Secure reuse of DfT during operation

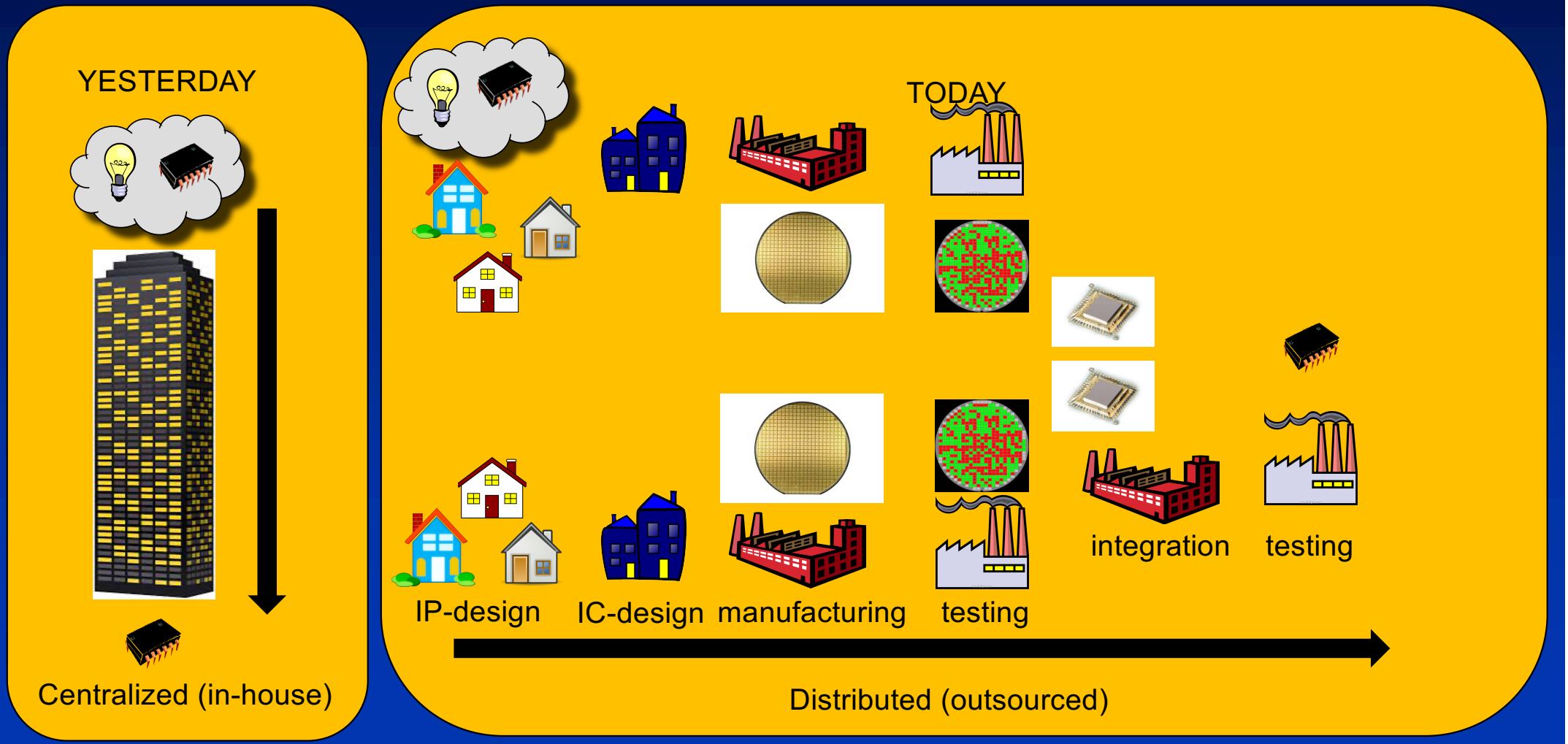
Erik Larsson

LUND
UNIVERSITY

More than 40 years of fantastic development

Computer	**IBM PC**	**Apple Imac**	**Difference**
Year	1981	2021	40 years
Price	45000 SEK (1981)	15000 SEK (2021)	9 times **cheaper**
Processor	**Intel 8088**	**Apple M1**	**Difference**
Transistors	29 000	16 000 000 000	550000 times **more**
Clock period	210000ps (4.77MHz)	310ps (3200MHz)	670 times **faster**
Technology	3000nm	5nm	600 times **smaller**

Supply-chain

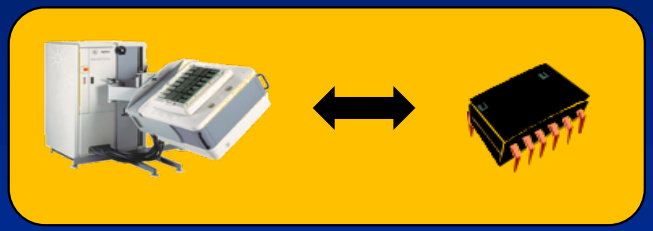


Some challenges

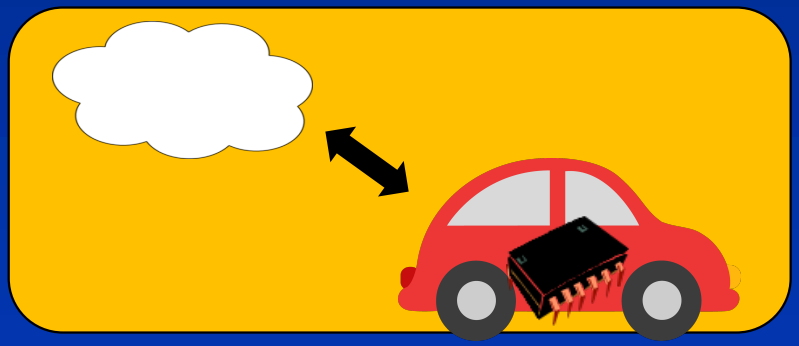
- Faster and smaller devices –> Handle tighter margins
- More transistors -> Reuse of logic and use of IP-blocks
- Variations (process, ageing) -> In-field (through life-time) adjustment and control
- Distributed supply-chains -> need of standards to ease communication and exchange of information

The trend

- Yesterday: External instruments, like ATEs, only at manufacturing



- Tomorrow: On-chip instruments accessible through the lifetime



ISO 26262, “ISO26262: Road Vehicles Functional Safety-part 5,” 2018.
D. Tille, L. Klimasch, and H. Sebastian, “A novel LBIST signature computation method for automotive microcontrollers using a digital twin,” 41st IEEE VLSI Test Symposium (VTS), 2023.

What do we need?

