Distributed MILS Project Work-in-Progress

Rance DeLong

THE Open GROUP
Making standards work®

Distributed MILS (D-MILS) Project

- European Commission FP7
  - Project #318772
  - December 2012 – December 2015
- D-MILS Project Consortium Partners
  - Fondazione Bruno Kessler – Italy
  - Fortiss – Germany
  - Frequentis – Austria
  - LynuxWorks – France
  - RWTH Aachen University – Germany
  - The Open Group – United Kingdom – Lead
  - TTTech – Austria
  - Université Joseph Fourier – France
  - University of York – United Kingdom

Short MILS Review

- MILS is a component-based approach for the construction, assurance, and certification of dependable systems that encourages a commercial marketplace of off-the-shelf high-assurance components
- MILS can be understood as a two phase approach:
  - Architecture
    - Abstract policy architecture represented with "boxes" (operational components) and "arrows" (interactions)
    - System purpose is achieved by behavior of the operational components and their interactions
    - Assumption: the architecture will be strictly enforced
  - Implementation
    - A robust resource-sharing platform composed of MILS foundational components creates strongly isolated "exported resources"
    - Components individually developed and assured according to standard specifications
    - Components compose "additively" to form a distributed trusted sharing substrate, the MILS Platform

MILS Policy Architecture

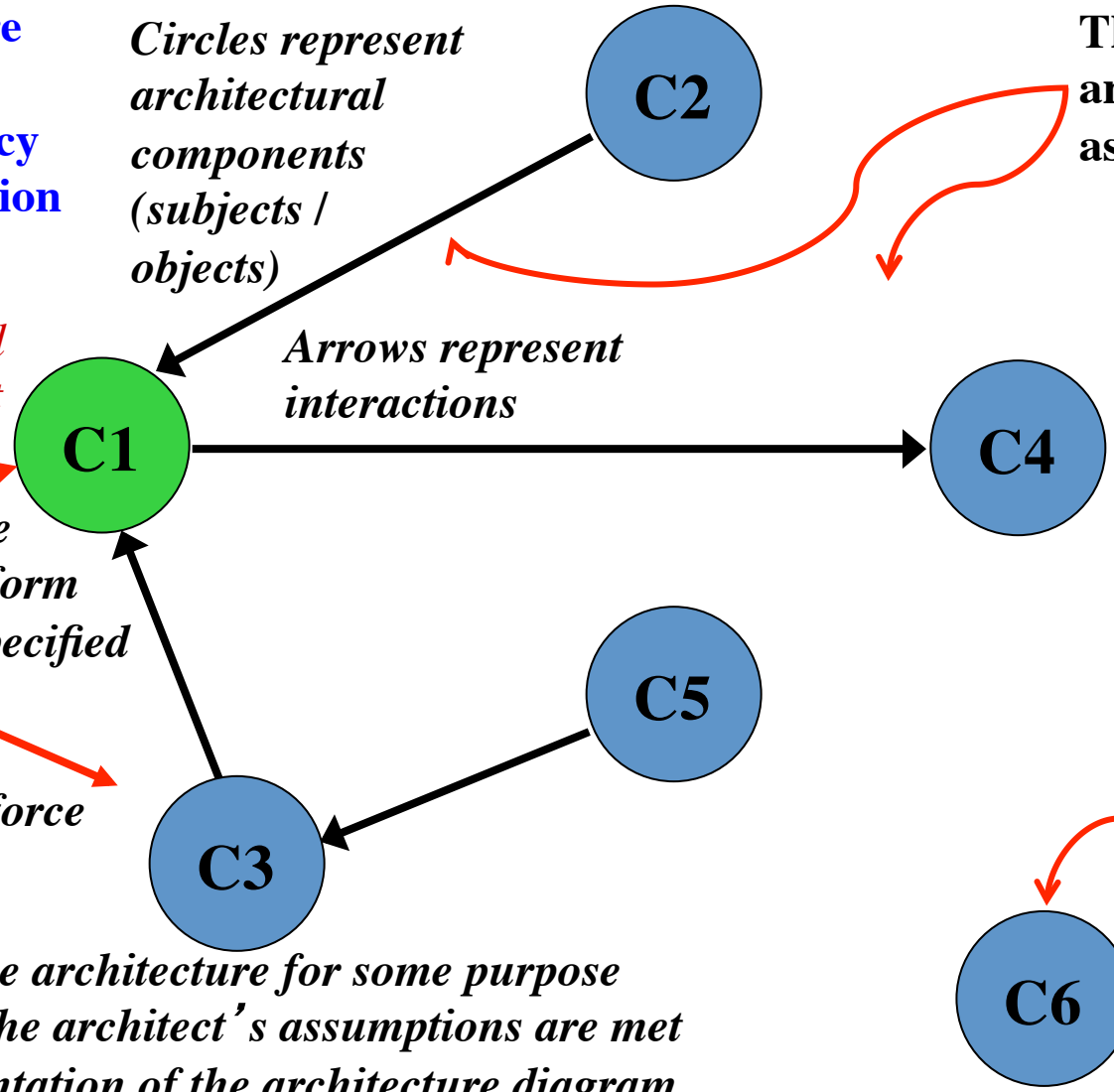
The architecture expresses an interaction policy among a collection of components

Circles represent architectural components (subjects / objects)

