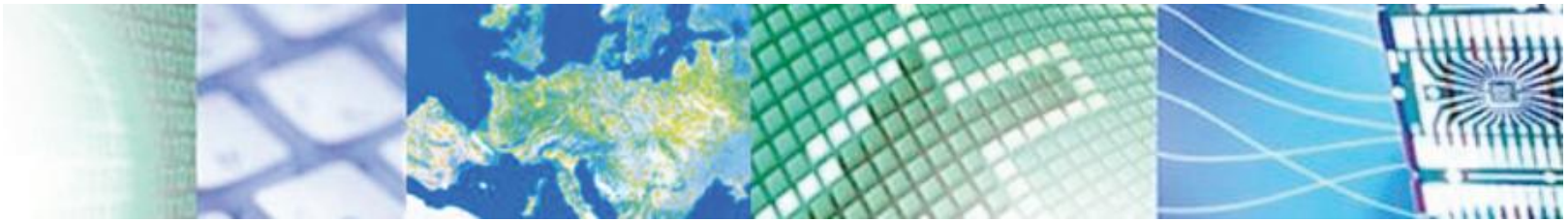


CHIST-ERA Projects Seminar
Day 2, Cross Topics

Resilient Trustworthy Cyber-Physical Systems (RTCPS)

COPES – (Tobias Oechtering, KTH) &
SECODE, I-DRESS, DYPOSIT
(presented by Irene Y.-H. Gu , Chalmers)

