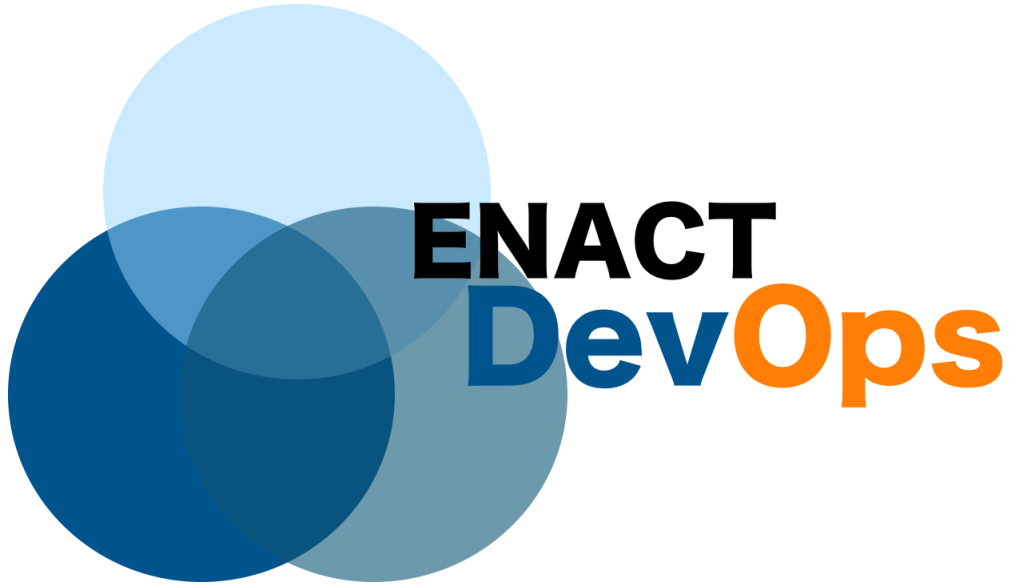


ENACT: Development, Operation, and Quality Assurance of Trustworthy Smart IoT Systems

Nicolas Ferry

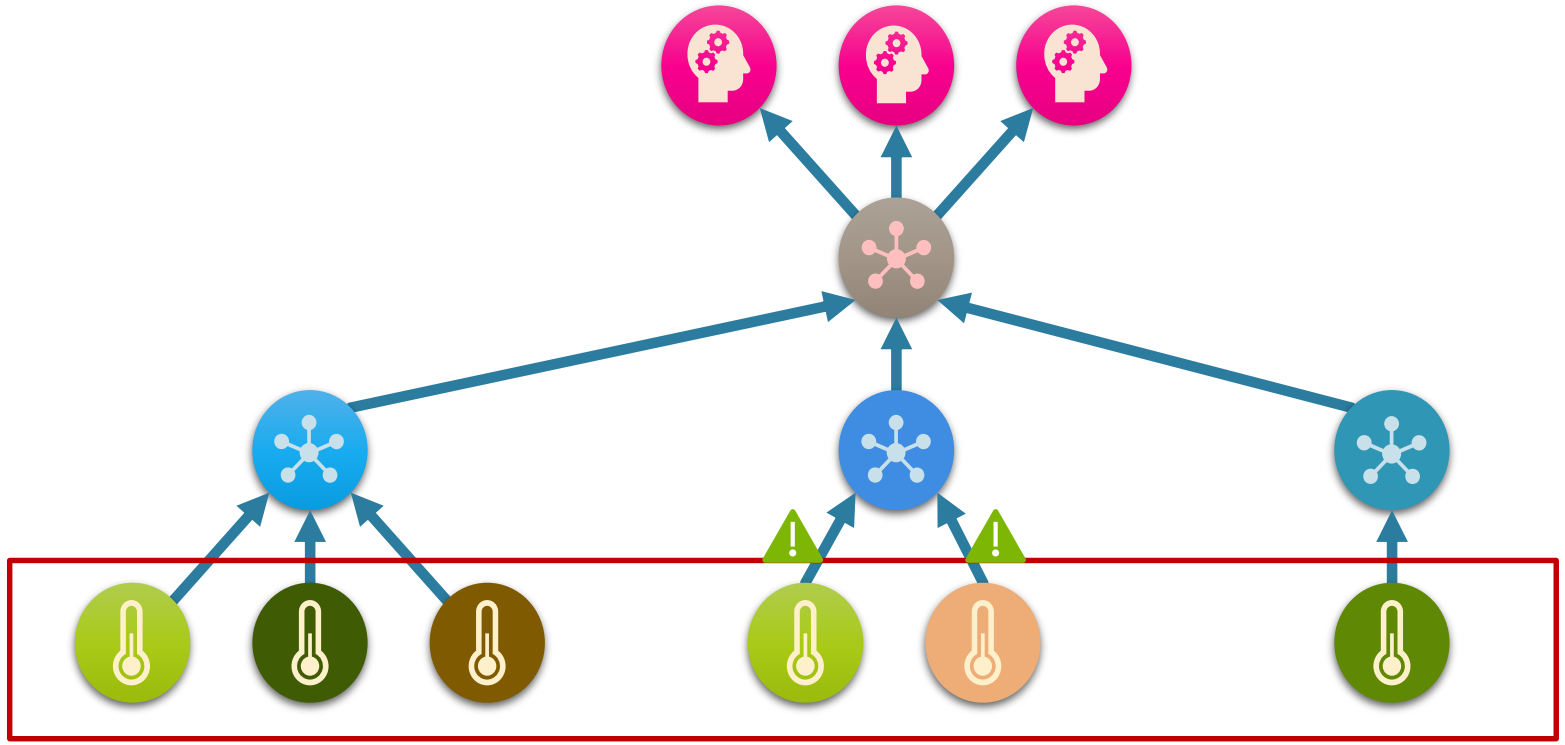
December 11th, 2018

European Commission

www.enact-project.eu

Context

- IoT system innovations were focused on:
  - From **sensors to the cloud** for processing and analysis.
  - Handling **heterogeneity**, **scalability** and **dynamicity** of IoT systems.