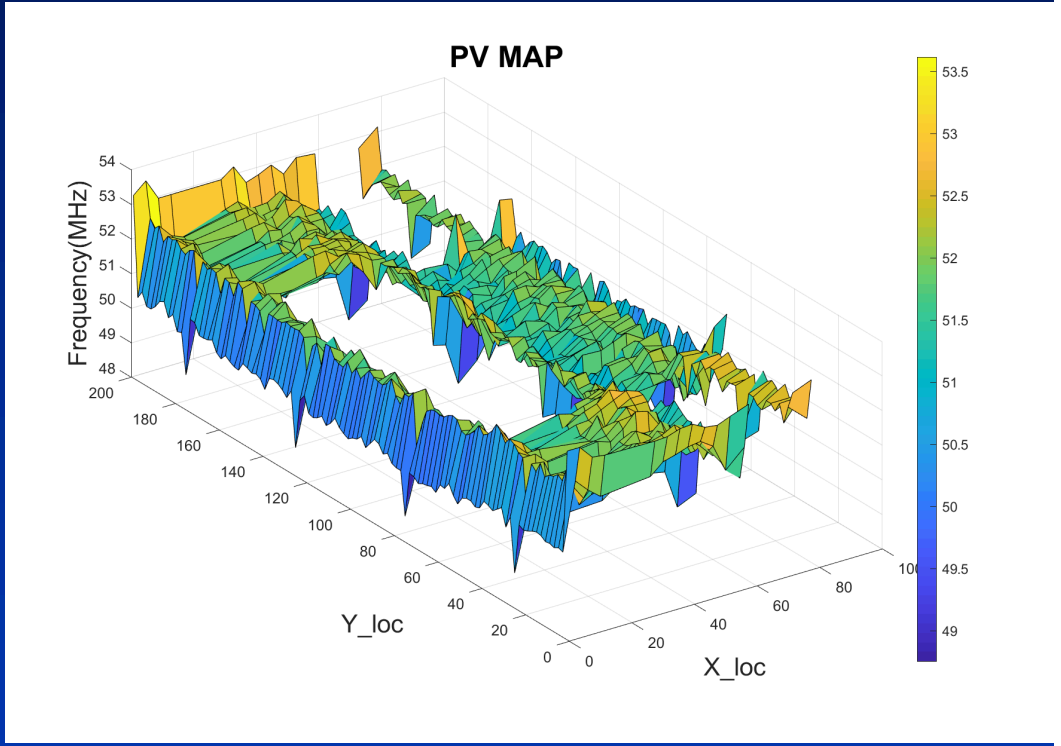
- High accessibility - controllability and observability - through the life-time
- Access should be:
  - For those who are trusted
  - Practical and easy to use

Outline

- Instruments
- Securing the access port
- Accessing instrument in functional mode
- Conclusions

How many instruments are needed?

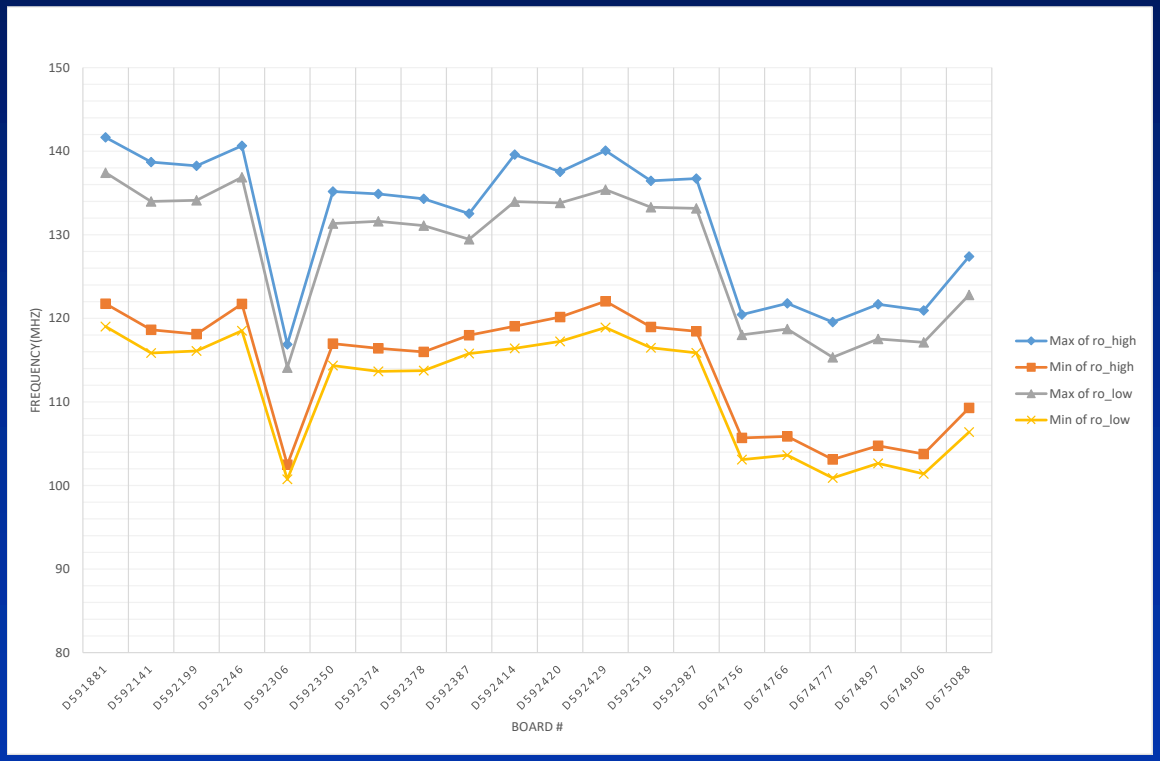
- Instrument for measuring performance variation (PV)
- On the used FPGAs it was possible to implement 1400 instruments



P. Cheng, “Study of monitoring circuitry for ageing in FPGAs,” 2021, Master thesis at Lund University, Sweden.

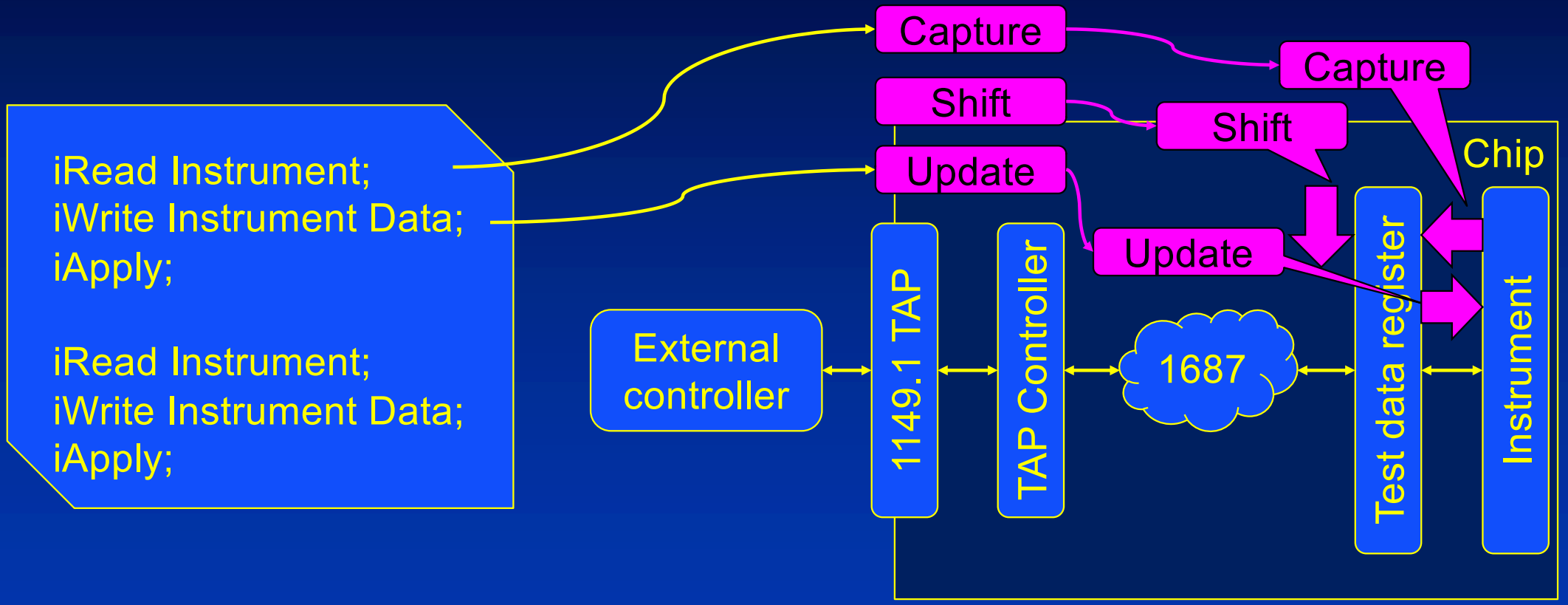
How many instruments are needed?