Trusted Subject

Arrows represent interactions

The *absence* of an arrow *is as significant* as the *presence* of one



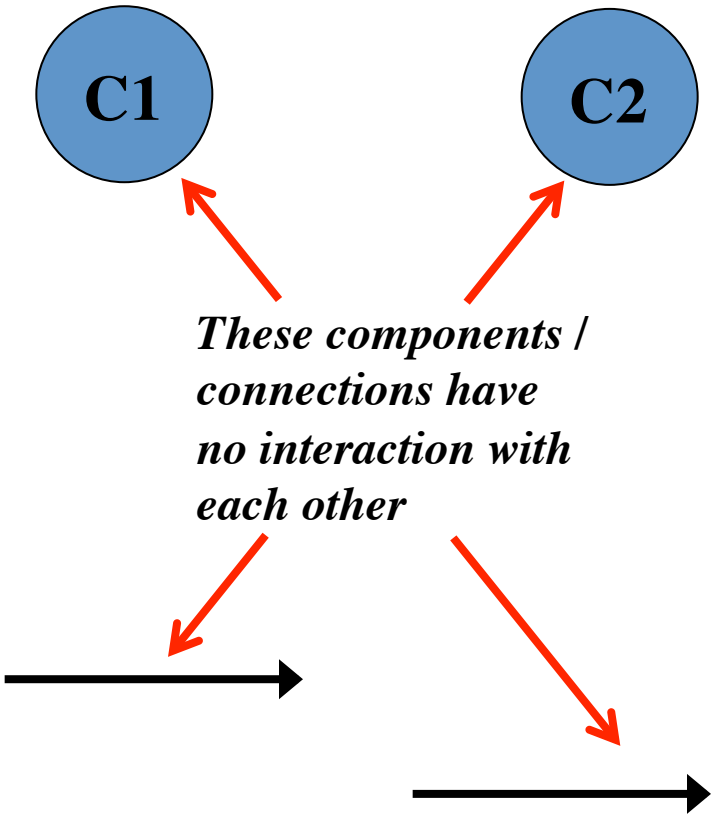
Components are assumed to perform the functions specified by the architect (trusted components enforce a local policy)

This component has *no interaction* with any other

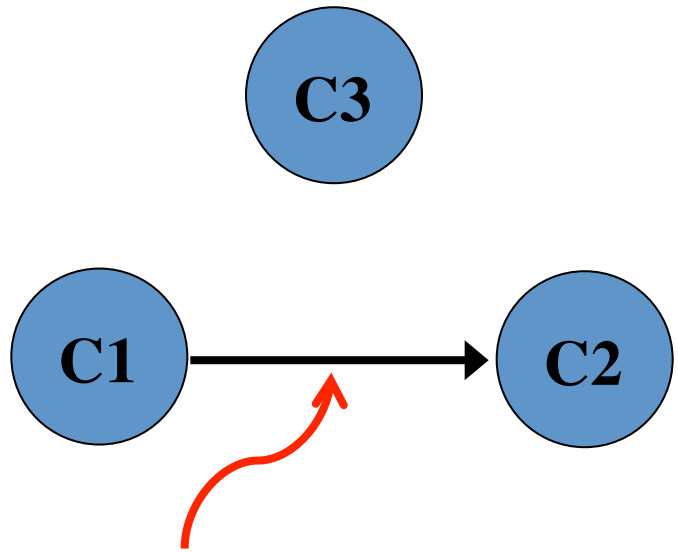
Suitability of the architecture for some purpose presumes that the architect's assumptions are met in the implementation of the architecture diagram.

