SECURE-IC

THE SECURITY SCIENCE COMPANY

Securing against cyber-attacks at physical level: Cyber-CPU

April 24, 2017 - Tokyo, Japan

Yan-Tarō CLOCHARD – クロシャー ル　威安太郎 – Director, Secure-IC Japan

Sylvain GUILLEY – ギーエイ シルヴァン – Co-founder, director of the "Think Ahead" business line

Table of contents

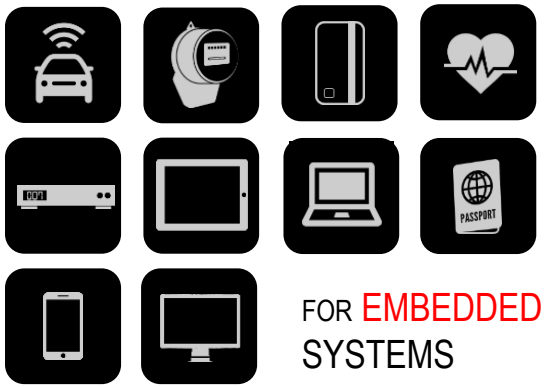
Presentation Outline

CORPORATE PRESENTATION

OUR ACTIVITY

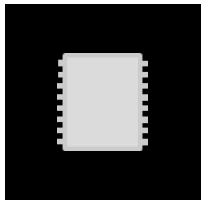
WHAT DO WE DO?

SECURITY TECHNOLOGIES



FOR EMBEDDED SYSTEMS

FOR WHOM?



CHIPSET/DEVICE VENDORS

IC DESIGN HOUSES

CERTIFICATION LABS

GOVERNMENTAL AGENCIES

FOR WHICH MARKETS?

OUR VISION

Going forward, there will be more and more interconnected devices or objects in various market verticals, this is what we call Internet of Things or Internet of Everything. All those objects being interconnected to the cloud, each and every object could be a threat for the whole network. Therefore the security of the objects or the devices is key. Even more, security will become one of the most important asset of the digital world.

CORPORATE PRESENTATION

THE COMPANY

EMBEDDED SYSTEMS SECURITY RESEARCH

2010 FOUNDING

2017 ~45 PEOPLE 4 COUNTRIES

MORE THAN
15 YEARS OF RESEARCH

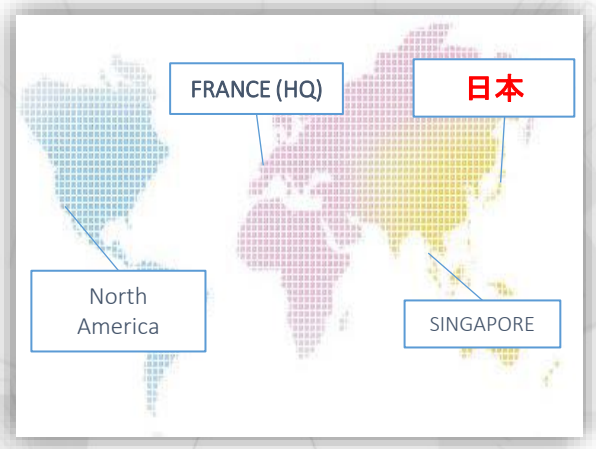
MORE THAN
200 PUBLICATIONS

SPIN-OFF FROM
INSTITUT MINES-TELECOM

Institut Mines-Télécom

SECURE-IC
THE SECURITY SCIENCE COMPANY

PÔLE D'EXCELLENCE CYBER



Technology Fast 50 2015 FRANCE

bpifrance EXCELLENCE

FRENCH TECH PASS IMAGES & RÉSEAUX 2015

CORPORATE PRESENTATION

BUSINESS LINES

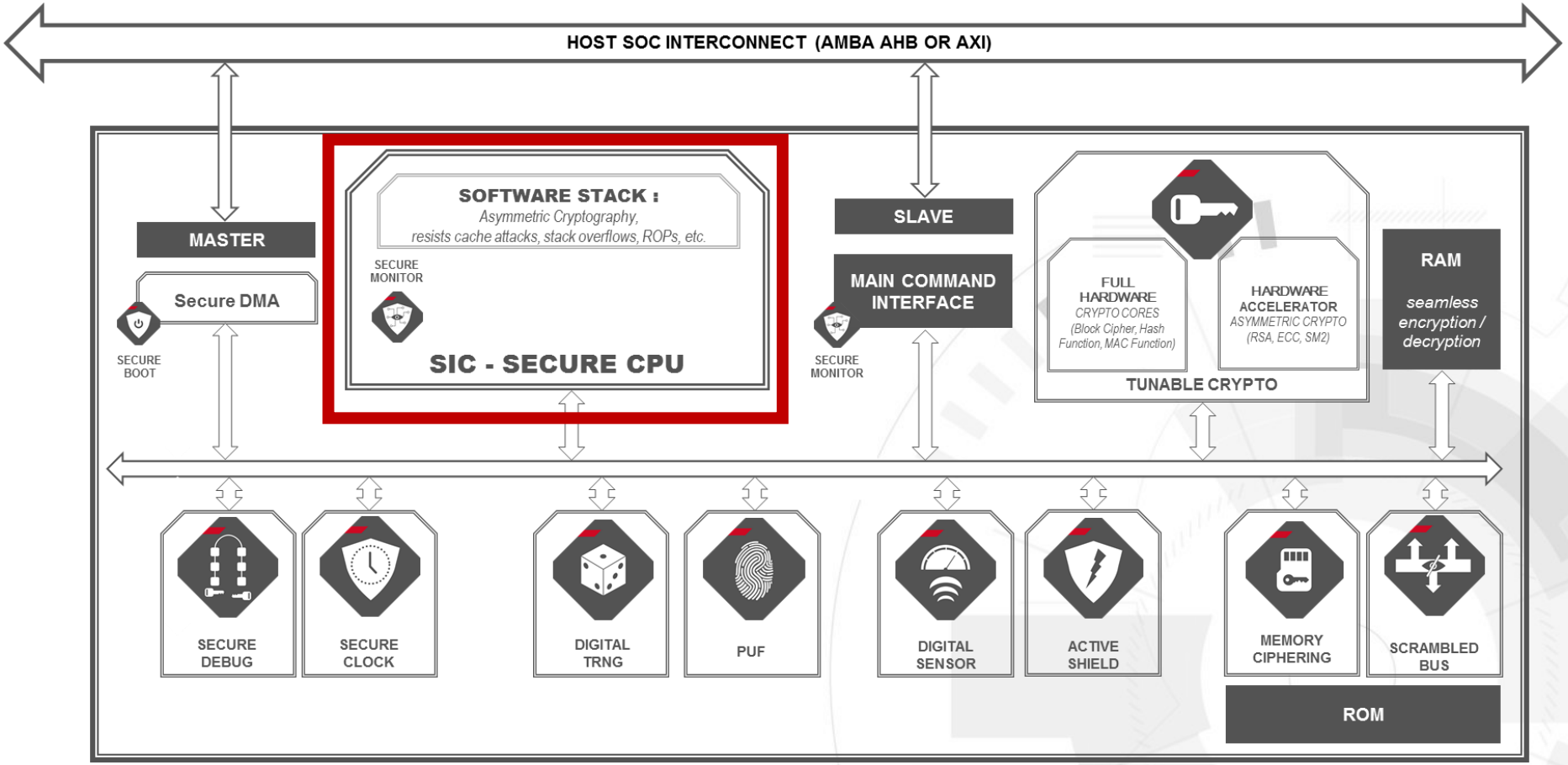
PROTECT	EVALUATE	SERVICE
SECURYZR	**LABORYZR**	**EXPERTYZR**
COMBINATION OF **SMART UNITS** AND **EXPERTISE RESULTS**	READY-TO-USE **PRE** AND **POST-SILICON ANALYSIS PLATFORMS**	THE **NEXT STEPS** TOWARDS **SECURITY CHALLENGES**

CORPORATE PRESENTATION

SECURYZR

PROTECT

SECURYZR



Presentation Outline

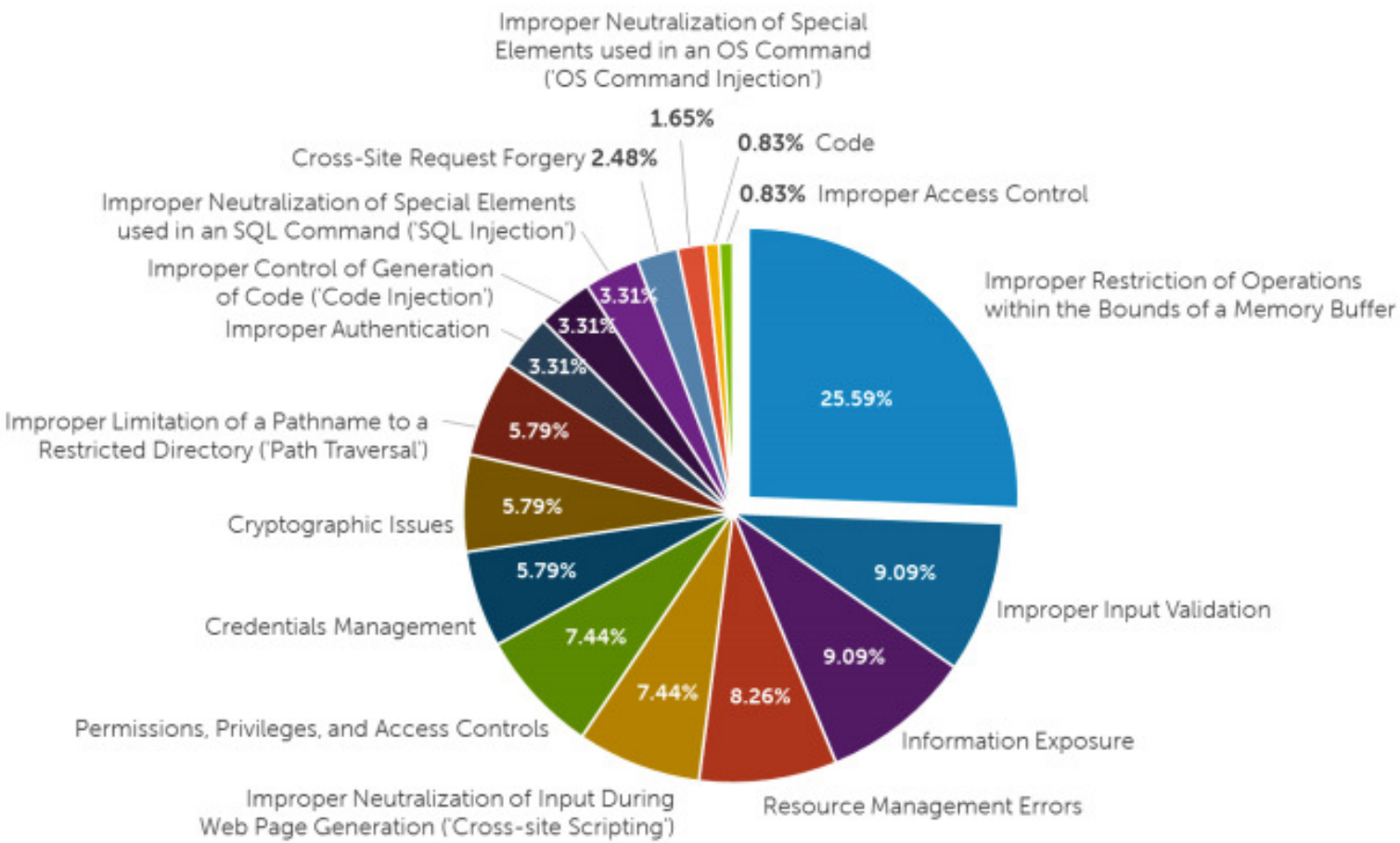
Industrial systems, a new target

Attacks on industrial systems are nowadays real:

- Large deployment ⇒ attacks scale
- Physical access to the devices ⇒ physical attacks
- Remote access to the devices ⇒ cyber attacks
- Do not always run an OS
- Little protections
- Problem of updates
- Little or no configuration
- Many vulnerabilities

⇒ Importance to strengthen the security of industrial systems against both *cyber* and *physical* attacks.

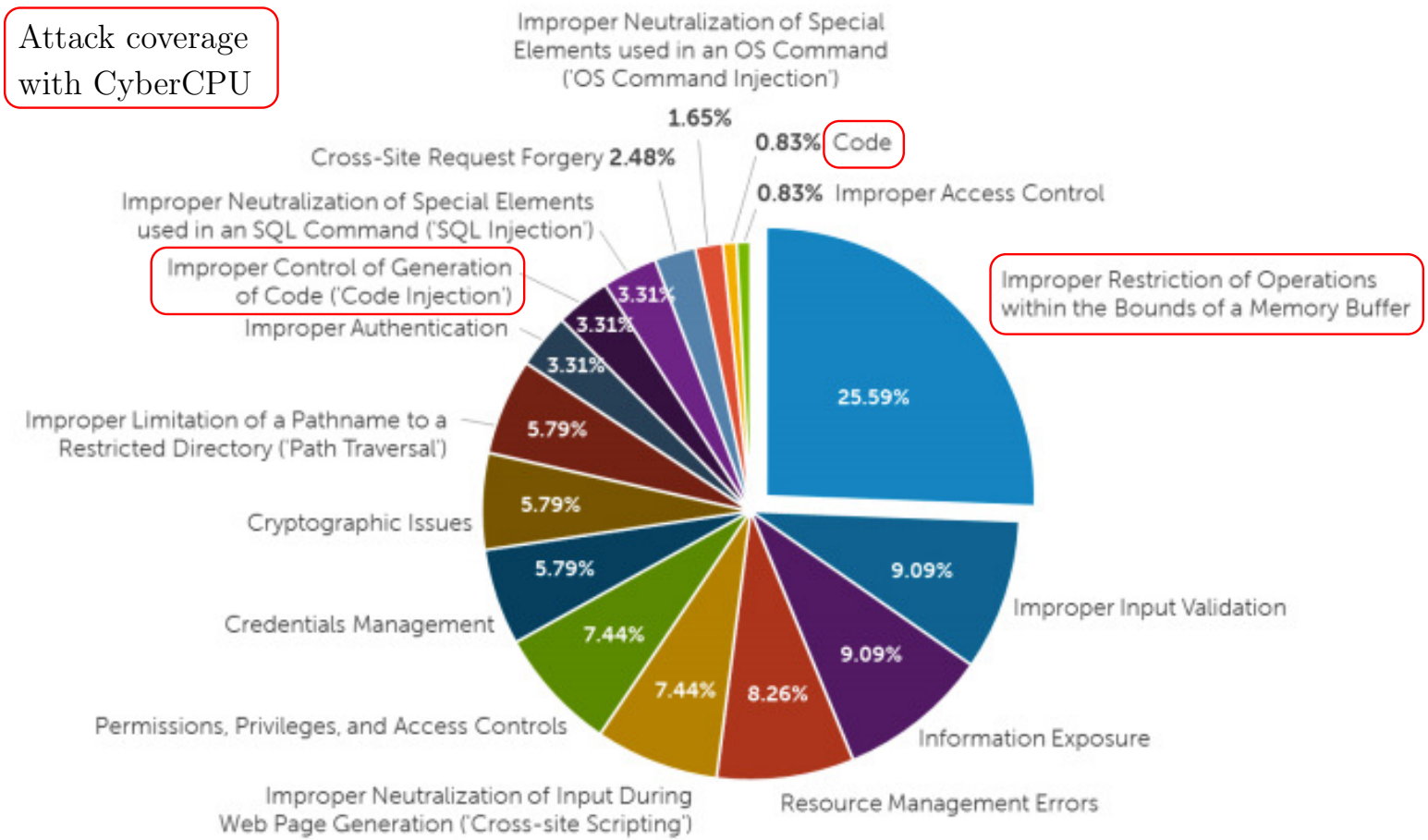
Most frequent attack methods on SCADA



Source: https://threatpost.com/dell-threat-report-claims-100-percent-increase-in-scada-attacks

Most frequent attack methods on SCADA

Attack coverage with CyberCPU



Source: https://threatpost.com/dell-threat-report-claims-100-percent-increase-in-scada-attacks

Common Weakness Enumeration
A Community-Developed List of Software Weakness Types

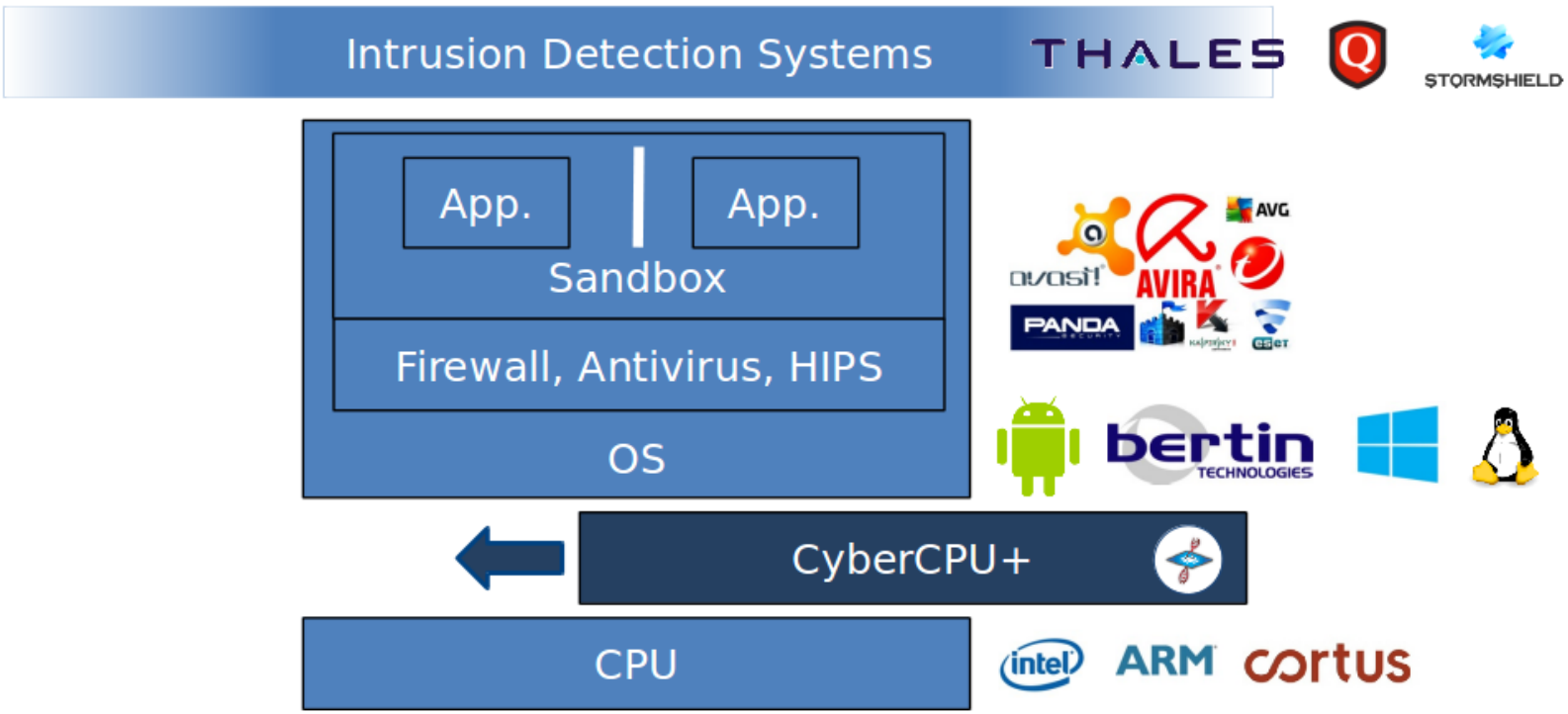
CyberCPU weaknesses mitigation :

- Authentication Issues — CWE-287
- Buffer Errors — CWE-119
- Code — CWE-17
- Code Injection — CWE-94
- Command Injection — CWE-77
- Configuration — CWE-16
- Credentials Management — CWE-255
- Cross-Site Request Forgery (CSRF) — CWE-352
- Cross-Site Scripting (XSS) — CWE-79
- Cryptographic Issues — CWE-310
- Data Handling — CWE-19
- Format String Vulnerability — CWE-134
- Improper Access Control — CWE-284
- Indicator of Poor Code Quality — CWE-398
- Information Leak / Disclosure — CWE-200
- Information Management Errors — CWE-199
- Injection — CWE-74
- Input Validation — CWE-20
- Insufficient Information — NVD-CWE-noinfo
- Insufficient Verification of Data Authenticity — CWE-345
- Link Following — CWE-59
- Location — CWE-1
- Numeric Errors — CWE-189
- OS Command Injections — CWE-78
- Other — NVD-CWE-Other
- Path Equivalence — CWE-21
- Path Traversal — CWE-22
- Permissions, Privileges, and Access Control — CWE-264
- Race Conditions — CWE-362
- Resource Management Errors — CWE-399
- Security Features — CWE-254
- Source Code — CWE-18
- SQL Injection — CWE-89
- Time and State — CWE-361