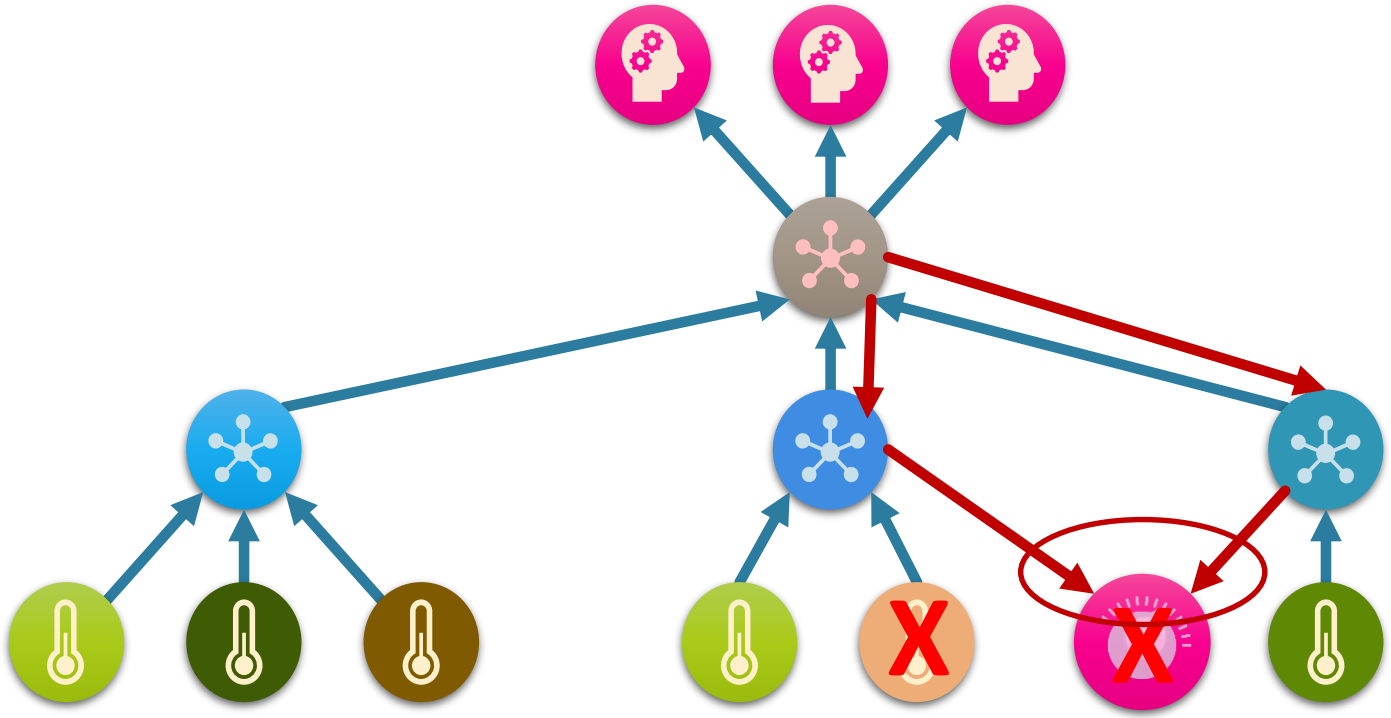


ENACT DevOps

Towards Smart IoT Systems

- The next generation of **Smart IoT Systems** need to:
  - manage the closed loop **from sensing to actuation**,
  - be distributed accross **IoT, edge and cloud** infrastructures,
  - and operate in an **unpredictable physical world.**