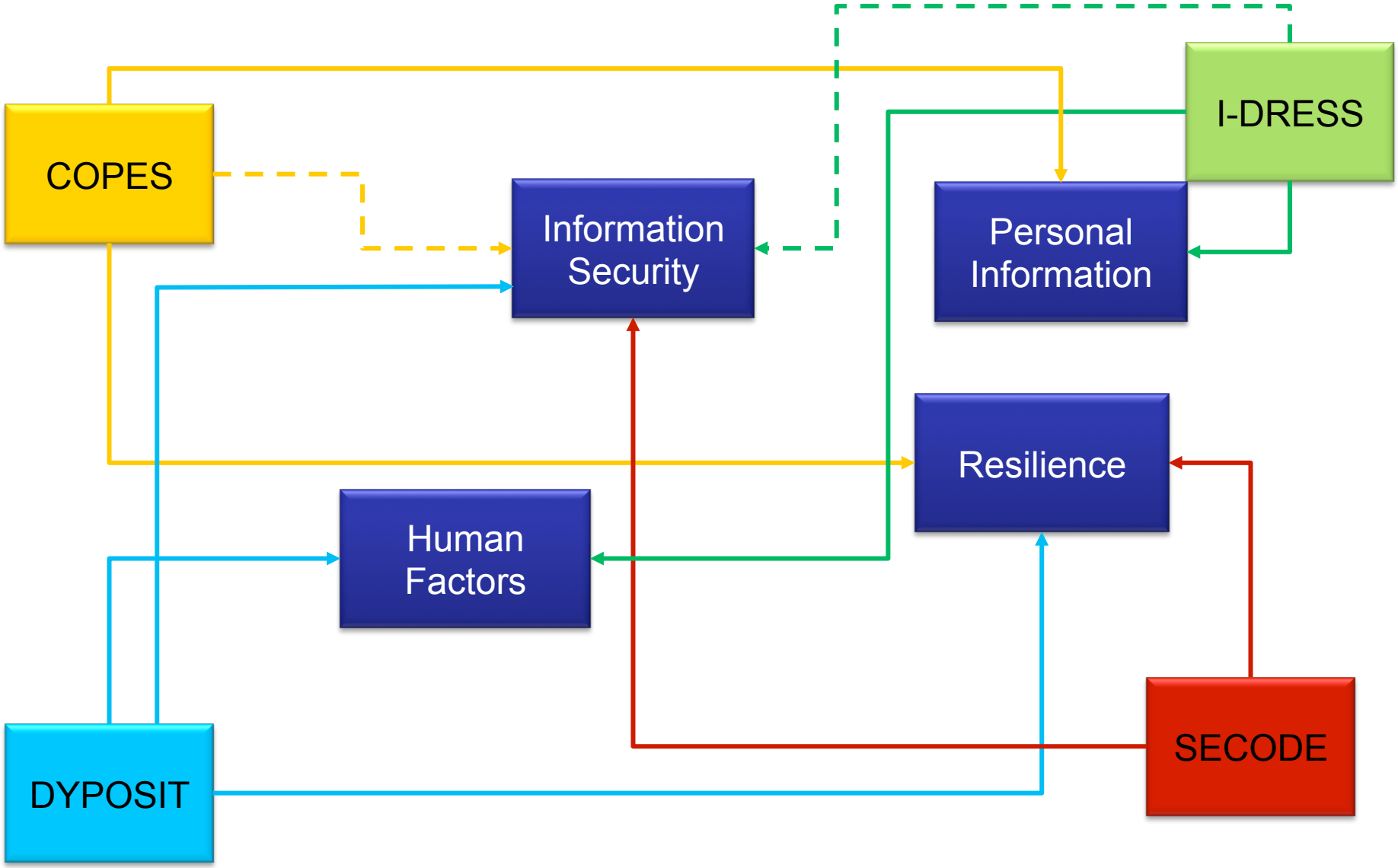
Bucharest, April 4th, 2019

FUNDING OPPORTUNITIES from the
FUTURE & EMERGING TECHNOLOGIES scheme

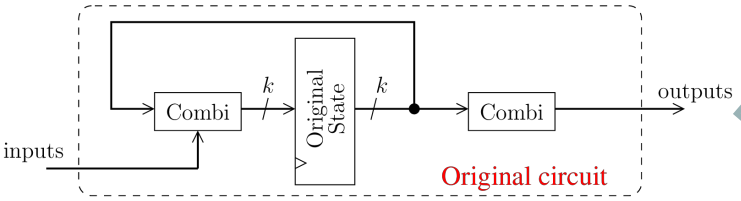
Resilient Trustworthy Cyber-Physical Systems (RTCPS)

- **SECODE**
  - ✓ Secure Codes To Thwart Cyber-Physical Attacks
- **I-DRESS**
  - ✓ Assistive Interactive Robotic System For Support In Dressing
- **DYPOSIT**
  - ✓ Dynamic Policies For Shared Cyber-Physical Infrastructures Under Attack
- **COPES**
  - ✓ COnsumer-Centric Privacy In Smart Energy GridS

Projects of the Resilient Trustworthy Cyber-Physical Systems (RTCPS)

