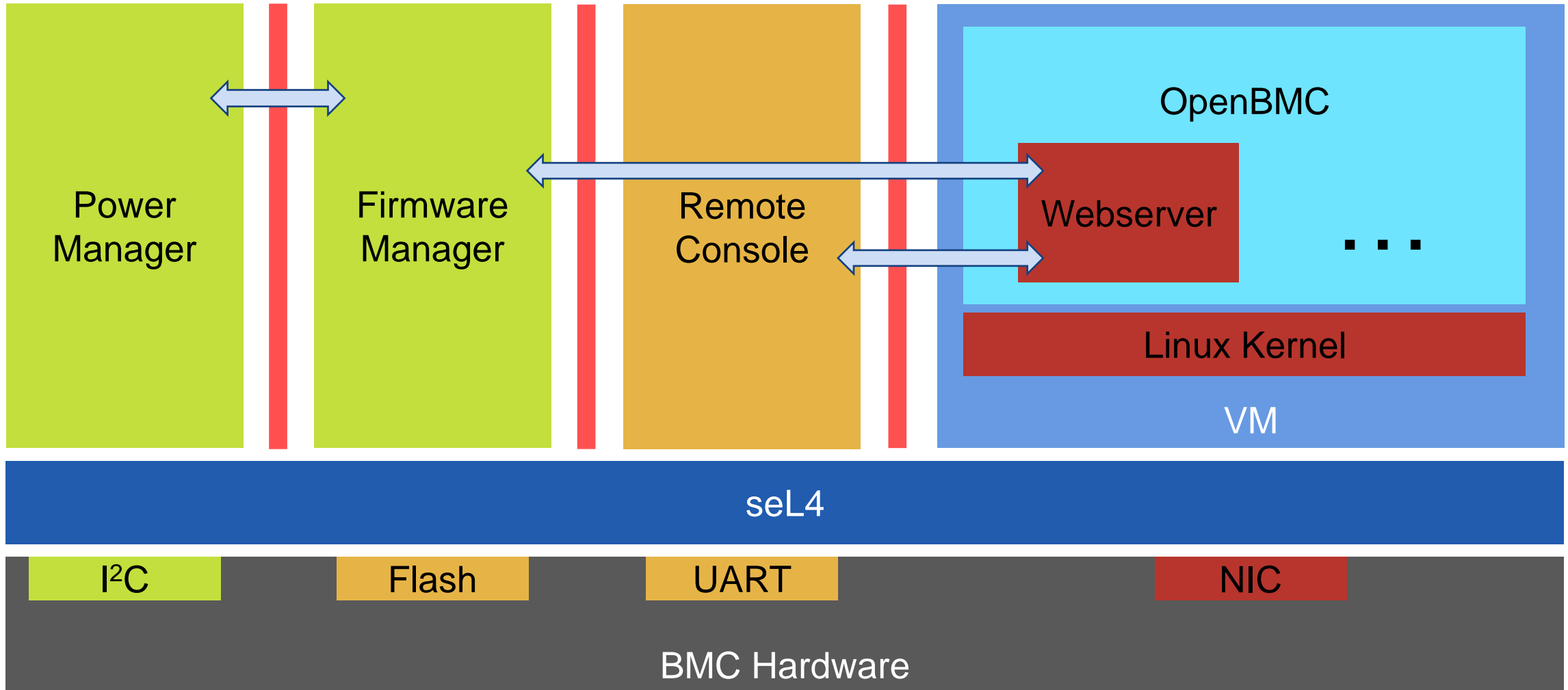
# How to make correctness statement at system level?