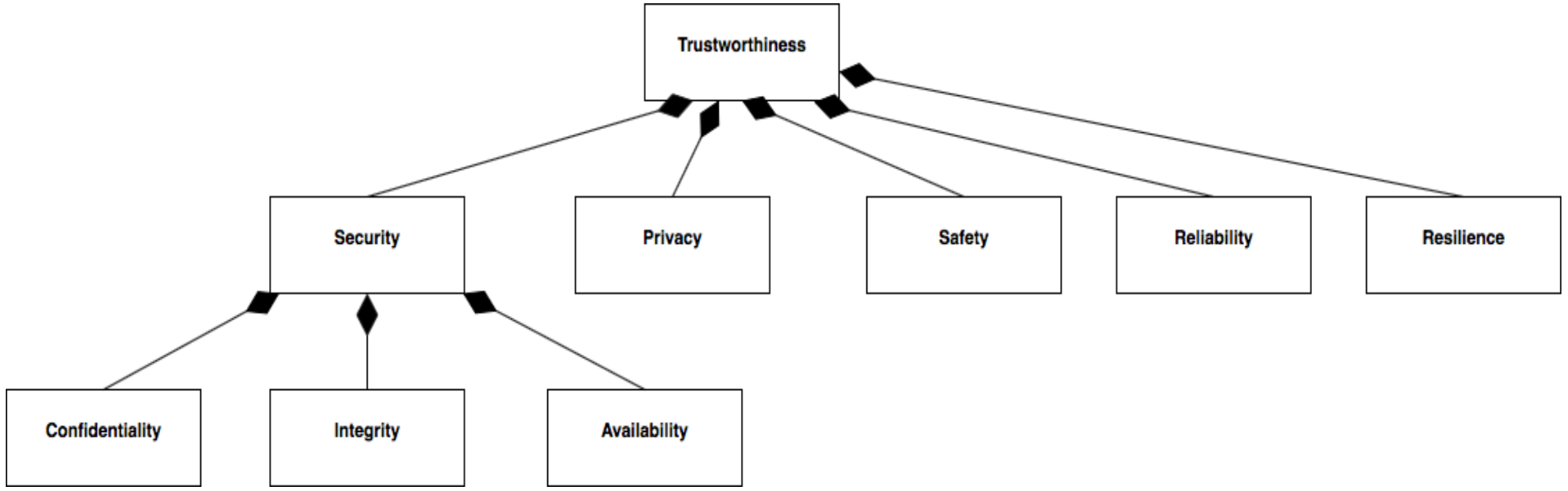
Trustworthiness



ENACT DevOps

www.enact-project.eu

Trustworthiness



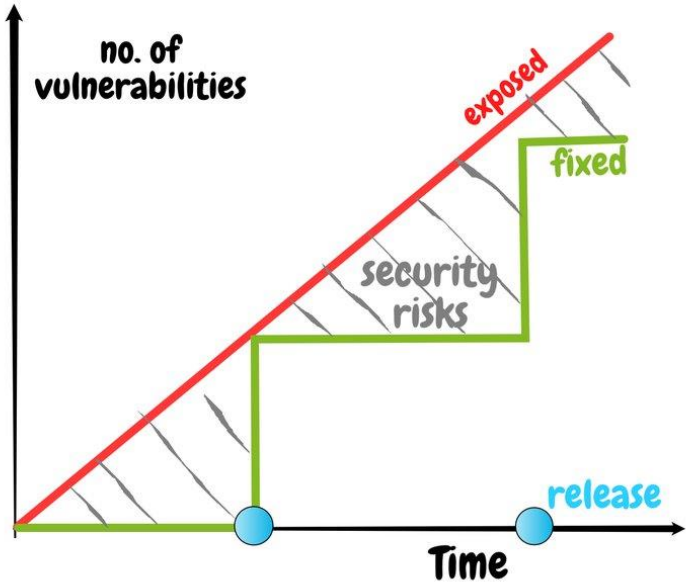
*"**Trustworthiness** refers to the preservation of security, privacy, safety, reliability, and resilience**

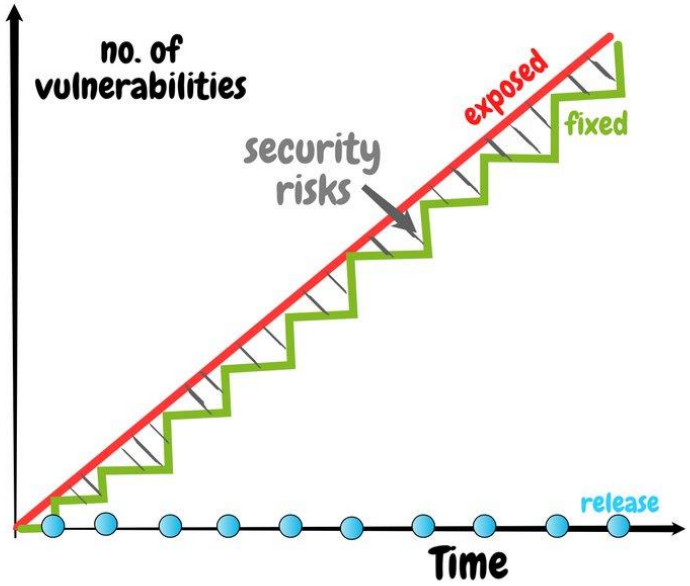
ENACT DevOps

* National Institute of Standards and Technology. NIST SP 1500-201, Framework for Cyber-Physical Systems: Volume 1, Overview, V1.0, 2017.

Continuous Evolution & Trustworthiness

- SIS Infrastructure, requirements, context, might **frequently change** thus **introducing** new internal/external **threats to trusworthiness**
- The ability of these systems to **continuously evolve** to their evolving environment is decisive to ensure and increase their **trustworthiness and quality**.