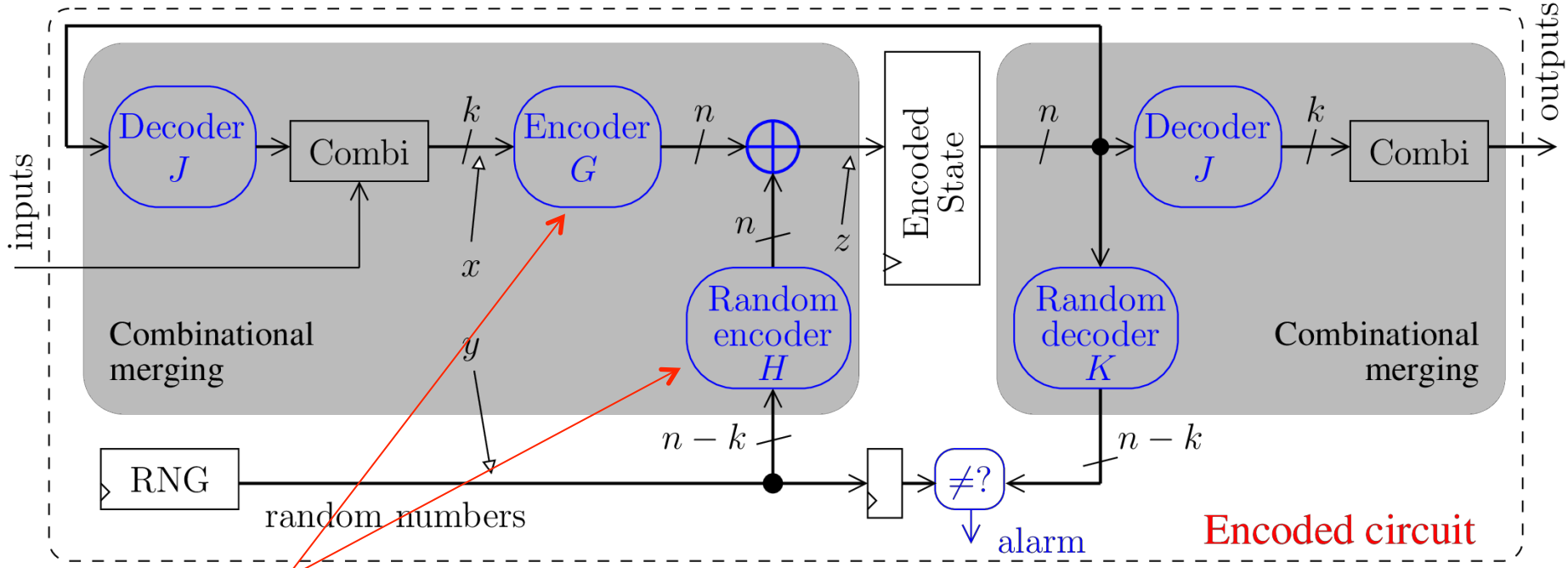


SECODE big picture



Transformation With masking protection based on codes

Threats =
*** Side-channel attacks**
*** Active Attacks**



1. What are the best Codes ?

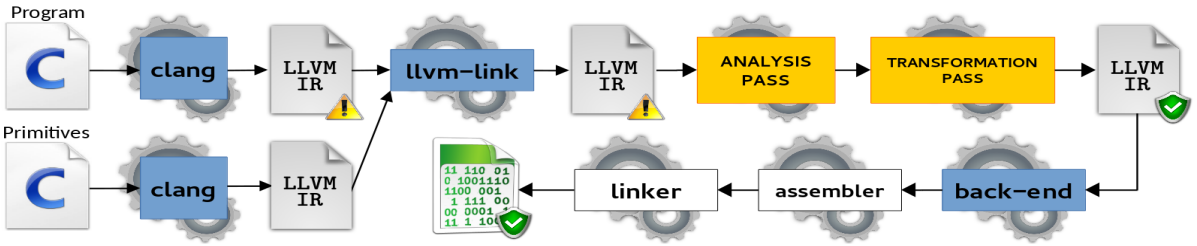
3. Can we automatize ?

2. What are the security parameters of the implementation?

SECODE Major achievements and challenges

- **Code theory :** How to construct LCD codes (the Best codes) Generalized Quasi-Cyclic Codes , AG Codes, Any linear code with q>3, LCP codes,etc.
- **Security at implementation level**
  - ✓ Generic security parameters for both SW and HW
  - ✓ Study of Inner-Product Masking codes at Byte/bit security level
  - ✓ Impact of code properties on security order
- **Automatic Compiler to insert protections**

- 14 journal papers
- 6 conference papers



What have been done:

- **Tested against both SCA and FIA**
- **Refined code/implementation to reduce the physical leakage**
- **Optimized complexity and latency of the automatically compiled code**

What remain: extension of 1 yr to fix issues on Side-channal and fault injection attacks

I-DRESS: Assistive Interactive Robotic System for Support in Dressing

I-DRESS consortium/expertise:

- Perception, multi-modal interaction
- Safety, human factors, interface design
- Robot learning

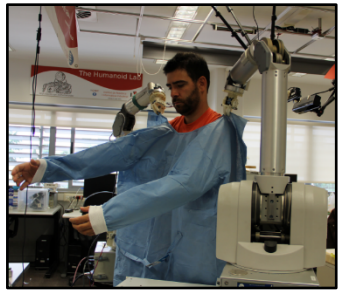
Institut de Robòtica i Informàtica Industrial

Bristol Robotics Laboratory

idiap RESEARCH INSTITUTE

Application scenarios:

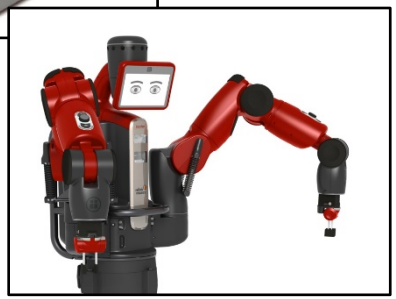
Shoe fitting



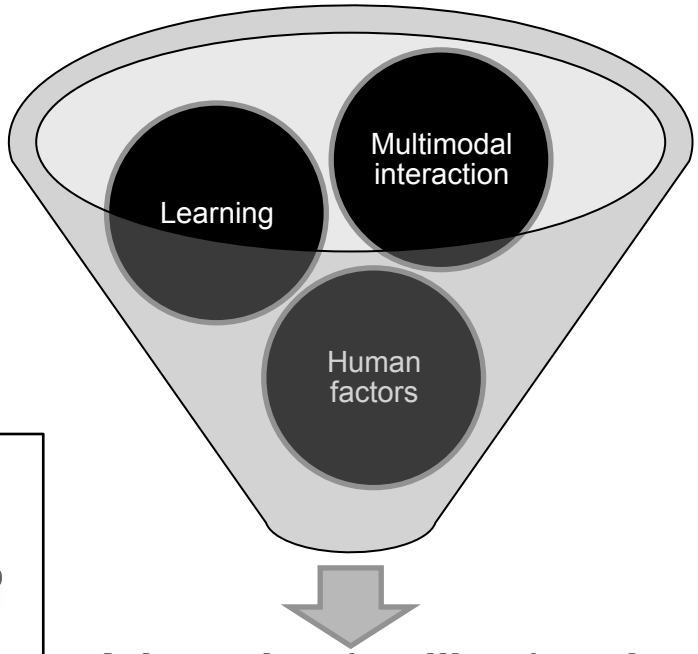
Gown dressing

Robotic platforms:

Barrett's WAM



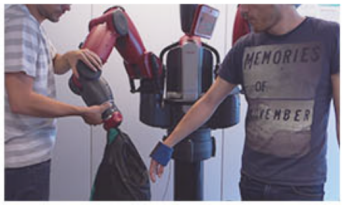
Rethink robotics' Baxter

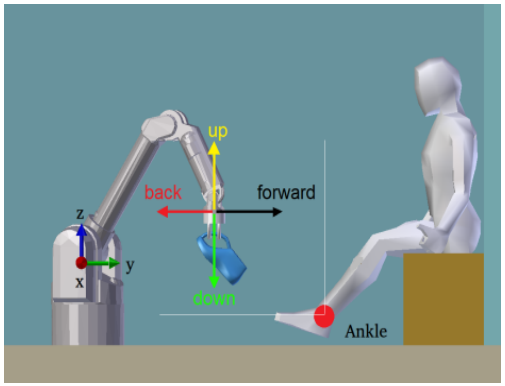


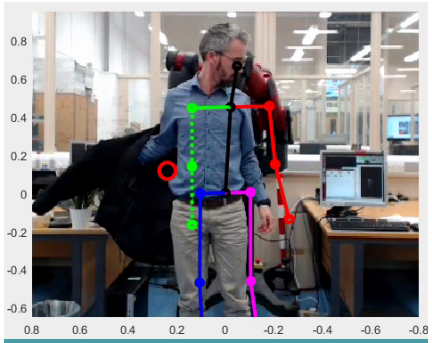
Adaptation (resilient) and safety (trustworthy)

Major advances

- Human-human interaction study
- Adaptation through multimodal interaction
- Robot learning and task planning
- Safety analysis







Predicting elbow position from occluded vision data

Project impact and future work

- Evaluated on the system relevant to some realistic environment.

- Handled complex situations, including limiting variation, sound, occlusions during the dressing, using deep learning and PoE (product of expert).

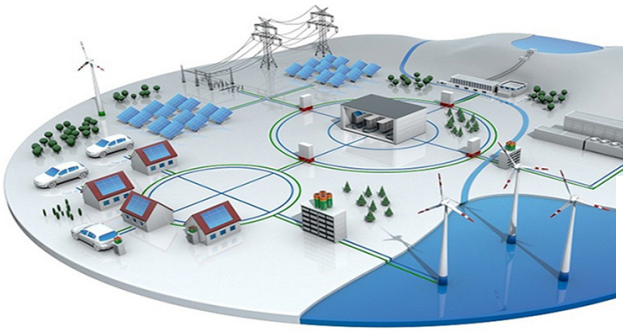
- Developed two prototypes of single arm robot dressing assistants: Barret WAM manipulator and Baxter robot;

