

ROBUSTNESS PROPAGATION THROUGH SYSTEMS OF HETEROGENEOUS COMPONENTS - Lego Methodology

Mohamad Hajj (Presenter) & Claire Loiseaux, Internet of Trust

PCM 2018

Lille, December 07, 2018

Context and objective

- The lego methodology is an industry oriented approach for the evaluation of systems. It has been developed during the ODSI project.
- ODSI (On Demand Secure Isolation) is a Celtic-Plus project C2014/2-12 (Nov 2015-> February 2019)
 - It has 11 partners (from France, Spain and Romania) and is driven by Orange
 - Celtic review held in November 2018 states that the protokernel and the lego methodology were the 2 major outcomes of the project.



Objectives

- **End-to-end security evaluation** methodology for systems based on three concepts:
 - **Improving** the security and **simplifying** the evaluation relying on a proved kernel (Re-use of formal proofs)
 - **Defining a Use Case based security evaluation** methodology
 - Risk analysis to determine the list of assets, threats, security functions and the robustness level
 - Only some Security Functions (e.g. Isolation) are required when we choose a restricted configuration corresponding to a UC
 - Evaluation of required functions from components at the appropriate robustness level
 - **Adapt and combine CC features**
 - Composition (CC Composite)
 - Evaluation of the integration between components (ACO)
 - Multi-Assurance (under definition in future version of ISO 15408 (Common Criteria))
 - Plug and Play including the patch management



Main current issues of the system evaluation under the existing approaches

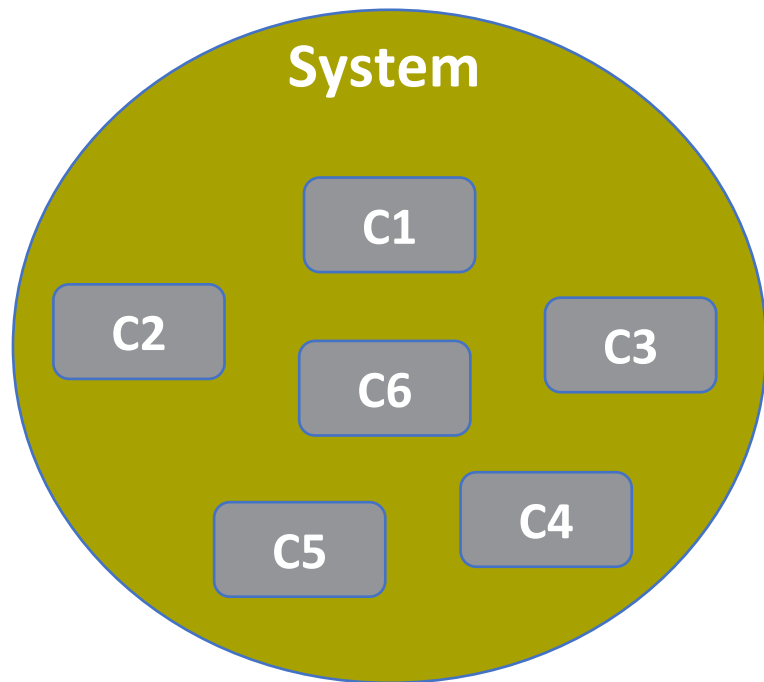
- Evaluation of the system = Evaluation of components in their entirety