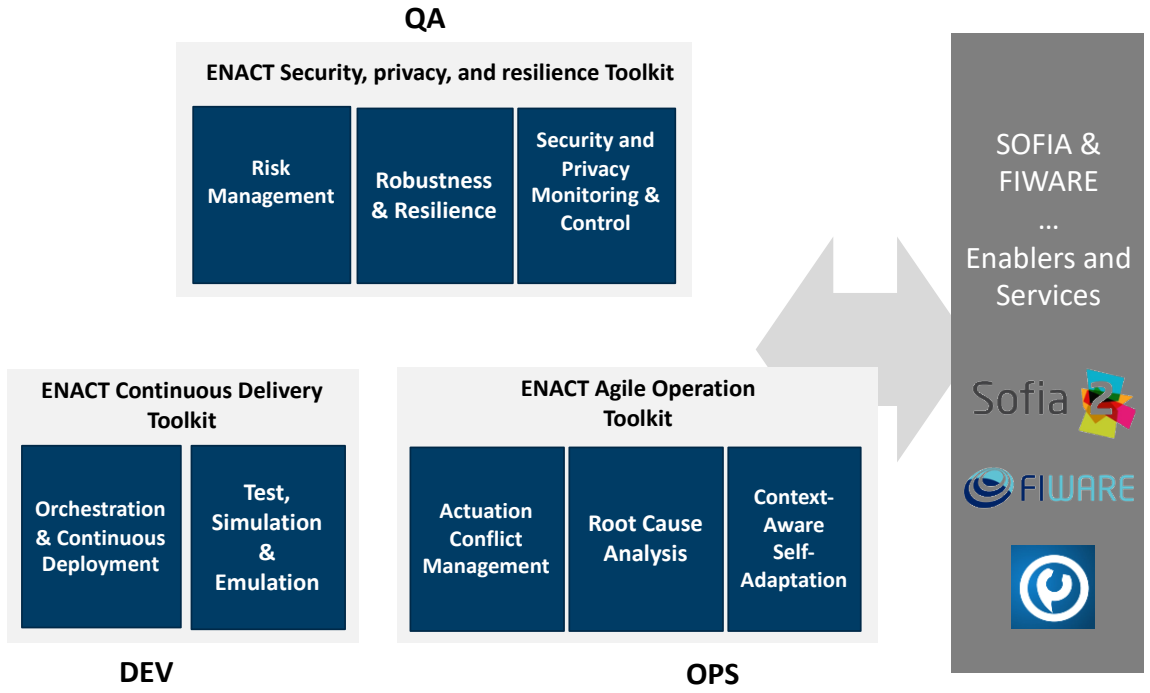




ENACT DevOps

ENACT Objective

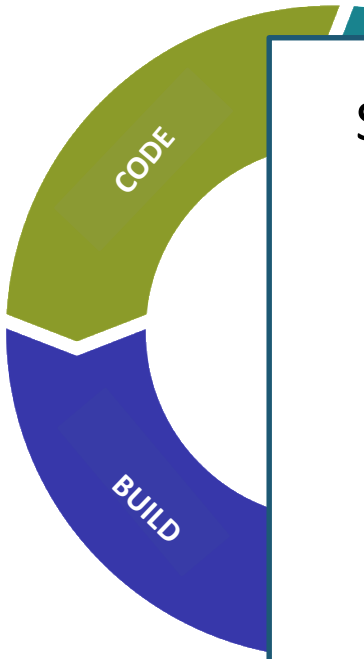
*“**ENACT** will deliver a set of loosely coupled **enablers** to support the continuous **development** and **operation** of **trustworthy** Smart IoT Systems*



