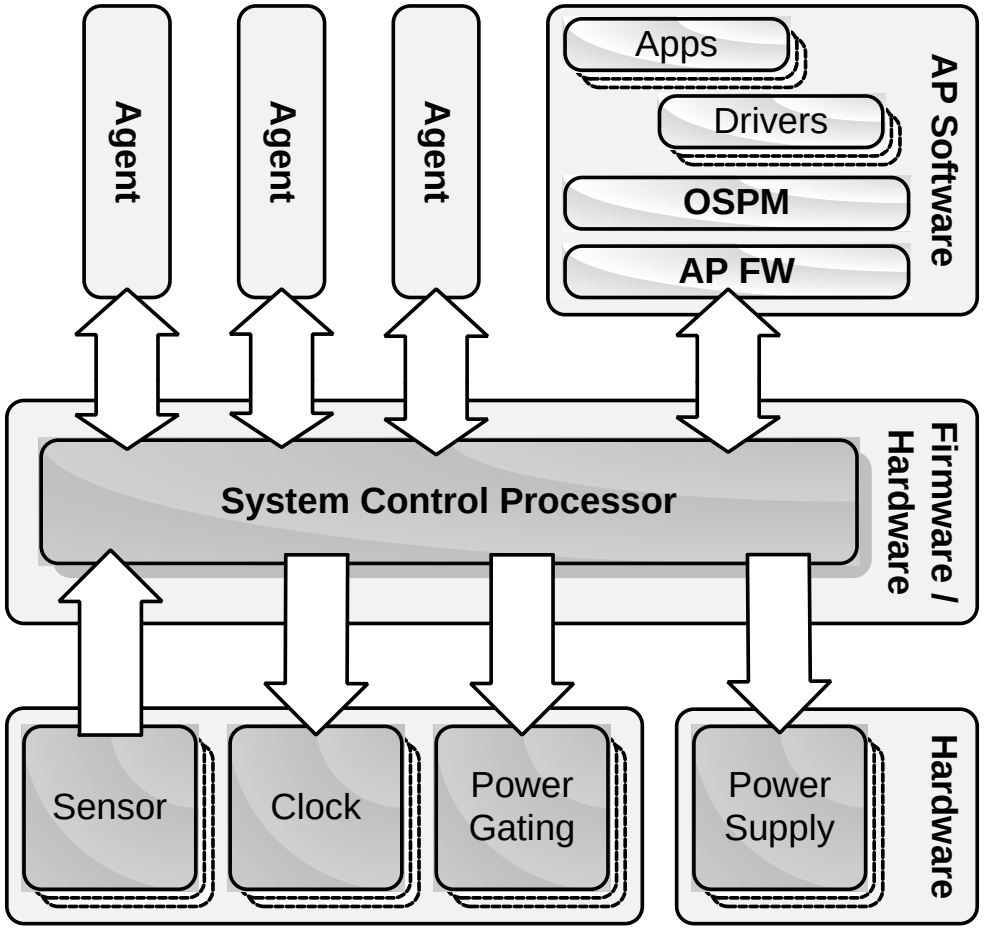
arm

SCP firmware threat model v2

System Control Processor (SCP) concept - Power Control System Architecture (PCSA) specification



System Control Processor (SCP) concept - Power Control System Architecture (PCSA) specification

- In the upper part of the diagram, the application processor (AP) software stack is shown as a requestor of SCP services. Other agents in the system might also have the capability to directly generate requests for resources that the SCP controls. Examples of such agents might be a modem subsystem in a mobile SoC or a management function in a server SoC.