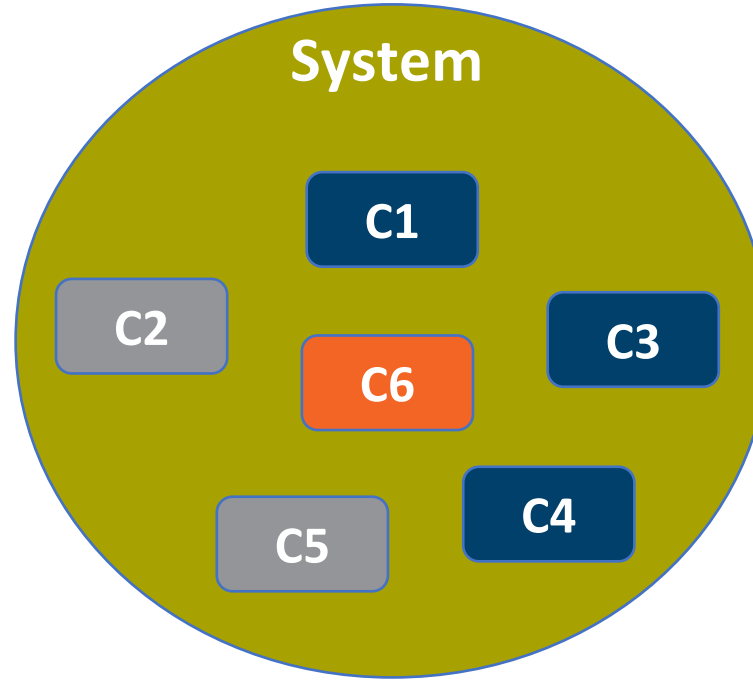
- Hard to reach a high robustness level for all the functions
- High effort, time and cost for the evaluation
- An expensive reevaluation process is required to update, add or remove components

Three configurations of system integration

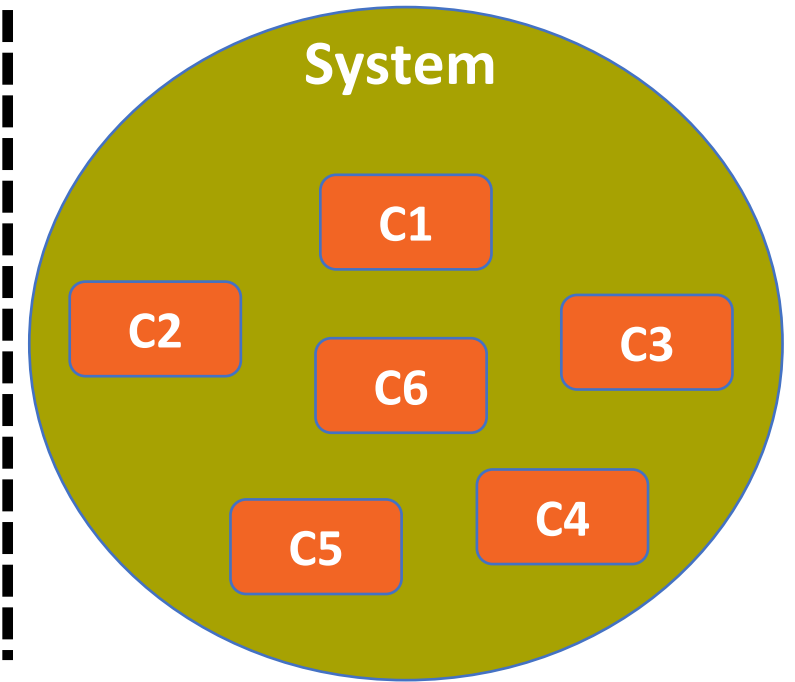
C: Component



System = non-evaluated components



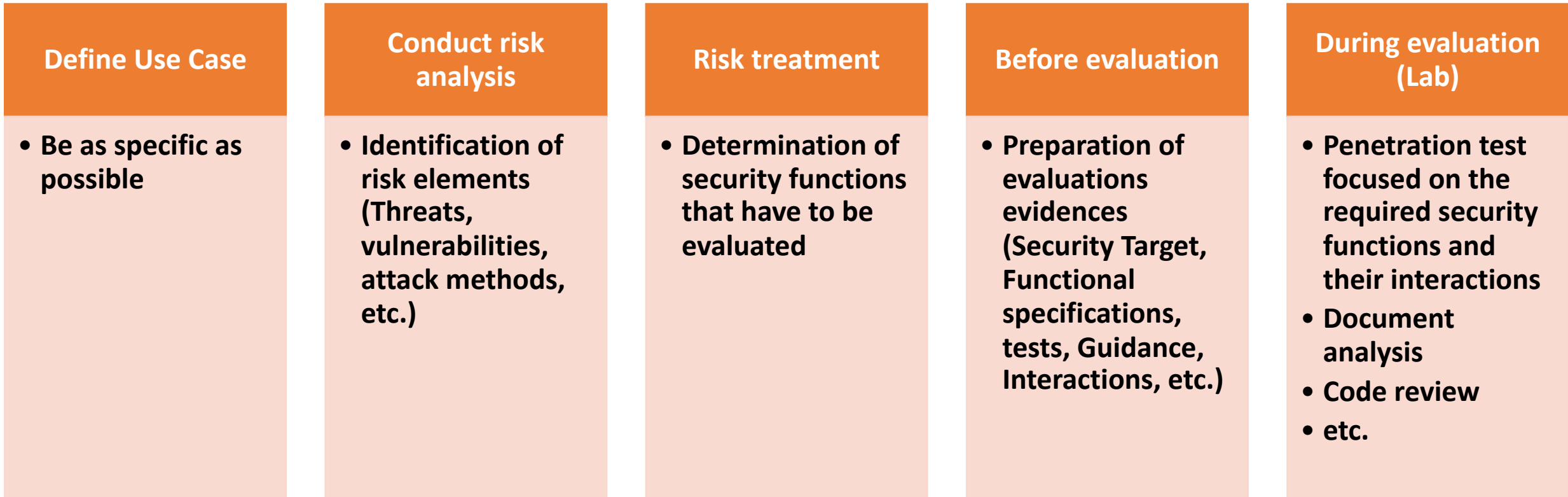
System = both non-evaluated and evaluated components with different robustness levels