ENACT DevOps

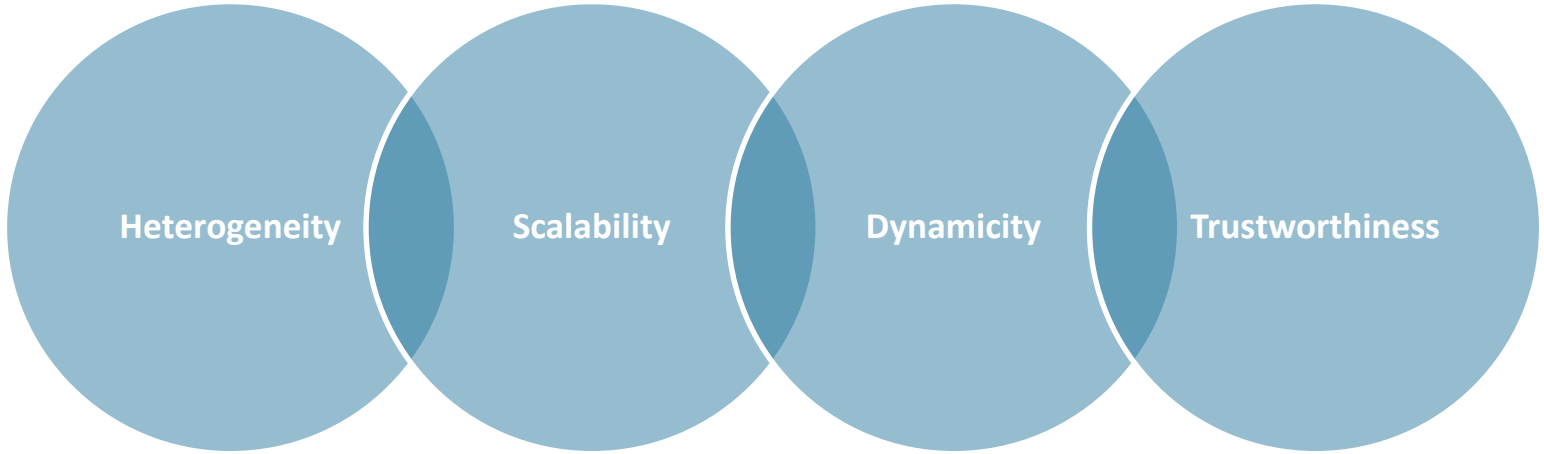
www.enact-project.eu

DevOps in a nutshell



- **DevOps core values:**

Smart IoT Systems characteristics challenge DevOps practices

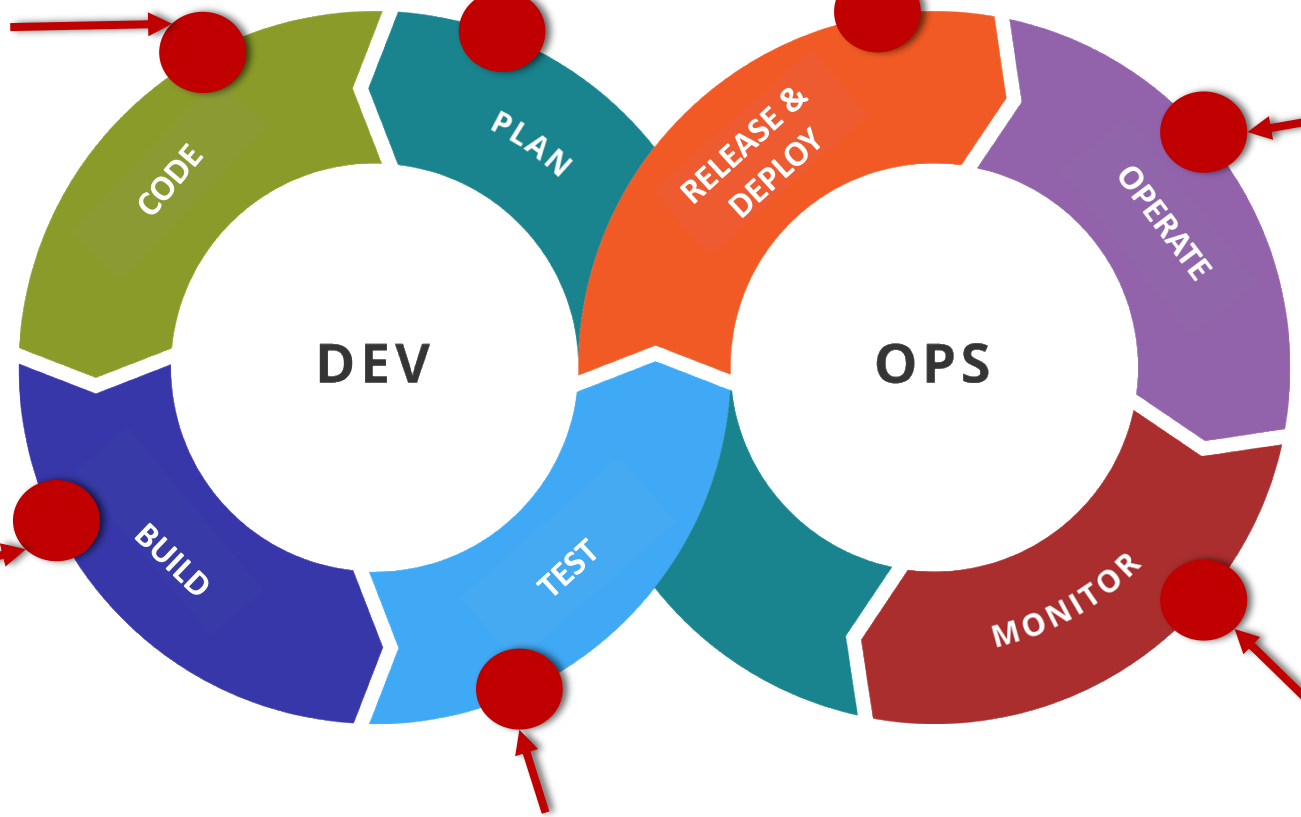


e.g., coordinated behavior distributed locally in its own open context

ng
ycle
e,
edback

ENACT DevOps

ENACT DevOps for Smart IoT Systems



Thing Functional Modelling & Orchestration of sensors, actuators, and software services and trustworthiness mechanisms

Continuous Risk Management (business and non-functional risks)

