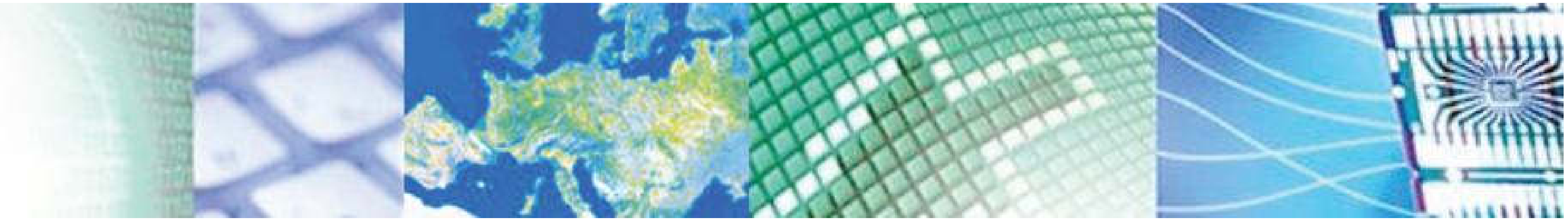


CHIST-ERA Projects Seminar

Day 2, Cross Topics

# Resilient Trustworthy Cyber-Physical Systems (RTCPS)

*Speaker*

*T. Oechtering (KTH), J.-L. Danger (Telecom Paris), A. Jevtic (UPC), S. Foley (IMT Atlantique)*