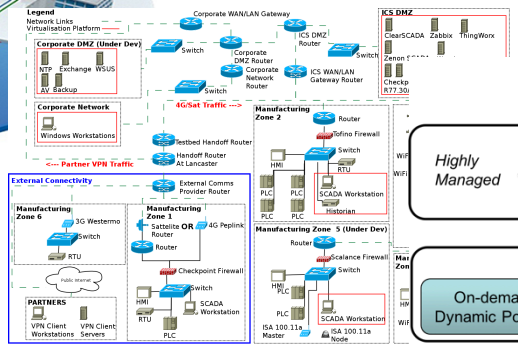
- Published 22 journal papers, and 20 conf. papers;

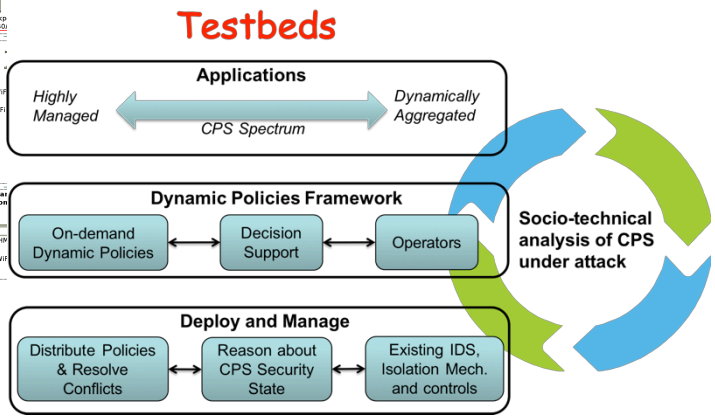
2 new projects (Spain + EU H2020)

DYPOSIT: Dynamic Policies for Shared Cyber-Physical Infrastructures under Attack

chist-era







- Volatile, multi-stakeholder CPS environment under attack
- Security controls/policies provide defenses against attack.
- Dynamic policy changes support resilience.
- Distributed, dynamic and human-centered security

KU LEUVEN VEN DistriNet iMinds KU LEUVEN KU LEUVEN

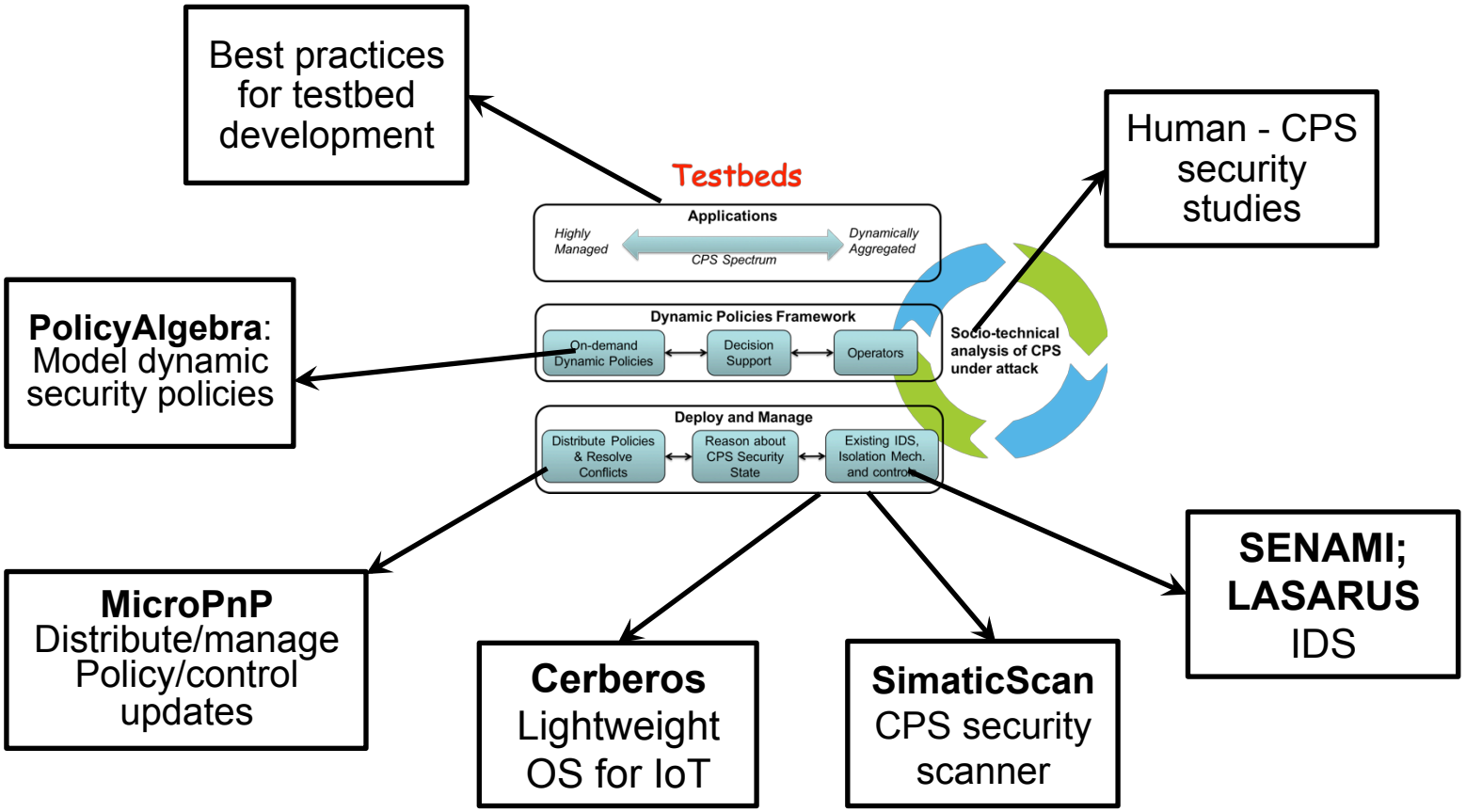
Security Lancaster | Lancaster University