Continuous deployment of trustworthy SIS & security mechanisms

Context-aware Access control, Security control, Adaptation improvement

Automatic building of ENACT generated code & Software diversification

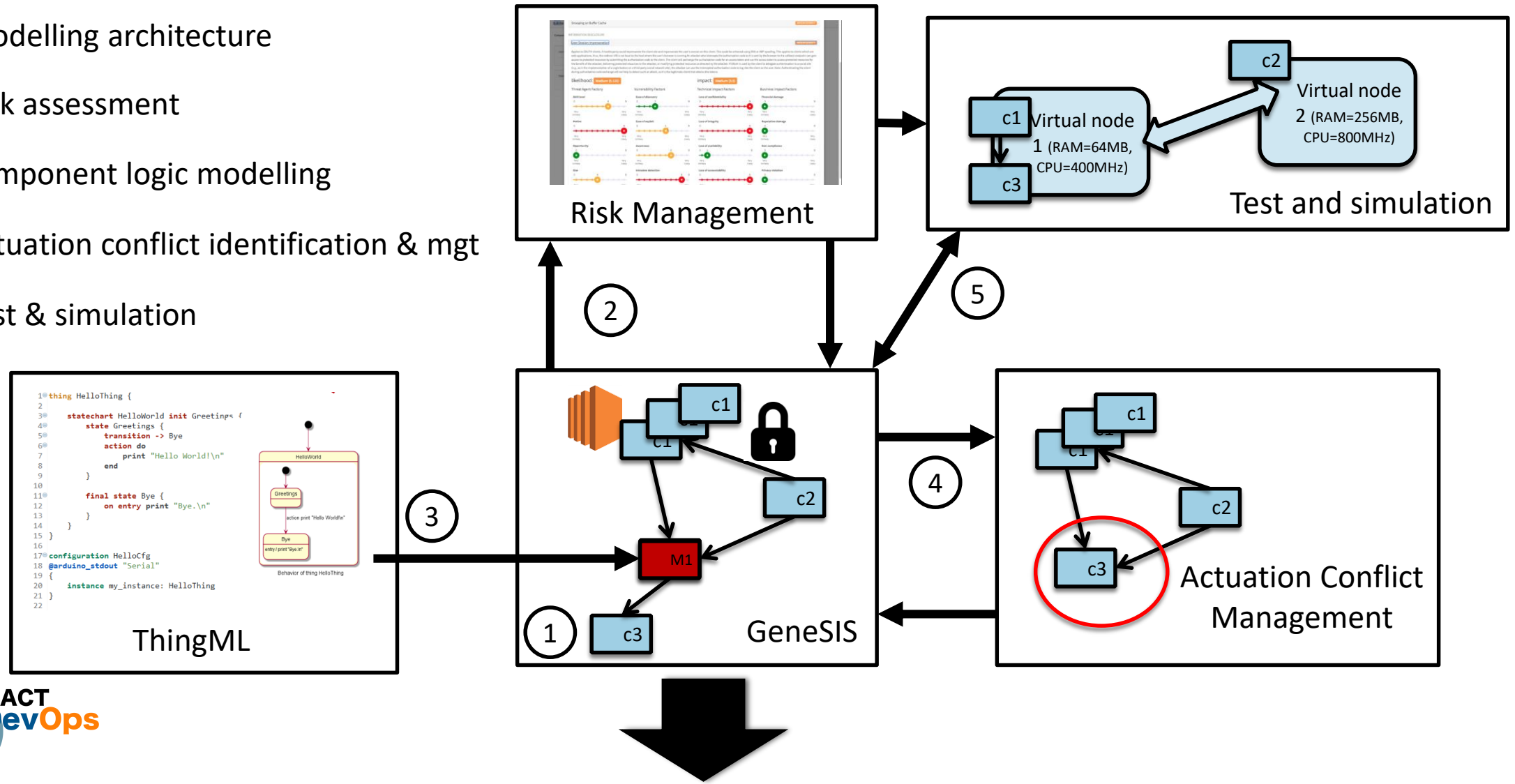
SIS simulation and security, privacy and scalability testing

Security and privacy monitoring, Behavioral drift analysis, Deployment status, Application execution flow, Root cause analysis

ENACT DevOps

An example

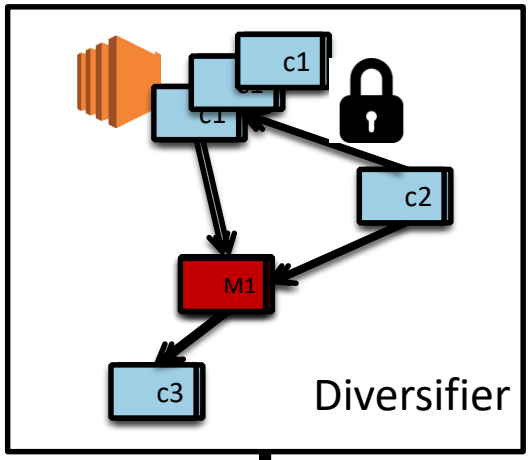
1. Modelling architecture
2. Risk assessment
3. Component logic modelling
4. Actuation conflict identification & mgt
5. Test & simulation