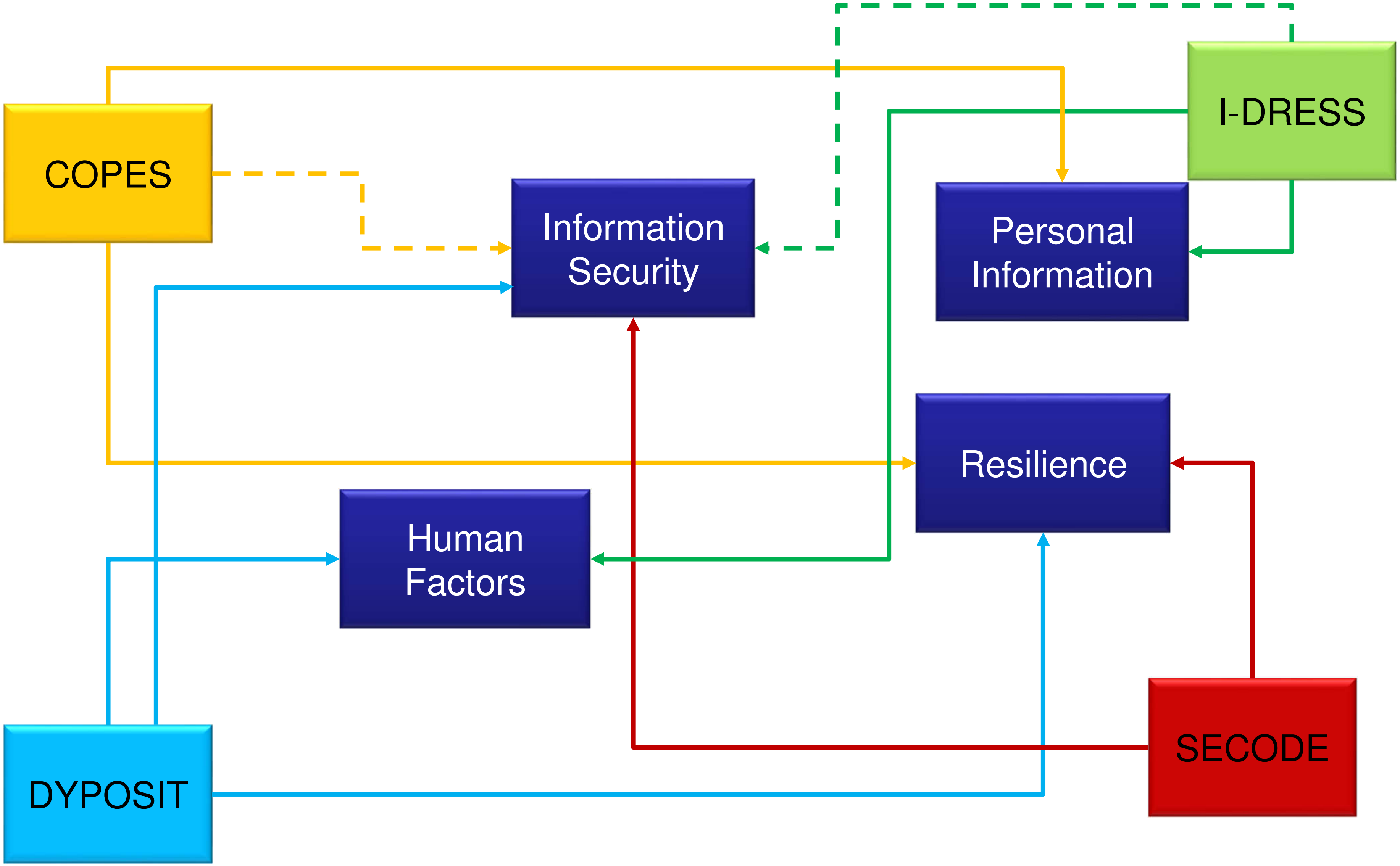
**Paris, April 11th, 2018**

FUNDING OPPORTUNITIES from the
FUTURE & EMERGING TECHNOLOGIES scheme

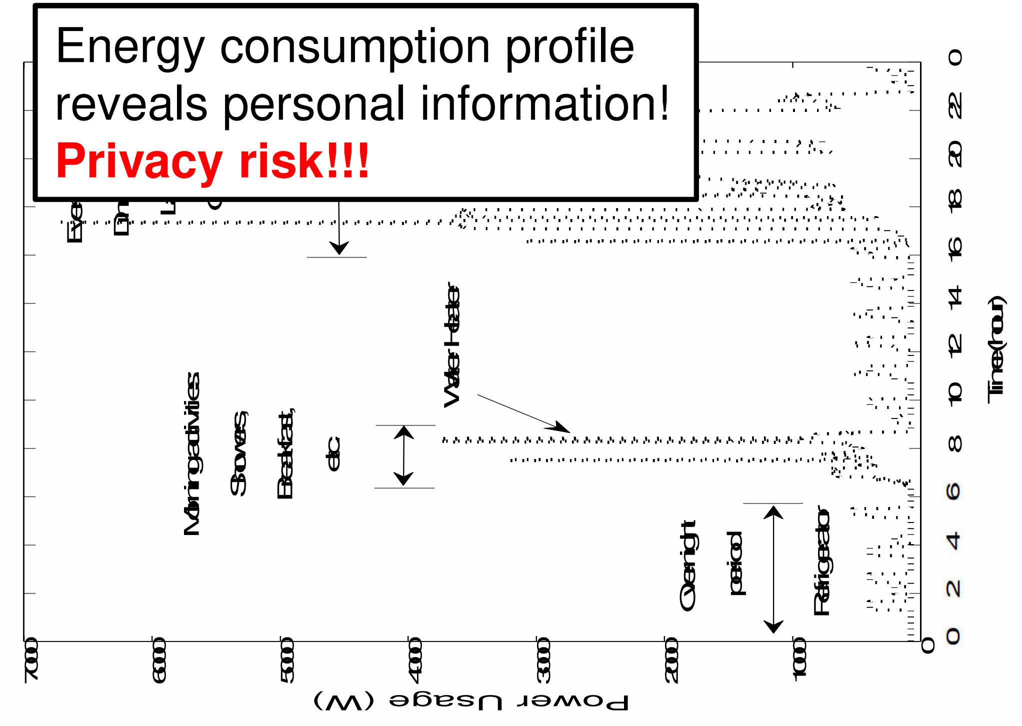
# Resilient Trustworthy Cyber-Physical Systems (RTCPS)

- **COPES**
  - ✓ COnsumer-Centric Privacy In Smart Energy GridS
- **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