Assumptions Implicit in the Architecture Represent Two Primitive Policies

1. Isolation

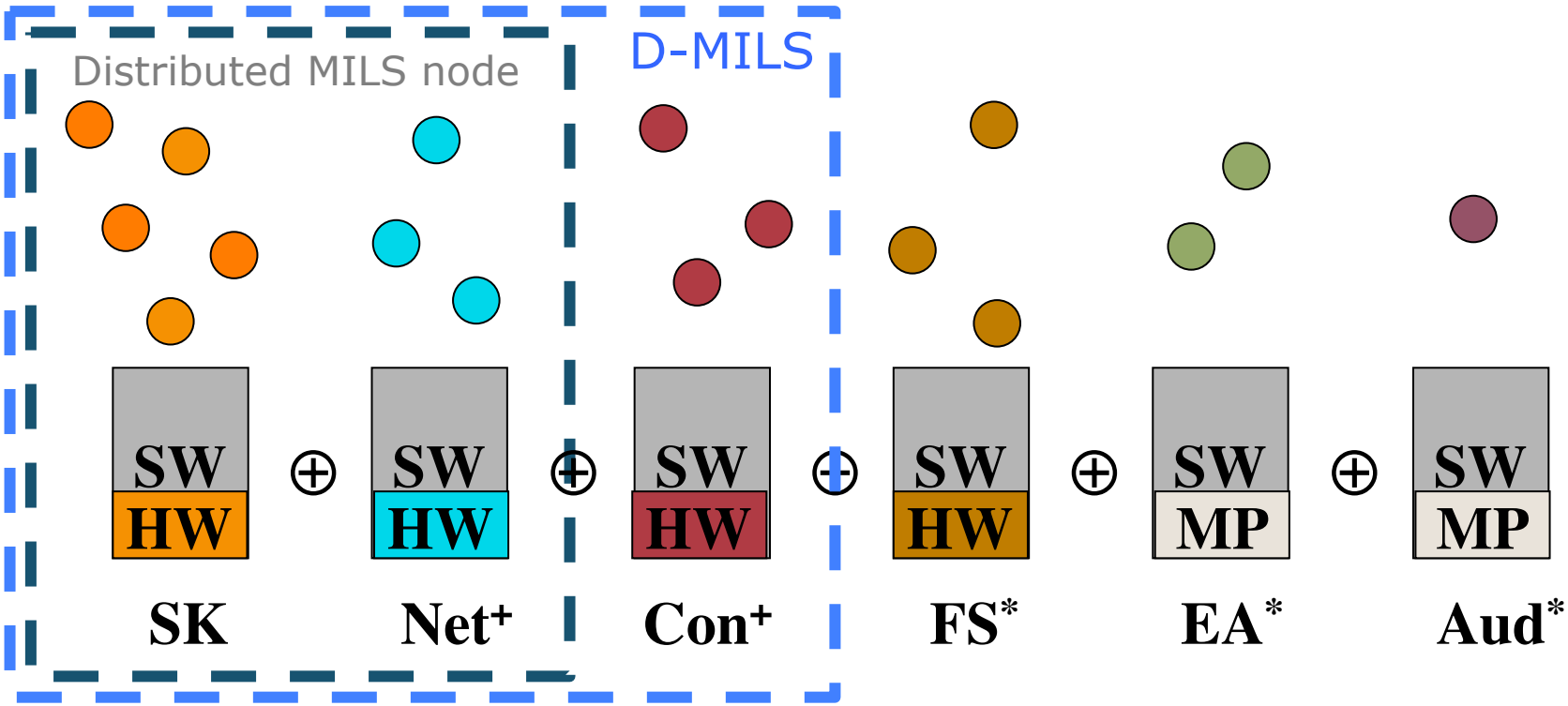


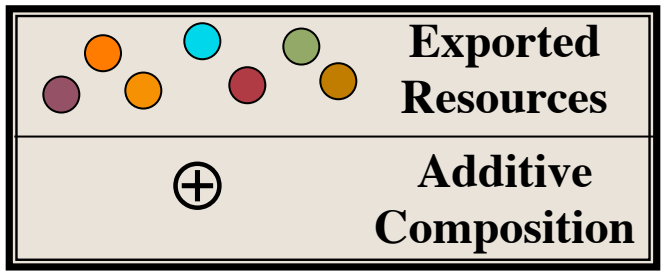
2. Information Flow Control



Only *explicitly permitted* causality, data flow, or *interference*, is permitted. The architecture *permits* this flow. Only C1 or C2 can *cause* the flow, C3 can not. The flow is directional and intransitive.

The MILS Platform: Resource-Sharing Components





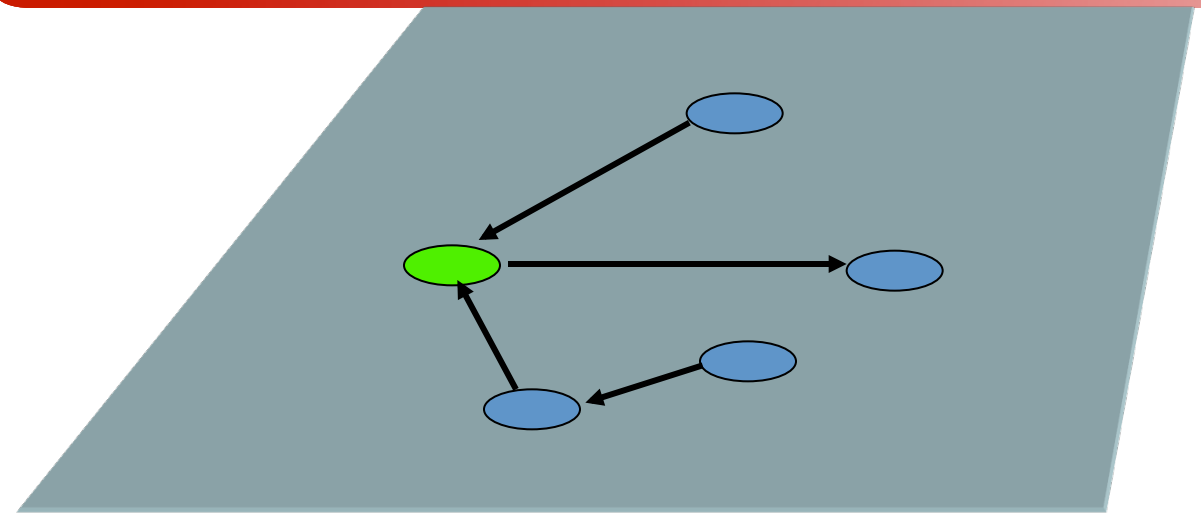
additive compositionality – e.g.,
Partitioning Kernel ⊕ Partitioning Net
= Partitioning (Kernel + Net)

MP = MILS Platform

+ D-MILS includes limited versions of Net(work) and Con(sole)

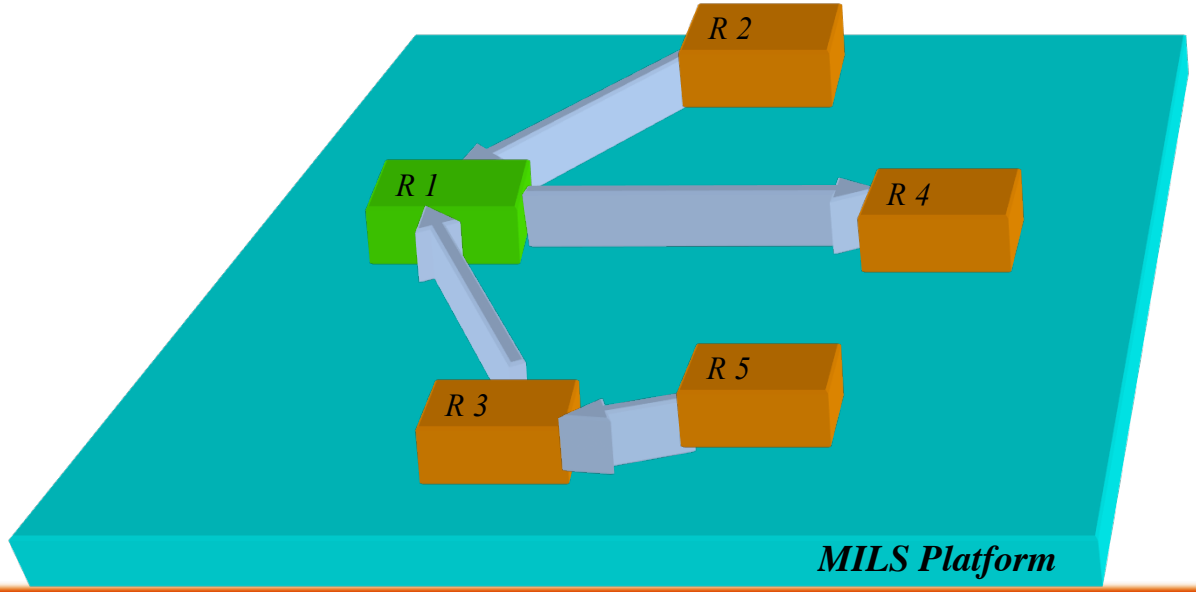
* D-MILS does not include MILS FS, EA and Aud components