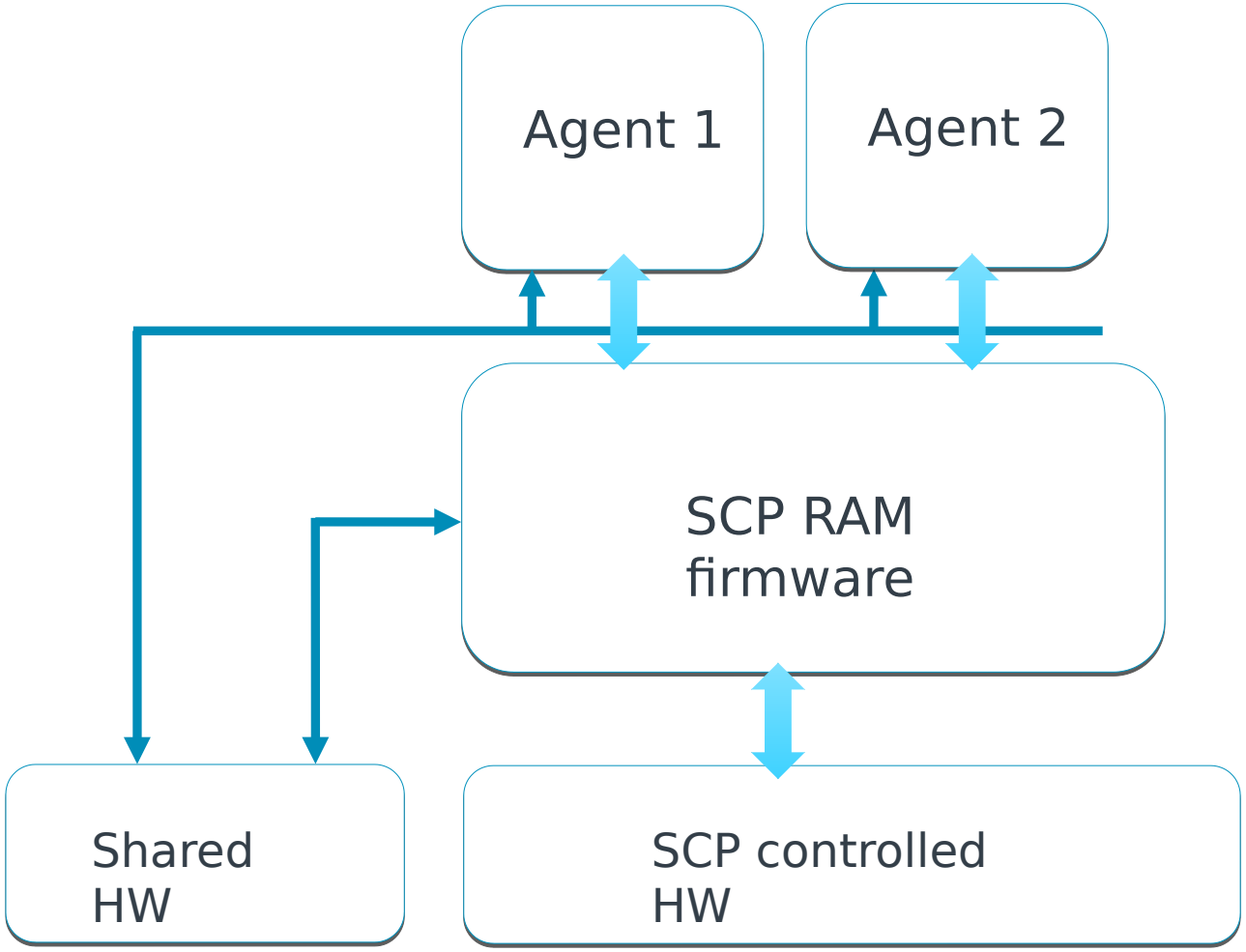
- The SCP reconciles requests from all agents, managing the availability of shared resources and power-performance limits according to all constraints.

- The central part of the figure reflects that the SCP is a processor based system running dedicated firmware controlling a set of hardware resources. Although not shown in the figure, the SCP has a minimum set of resources, including local private memory, timers, interrupt control, and registers for system configuration, control and status.

- The lower part of the figure shows a simplified set of SCP controlled hardware resources such as clock sources, power domain gating, voltage supplies, and sensors.