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



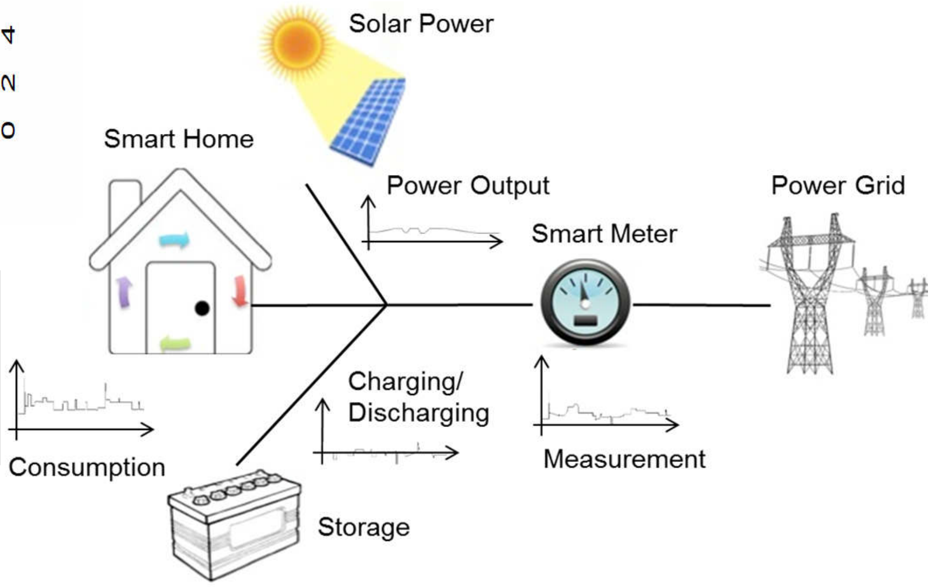
# COPES approach to Smart Meter Privacy



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

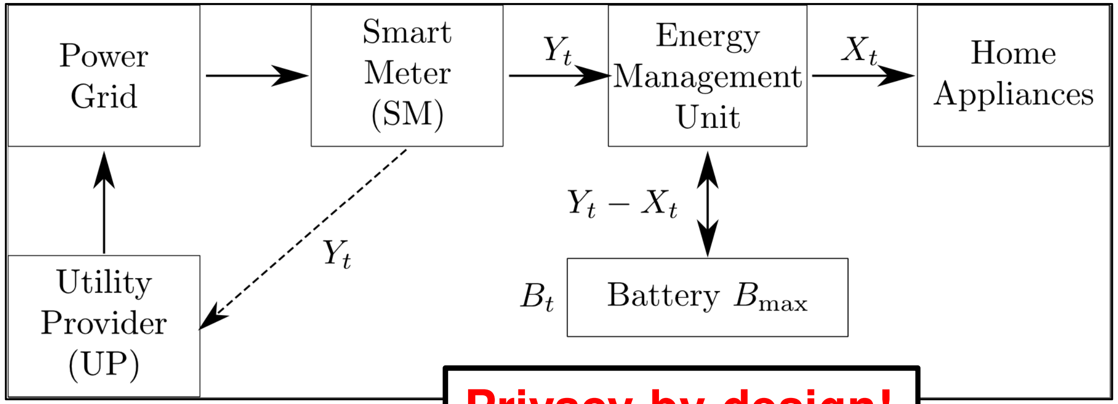
(Updated) EU General Data Protection Regulation strongly protects private life

- Potential show stopper



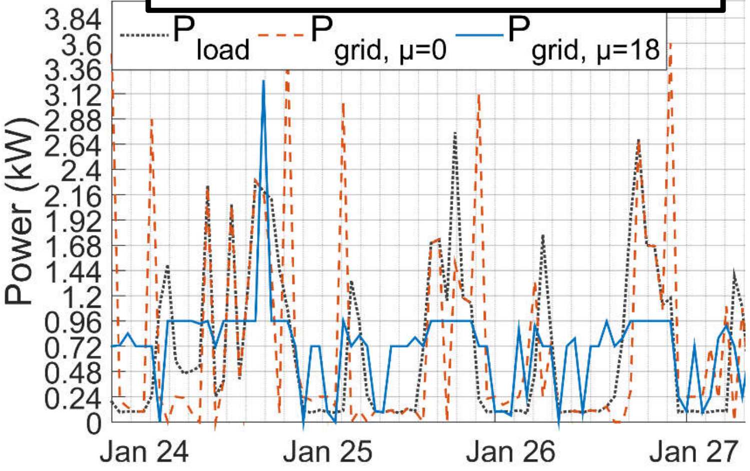
**COPES approach:** Manipulate actual energy prosumption profile using energy storage & alternative sources

# Major Results: SM Privacy Measures and Privacy Enhancing Technology



**Privacy-by-design!**

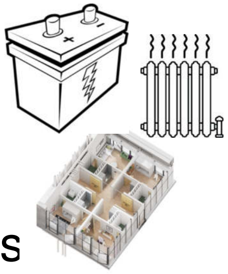
**Privacy – cost tradeoff**



- ❖ **Design of several energy flow control algorithms considering**
  - ✓ Different privacy measures (past focus)
  - ✓ Utility (e.g. energy-cost) – privacy trade-off (past focus)
  - ✓ Implementation and integration of cross-disciplinary aspects (future

- 12 conference & 6 journal papers published/submitted
- 8 student projects
- Outreach at WEF’18 (Davos), MOOC, companies & events

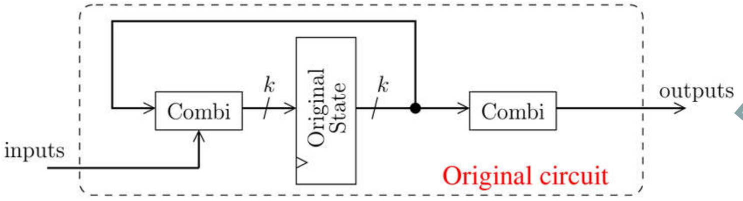
- 3(+1) granted *follow-up projects* on impact of energy storage technology
- Proof-of-concept experiments in KTH Live-In-Lab in progress