UCC University College Cork, Ireland Coláiste na hOllscoile Corcaigh

IMT Atlantique Bretagne-Pays de la Loire École Mines-Télécom

University of BRISTOL

DYPOSIT: Dynamic Policies for Shared Cyber-Physical Infrastructures under Attack



Upcoming challenges and needs

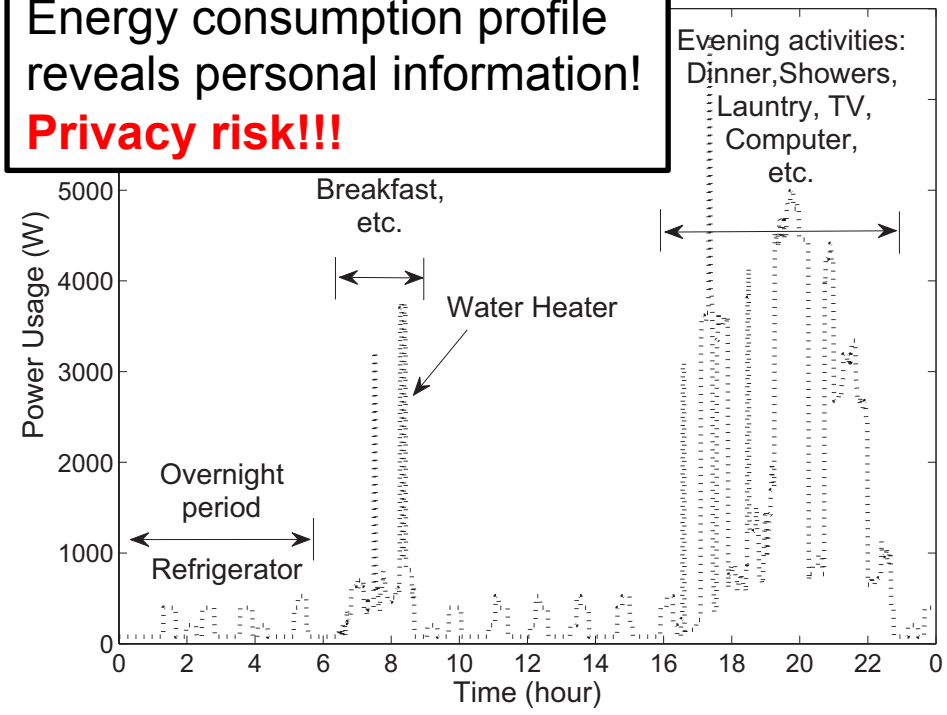
- Challenges
  - ✓ Map policy models to real-world security infrastructure.
  - ✓ Evaluation of efficacy including human factors
  - ✓ Tradeoff security policy change against service continuity
- Roadmap
  - ✓ Defend against unknown attacks.
  - ✓ Security of CPS built with contemporary SW development