System = only evaluated components with homogenous robustness level

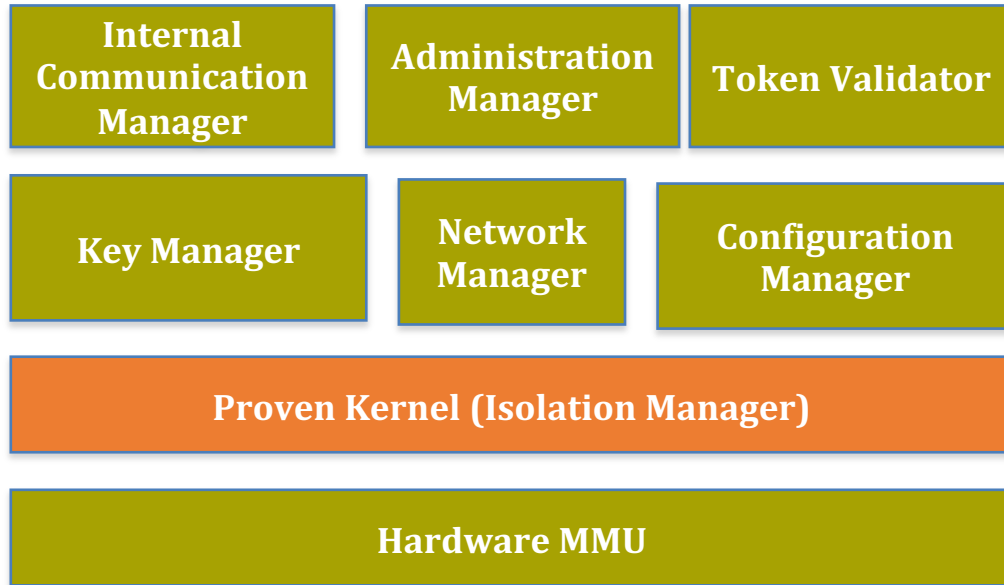
Use Case and Risk Analysis

The Lego Methodology methodology is performed following five steps:

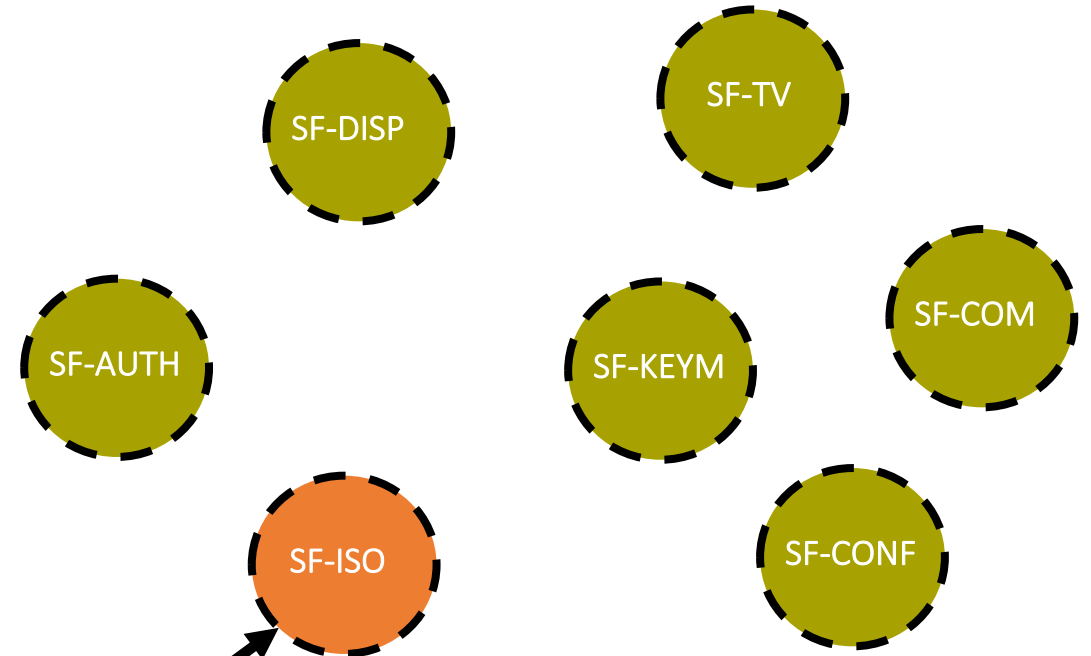


ODSI Components & Security Functions

ODSI Components



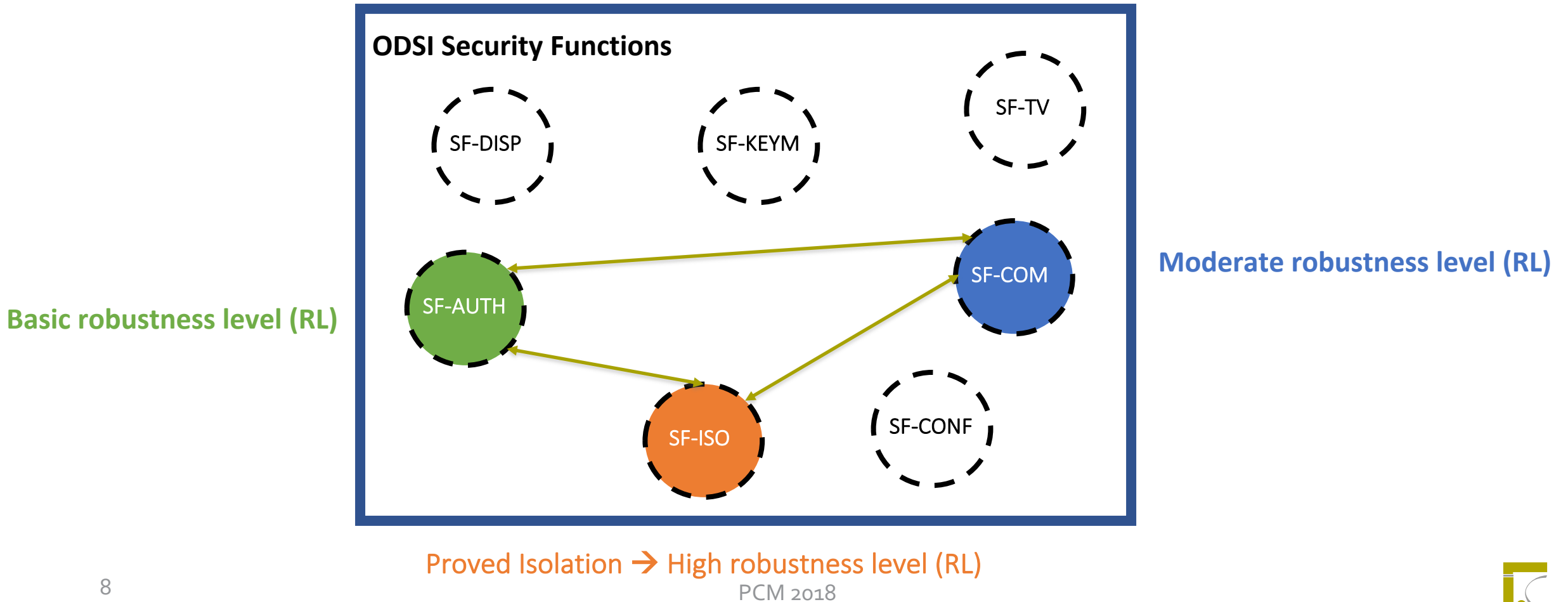
ODSI Security Functions



- Proved Isolation → High robustness level (RL)
- Trusted Ground

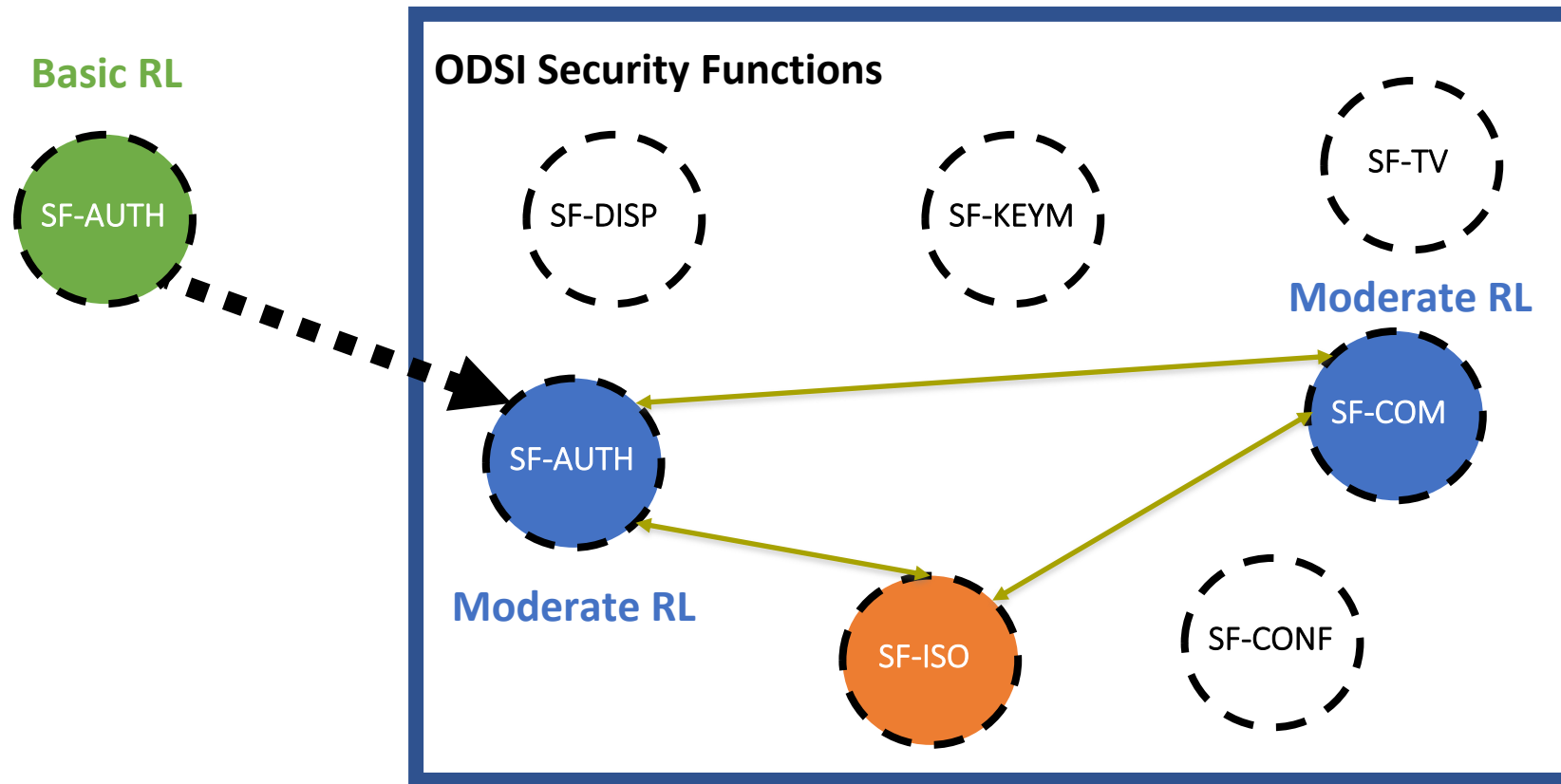
Reduction of the evaluation perimeter

- Within a well defined use case only some required security functions (SF) are used.
- In this example, the scope of the evaluation is : SF-ISO, SF-COM, SF-Auth with different robustness levels