# Challenges – Future Roadmap

- **COPES – challenges**
  - ✓ Sufficiently reliable data in real-time for online adaptation
  - ✓ Complexity of algorithms
  - ✓ Certification of acceptable privacy measures & guarantees
  - ✓ Impact on operational procedures of utility
    - **Conservative attitude of critical infrastructure operator delays technology implementation**
  - ✓ User-empowerment
    - **Enable them to make sustainable privacy decisions**
    - **Trade-off between automation and manual decisions**

# SECODE big picture



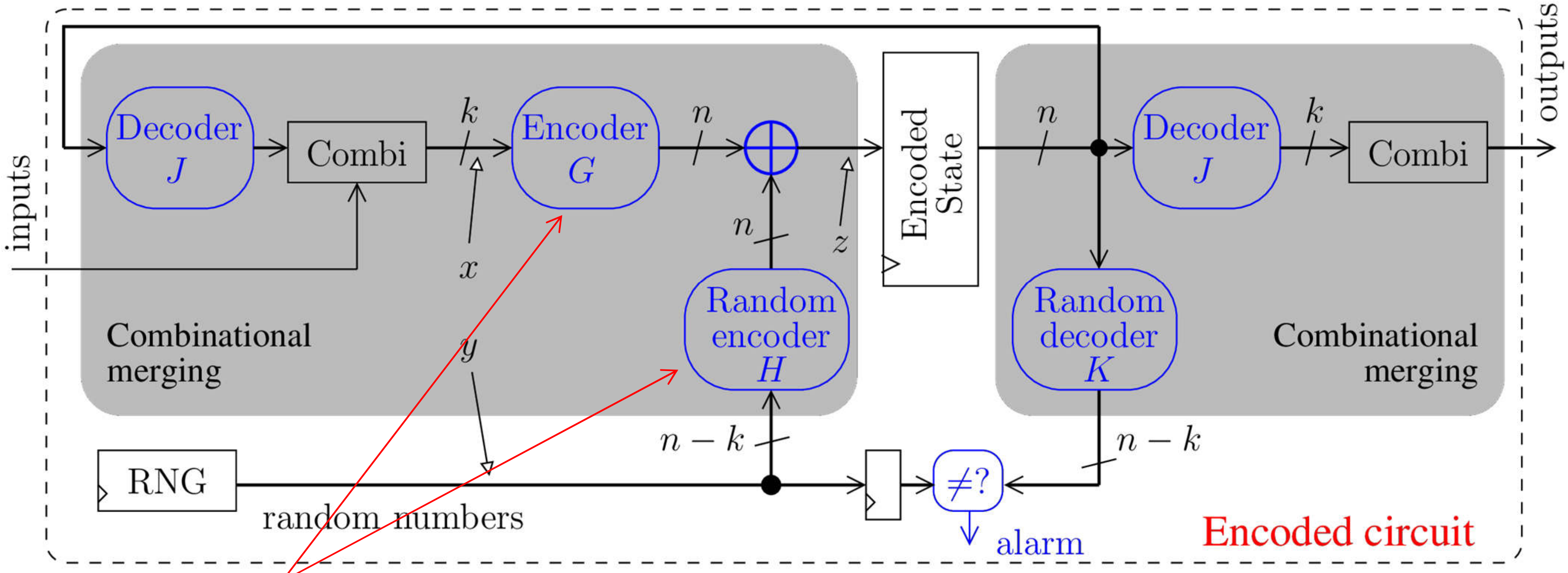
Original circuit

**Transformation With masking protection based on codes**

**Threats =**

*** Side-channel attacks**

*** Active Attacks**



Encoded circuit