Presentation Outline

CyberCPU:

a complementary technology against cyber-physical attacks

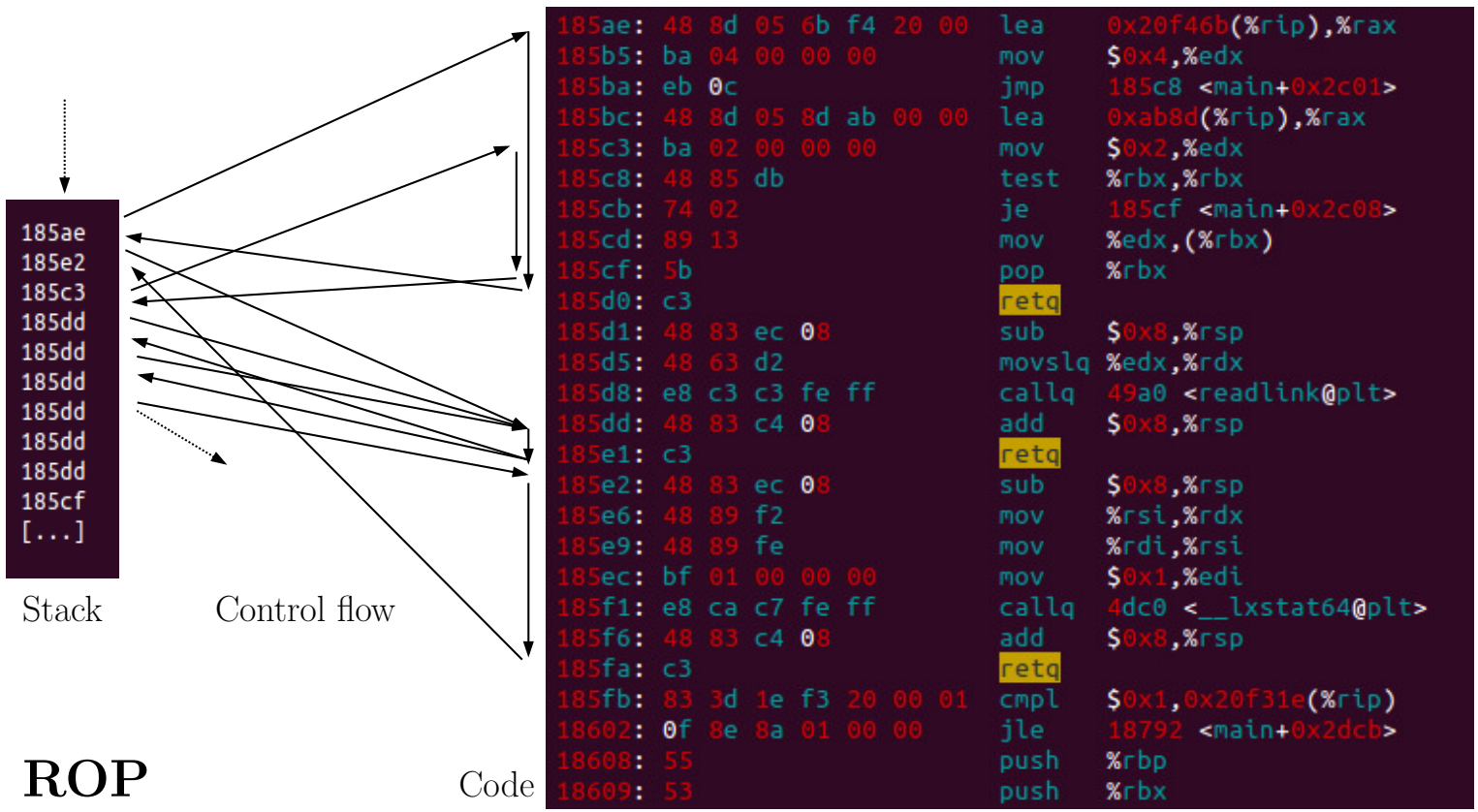


TELECOM ParisTech

rapid

INNOVATION 2030
CONCOURS MONDIAL D'INNOVATION

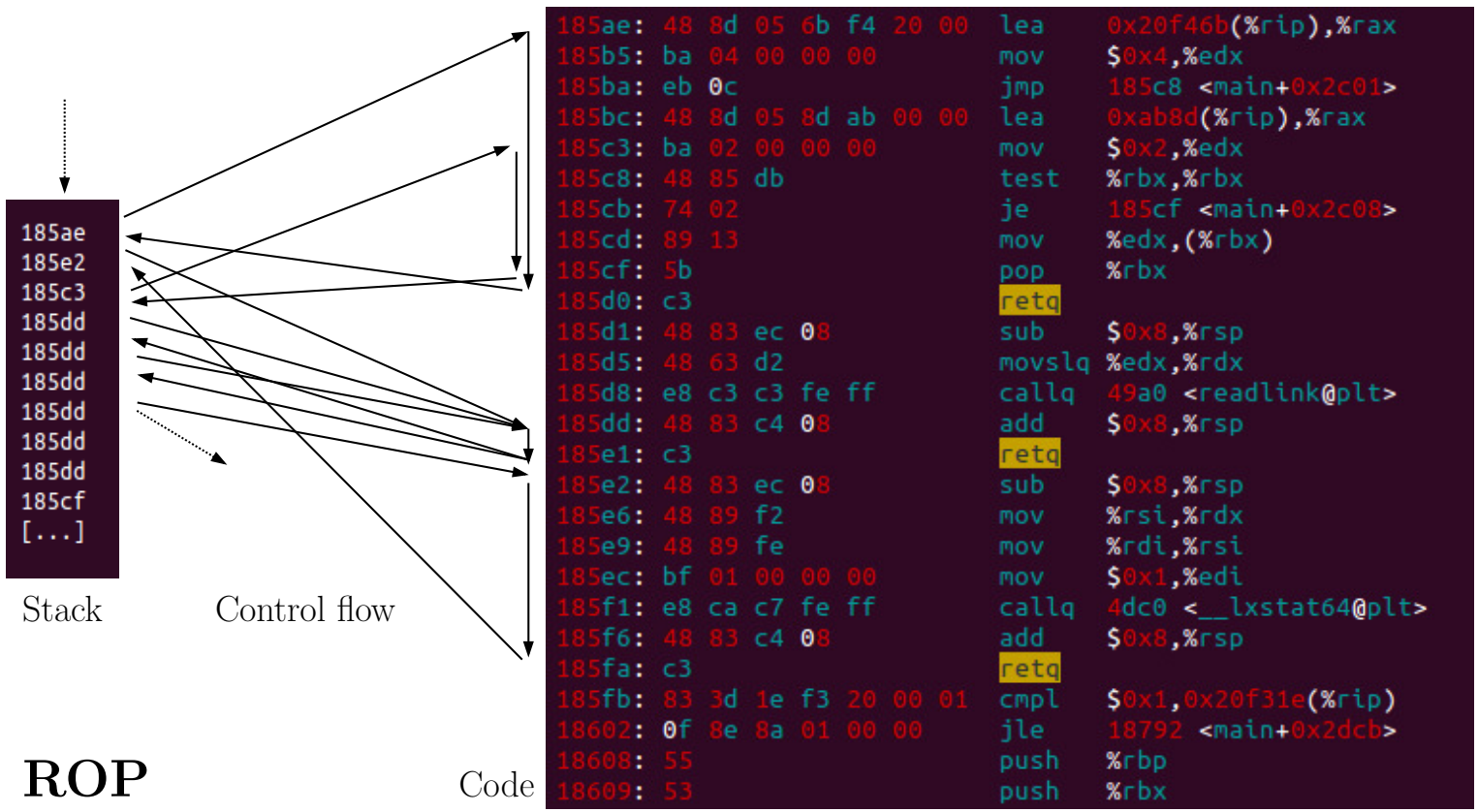
Why shall we react quickly against memory errors?



① smash the stack,

② exploit in a few instructions.

Why shall we react quickly against memory errors?



Analyzing behaviour $\Longrightarrow$ way too late!

Wait for next execution slot $\Longrightarrow$ also too late...

Pros and Cons of hardware-based solutions

Pros:

- Real-time detection: stops the injection before malware is spread
- Maximal coverage of code, always on
- Hardware = simple, hence less chance to have a bug
- Cannot be exploited (unavailable to the attacker)
- No false positives, because we trace low level execution

Cons:

- More hardware = more costs, more validation
- Requires a new design, hence cannot be used with COTS.
  Alternatives:
  1. Augment an existing processor (example of the SPARC LEON)
  2. Design a new processor (example of a security crypto-processor)

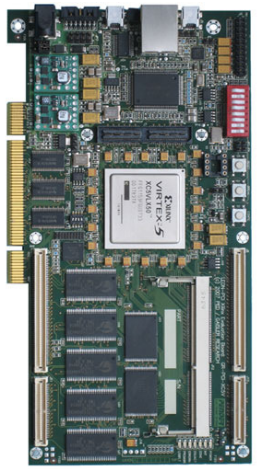
❶ LEON patch

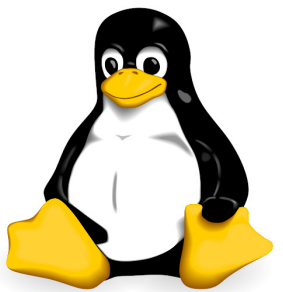
gaisler/leon3v3/iu3.vhd

```
procedure logic_op(r : registers; aluin1, aluin2, mey : word;
      ymsb : std_ulogic; logicres, y : out word) is
variable logicout : word;
begin
  case r.e.aluop is
  when EXE_AND   => logicout := aluin1 and aluin2;
  when EXE_ANDN  => logicout := aluin1 and not aluin2;
  when EXE_OR    => logicout := aluin1 or aluin2;
  when EXE_ORN   => logicout := aluin1 or not aluin2;
  when EXE_XOR   => logicout := aluin1 xor aluin2;
  when EXE_XNOR  => logicout := aluin1 xor not aluin2;
  when EXE_DIV   =>
    if DIVEN then logicout := aluin2;
    else logicout := (others => '-'); end if;
  when others => logicout := (others => '-');
  end case;
  if (r.e.ctrl.wy and r.e.mulstep) = '1' then
    y := ymsb & r.m.y(31 downto 1);
  elsif r.e.ctrl.wy = '1' then y := logicout;
  elsif r.m.ctrl.wy = '1' then y := mey;
  elsif MACPIPE and (r.x.mac = '1') then y := mulo.result(63 downto 32);
  elsif r.x.ctrl.wy = '1' then y := r.x.y;
  else y := r.w.s.y; end if;
  logicres := logicout;
end;
```

