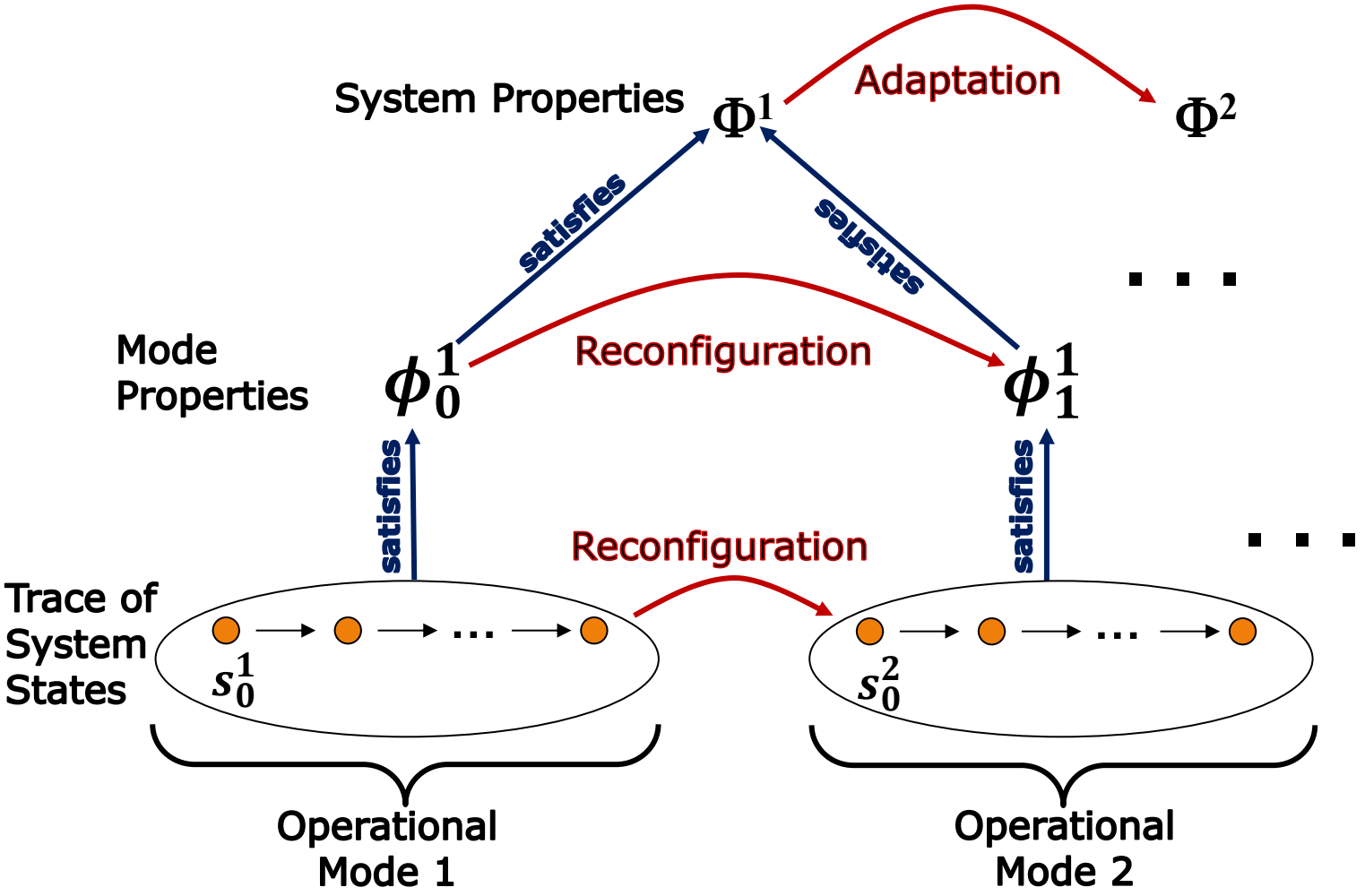
CITADEL Adaptive Systems for High-Assurance Protection

Stefano Tonetta (FBK)

Need of adaptive systems

- COMPASS provides a set of formal methods to analyze dependability requirements
- Not cost effective for many systems but essential for high-assurance systems (safety critical, security critical, or mission critical)
- Particularly appealing for model-based design of FDIR (also for security-related failures)
- However, most software-related accidents involve incomplete requirements and unhandled or mishandled conditions
- Need resilience to unforeseen faults/attacks
- To be resilient, a system must be adaptive, dynamically changing reconfiguration at run-time

Reconfiguration vs. Adaptation



Adaptive systems

- New properties/requirements represent fixes to the previous specification
- Anomaly detection can be used to detect unhandled faults/attacks
- Quite common in intrusion detection and system health monitoring
- To be integrated into a model-based design of FDIR
- Run-time change of requirements need high automation of the development and deployment process
- Needs:
  - Model-based approach to adaptations
  - Automated determination of new target configuration to achieve adaptation
  - Automated synthesis of steps to transition to the new target configuration
  - Automated adaptation of verification/validation/assurance

CITADEL

- H2020 project started on June 1st, 2016
- 3-year IA (Innovation Actions) project
- Led by The Open Group
- Consortium partners:

TTTech
THE Open GROUP
FREQUENTIS
TU/e Technische Universiteit Eindhoven University of Technology
@SEC the information security provider
FONDAZIONE BRUNO KESSLER
IK4 IKERLAN Research Alliance
Université Grenoble Alpes
oas AKTIENGESELLSCHAFT
ATB Institut für angewandte Systemtechnik Bremen GmbH
SYSGO EMBEDDING INNOVATIONS
UniControls Transport and Industrial Control Systems
J.W. OSTENDORF
KASPERSKY lab

CITADEL Objectives

- Build on the MILS technology accomplishments of D-MILS and EURO-MILS
  - Declarative specification of dynamic policy architectures
  - COMPASS-based analysis of the policy architecture
  - Automatic configuration of MILS platform to enforce the policy architecture
  - MILS platform components to enforce Isolation and Information Flow Control and provide dynamic reconfiguration
- Develop a monitoring framework integrating model-based FDI and anomaly detection
- Develop an adaptation framework to reconfigure the architecture at run-time preserving system properties
- Develop an assurance framework to support the claims about the adaptive systems