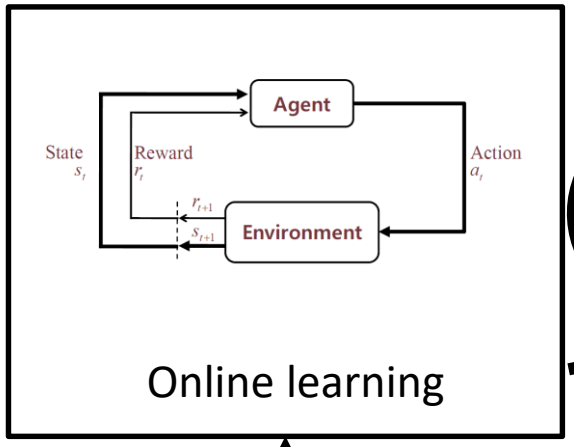


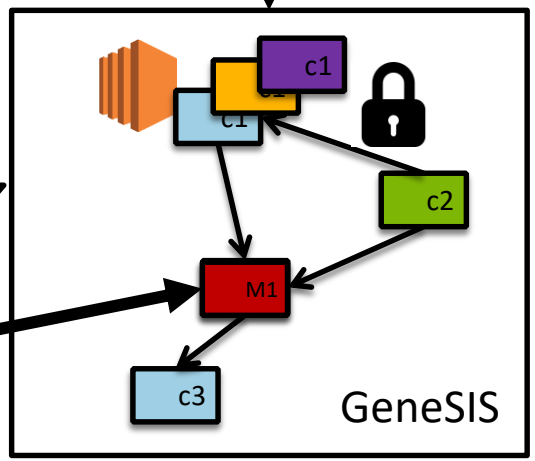
ENACT DevOps

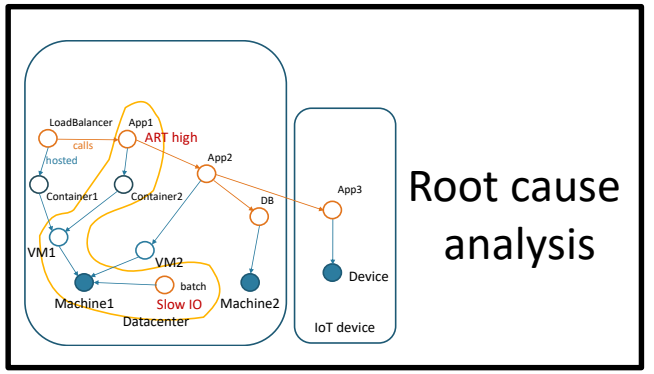
www.enact-project.eu

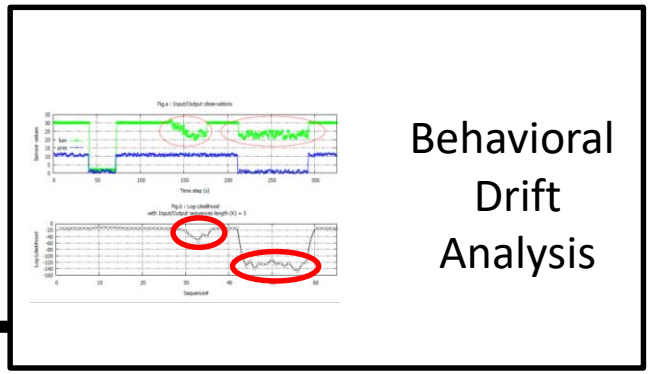
An example







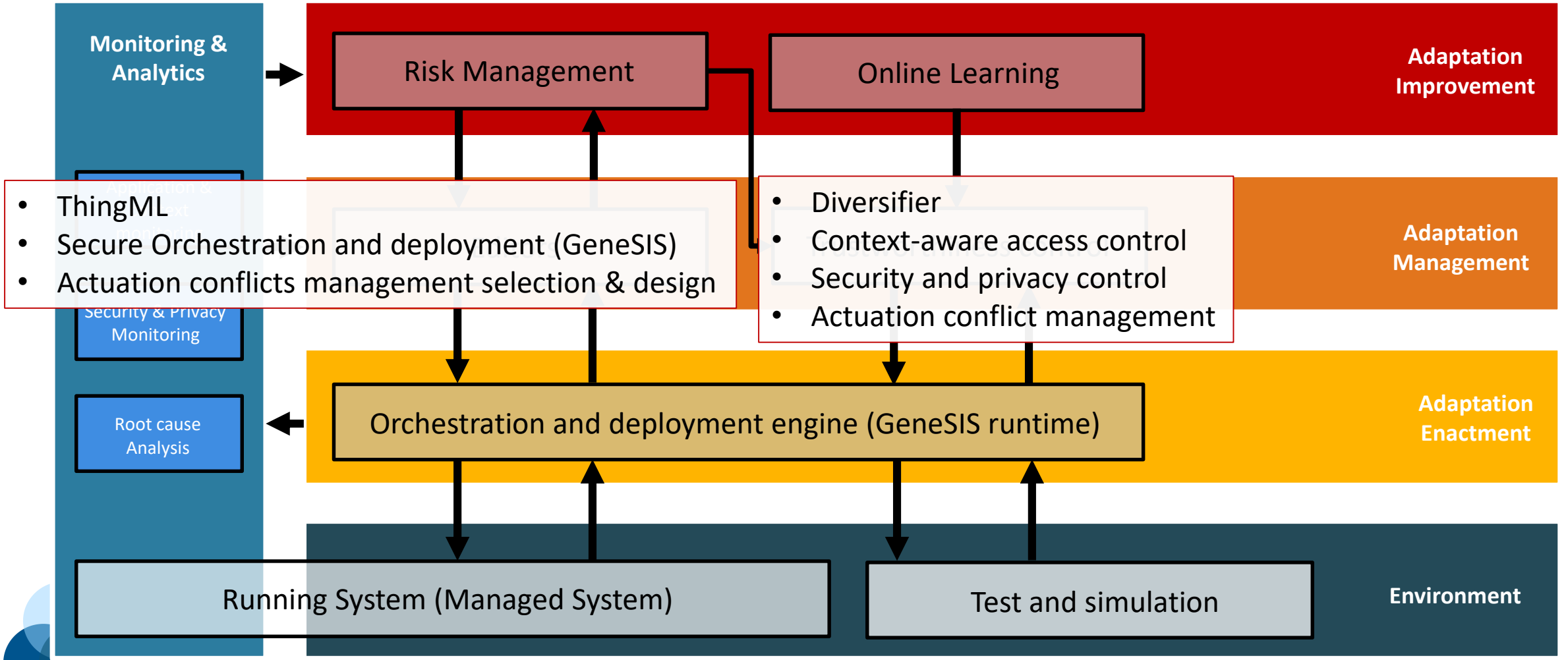




ENACT DevOps

www.enact-project.eu

Architecture



Case studies

Rail Domain

indra

INSTITUTE OF ELECTRONICS AND COMPUTER SCIENCE

BOSC

Smart Building

tecnalia

I.S.R.A.A.
Istituto per Servizi di Ricovero e Assistenza agli Anziani

eHealth

tell.u

Enhancing train integrity control	Smart Energy Efficiency and Smart User Comfort applications	Personal health gateway Customization to end user needs

ENACT DevOps

www.enact-project.eu

Enablers/use cases matrix

ENACT Framework	Enabler	ITS Domain (Rail)	Digital Health	Smart Building
Continuous Delivery toolkit	Orchestration and Continuous Deployment Enabler	X	X	X
	Test, Emulation and Simulation Enabler	X	X	
Agile Operation toolkit	Context-Aware Self-Adaptation Enabler			X
	Run-time Quality Assurance and Root Cause Analysis Enabler		X	
	Context Monitoring and Actuation Conflict Management Enabler	X		X
Trustworthiness Toolkit	Robustness & Resilience Enabler		X	
	Risk-Driven Decision Support Enabler		X	X
	Security and Privacy Monitoring and Control Enabler	X	X	X