- What have been achieved:

- Developed 5 software prototypes/CPS testbeds:
  CerberOS, SENAMI, SimaticScan, PiVOTScan, DYPOSIT;
- 24 Conf. papers,, 1 journal paper, 3 PhD theses, workshops, keynotes/invited talks.
- Shared testbeds among partner universities/institute.

COPES approach to Smart Meter Privacy

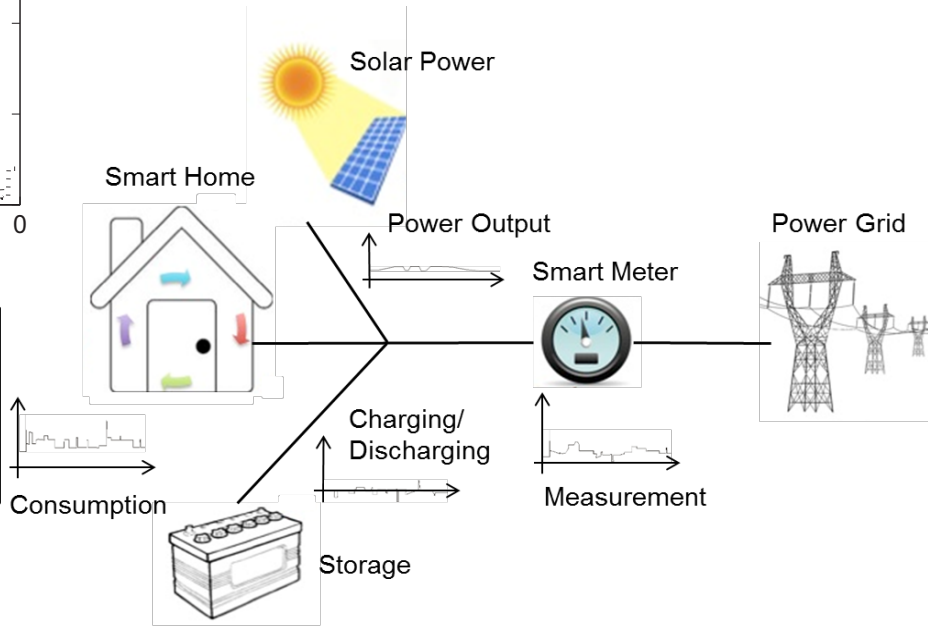
Energy consumption profile reveals personal information!
Privacy risk!!!



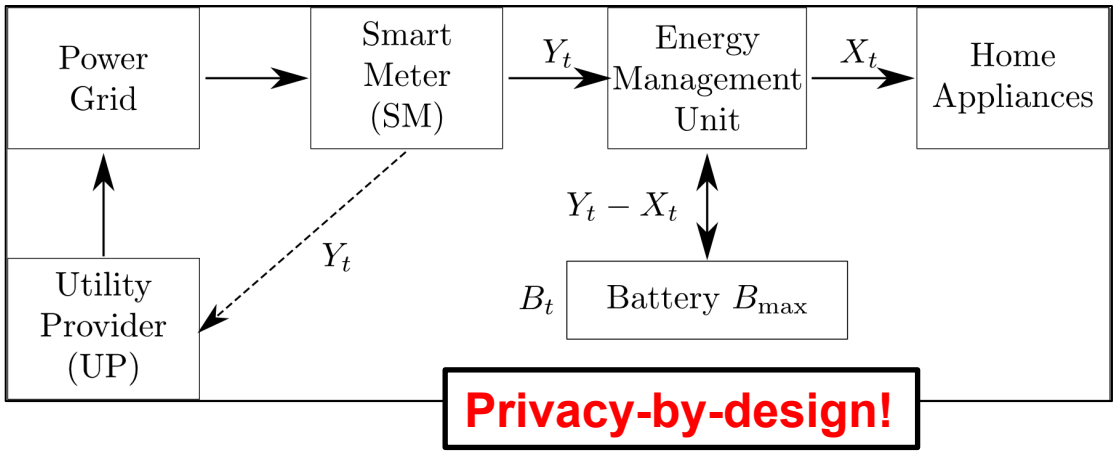
(Updated) EU General Data Protection Regulation strongly protects private life