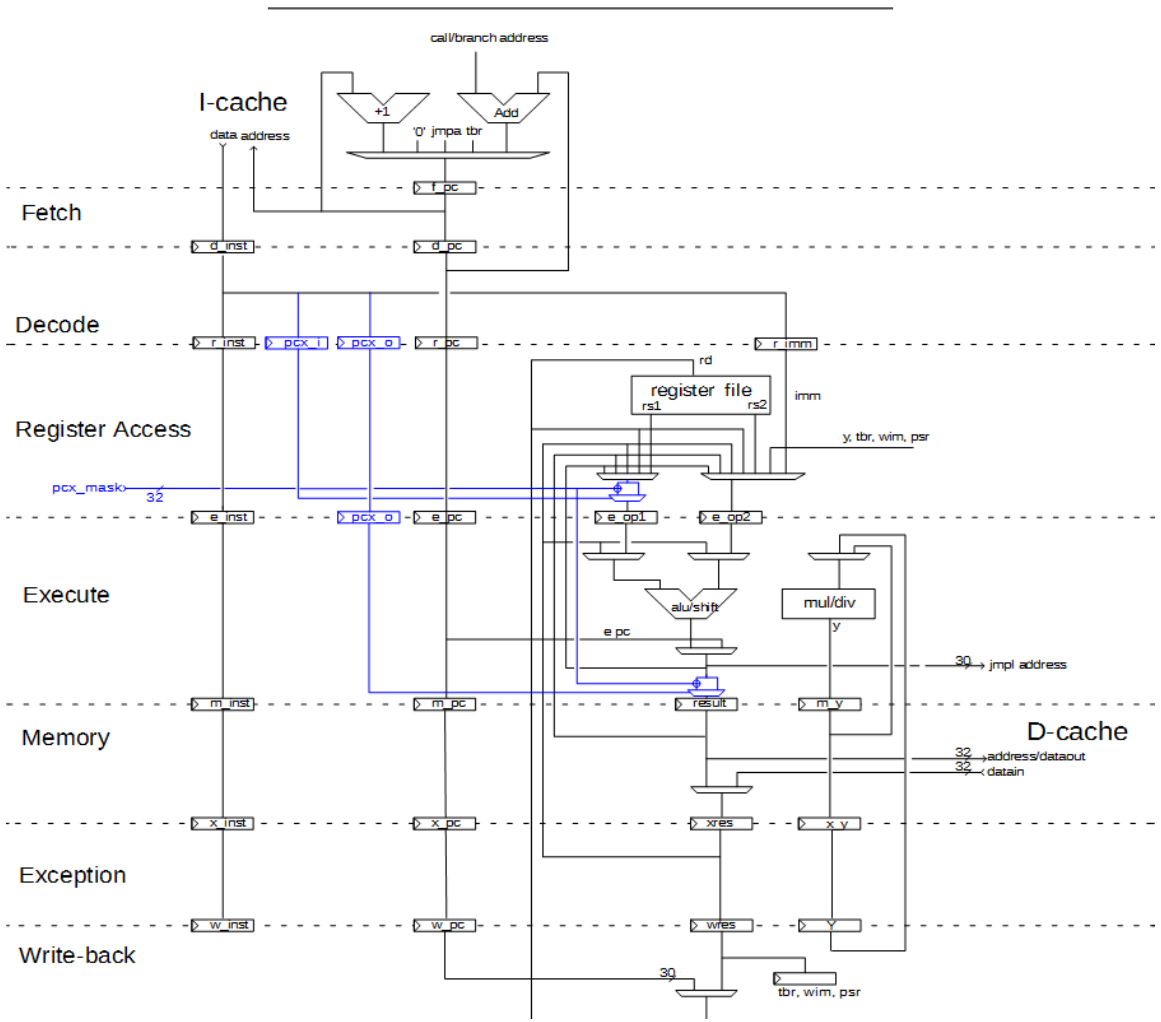
cybercpu/leon3v3/iu3_patch.vhd

```
hcode.op.stack <= r.e.aluop;
hcode.ip.stack <= r.e.ip;
```





❶ LEON patch



❷ Security (crypto-)processor

- Simple instruction set
- No cache, hence no cache attacks
- Accelerated for crypto: slow-down is mitigated
- Embeds physical protection: shield + sensors, and a management unit to aggregate them securely

Presentation Outline

CyberCPU project

The four protections:

Protection type	Protected asset	REV	PCX	SCALL	HCODE
Preventive	Code	✓			
Preventive	CFG		✓		
Detective	Code				✓
Detective	CFG			✓	✓

CFG: Control Flow Graph.

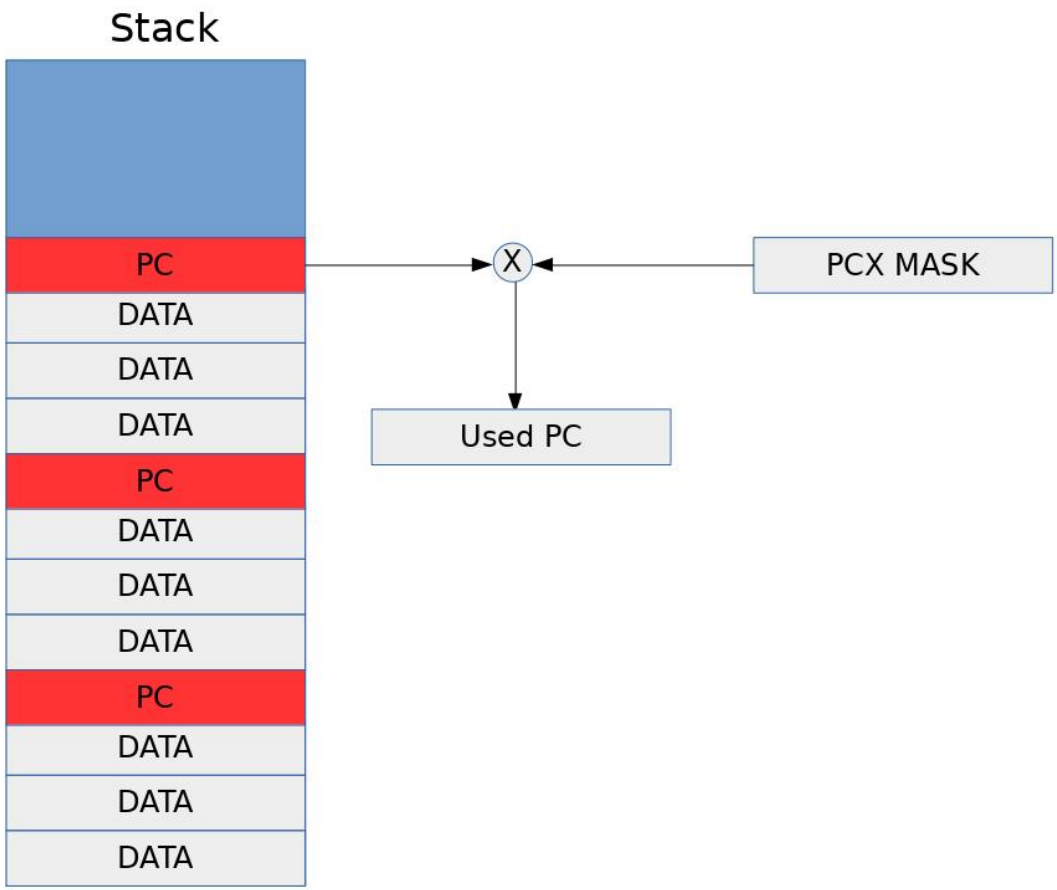
CyberCPU: the REV protection

The processor is added an instruction "REV", which allow the CPU to switch to "encrypted code" mode.

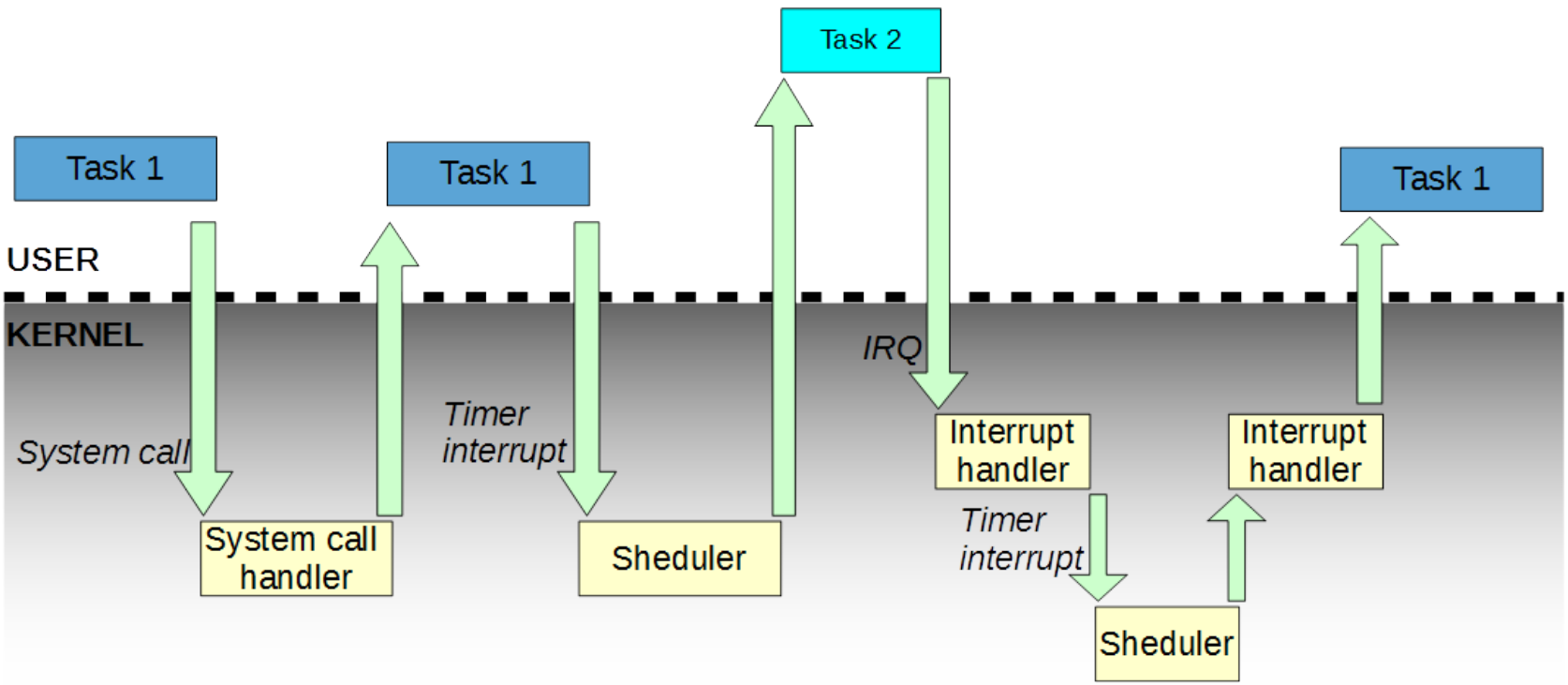
```
80 c8 2a 41 rev @       ! Activation de REV
de ad be ef       unknown           ! Instruction chiffrée
de ad be ef       unknown
de ad be ef       unknown
de ad be ef       unknown
de ad be ef       unknown
de ad be ef       unknown
de ad be ef       unknown           ! Désactivation de REV (80 c8 20
00)
c2 07 bf f8 ld [ %fp + -8 ], %g1
82 00 60 01       inc %g1
c2 27 bf f8       st %g1, [ %fp + -8 ]
c2 07 bf f8       ld [ %fp + -8 ], %g1
80 a0 60 09       cmp %g1, 9
04 bf ff f7       ble 14c <toto+0x20>     ! « branch » posant problème
01 00 00 00       nop
```