- Repeated the experiment on 20 different FPGAs



P. Cheng, “Study of monitoring circuitry for ageing in FPGAs,” 2021, Master thesis at Lund University, Sweden.

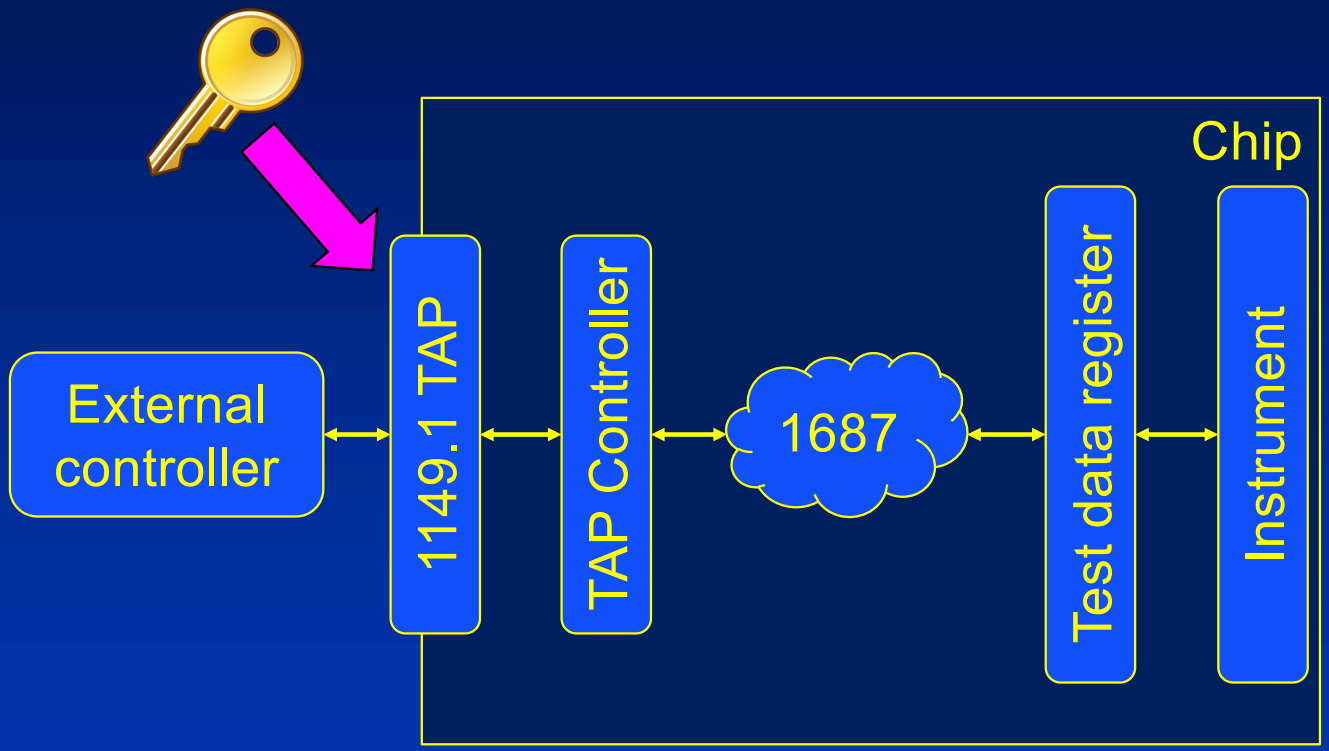
Standard access



Outline

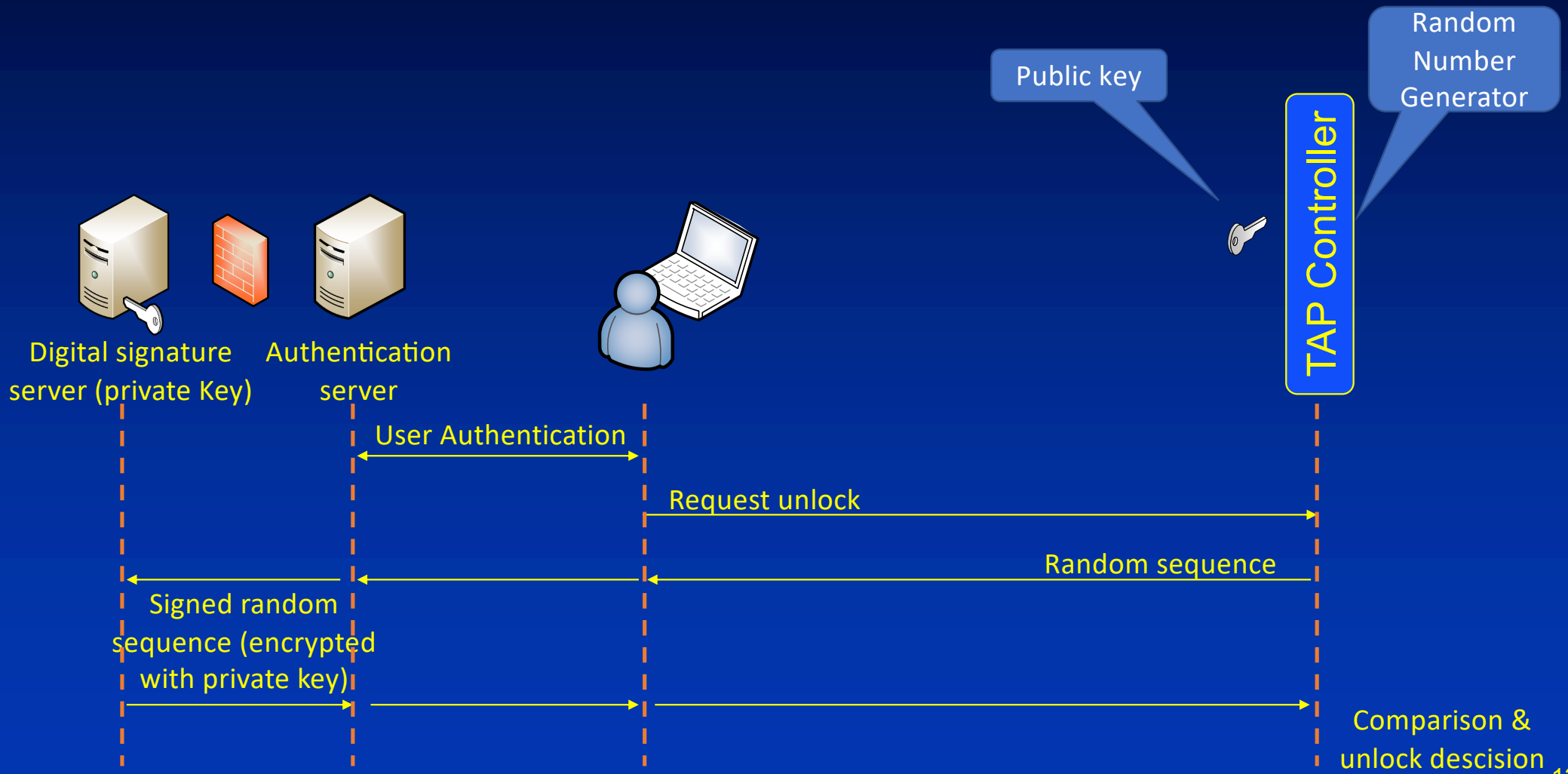
- Instruments
- Securing the access port
- Accessing instrument in functional mode
- Conclusions