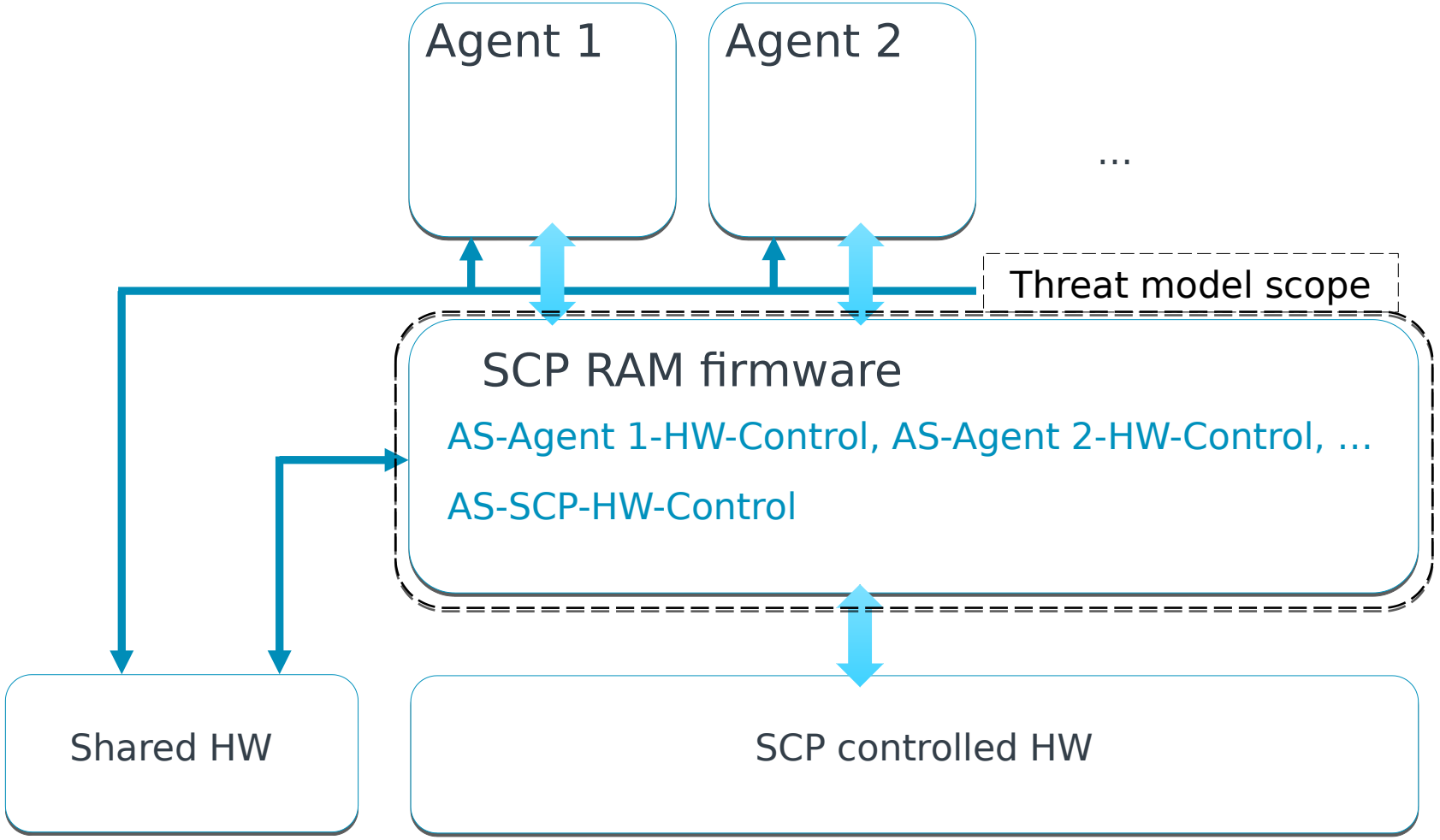
- The capabilities of an SCP implementation are dependent on the ability to access and control a set of resources within the SoC in addition to a required base set of functions within the SCP. SCP hardware requirements are further detailed in System Control Processor on page 7-4.

SCP RAM firmware Product Diagram



- SCP firmware provides system agents (OSPM, PSCI, MCP, …) access/control to the hardware resources it controls.
- SCP firmware can also access and interact with hardware which agents have direct access to.