CyberCPU: the PCX protection

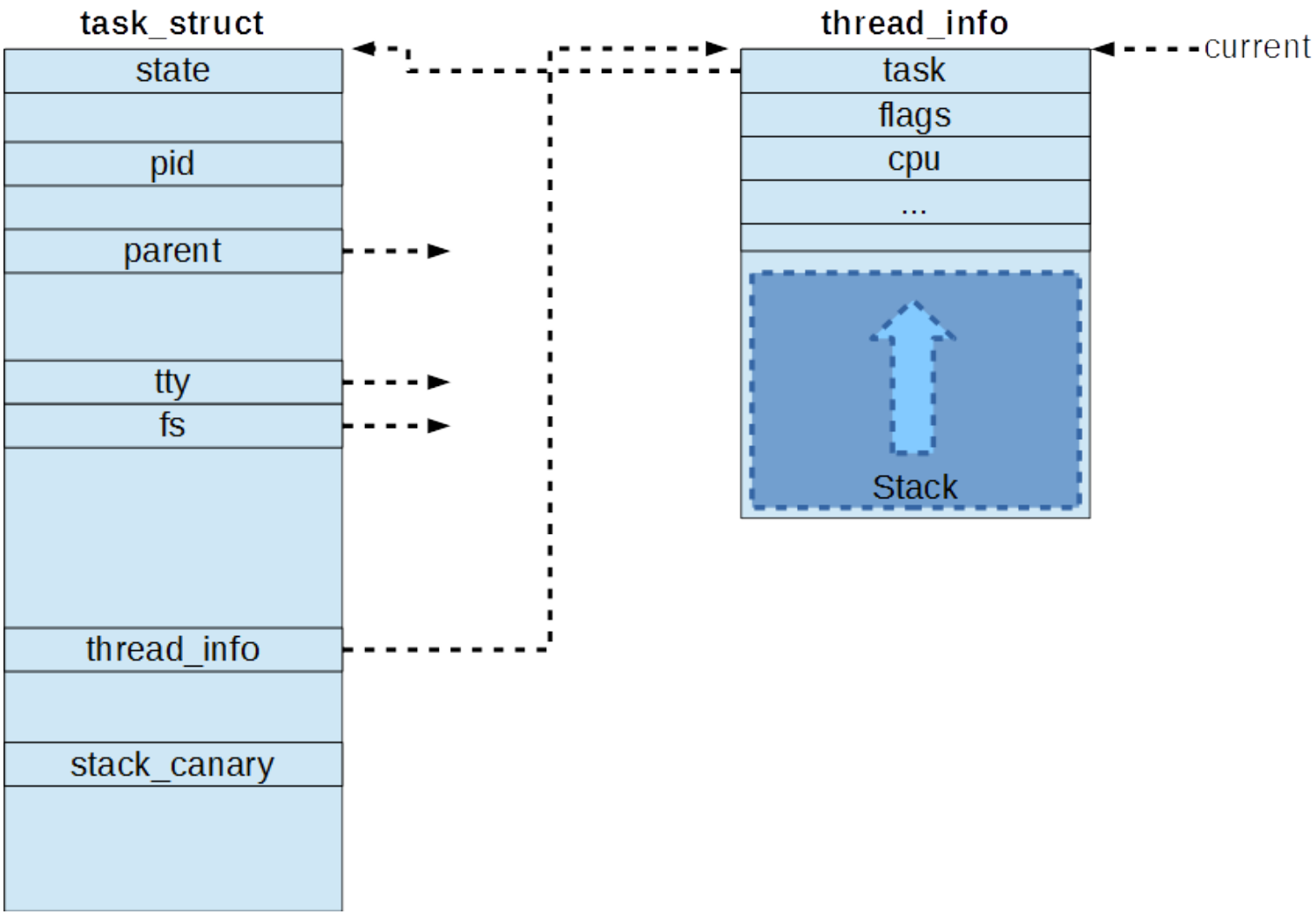
The processor "encrypts" the PC before saving it on the stack.