Standard access to instrument

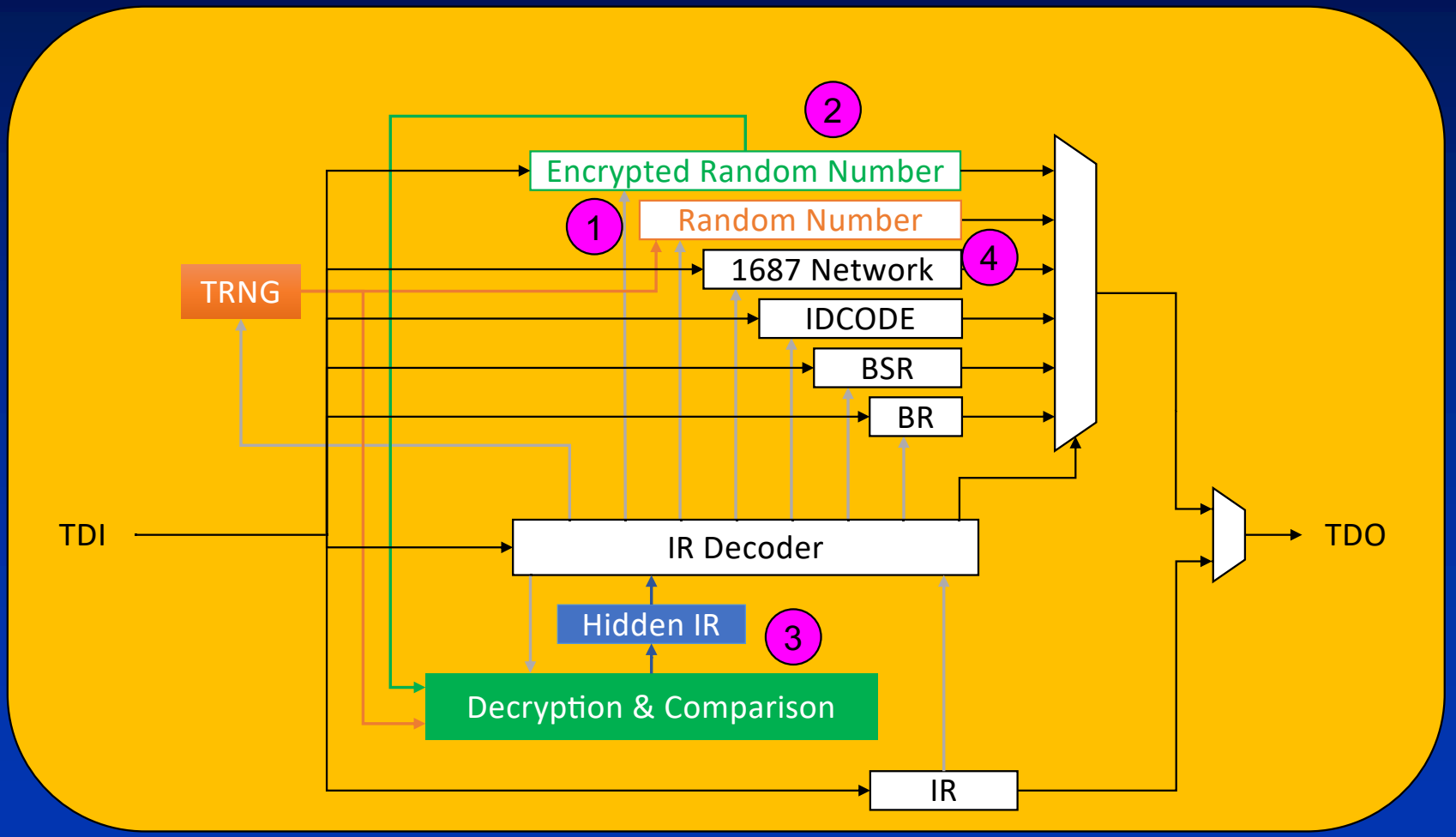


Problem if private keys get lost or become know

Authentication Method



Details of Method

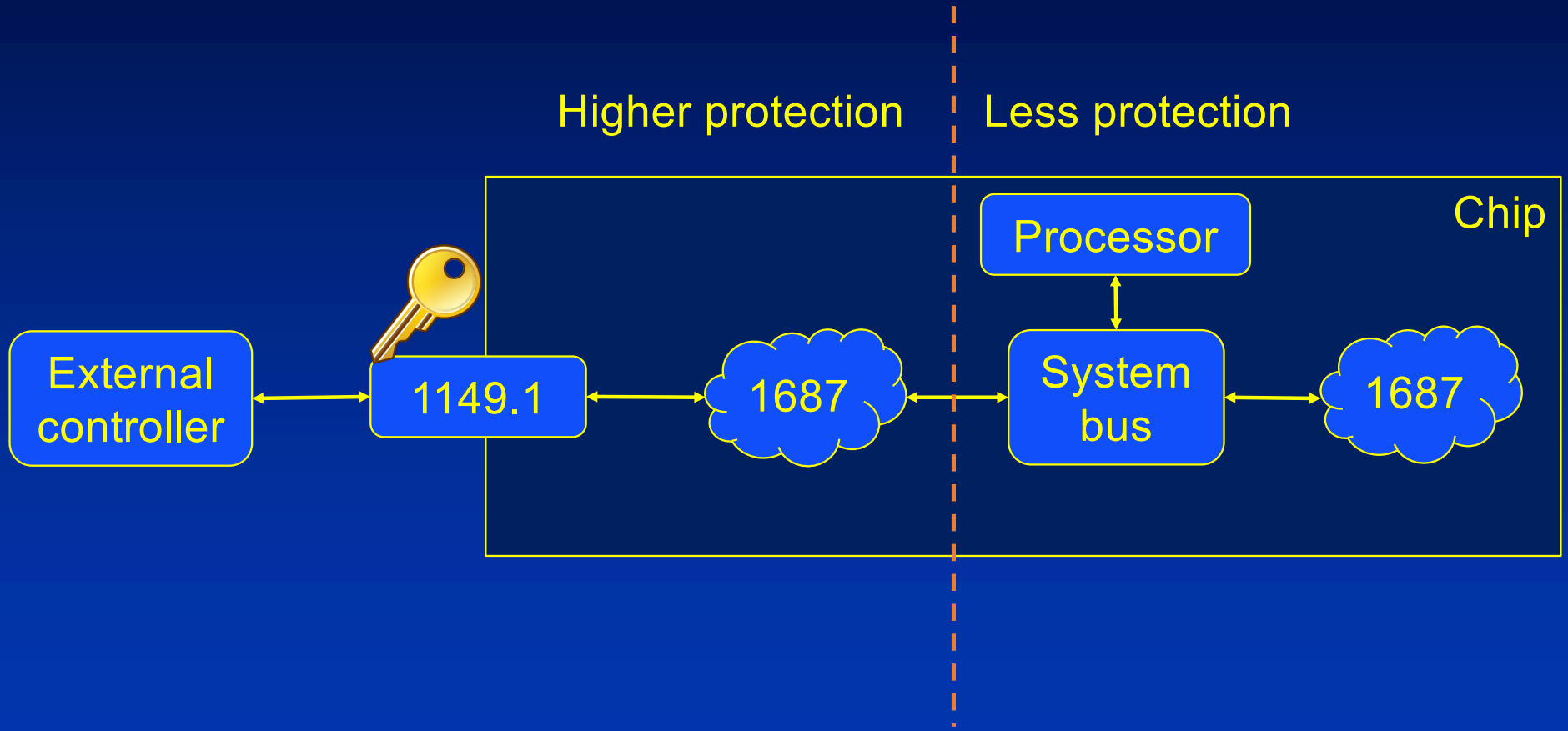


Outline

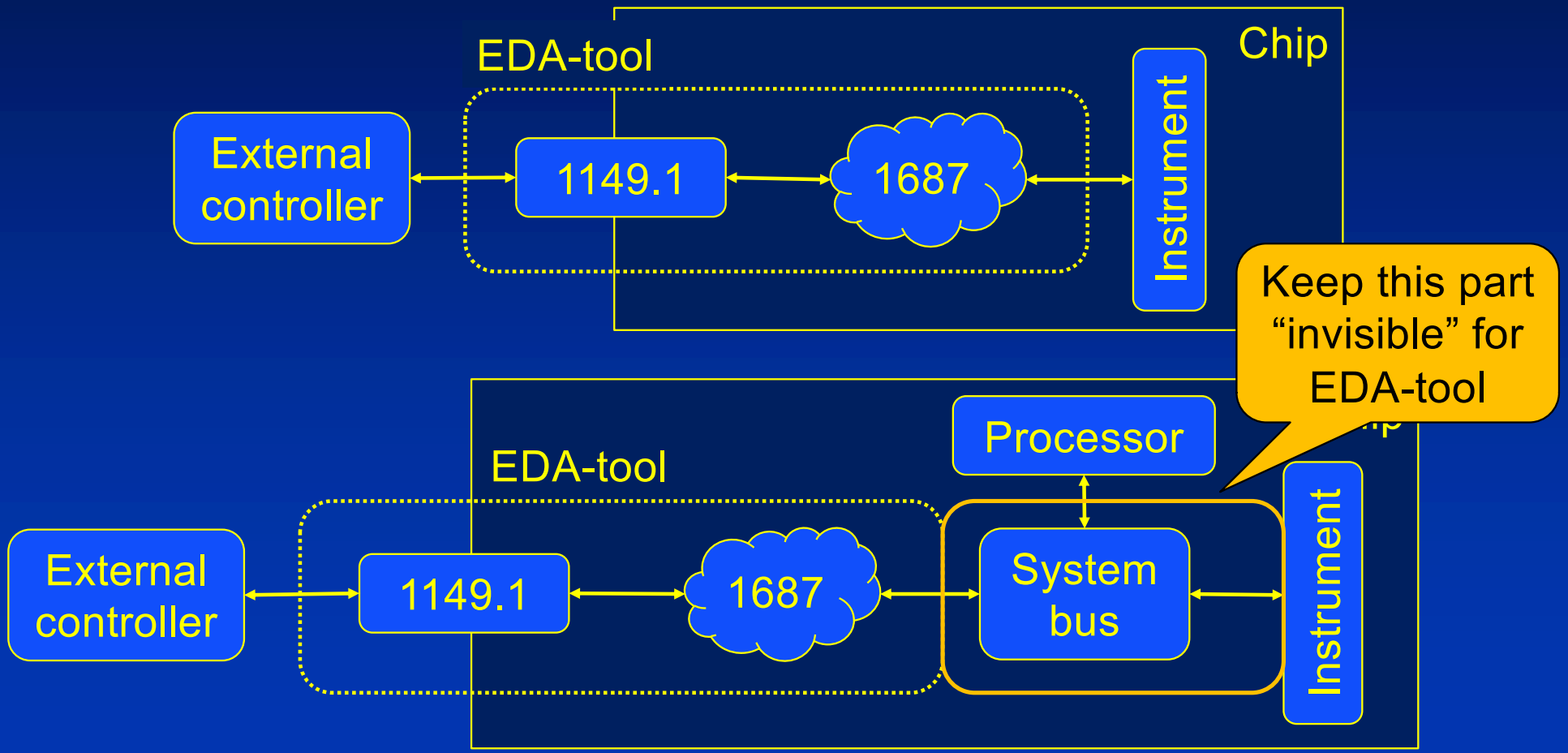