SCP RAM firmware Product Diagram with assets

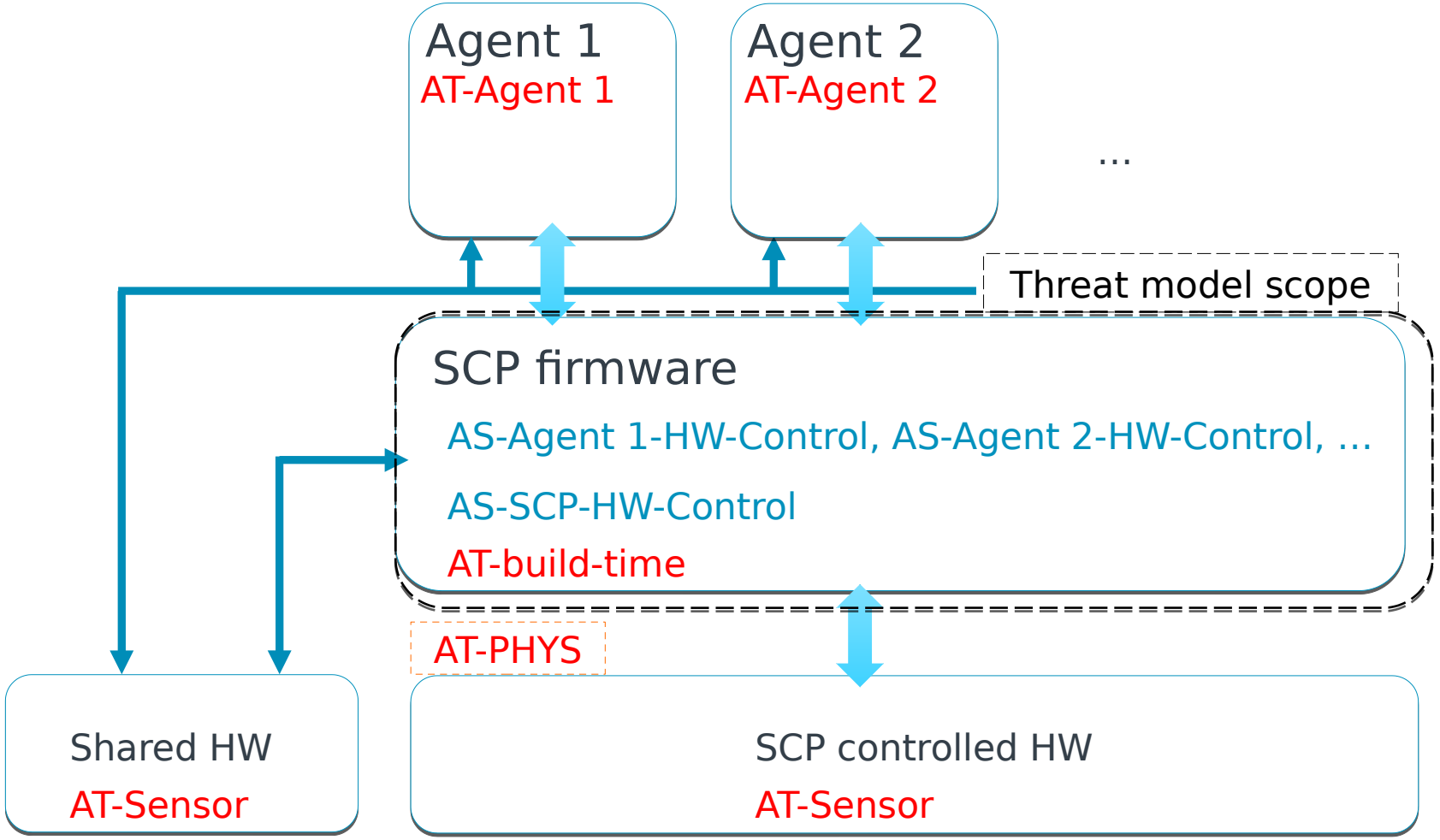


SCP RAM firmware Product assets

The scope of the SCP RAM firmware product threat model are the assets of a system the SCP RAM firmware is considered responsible for protecting. Those assets are:

Asset	Description
AS-Agent n-HW-Control	Control of the hardware, Agent n has been granted access to through SCP.
AS-SCP-HW-Control	Control of the hardware dedicated to SCP.

SCP RAM firmware Product Security Diagram



Mitigation requirement table

ID	Asset	Attacker	Attacker abilities	Attack type	Mitigation level	Rationale
1	AS-Agent n-HW-Control	AT-Agent m (m≠ n)	SO	S	Operational	Agent m should not be able to pretend being Agent n.
2	AS-Agent n-HW-Control AS-SCP-HW-Control	AT-Agent m (m≠ n)	SO	T	Operational	Agent m should not be able to tamper with commands related to agent n.
3	AS-Agent n-HW-Control AS-SCP-HW-Control	AT-Agent m (m≠ n)	SO	I	Operational	Agent m should not be able to see data associated with commands related to agent n.
4	AS-Agent n-HW-Control AS-SCP-HW-Control	AT-Agent n	SO	E	Mitigated	Agent m should not be able to access hardware it is not granted access to.