# How to make correctness statements about hardware interaction?



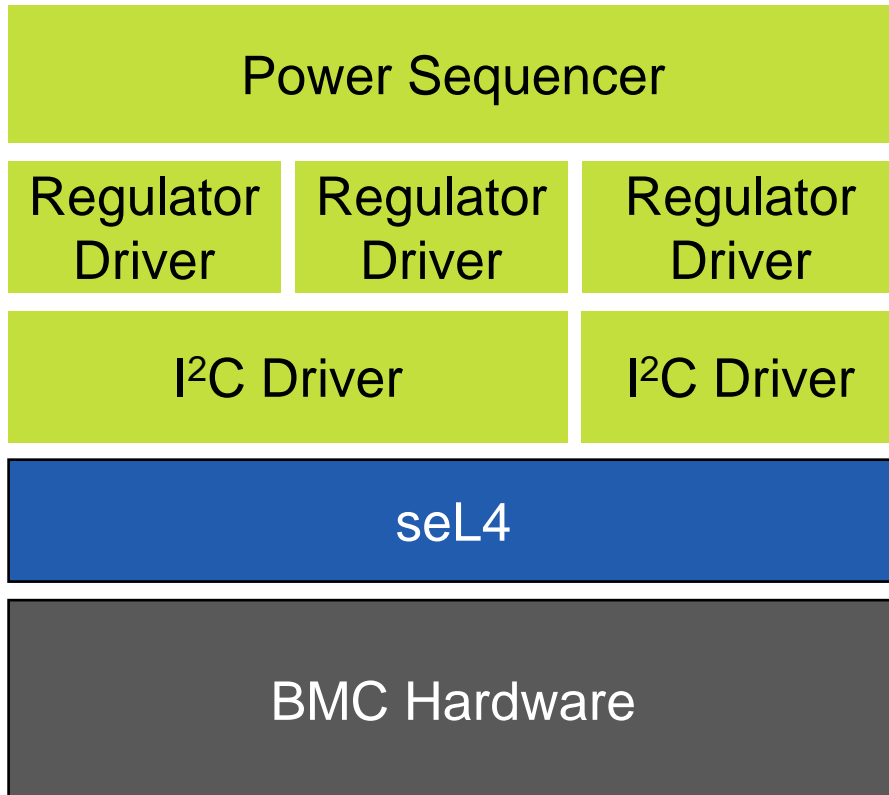
# How do components of different trust levels communicate?



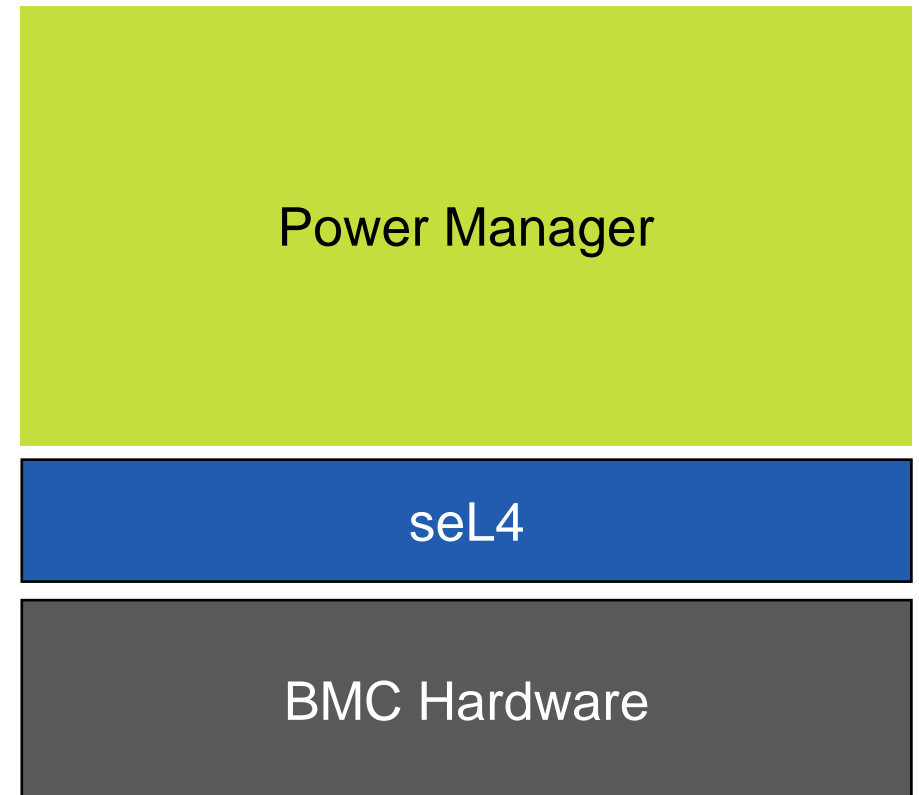
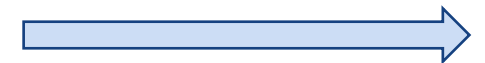


# How do we componentize the system?

Finer grained isolation



Lower communication overhead



...

# What tooling do we need to push the complexity of verifiable systems?