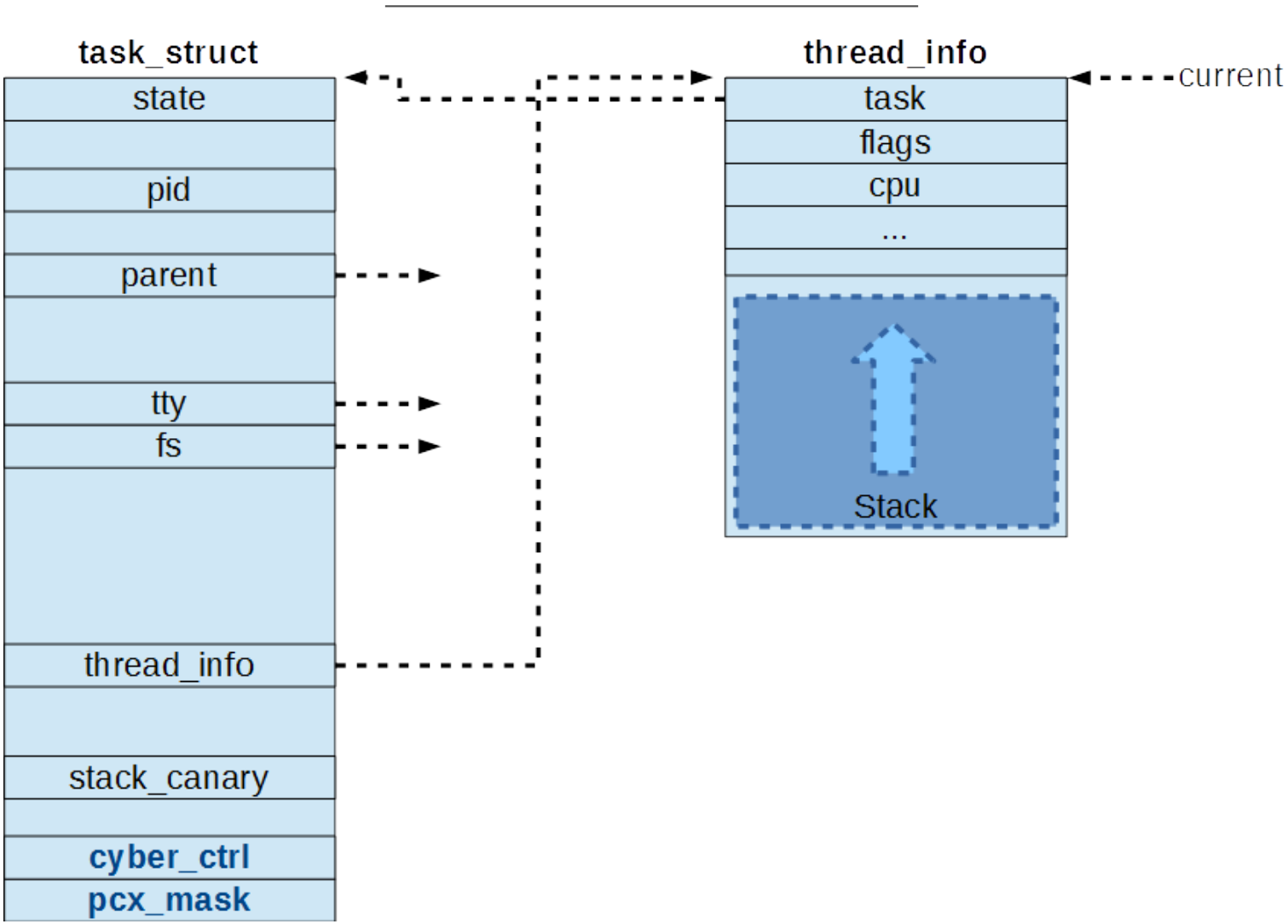
PCX integration



PCX integration



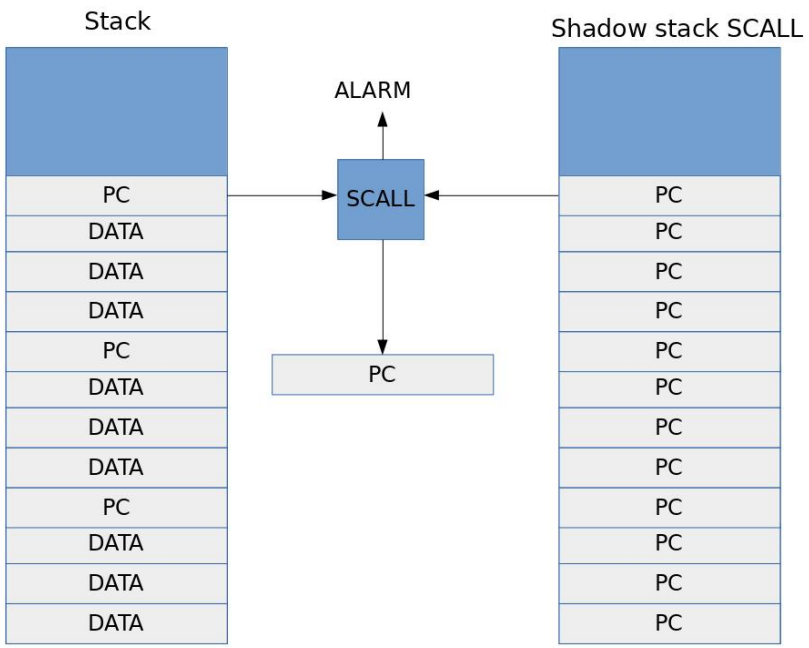
PCX integration



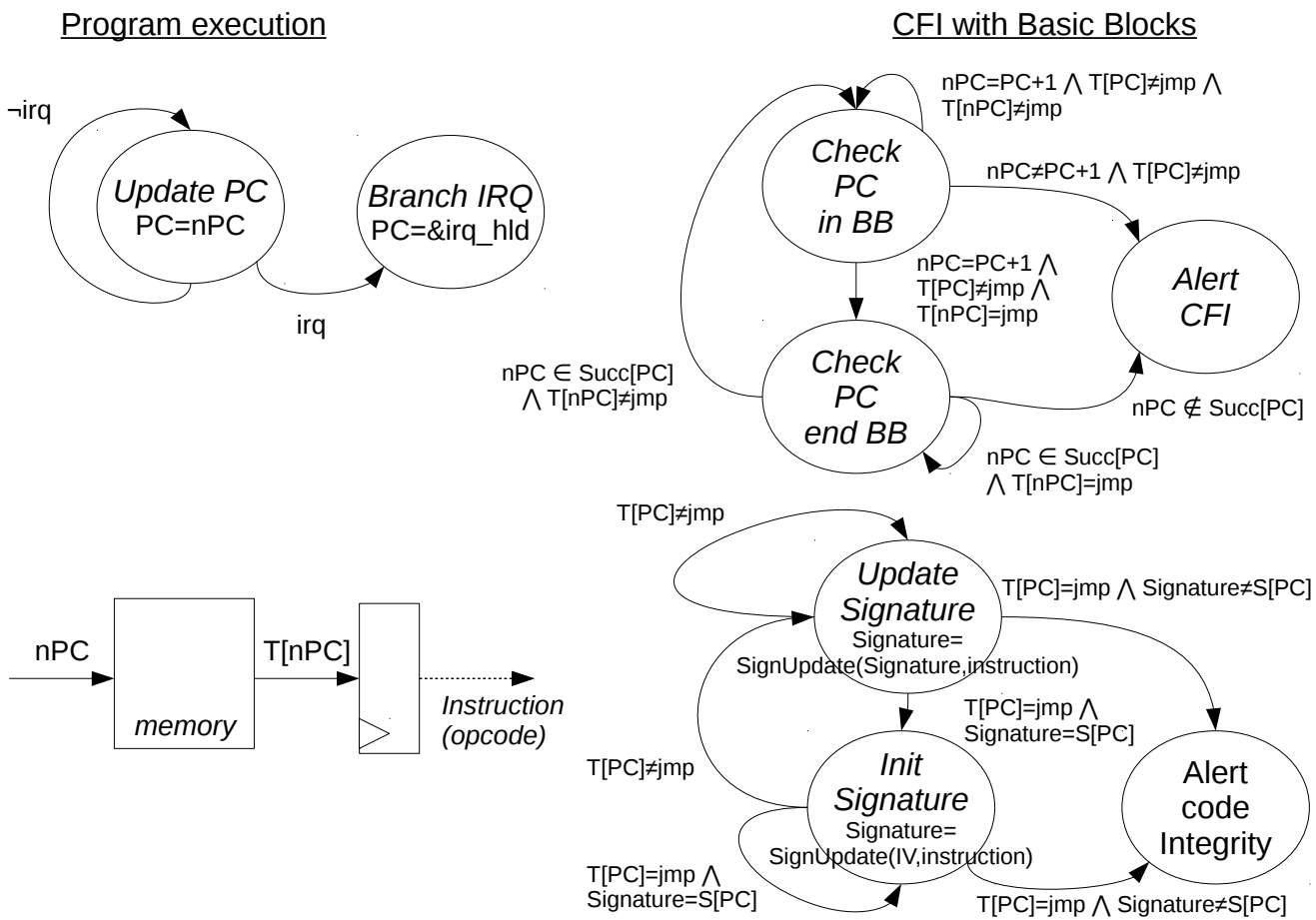
CyberCPU: the SCALL protection

Dual usage of the technology:

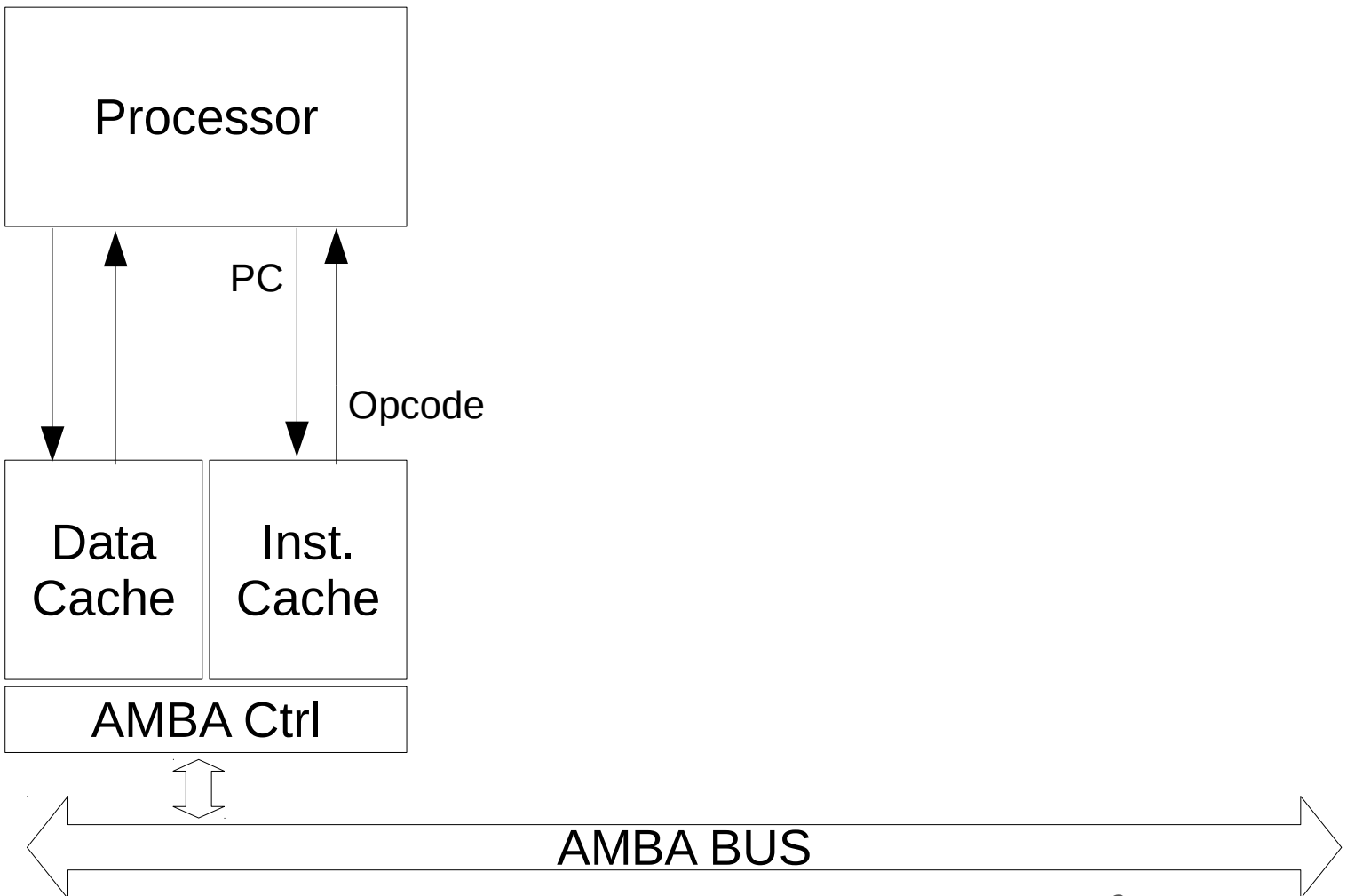
- in a *security* context: inform the OS of the mismatch,
- in a *safety* context: restore the PC, so that the system comes back to a stable state.