- Instruments
- Securing the access port
- Accessing instrument during operation
- Conclusions

Using keys is clumsy

Instrument sharing



Instrument sharing



Purpose

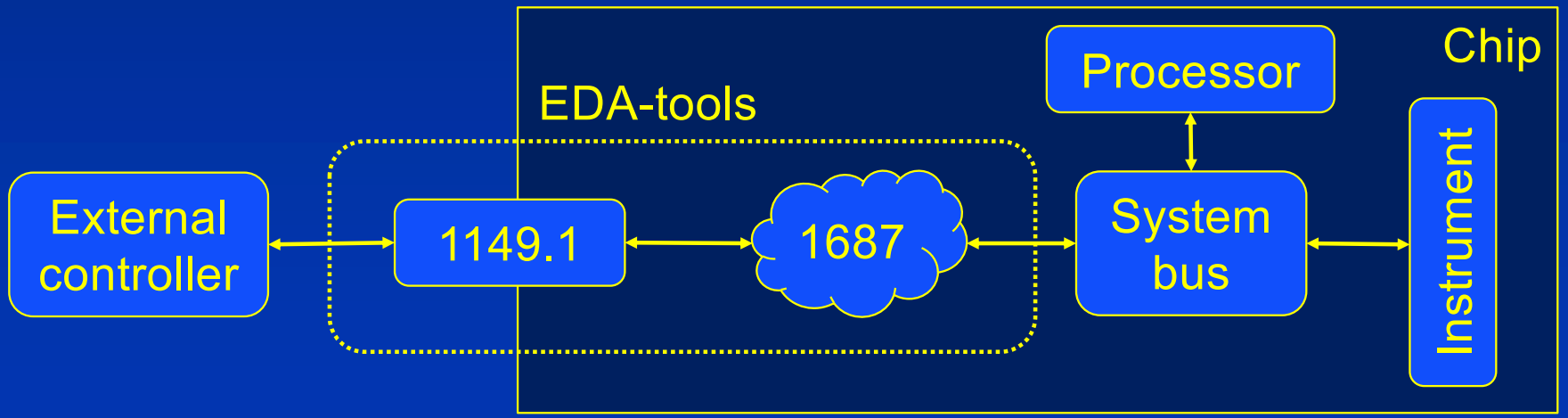
What is needed to avoid modifications?