MILS Platform – Provides Straightforward Implementation of Policy Architecture



Architecture

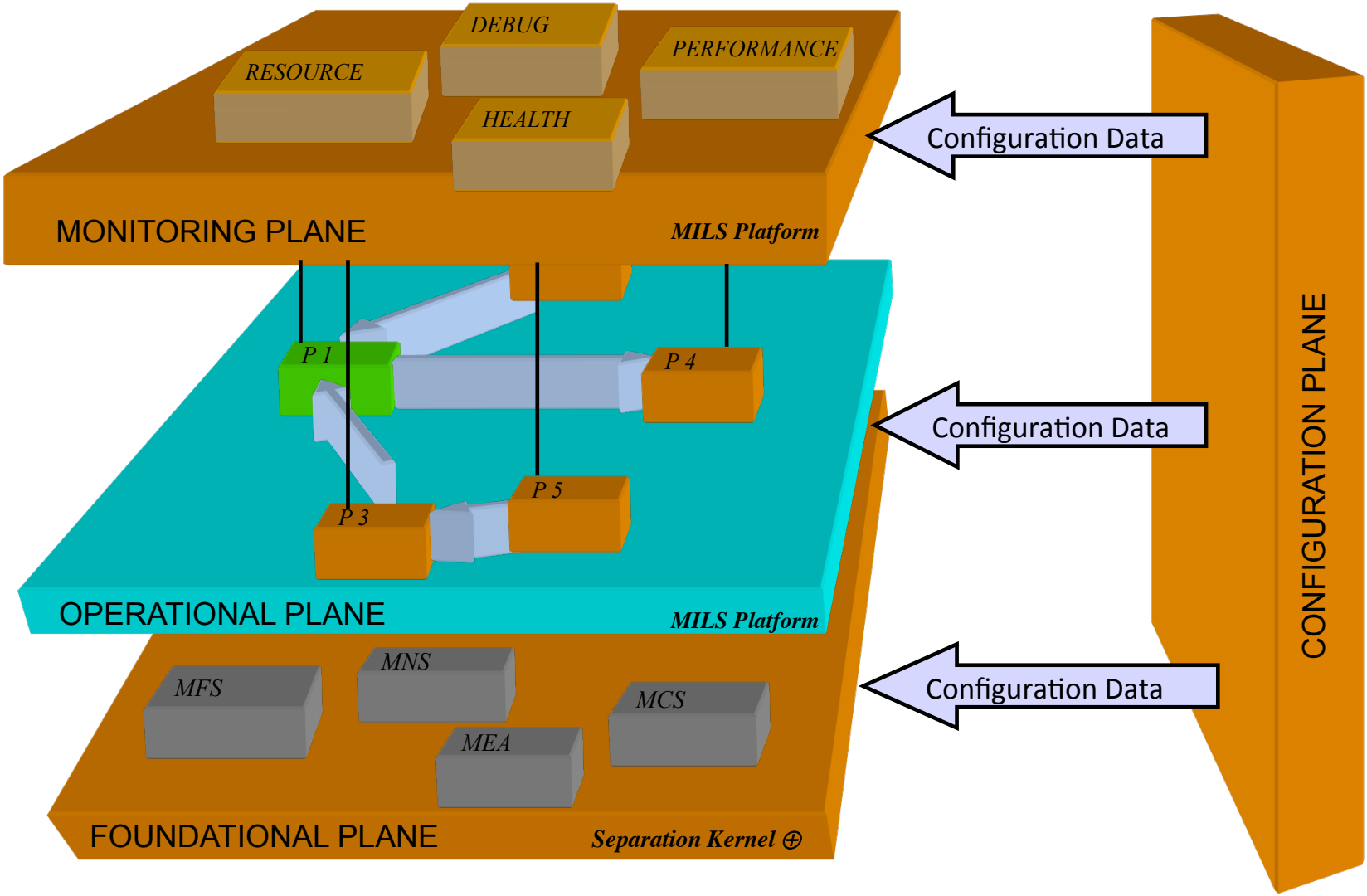
Validity of the architecture assumes that the *only* interactions of the circles (operational components) is through the arrows depicted in the diagram