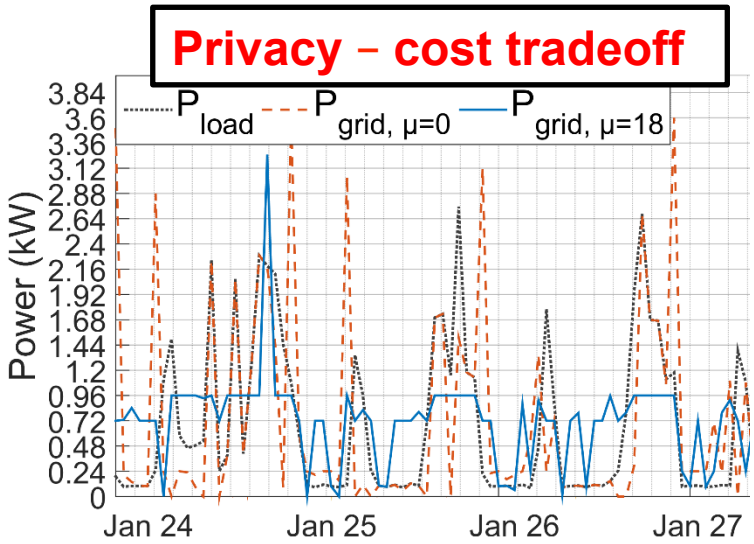
- Potential show stopper

COPES approach: Manipulate actual energy prosumption profile using energy storage & alternative sources



Major Results: SM Privacy Measures and Privacy Enhancing Technology

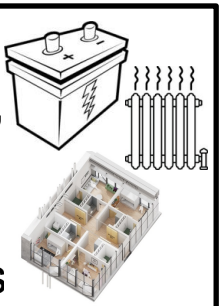




- **Design of several energy flow control algorithms considering**
  - ✓ Different privacy measures (stat. inference, inform. theory, computer sc.)
  - ✓ Utility – privacy trade-off (e.g. energy-cost, degradation, analytics, …)
  - ✓ Implementation and integration of cross-disciplinary aspects (e.g. HVAC, …)

- 17 conference & 10 journal papers
- 5 Phd projects (2 finished)
  - Best IEEE-IT UK Award ’18
- Online tutorial, 4 book chapters MOOC (>23k), outreach activities

- 3(+1) granted *follow-up proj.* impact on real energy storage, experimental setup + industry
- Proof-of-concept experiments in KTH Live-In-Lab in progress



Identified Future Research Challenges

- **Research challenges beyond COPES**
  - ✓ Statistical modeling of realistic systems
    - **Sufficiently reliable data in real-time for online adaptation**
  - ✓ Complexity efficient algorithms design
    - **Needed for deployment of technology**
  - ✓ Certification of acceptable privacy measures
    - **Provable guarantees on privacy (and utility?)**
    - **User empowerment to make sustainable privacy decisions**
  - ✓ Impact on operational procedures of energy provider
    - **Change of the roadmaps (e.g. forecasting, grid visibility)**
  - ✓ Distributed energy resources (e.g. storage) + intelligence -> new opportunities for grid management
    - **Exploit demand side resources, e.g. flexibility due to scheduling**

Overall summary (RTCPS)

- **Promise of Cyber-Physical Systems/digitalization of society**
  - ✓ Many opportunities
    - **Quality of Life**
    - **Sustainability**
    - **Economic growth**
- **Resilient Trustworthy CPS**
  - ✓ Many new security and privacy risks
    - **Most of them are not sufficiently explored**
    - **Digitalisation can be also used to mitigate them**

Paradigm shift: Security, privacy and resilience should be taken into account from the very beginning!!!

Questions

Questions ?