iWrite Instrument Data;
iApply;

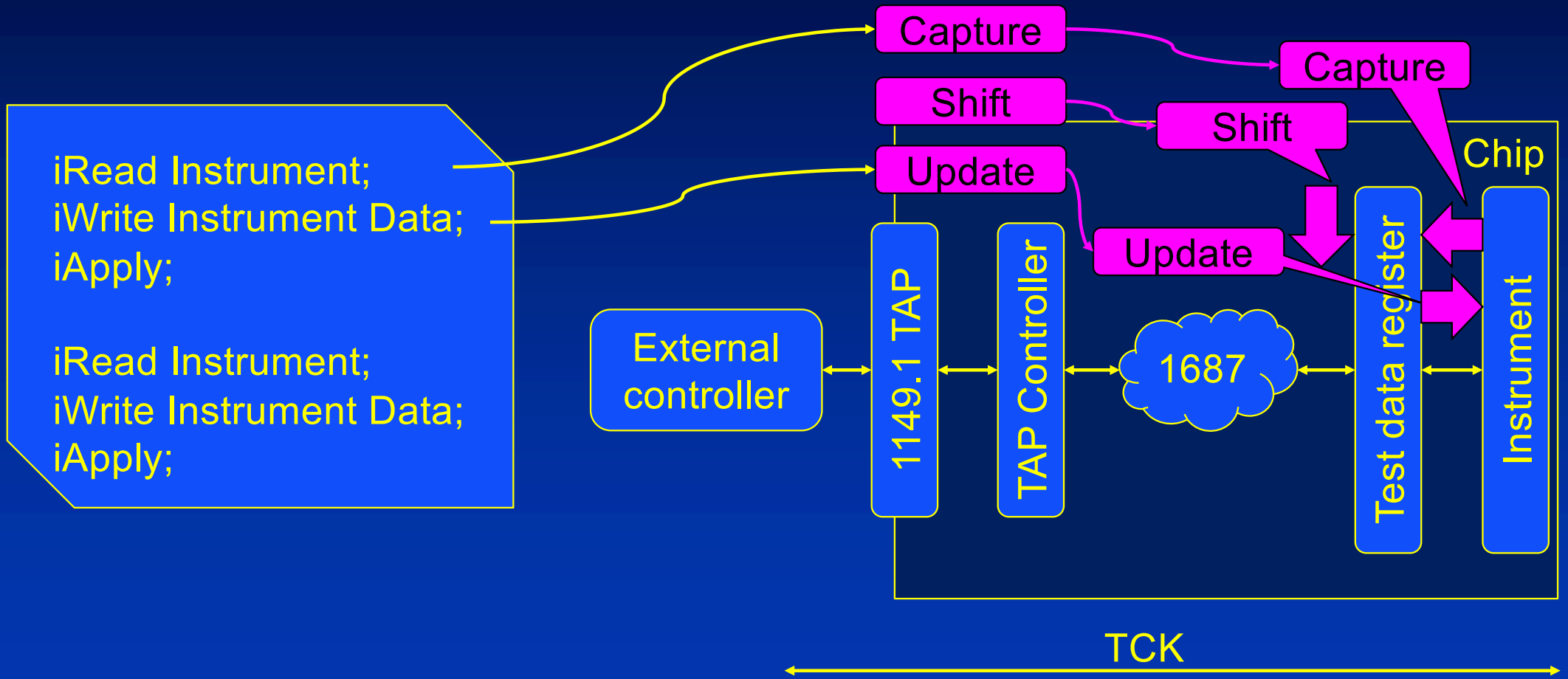
iRead Instrument;
iApply;

iWrite Instrument Data;
iWait xx;
iApply;

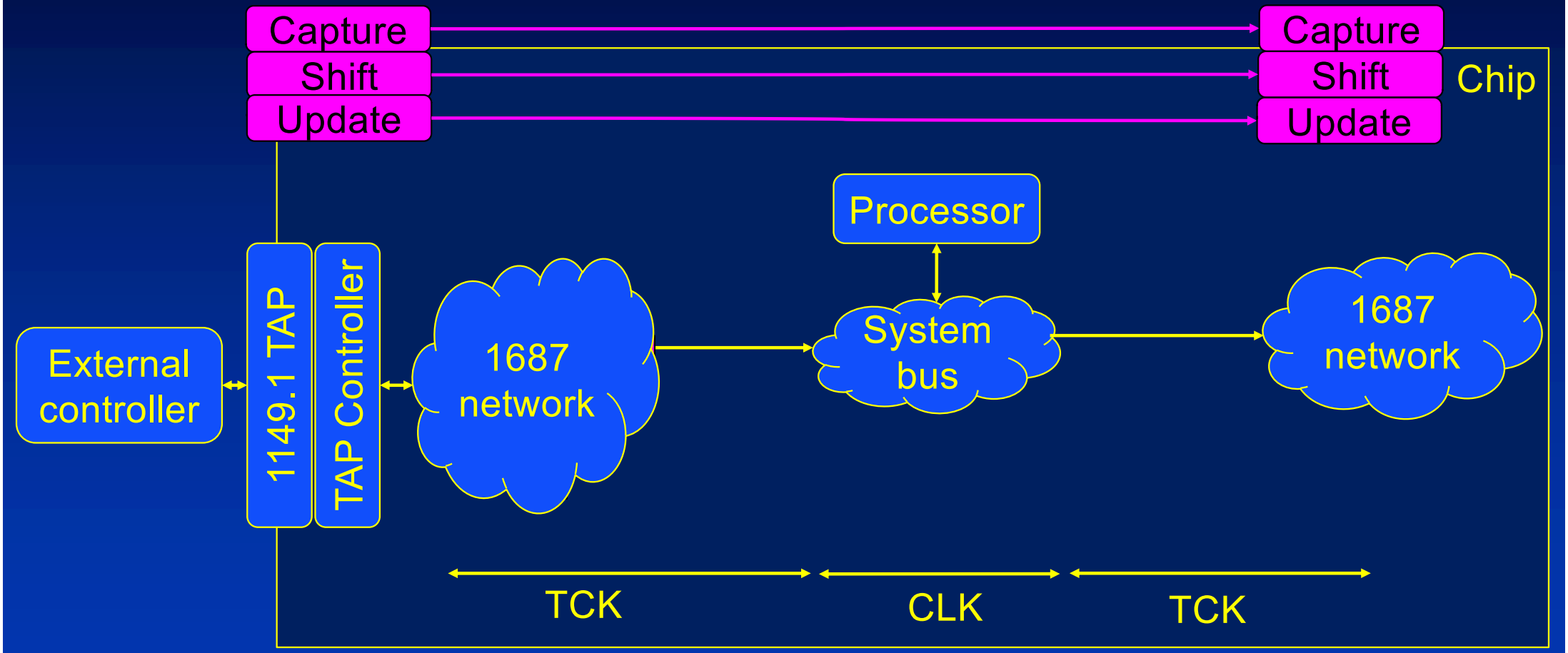
iRead Instrument;
iApply;