**1. What are the best Codes ?**

**3. Can we automatize ?**

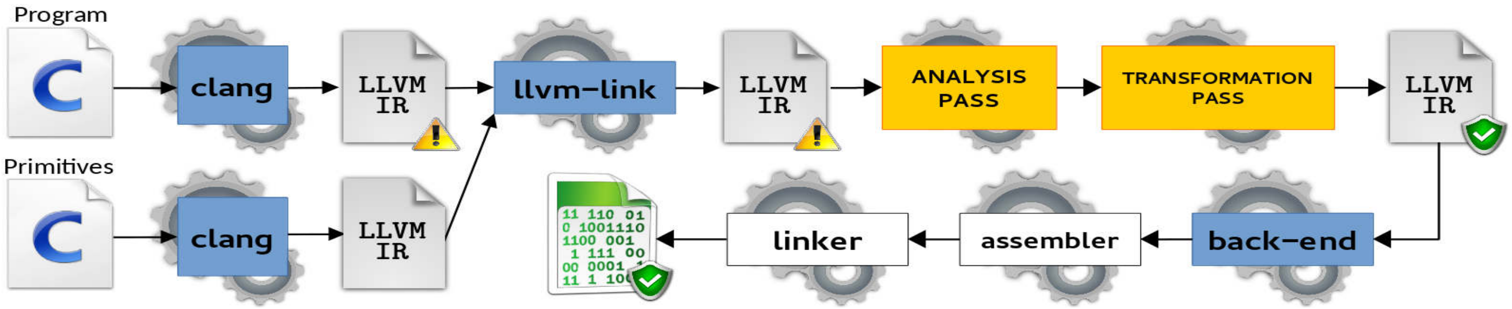
**2. What are the security parameters of the implementation?**

# 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
  - ✓ Codes used for PUF

- 9 journal papers
- 5 conference papers

- ❖ **Automatic Compiler to insert protections**



- Challenges:
- ❖ **To find codes to be robust against both SCA and FIA**
- ❖ **To refine code/implementation to reduce the physical leakage**
- ❖ **To optimize complexity and latency of the automatically compiled code**

# I-DRESS project

**I-DRESS consortium/expertise:**

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

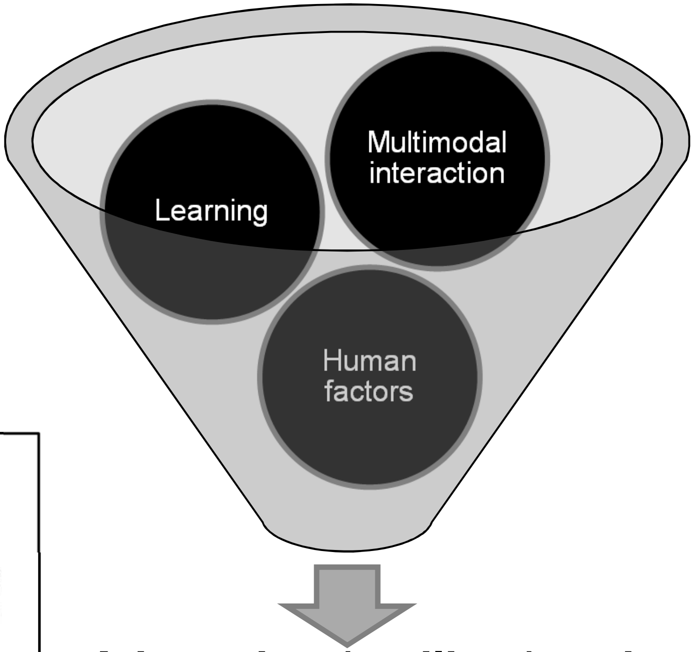
Institut de Robòtica i Informàtica Industrial