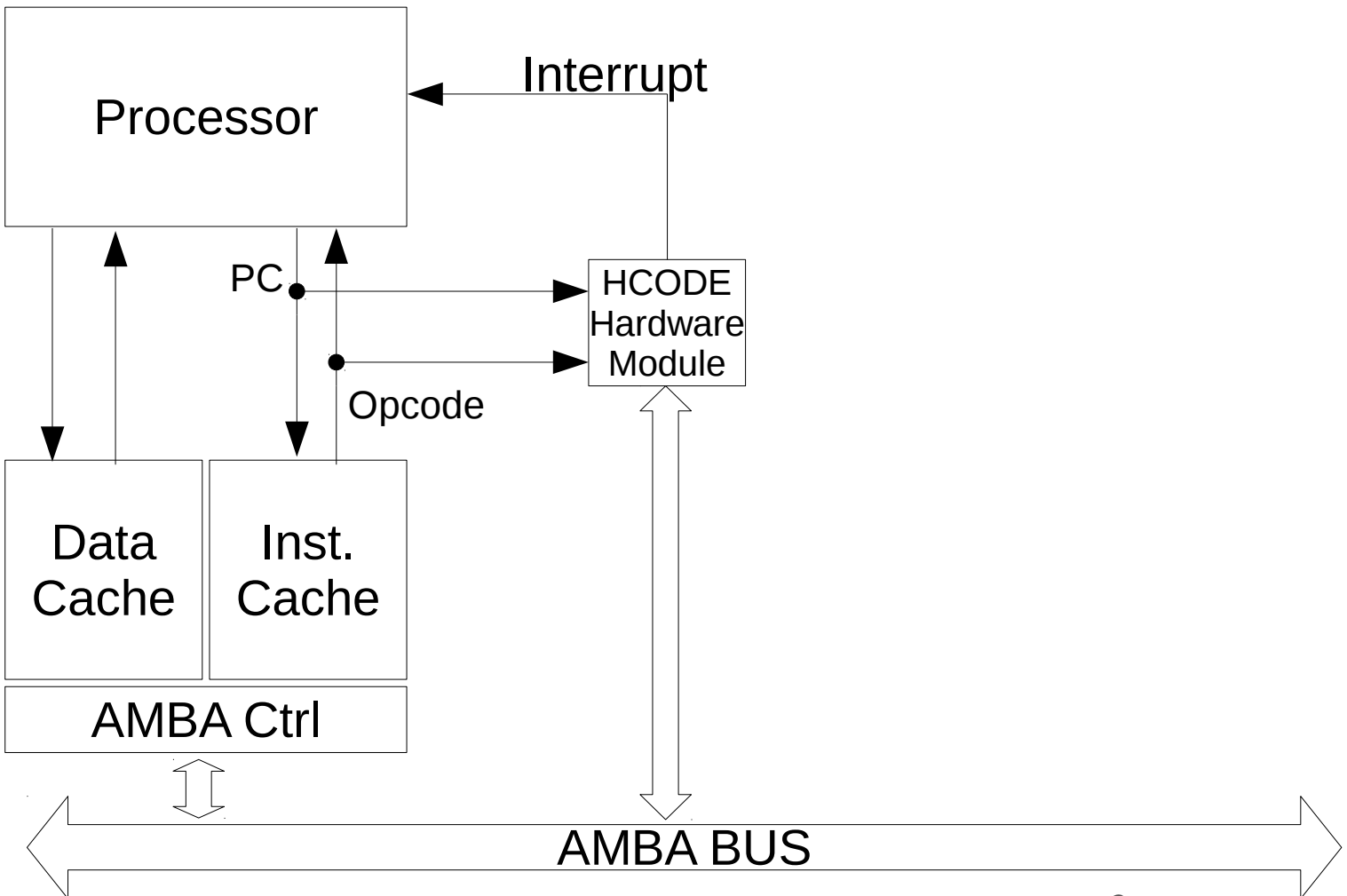
CyberCPU: the HCODE protection



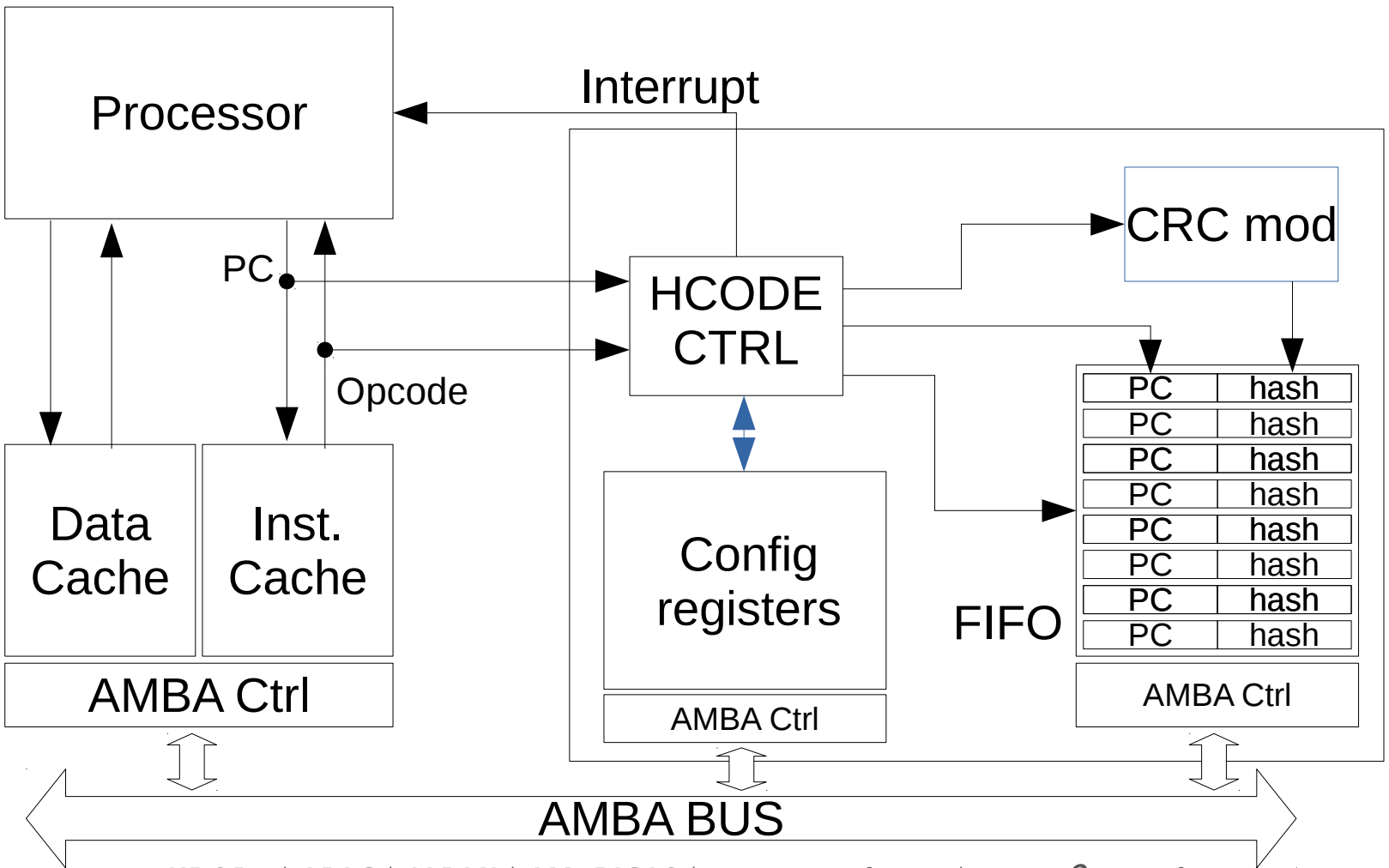
Hardware implementation of HCODE



Hardware implementation of HCODE



Hardware implementation of HCODE



Presentation Outline

Joint publications between Secure-IC and Japanese partners

2016

[1] Kazuhide Fukushima, Youssef Souissi, Seira Hidano, Robert Nguyen, Jean-Luc Danger, Sylvain Guilley, Yuto Nakano, Shinsaku Kiyomoto, and Laurent Sauvage. Delay PUF assessment method based on side-channel and modeling analyzes: The final piece of all-in-one assessment methodology. In *2016 IEEE Trustcom/BigDataSE/ISPA, Tianjin, China, August 23-26, 2016*, pages 201–207. IEEE, 2016.

2015

[2] Sho Endo, Yang Li, Naofumi Homma, Kazuo Sakiyama, Kazuo Ohta, Daisuke Fujimoto, Makoto Nagata, Toshihiro Katashita, Jean-Luc Danger, and Takafumi Aoki. A silicon-level countermeasure against fault sensitivity analysis and its evaluation. *IEEE Trans. VLSI Syst.*, 23(8):1429–1438, 2015.

[3] Daisuke Fujimoto, Makoto Nagata, Shivam Bhasin, and Jean-Luc Danger. A Novel Methodology for Testing Hardware Security and Trust Exploiting On-Chip Power Noise Measurement. In *ASPDAC*, IEEE Computer Society, January 2015. Tokyo, Japan.

2014

[4] Daisuke Fujimoto, Noriyuki Miura, Makoto Nagata, Yu-ichi Hayashi, Naofumi Homma, Takafumi Aoki, Yohei Hori, Toshihiro Katashita, Kazuo Sakiyama, Thanh-Ha Le, Julien Bringer, Pirouz Bazargan-Sabet, Shivam Bhasin, and Jean-Luc Danger. Power noise measurements of cryptographic VLSI circuits regarding side-channel information leakage. *IEICE Transactions*, 97-C(4):272–279, 2014.

[5] Daisuke Fujimoto, Daichi Tanaka, Noriyuki Miura, Makoto Nagata, Yu-Ichi Hayashi, Naofumi Homma, Shivam Bhasin, and Jean-Luc Danger. Side-Channel Leakage on Silicon Substrate of CMOS Cryptographic Chip. In *HOST*, IEEE Computer Society, May 2014. Arlington, USA.

[6] Yuto Nakano, Youssef Souissi, Robert Nguyen, Laurent Sauvage, Jean-Luc Danger, Sylvain Guilley, Shinsaku Kiyomoto, and Yutaka Miyake. A Pre-processing Composition for Secret Key Recovery on Android Smartphone. In David Naccache and Damien Sauveron, editors, *Information Security Theory and Practice. Securing the Internet of Things - 8th IFIP WG 11.2 International Workshop, WISTP 2014, Heraklion, Crete, Greece, June 30 - July 2, 2014. Proceedings*, volume 8501 of *Lecture Notes in Computer Science*, pages 76–91. Springer, 2014.

2013

[7] Y. Hayashi, N. Homma, T. Mizuki, T. Aoki, H. Sone, L. Sauvage, and J.L. Danger. Analysis of Electromagnetic Information Leakage From Cryptographic Devices With Different Physical Structures. *Electromagnetic Compatibility, IEEE Transactions on*, 55(3):571–580, June 2013.

[8] Y. Hayashi, N. Homma, T. Mizuki, H. Shimada, T. Aoki, H. Sone, L. Sauvage, and J.L. Danger. Efficient Evaluation of EM Radiation Associated With Information Leakage From Cryptographic Devices. *Electromagnetic Compatibility, IEEE Transactions on*, 55(3):555–563, June 2013.

[9] Yu-Ichi Hayashi, Naofumi Homma, Takaaki Mizuki, Takafumi Aoki, Hideaki Sone, Laurent Sauvage, and Jean-Luc Danger. Introduction to Recent Research on EM Information Leakage. In *Electromagnetic Compatibility (APEMC), 2013 Asia-Pacific Symposium on*, pages 1–4, May 2013.

[10] Yang Li, Sho Endo, Nicolas Debande, Naofumi Homma, Takafumi Aoki, Thanh-Ha Le, Jean-Luc Danger, Kazuo Ohta, and Kazuo Sakiyama. Exploring the relations between fault sensitivity and power consumption. In Emmanuel Prouff, editor, *Constructive Side-Channel Analysis and Secure Design - 4th International Workshop, COSADE 2013, Paris, France, March 6-8, 2013, Revised Selected Papers*, volume 7864 of *Lecture Notes in Computer Science*, pages 137–153. Springer, 2013.