Increase the robustness level (RL) of some SFs

SF-Auth from Basic RL to Moderate RL



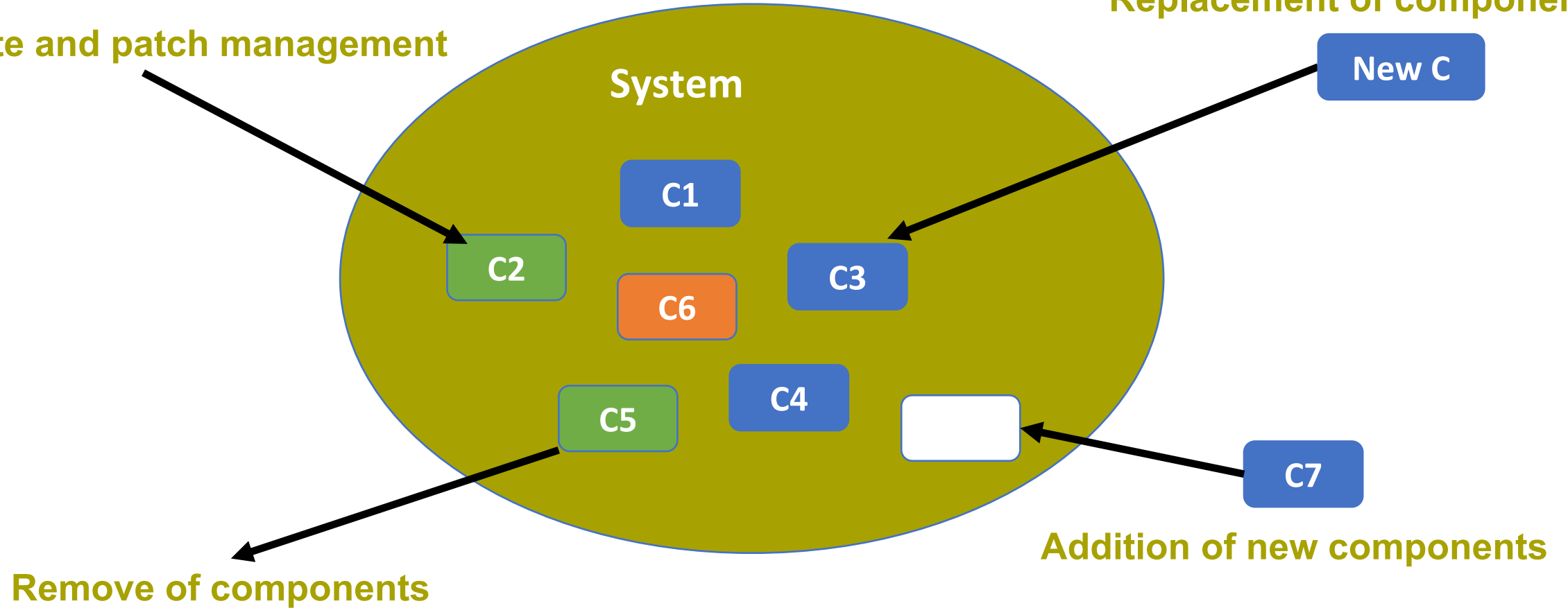
Proved Isolation → High RL
PCM 2018

Dynamic plug-and-play integration

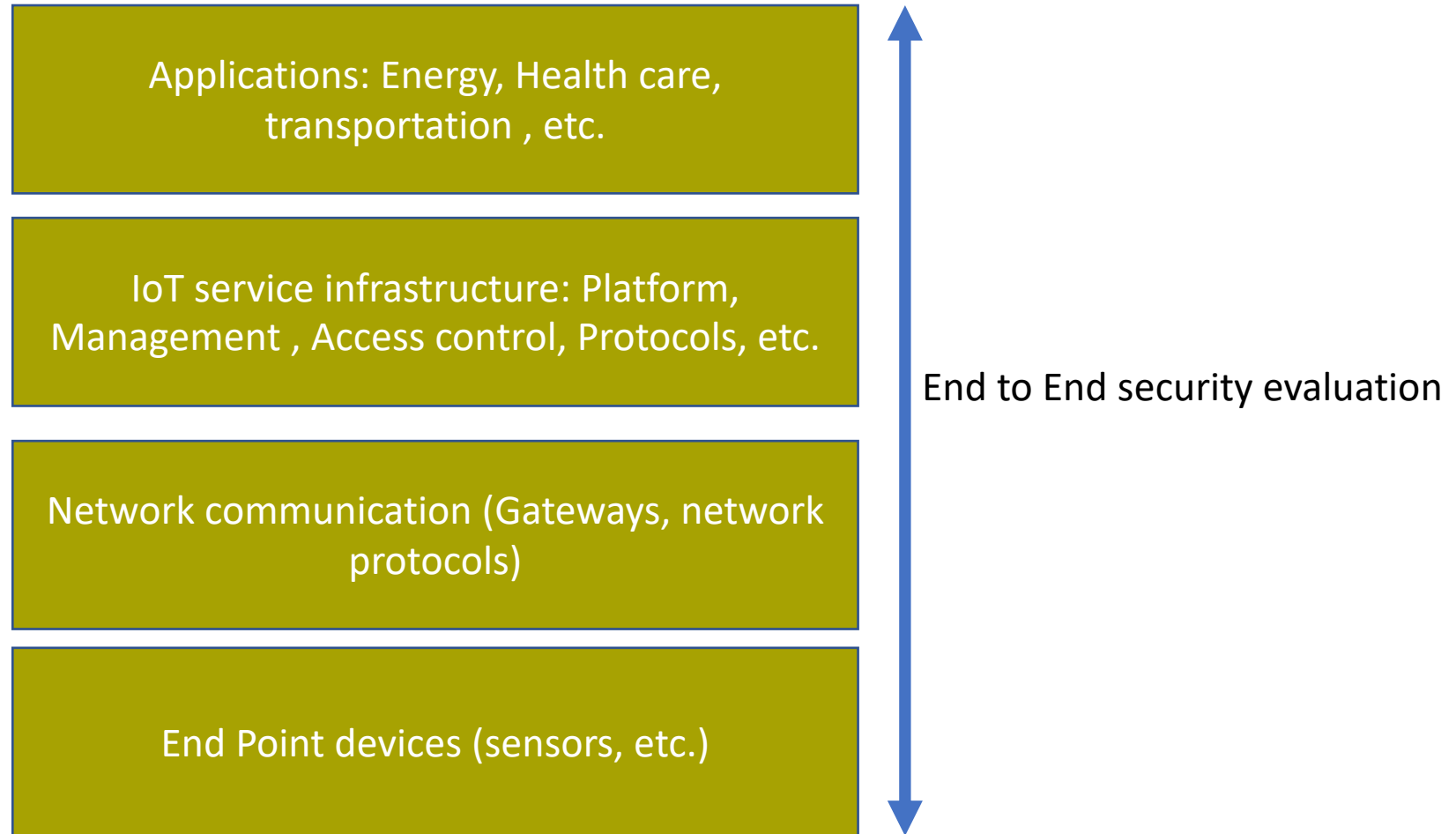
C: Component

Replacement of components

Update and patch management



Example of application – within IoT End-to End system



Conclusion

- Evaluation of the integration of components
- Reduction of the perimeter of the evaluation to only required Security Functions (SF) in a restricted configuration or use case
- Possibility to increase the robustness level of SFs
- Dynamic plug-and-play integration: possibility of adding, updating, removing or exchanging components
- Lightweight and compact approach that is targeted at IOT systems, from end-points, intermediate components such as gateways, up to integrated systems including cloud.
- Generic approach for addressing several industry sectors



Thank you

To know more about ODSI project: <https://www.celticplus.eu/13305-2/>

Contact for questions



- Lego methodology
 - Mohamad Hajj – mohamad.hajj@internetoftrust.com
 - Claire Loiseaux – claire.loiseaux@internetoftrust.com