Mitigation requirement table

ID	Asset	Attacker	Attacker abilities	Attack type	Mitigation level	Rationale
5	AS-Agent n-HW-Control AS-SCP-HW-Control	AT-Agent m (m≠ n)	SO	D	Mitigated	Agent m should not be able to prevent other agents and SCP to access hardware they are granted access to.
6	AS-Agent n-HW-Control AS-SCP-HW-Control	AT-Agent m (m≠ n)	SFI	STRIDE	Unmitigated	No specific hardware protection against those attack abilities.
7	AS-Agent n-HW-Control AS-SCP-HW-Control	AT-PHYS	IP, HFI	STRIDE	Unmitigated	
8	AS-SCP-HW-Control	AT-Sensor	S	E	Mitigated	Sensors should not be able to adversely affect the SCP operation through malformed data.

Threat Intelligence

Who might attack our system, why and how?

Attacker capabilities

Software-Only (SO)

Low-Resolution-Side-Channel (LRSC)

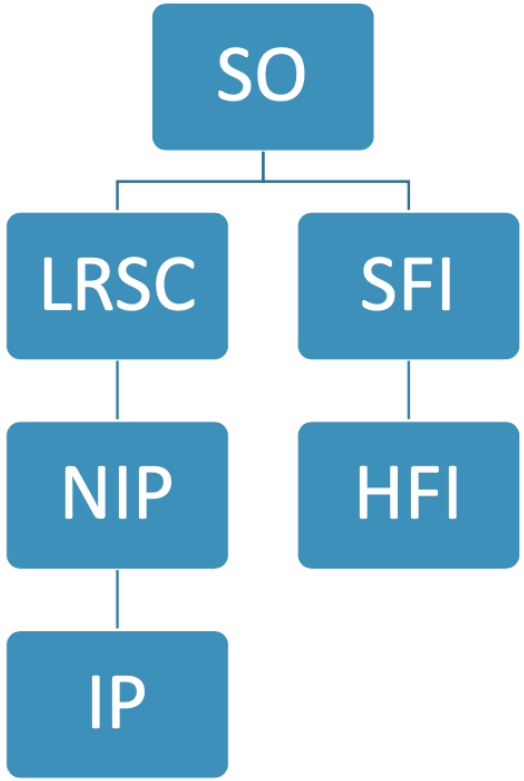
Non-Invasive-Physical (NIP)

Invasive-Physical (IP)

Software-Fault-Injection (SFI)

Hardware-Fault-Injection (HFI)