Bristol Robotics Laboratory

**Robotic platforms:**

*Barrett's WAM*

*Rethink robotics' Baxter*



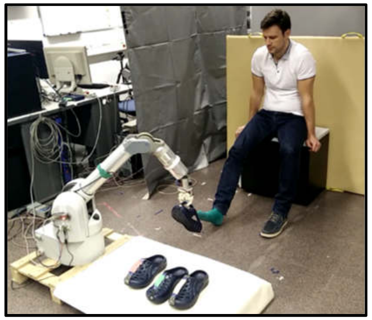
Learning

Multimodal interaction

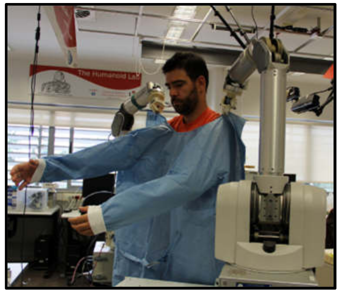
Human factors

**Adaptation (resilient) and safety (trustworthy)**

**Application scenarios:**

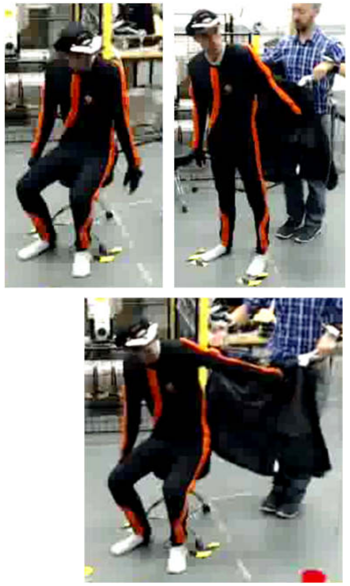


*Shoe fitting*



*Gown dressing*

# Major advances

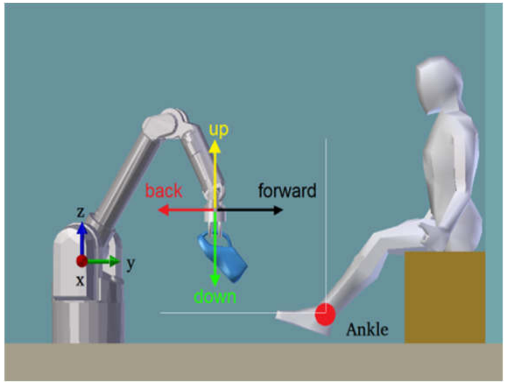


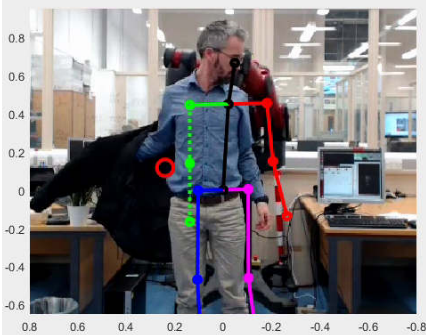
❑ Human-human interaction study

❑ Adaptation through multimodal interaction

❑ Robot learning and task planning

❑ Safety analysis





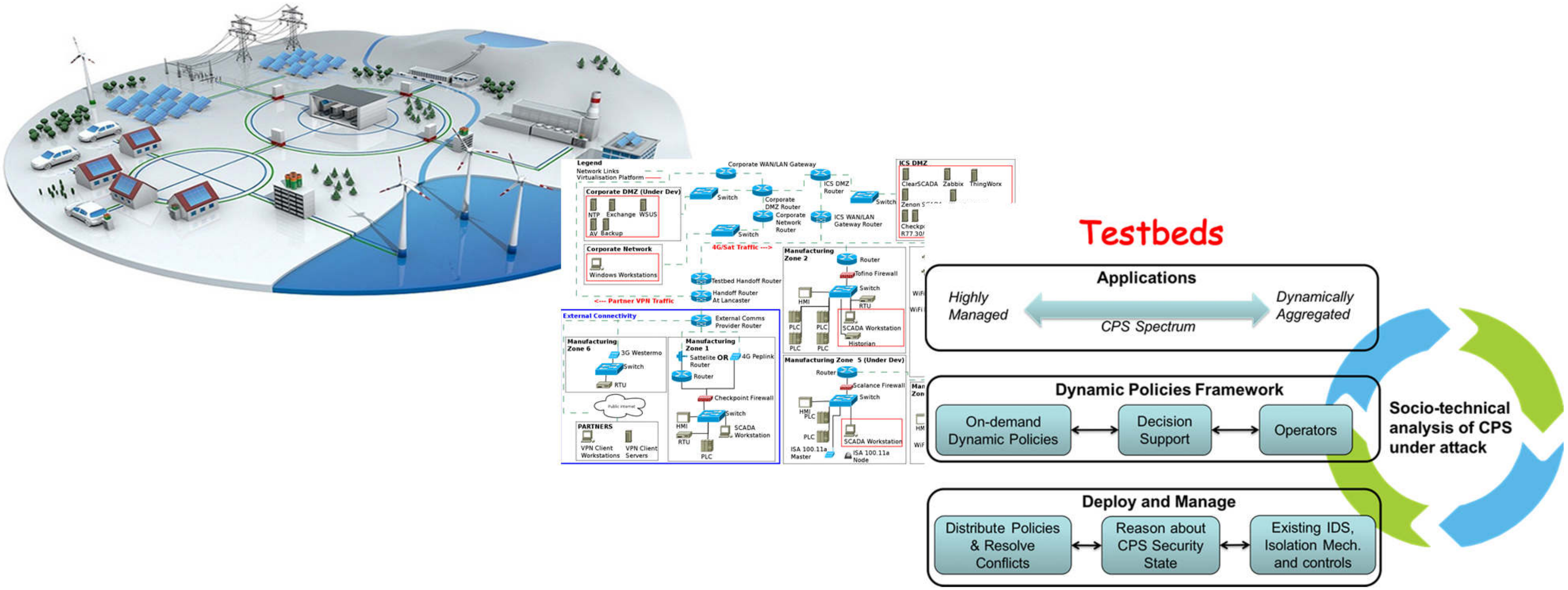
*Predicting elbow position from occluded vision data* chist-era

# Future challenges

- Evaluation of the system in relevant/realistic environment (above TRL 4).
- Perception is a limiting factor; occlusions occur during the dressing task.
- Cloth (deformable object) manipulation is very complex for the existing hardware.
- Long-term interaction studies are tedious and costly.
- Ethical issues for physical human-robot interaction.