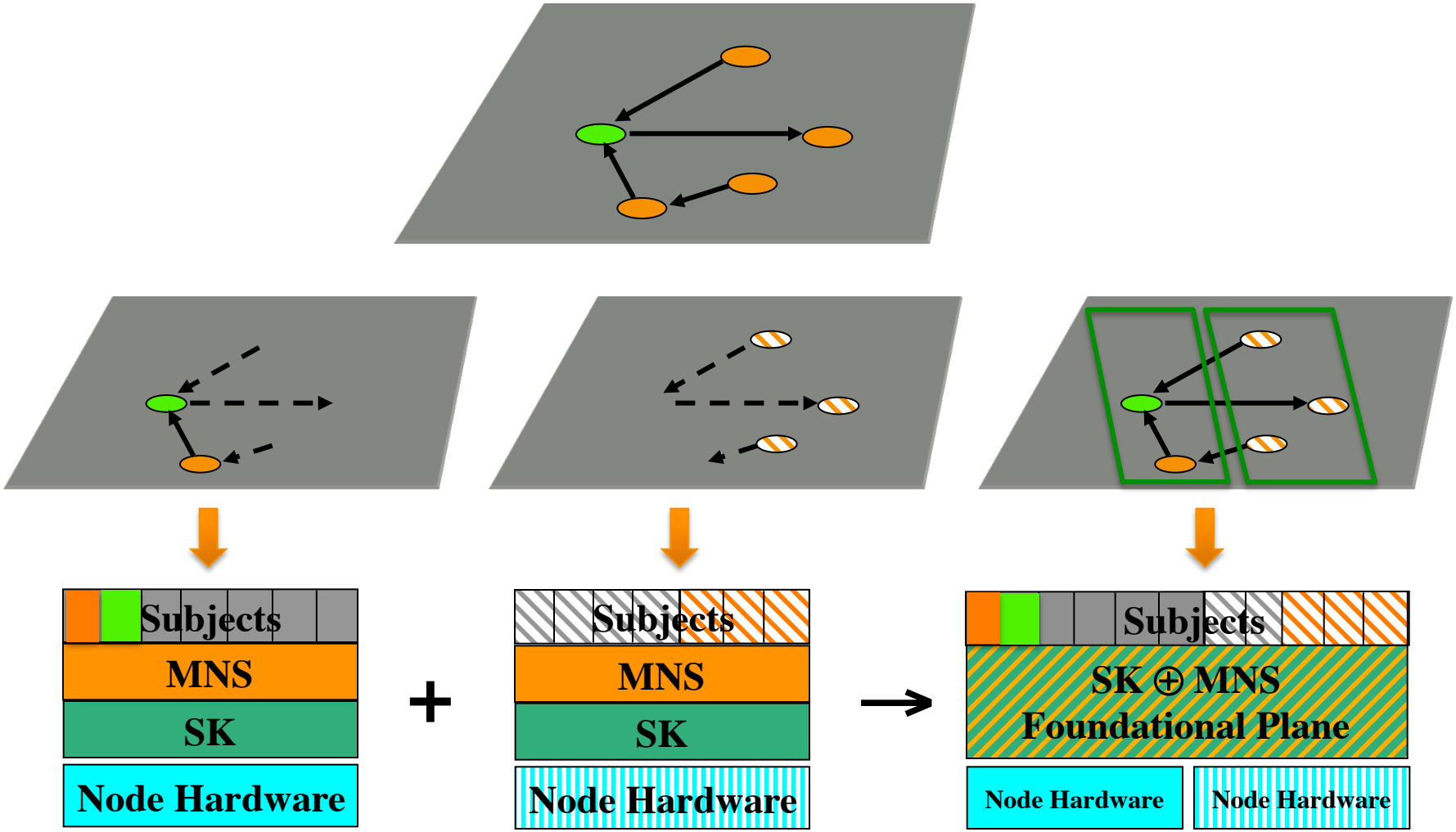
Implementation

SK, with other MILS foundational components, form the *MILS Platform* allowing operational components to share physical resources while enforcing Isolation and Information Flow Control

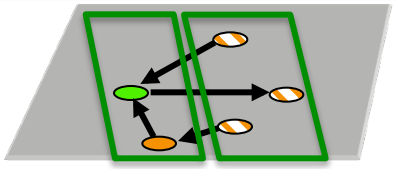
MILS Foundational, Operational, Monitoring, and Configuration Planes



Inspiration for Distributed MILS: Policy architecture deployment spanning nodes



Distributed MILS

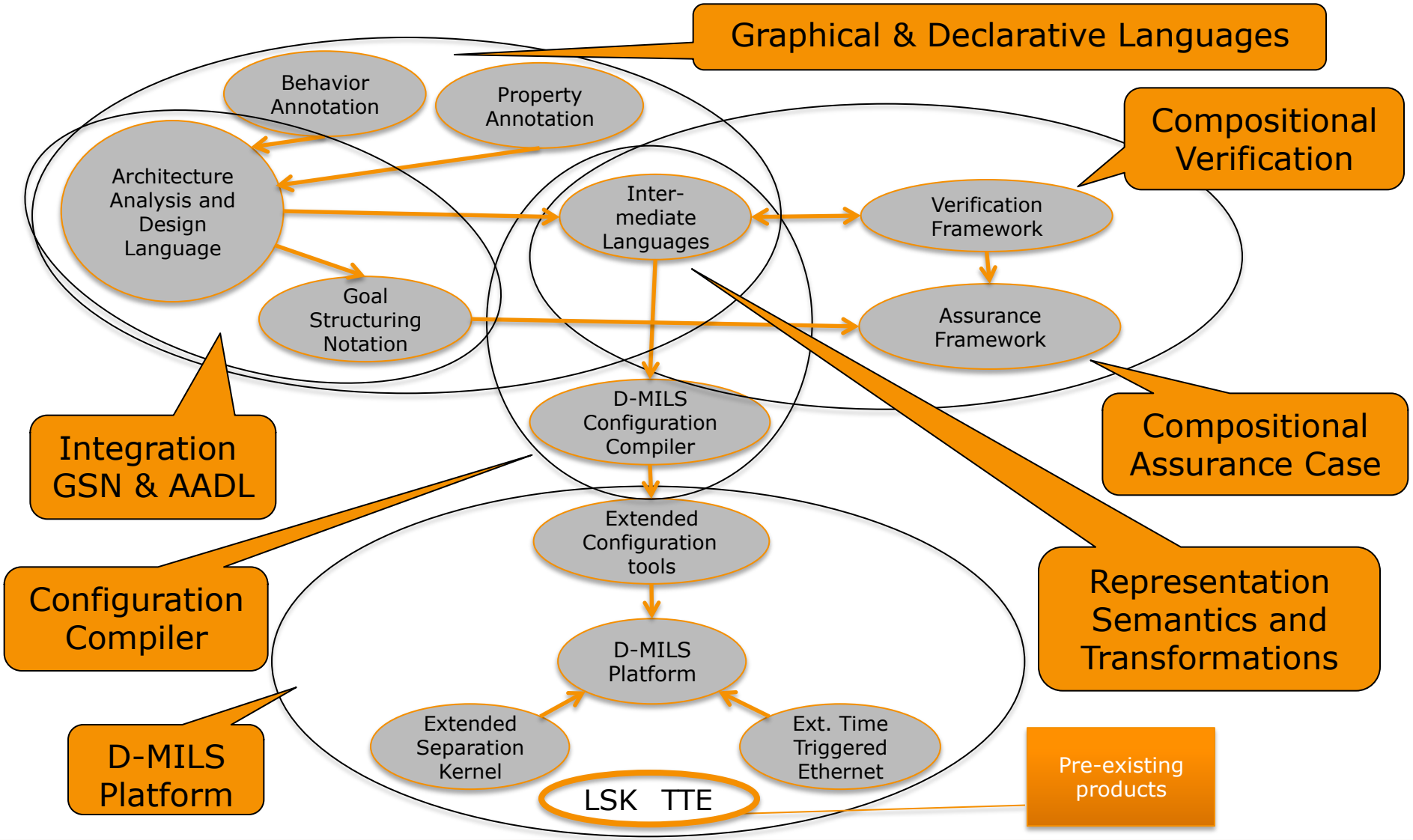


- A single policy architecture may span multiple D-MILS nodes expressed in declarative MILS-AADL
- Guarantees similar to a single MILS node: isolation, information flow control, determinism
- Determinism over network could be achieved in various ways – in D-MILS we use Time-Triggered Ethernet (TTE)
- Must configure and schedule the network and the processors of the nodes coherently
- Support verification of architectural properties, presentation of assurance case, and generation of configuration with integrated automation with the greatest practical use of existing verification technology