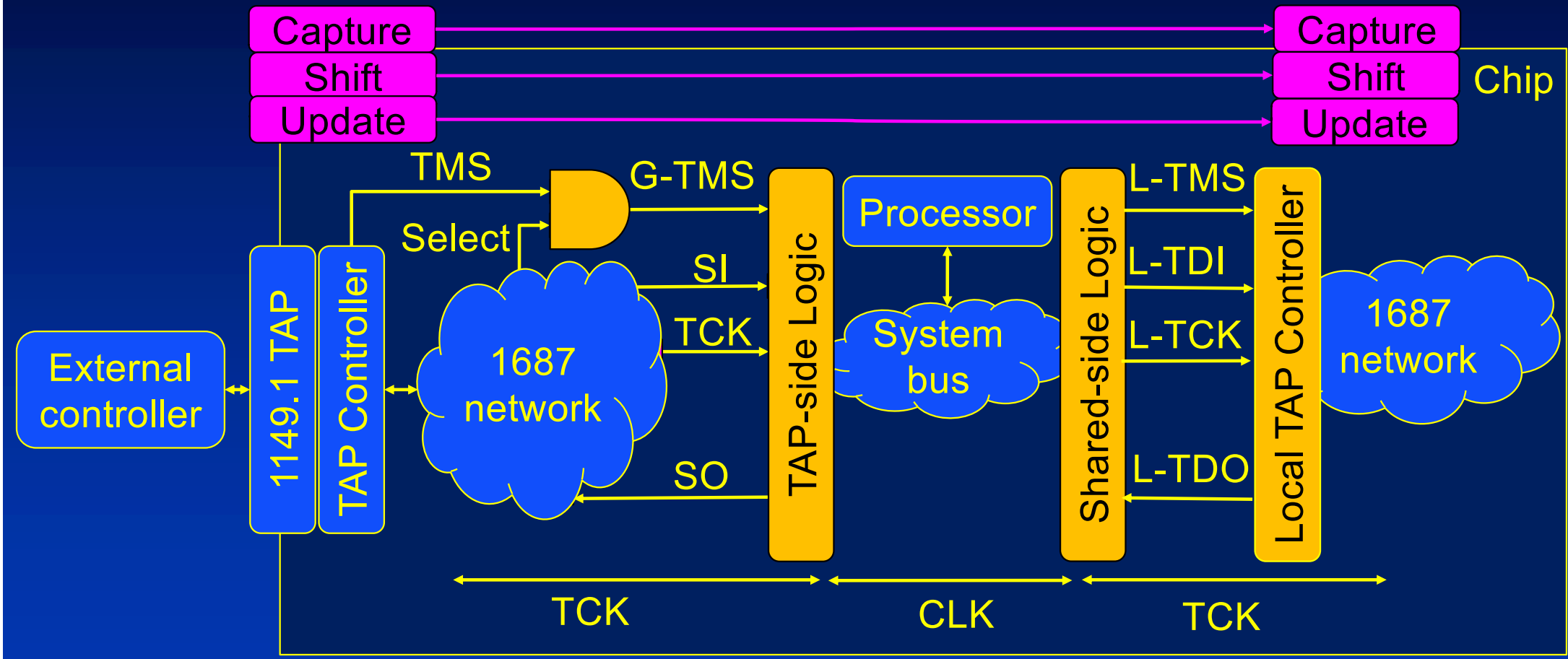
Standard access



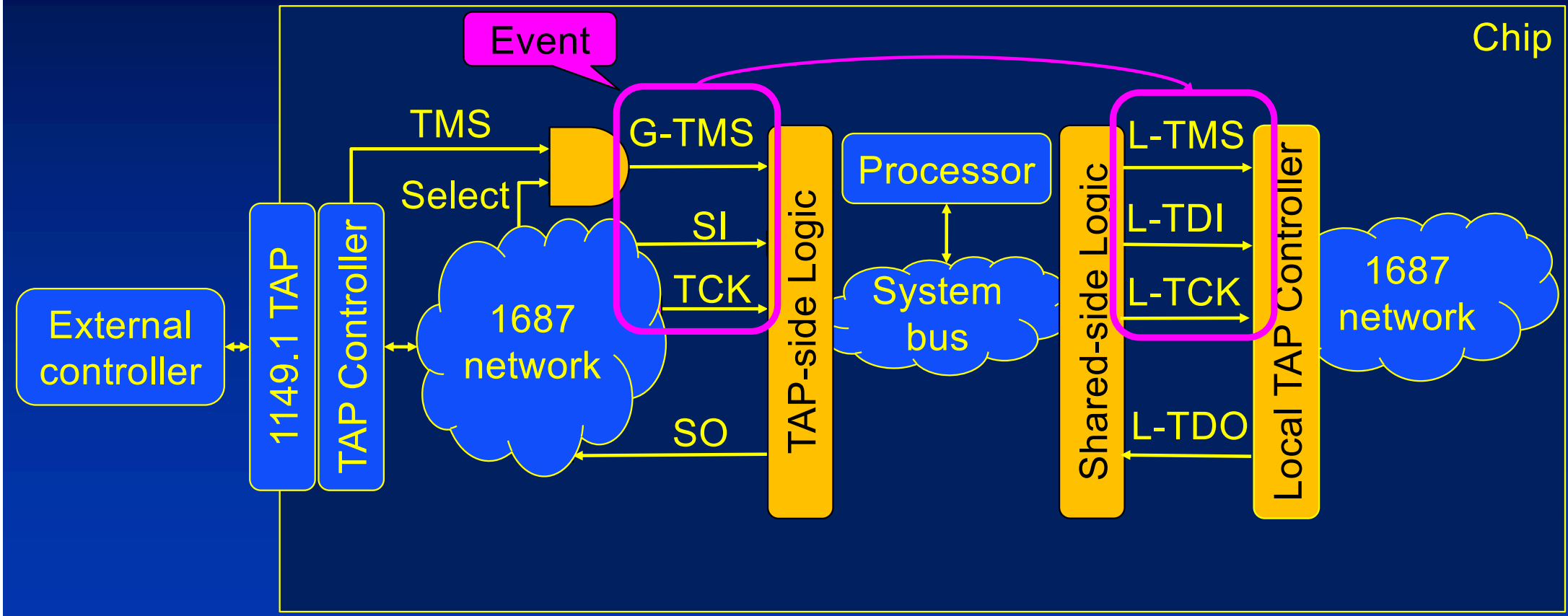
Segment sharing



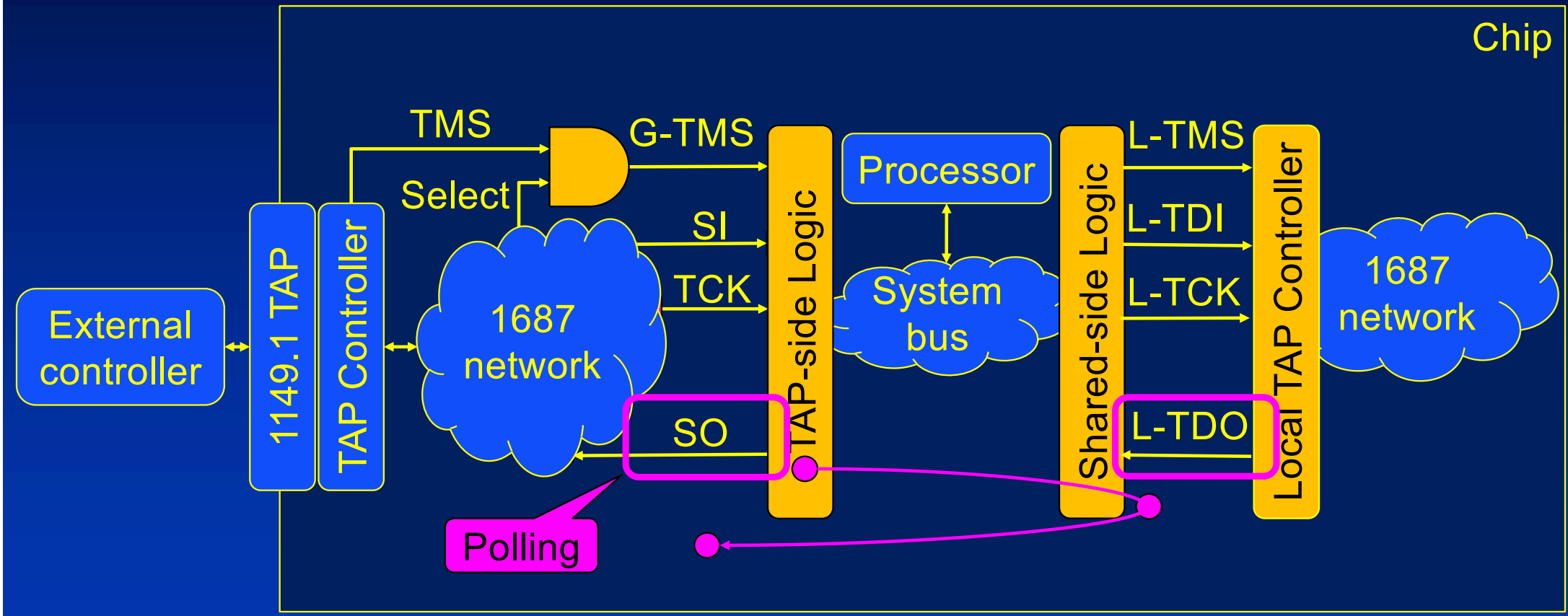
Segment sharing



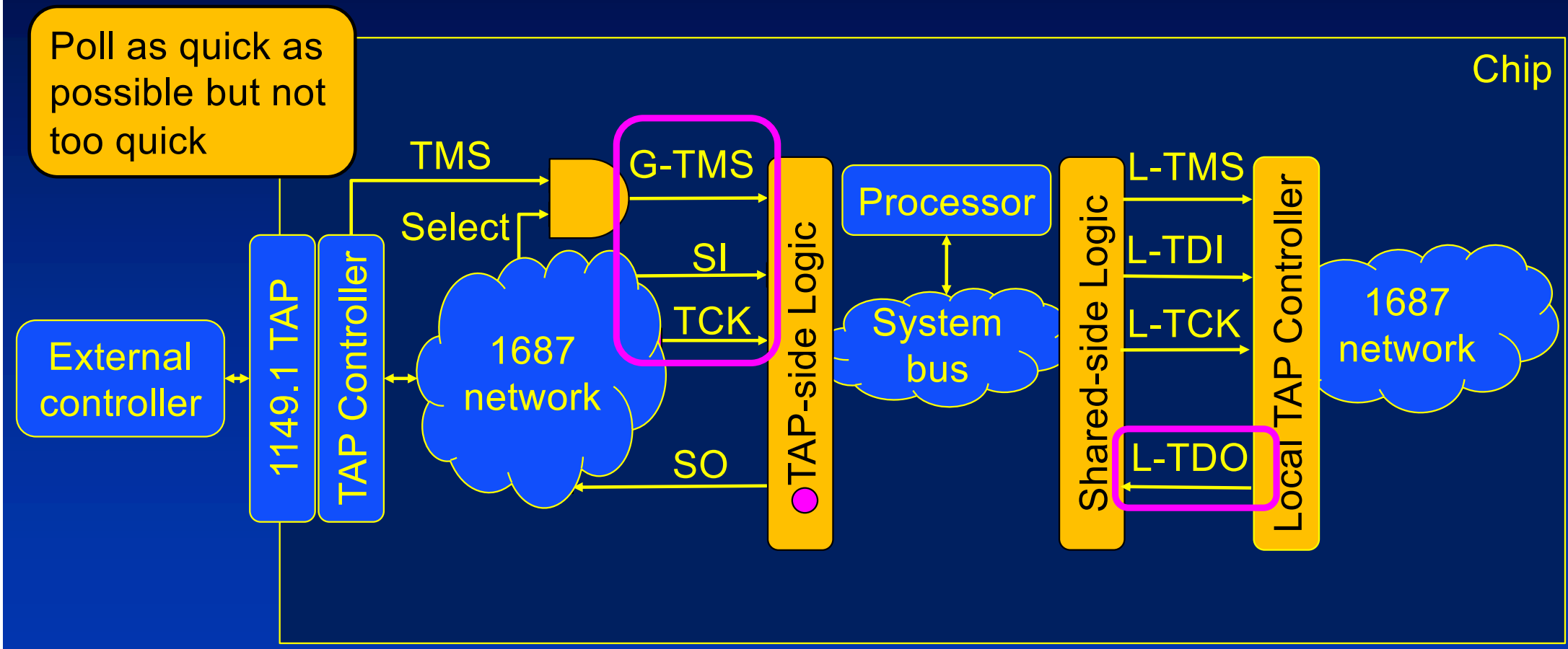
Segment sharing



Segment sharing



Segment sharing



Demonstration

- FPGA with an AXI Interconnect as the system bus
- Computed clock ration (TCK/CLK)
- Validated using Siemens Tessent IJTAG without modifications

F. G. Zadegan, Z. Zhang, K. Peterse´n, and E. Larsson, “Reusing ieee 1687-compatible instruments and sub-networks over a system bus,” in 2022 IEEE International Test Conference (ITC), 2022, pp. 219–228.

Summary

- High accessibility - controllability and observability - through the life-time
- Access should be for those who are trustable
- Access must be practical and easy to use
- Challenge to integrate access with functional operation
- Standardization initiatives (1687.1 and 2654)

Secure reuse of DfT during operation

Erik Larsson

LUND
UNIVERSITY