[11] Laurent Sauvage, Jean-Luc Danger, Sylvain Guilley, Naofumi Homma, and Yu-Ichi Hayashi. Advanced Analysis of Faults Injected Through Conducted Intentional Electromagnetic Interferences. *IEEE Transactions on Electromagnetic Compatibility*, 55(3):589–596, June 2013. Sponsored by the IEEE Electromagnetic Compatibility Society.

2012

[12] Jean-Luc Danger, Olivier Meynard, Sylvain Guilley, Yu-Ichi Hayashi, and Naofumi Homma. *"Electromagnetic Radiation", chapter 10, entitled "Characterisation of the Information Leakage of Cryptographic Devices by using EM Analysis"*. InTech, 2012. ISBN: 978-953-51-0639-5. Available from: http://www.intechopen.com/books/electromagnetic-radiation/characterization-of-the-information-leakage-of-cryptographic-devices-by-using-em-analysis.

[13] Laurent Sauvage, Sylvain Guilley, Jean-Luc Danger, Naofumi Homma, and Yu-Ichi Hayashi. A Fault Model for Conducted Intentional ElectroMagnetic Interferences. In *Electromagnetic Compatibility (EMC), 2012 IEEE International Symposium on*, pages 788–793, August 5-10 2012. Pittsburgh, PA, USA (`http://2012emc.org/`). DOI: 10.1109/ISEMC.2012.6351664.

[14] H. Shimada, Y.-I. Hayashi, N. Homma, T. Mizuki, T. Aoki, H. Sone, L. Sauvage, and J.-L. Danger. Efficient mapping of EM radiation associated with information leakage for cryptographic devices. In *Electromagnetic Compatibility (EMC), 2012 IEEE International Symposium on*, pages 794–799, Aug 2012.

2011

[15] Olivier Meynard, Sylvain Guilley, Jean-Luc Danger, Yu-Ichi Hayashi, and Naofumi Homma. Identification of Information Leakage Points on a Cryptographic Device with an RSA Processor. In *IEEE EMC, Session Information Leakage*, pages 773–778, August 14-19 2011. Long Beach, CA, USA (`http://www.emc2011.org`). DOI: 10.1109/ISEMC.2011.6038413.

[16] Olivier Meynard, Denis Réal, Sylvain Guilley, Jean-Luc Danger, and Naofumi Homma. Enhancement of Simple Electro-Magnetic Attacks by Pre-characterization in Frequency Domain and Demodulation Techniques. In *DATE*. IEEE Computer Society, March 14-18 2011. Grenoble, France.

[17] Laurent Sauvage, Sylvain Guilley, Jean-Luc Danger, Naofumi Homma, and Yu-Ichi Hayashi. Practical Results of EM Cartography on a FPGA-based RSA Hardware Implementation. In *IEEE EMC, Session Information Leakage*, pages 768–772, August 14-19 2011. Long Beach, CA, USA (`http://www.emc2011.org`). DOI: 10.1109/ISEMC.2011.6038412.

Normalization

- **ISO 20897**: Physically Unclonable Functions, with Soshi HAMAGUCHI
- **ISO 20085**: Calibration of Side-Channel Platforms, with Hirofumi SAKANE
- **SP WBC**: Contributed document with Shinsaku KIYOMOTO and Jean-Louis LANET

New topics

- **IoT**:
  - PUF: metrics and stochastic models, to increase the confidence for wider adoption
- **Automotive**:
  - Innovative techniques to prevent & detect Trojan horses
  - Safety vs security tradeoff
  - High perf, low latency cryptography
  - Resilient hardware in harsh environment
  - Security architecture
- **5G**:
  - Secure-IC will be the moderator of the 1st security session held in a 5G summit
- **Quantum-safe cryptography**:
  - Hardware acceleration, CC and FIPS-140 ready
  - With built-in resistance to cache-attacks .... (my presentation tomorrow in WG4)

SECURE-IC

THE SECURITY SCIENCE COMPANY

THANKS FOR YOUR ATTENTION

ご清聴ありがとうございました

CONTACT

EUROPE sales-EU@secure-IC.com
APAC sales-APAC@secure-IC.com
JAPAN sales-JAPAN@secure-IC.com
AMERICAS sales-US@secure-IC.com

Publications on CyberCPU technology

[1] Jean-Luc Danger, Sylvain Guilley, Thibault Porteboeuf, Florian Praden, and Michaël Timbert.
HCODE: Hardware-Enhanced Real-Time CFI.
In *Proceedings of the 4th Program Protection and Reverse Engineering Workshop*, PPREW-4, pages 6:1–6:11, New York, NY, USA, 2014. ACM.

[2] Jean-Luc Danger, Sylvain Guilley, Thibault Porteboeuf, Florian Praden, and Michaël Timbert.
Hardware-enforced protection against buffer overflow using masked program counter.
In Peter Y. A. Ryan, David Naccache, and Jean-Jacques Quisquater, editors, *The New Codebreakers - Essays Dedicated to David Kahn on the Occasion of His 85th Birthday*, volume 9100 of *Lecture Notes in Computer Science*, pages 439–454. Springer, 2016.

[3] Jean-Luc Danger, Sylvain Guilley, and Florian Praden.
Hardware-enforced Protection against Software Reverse-Engineering based on an Instruction Set Encoding.
In Suresh Jagannathan and Peter Sewell, editors, *Proceedings of the 3rd ACM SIGPLAN Program Protection and Reverse Engineering Workshop 2014, PPREW 2014, January 25, 2014, San Diego, CA*, page 5. ACM, 2014.

[4] Sylvain Guilley.
Hardware cyber-protections against stack smashing and return-oriented programming.
CHIPEX conference 2017, May 10, 2:30pm-3:30pm. Track G: Hardware security; Tel Aviv, Israel.

[5] Sylvain Guilley, Jean-Luc Danger, Michaël Timbert, and Thibault Porteboeuf.
Cyber-Physical Protections for IoT Devices, November 21-23 2016.
C&ESAR 2016 (Computer & Electronics Security Applications Rendez-vous). "*Internet des Objets : Vous avez dit sécurité ?*", Rennes, France. Program:
http://www.cesar-conference.org/wp-content/uploads/2016/09/CESAR-2016_Programme_v1.pdf.

CORPORATE PRESENTATION

KEY TECH

ANTI-TAMPER TECHNOLOGIES
Shielding, Tampering detection, digital attack sensing, data at-rest/in-transit scrambling.

TUNABLE CRYPTOGRAPHY
Ideal balance between security level and performance.

STRONG SECRET STORAGE
Secret generation tool based on Physically Unclonable Functions (PUF).

HIGH-QUALITY RANDOM GENERATION
Digital TRNG with resilience against harmonic injection, DRBG for high bitrates requirements.

PRE-SILICON EVALUATION
Emulation of the design behavior, simulated attacks in perfect confitions.

POST-SILICON EVALUATION
Security evaluation of the SoC against state-of-the-art attacks.

CONTENT PROTECTION
Digital watermarkking to hide irremovable and invisible mark into a signal or a dataset.

POST-QUANTUM TECHNOLOGIES
Security technologies renewal prior to the quantum era for a safe and sound transition.

CORPORATE PRESENTATION

PROTECT

SECURYZR

KEY TECH

TUNABLE CRYPTO
FOR SSL/TLS (RSA, ECC, AES, 3-DES, HASH, ...)

DIGITAL TRNG
TRUE RANDOM CRYPTOGRAPHIC NUMBER GENERATION

PHYSICALLY UNCLONABLE FUNCTION
100% UNIQUE, RANDOM AND STEADY ID GENERATION

DIGITAL SENSOR
ALL-IN-ONE FAULT INJECTION DETECTOR, ENTIRELY DIGITAL

ACTIVE SHIELD
ACTIVE PROTECTION AGAINST INTRUSIVE ATTACKS ON ASIC

SCRAMBLED BUS
ENCRYPTED INFORMATION TO PREVENT PROBING ON BUS

MEMORY CIPHERING
MEMORY PROTECTION AGAINST REVERSE ENGINEERING AND TAMPERING

SECURE CLOCK
ANTI-SYNCHRONIZATION TO PREVENT EFFICIENT SCA AND FIA

WATERMARKING
PROTECTION OF COPYRIGHTED CONTENT

SECURE JTAG
AUTHENTICATION SYSTEM TO SECURE THE DEBUGGING CHANNEL ON CHIP

SECURE BOOT
MAXIMUM SECURITY-ENABLING ROOT-OF-TRUST

SECURE MONITOR
MAXIMUM SECURITY-ENABLING MONITORING

CYBERCPU
CPU-AGNOSTIC CYBER ATTACK SENSOR

ON-SITE INTEGRATION
SUPPORT UNTIL CERTIFICATION
ANALYSIS SERVICE (ON DEMAND)

CORPORATE PRESENTATION

EVALUATE – THE KEY TO A GUARANTEED CERTIFICATION

EVALUATE

LABORYZR

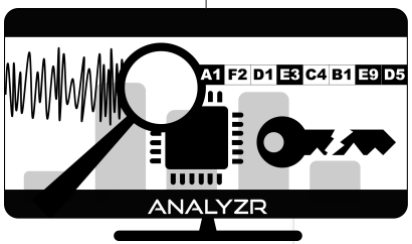
PERFORM **SIDE-CHANNEL ATTACKS** AND **FAULT INJECTION ATTACKS** ON **HARDWARE** AND **SOURCE CODE**
USE **BIG DATA PROCESSING** TO **DRAMATICALLLY INCREASE** YOUR **ANALYSIS CAPABILITIES**

EQUIPMENT

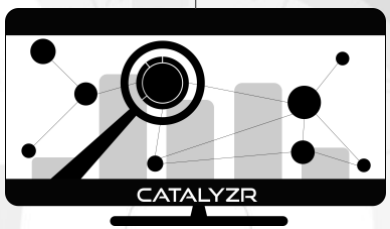
LABORYZR

TRAINING & METHODOLOGY

UPSTREAM ANALYSIS
on VHDL/Verilog Source Code



DOWNSTREAM ANALYSIS
on ASIC, FPGA, device



LEAKAGE EXTRACTION
via Data Mining

CORPORATE PRESENTATION

SERVICE – THE SECURITY SCIENCE EXPERTISE

SERVICE

EXPERTYZR

EXPERTYZR

Standardization

Preparing and drafting new emerging rules

Targeted Advanced Studies

Explore new Fields at the frontier of the state-of-the-art

Consulting/Expertise

Answer every request during the whole design cycle

Collaborative Projects

Prepare the up-coming challenges

Tutorials/Training

Learn everything you need to know from theory to practice