chist-era

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



Testbeds

Applications

*Highly Managed* ⟷ *Dynamically Aggregated*

*CPS Spectrum*

Dynamic Policies Framework

On-demand Dynamic Policies ⟷ Decision Support ⟷ Operators

Deploy and Manage

Distribute Policies & Resolve Conflicts ⟷ Reason about CPS Security State ⟷ Existing IDS, Isolation Mech. and controls

Socio-technical analysis of CPS under attack

- 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
DistriNet
iMinds KU LEUVEN

Security Lancaster

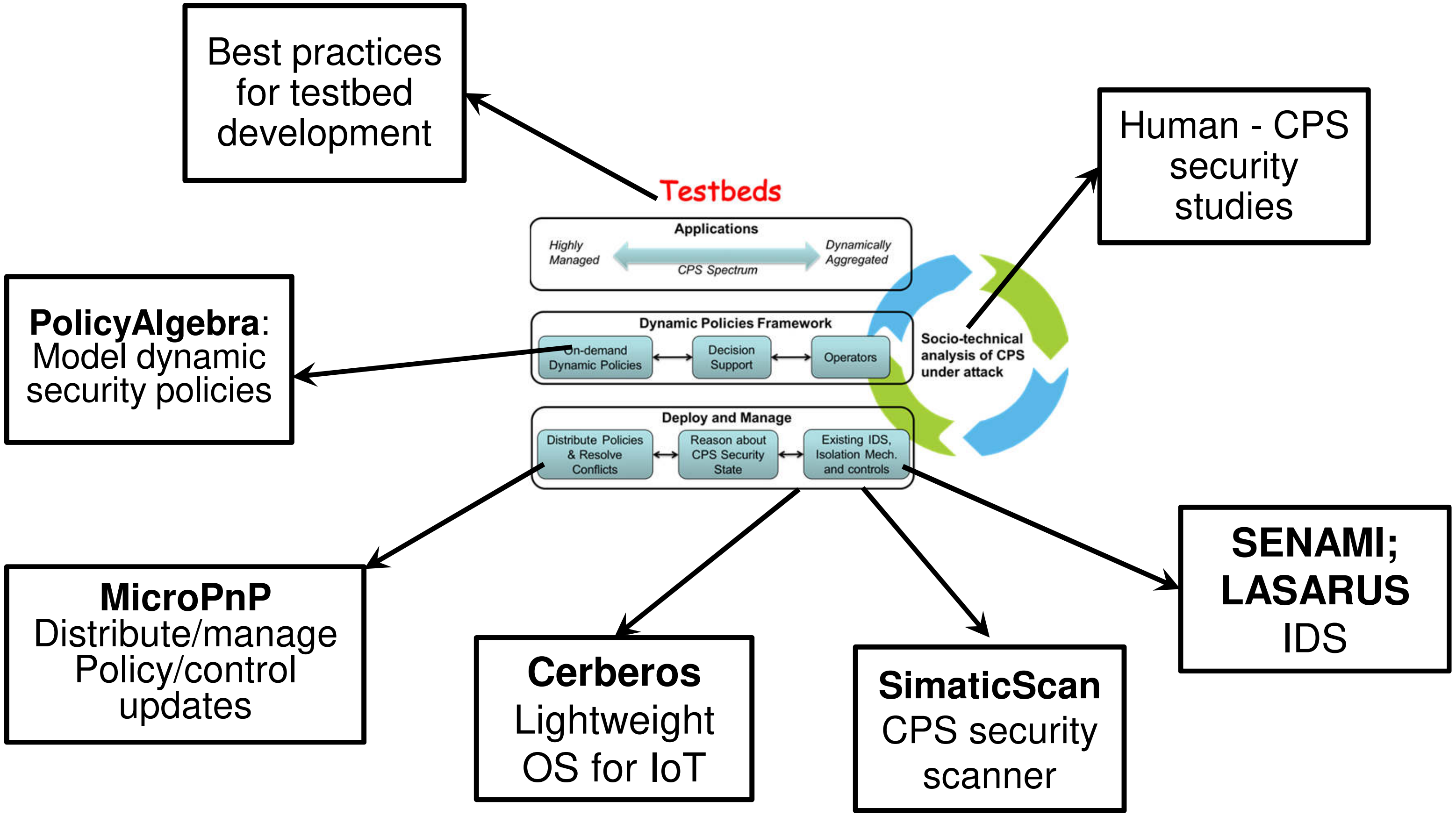
Lancaster University

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



Best practices for testbed development

Human - CPS security studies

**PolicyAlgebra**: Model dynamic security policies

**MicroPnP** Distribute/manage Policy/control updates

**Cerberos** Lightweight OS for IoT

**SimaticScan** CPS security scanner

**SENAMI; LASARUS** IDS

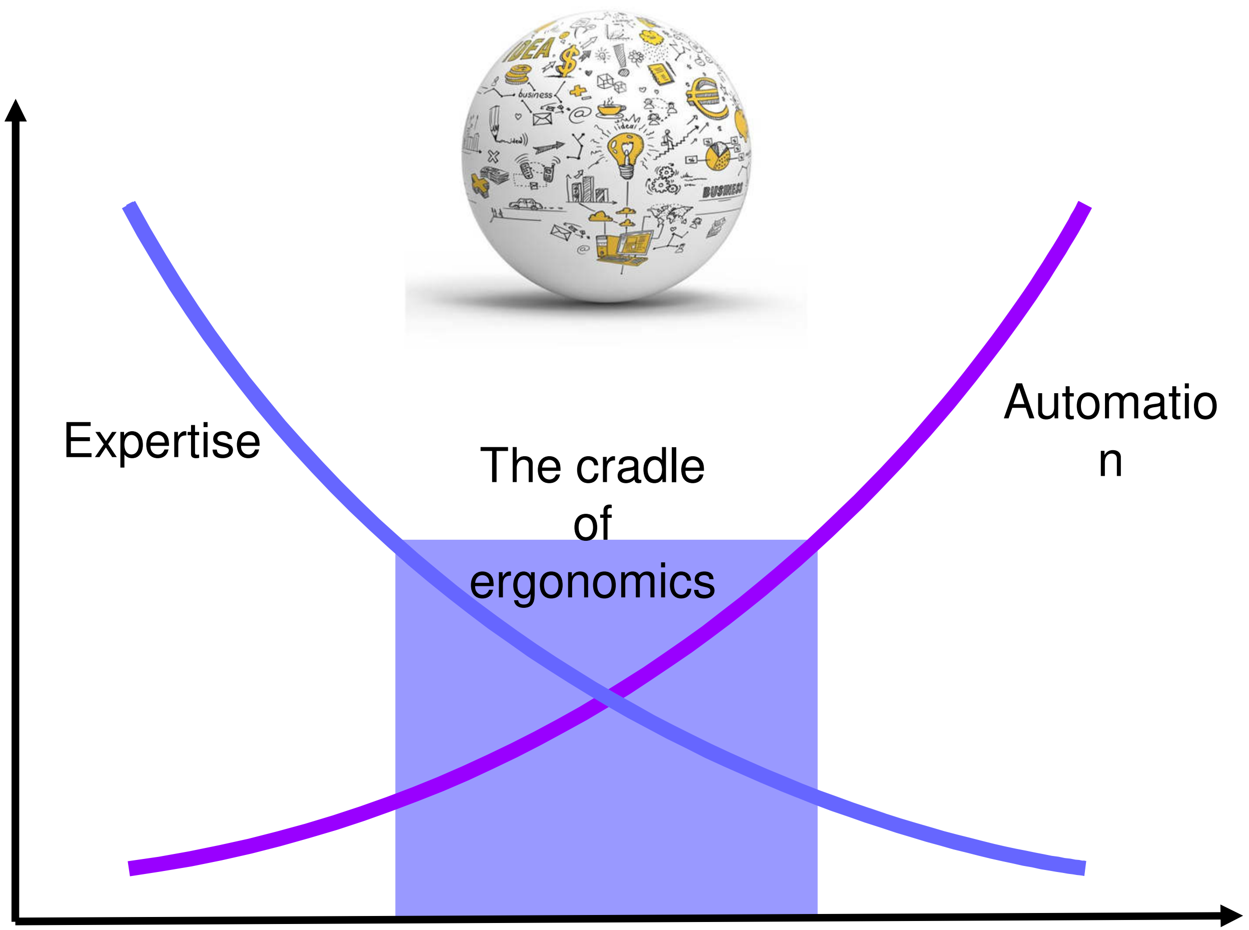
Testbeds
Applications
Highly Managed
CPS Spectrum
Dynamically Aggregated
Dynamic Policies Framework
On-demand Dynamic Policies
Decision Support
Operators
Socio-technical analysis of CPS under attack
Deploy and Manage
Distribute Policies & Resolve Conflicts
Reason about CPS Security State
Existing IDS, Isolation Mech. and controls

- Lancaster & KUL CPS testbeds; 4 software prototypes/tools
- 17 international peer-reviewed papers; 3 theses completed
- 2 International CPS-security workshops organized
- 8 keynotes and invited talks/seminars

# 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.

# Security and Privacy Ergonomics



Digitalization

Expertise

The cradle of ergonomics

Automatio n

Security and Privacy

# Questions

Questions ?