Attacker capability hierarchy

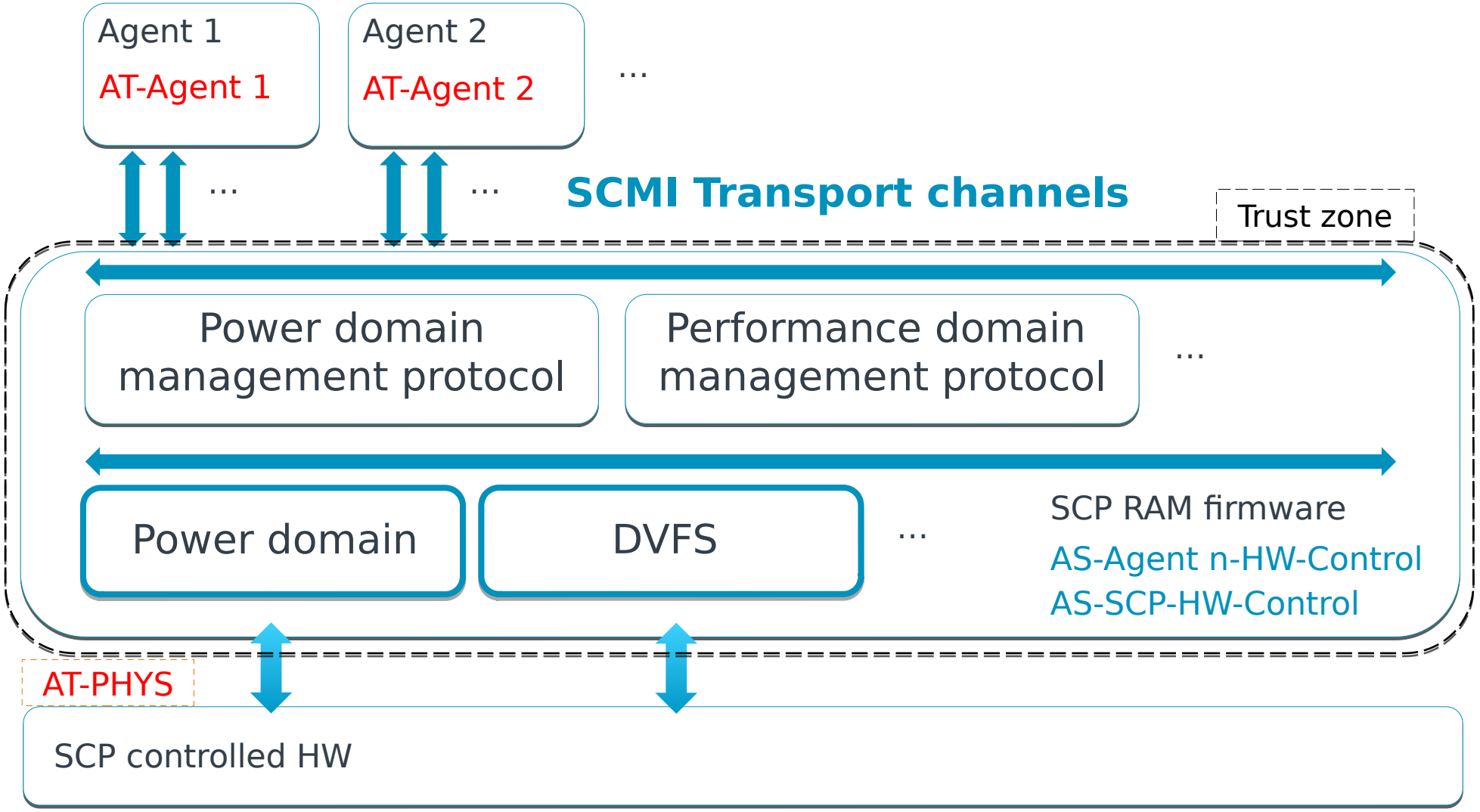


Threat Intelligence

STRIDE Analysis

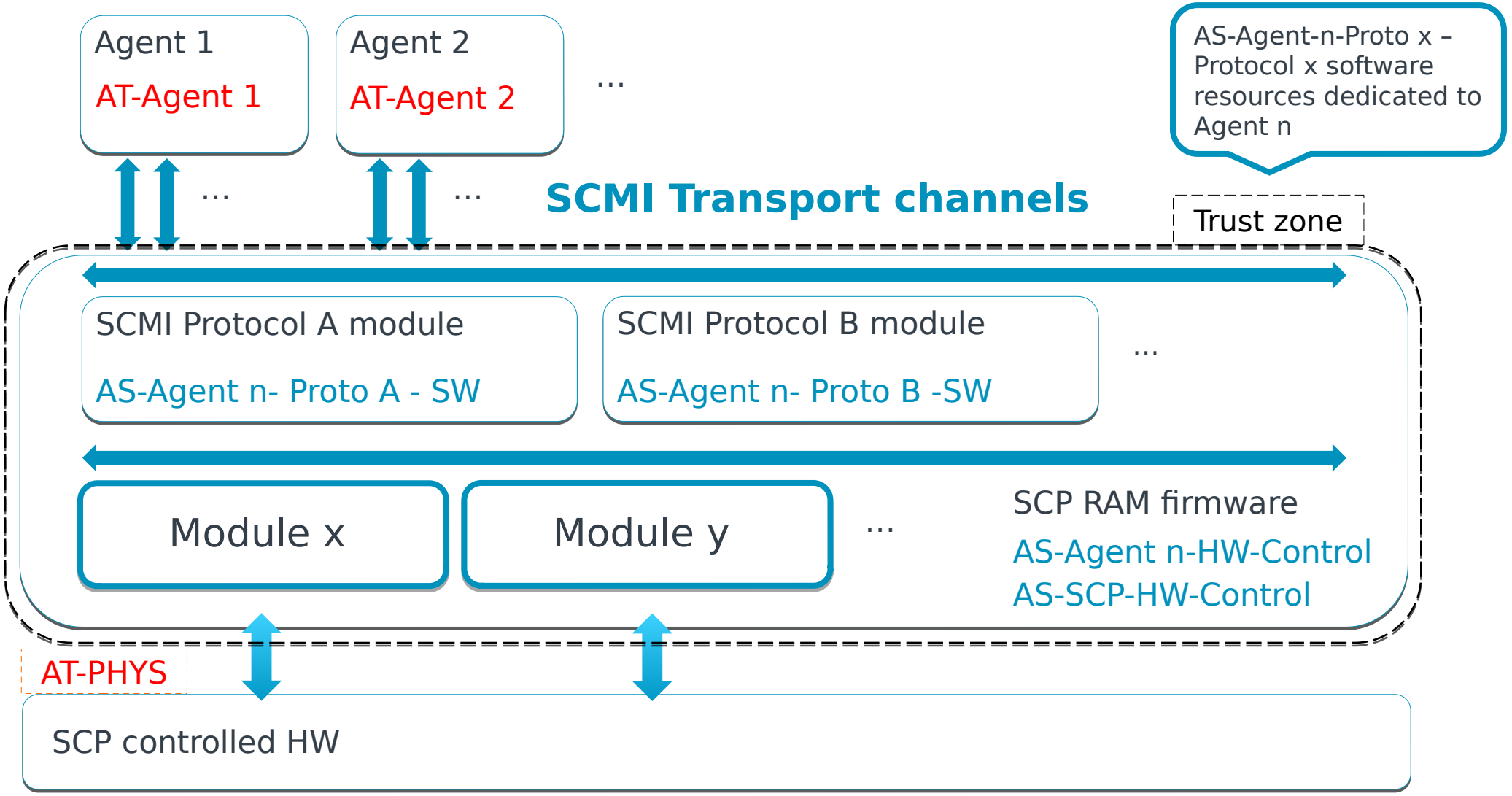
- Spoofing: A process or external entity pretends to be something else.
- Tampering: Data in a process store or data flow is changed.
- Repudiation: Denial of an action by an external entity or process.
- Information disclosure: Sensitive data in a process store or data flow is exposed.
- Denial of Service: Operation of a process store or data flow is disrupted.
- Elevation of Privilege: A process is used to perform unauthorized actions.