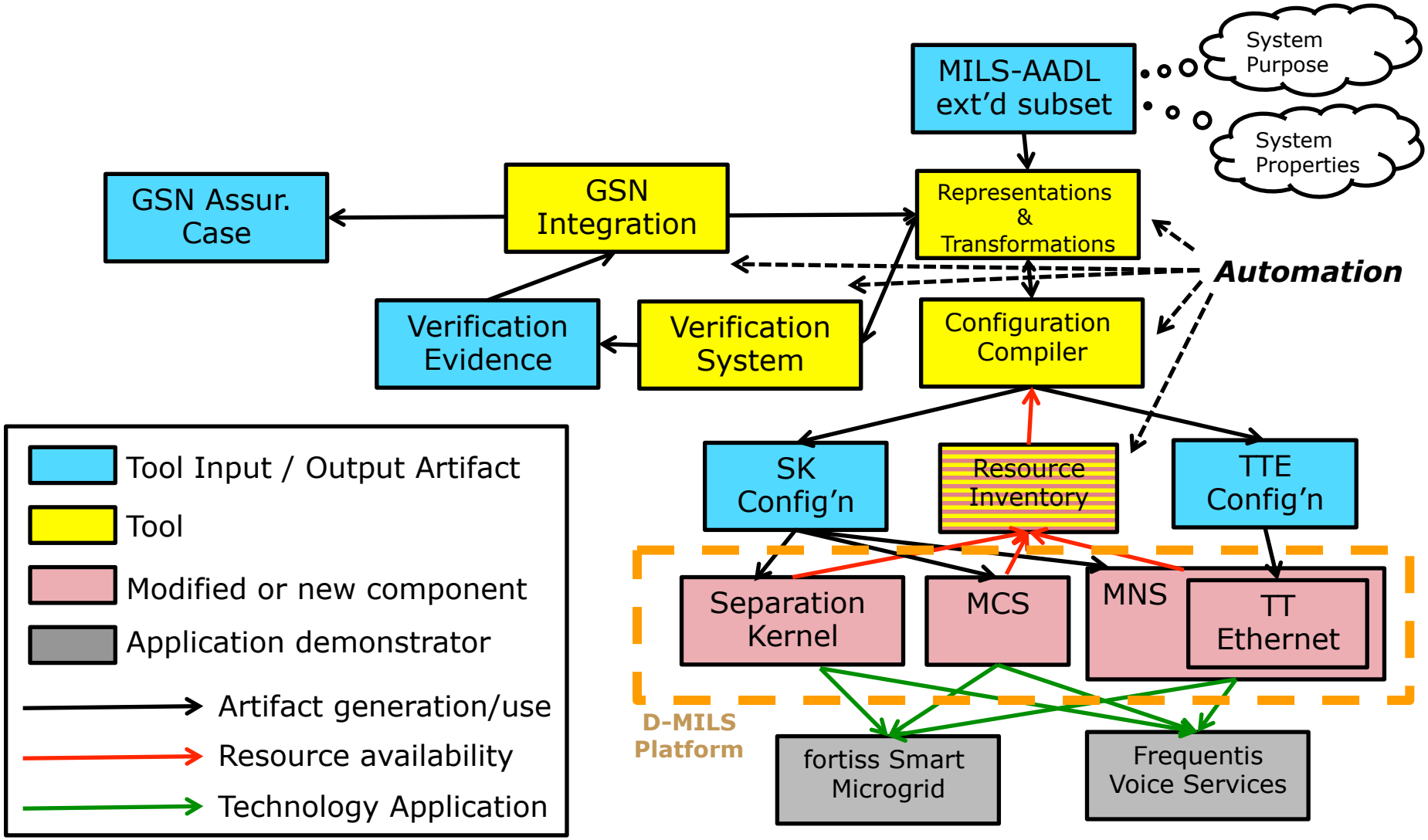
D-MILS Technology and Application Areas

- Graphical and Declarative Languages (front-end)
  - Architecture Analysis and Design Language, MILS extended subset (MILS-AADL)
  - Goal Structuring Notation (GSN)
- Integration of GSN and MILS-AADL
  - Structure of GSN assurance case informed by information gleaned from MILS-AADL model
- Representation Semantics and Transformations
  - Semantics preserving transformation between front-end languages and intermediate and back-end languages of the analysis tools
- Compositional Verification
  - Reduce verification of system to independent verification of its parts
  - Properties to verify and appropriate verification strategies and tools
- Compositional Assurance Cases
  - Modular GSN - Rely / guarantee argumentation
- Configuration Compiler
  - Generate configuration information for D-MILS nodes and connecting TT network infrastructure
  - Configuration constrained by actual physical resources available and other semantic analyses
- D-MILS Platform
  - TTEthernet – Distributed MILS network drivers and configuration
  - LynxSecure separation kernel with MILS Networking Subsystem (MNS)
- D-MILS Industrial Demonstrators
  - Smart Micro Grid – fortiss
  - Voice Services – Frequentis