ENACT in the cluster of IoT projects

- ENACT provides mechanisms and tools to facilitate the instantiation, integration and maintenance of trustworthiness mechanisms into IoT systems.
  - Contrary to other projects we do not necessarily contribute with new mechanisms for security and privacy.
  - But we can integrate, leverage, or support (e.g., the deployment) the mechanisms from the other projects

ENACT involvement and contribution

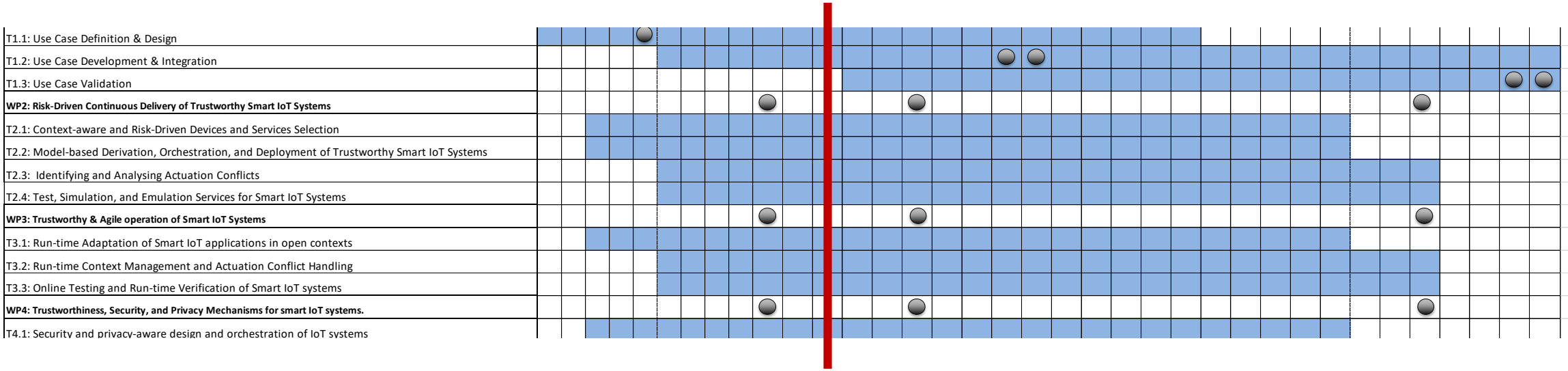
- We contributes to the following topics:
  - *IoT Platform Interoperability.*
  - *Identify relevant existing standards for lifecycle management of security and trust.*
  - *Risk management and assessment.*

- We lead the activity on building a *"**repository of tools and approaches** to support/enforce the **trustworthiness of IoT systems** at design- and/or run-time "*

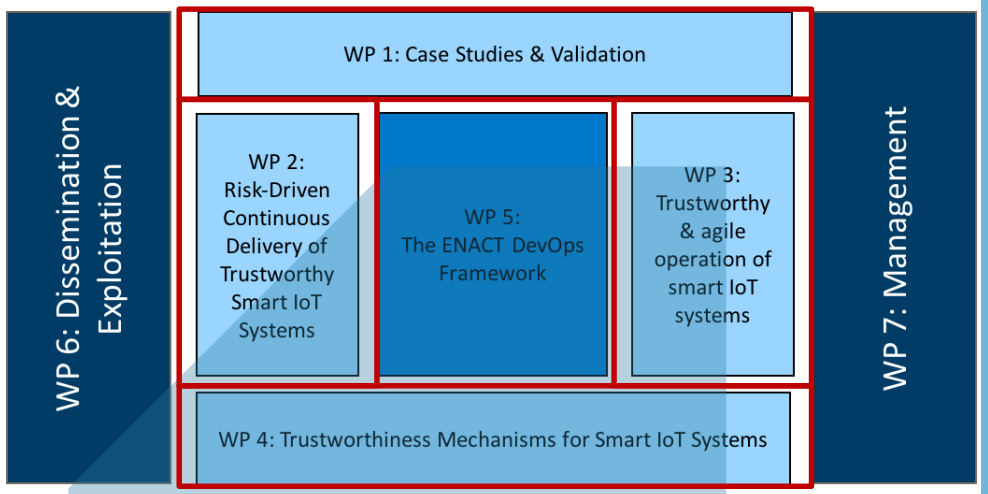
- We are involved and contributed to several dissemination activities:
  - ICT event, CHARIOT workshop, ETSI security week

Brief overall status M12

- First technical deliverables all submitted
- Next deliverables are due at M15



In the next presentations



ENACT DevOps

Project highlights

- **Technical highlights:**
  - Extensive state-of-the-art analysis (including SLR, and SMS)
    - That illustrates the needs for ENACT
  - Some initial prototypes (e.g., GeneSIS, Access control) & design of all enablers
  - First architecture
  - Integration guidelines

- **Dissemination:**
  - 7 publications
  - Organized 1 conference (QUATIC) and 1 research workshop (MDE4IoT)
  - 1 Video of prototype
  - Invited lectures

ENACT DevOps

Development, Operation, and Quality Assurance of Trustworthy Smart IoT Systems.

***Contact**: nicolas.ferry@sintef.no*