SCP RAM firmware Architecture diagram



arm

SCP RAM firmware Architecture diagram



arm

Mitigation implementation/ Security requirement table

Mit. Imp. ID	Threat ID	Asset	Attacker	Mitigation implementation/ Security requirement
1	1,2,3	AS-Agent n-HW-Control	AT-Agent m (m≠ n)	Impersonation attacks should be mitigated by the system by for example making impossible for an agent to access the SCMI transport channels of another agent.
2	4	AS-Agent n-HW-Control AS-SCP-HW-Control	AT-Agent m (m≠ n)	Comprehensive validation of SCMI command input parameters to prevent malformed/malicious SCMI commands interfering with SCP execution flow.
3	1,2	AS-Agent n-HW-Control AS-SCP-HW-Control	AT-Agent m (m≠ n)	Integrity of SCMI command parameters. There should be no way for an agent to tamper with the parameters of a command whose processing is on-going. If commands reside in shared memory, the SCP should make a copy of it in SCP dedicated memory before to process it.

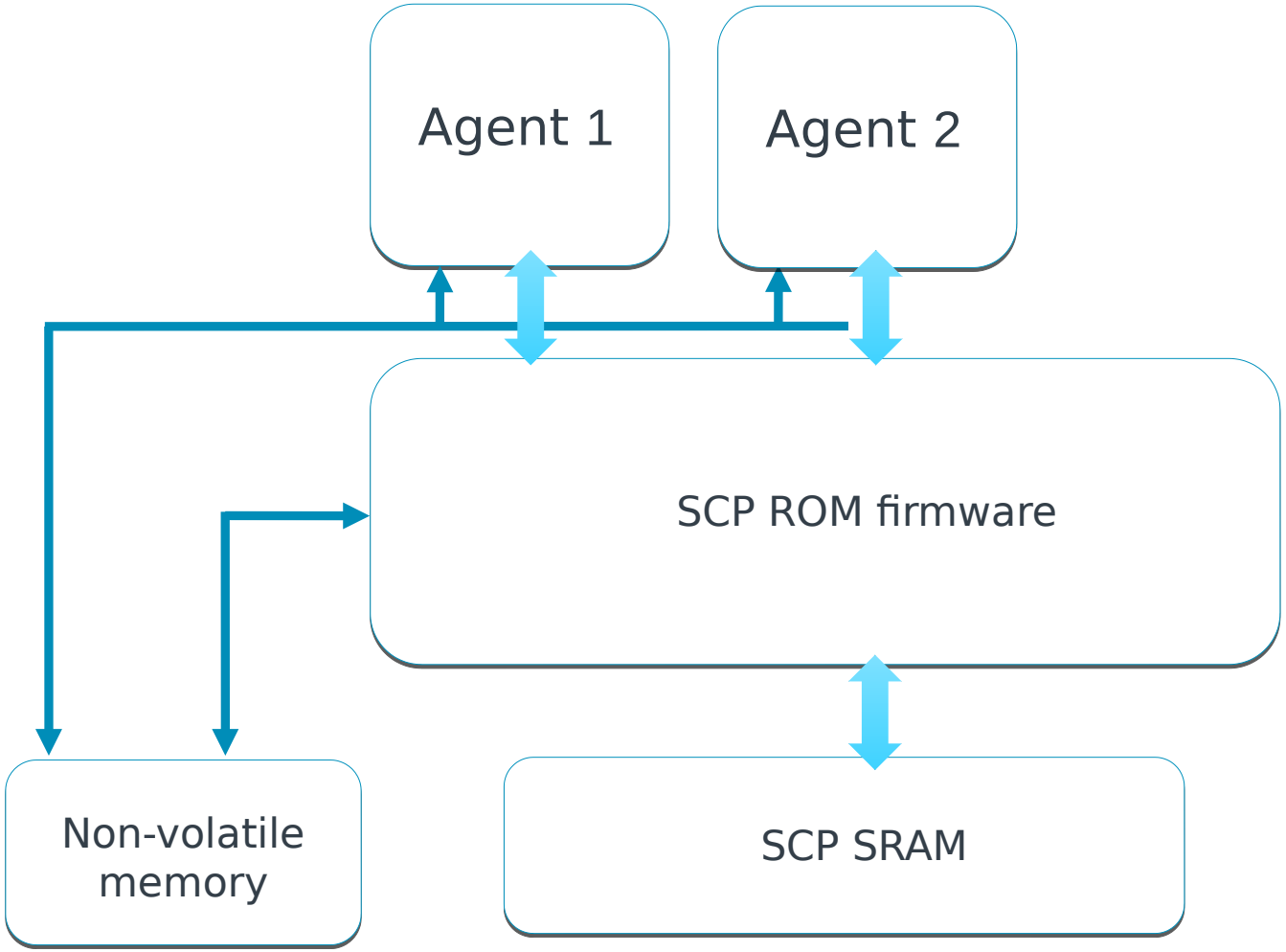
Mitigation implementation/ Security requirement table

Mit. Req. ID	Threat ID	Asset	Attacker	Mitigation implementation/ Security requirement
4	5	AS-Agent n-HW-Control AS-SCP-HW-Control	AT-Agent m (m≠ n)	The commands of different agents should be processed with the same level of priority. That way an ‘higher’ priority agent cannot prevent another ‘lower’ priority agent to access SCP services.
5	4,5	AS-Agent n-HW-Control AS-SCP-HW-Control	AT-Agent m (m≠ n)	The SCMI protocol modules should allocate the necessary software resources AS-Agent n- Proto x – SW to process the commands per agents and not share them between agents.
6	5	AS-Agent n-HW-Control AS-SCP-HW-Control	AT-Agent m (m≠ n)	Interrupts that can be asserted to the SCP directly by agents (through Shared HW) should be handled to avoid the possibility of continuous interruption of the SCP.

Mitigation implementation/ Security requirement table

Mit. Req. ID	Threat ID	Asset	Attacker	Mitigation implementation/ Security requirement
7	1,2,3,4,5	AS-Agent n-HW-Control AS-SCP-HW-Control	AT-build-time	The SCP firmware configuration must be valid/verified to ensure correct operation of the SCP. Any invalid configuration will result in the SCP being non-operational.
8	8	AS-SCP-HW-Control	AT-Sensor	The SCP firmware will validate all sensor data to ensure it is within operational parameters.

SCP ROM firmware Product Diagram



SCP ROM firmware gets the SCP RAM firmware image from an agent or from non-volatile memory, loads it into SCP dedicated SRAM and passes control to the SCP RAM firmware image.

At present there is no verification of the firmware image loaded into SCP RAM. Otherwise, The same threat model applies to the SCP firmware whether it is running in RAM or ROM.