D-MILS Technology Areas

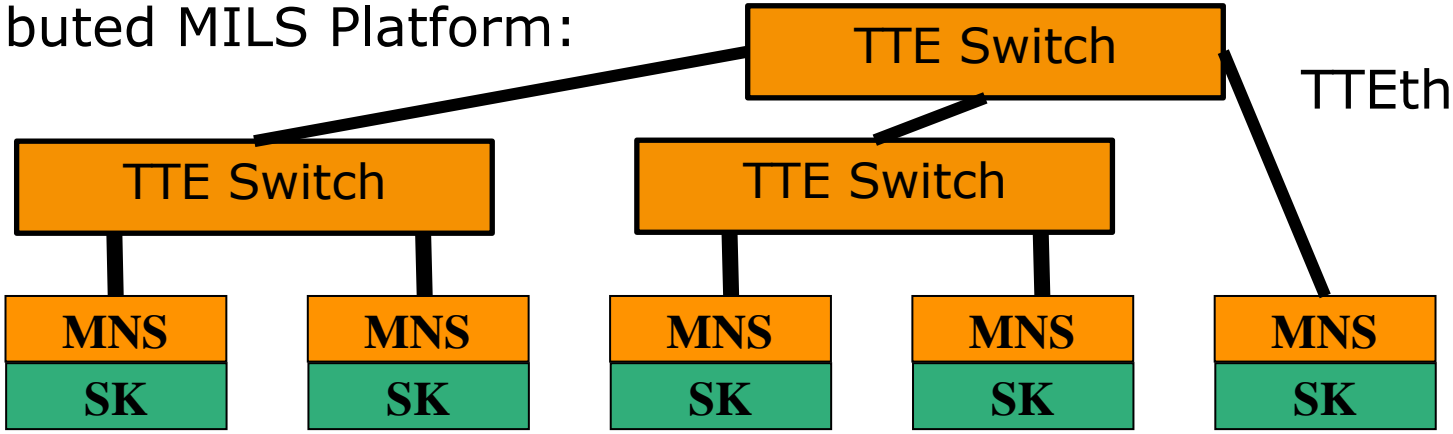


Distributed MILS Technology Elements

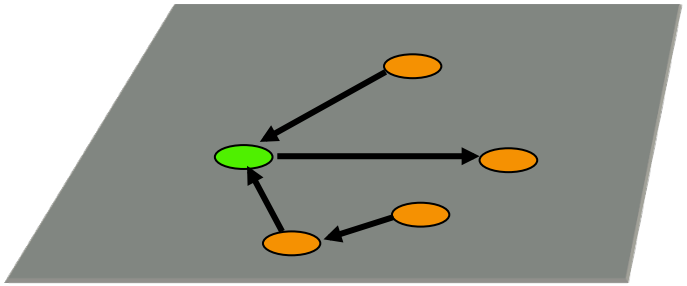


Distributed MILS Platform – MILS nodes with deterministic communication

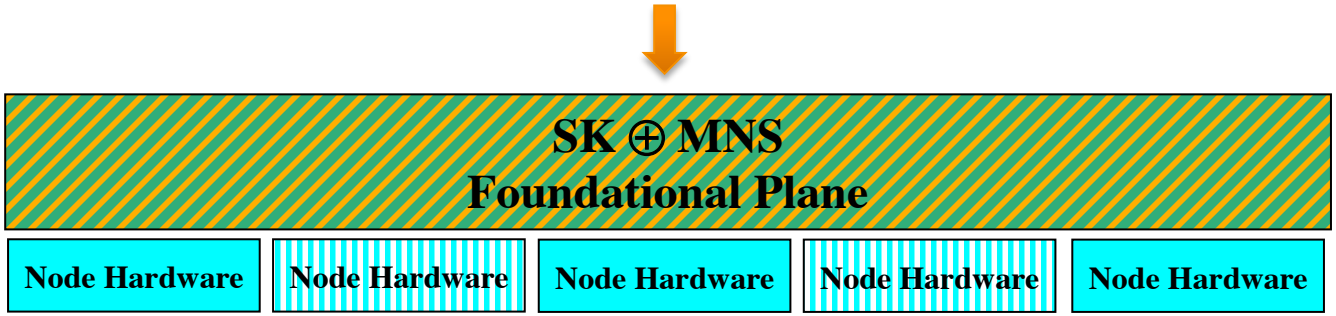
A Distributed MILS Platform:



Enables:

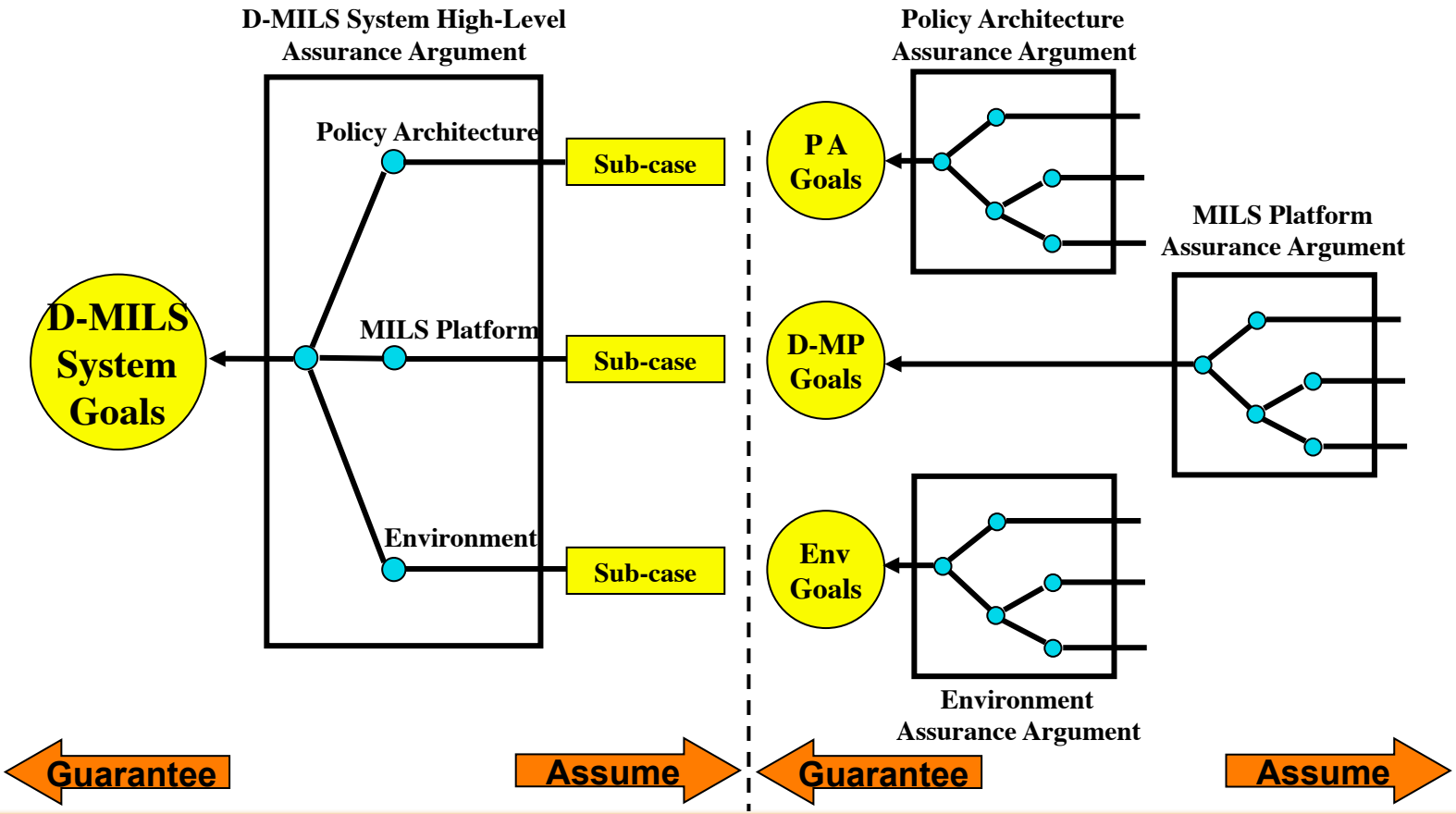


Realization of deterministic distributed MILS architectures



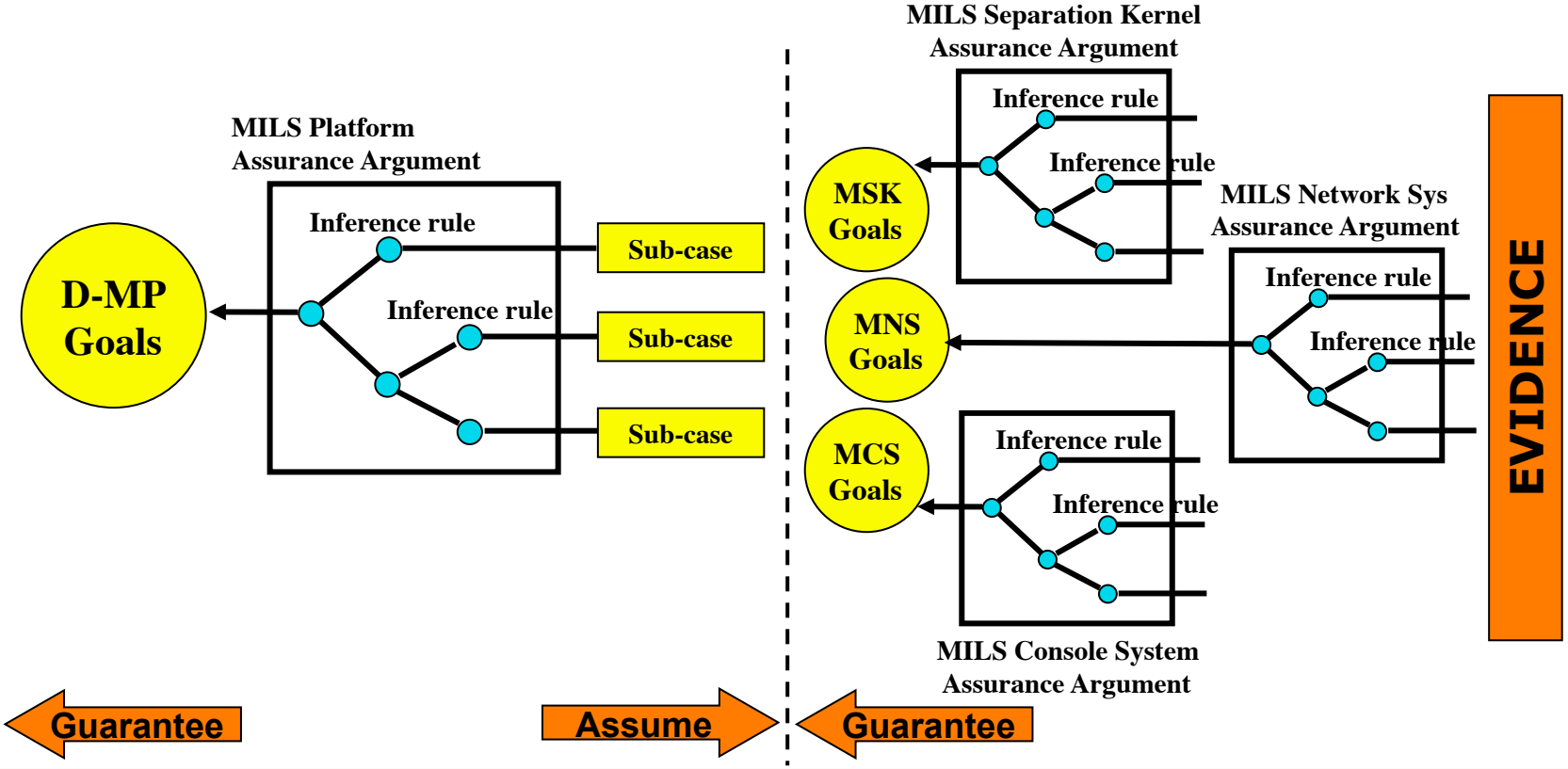
D-MILS System Assurance Case Structure

- Compose assurance cases modularly using Assume-Guarantee Reasoning
- D-MILS System assurance requires the validity of three sub-cases
- Assumptions from D-MILS System assurance case become obligations on the sub-cases

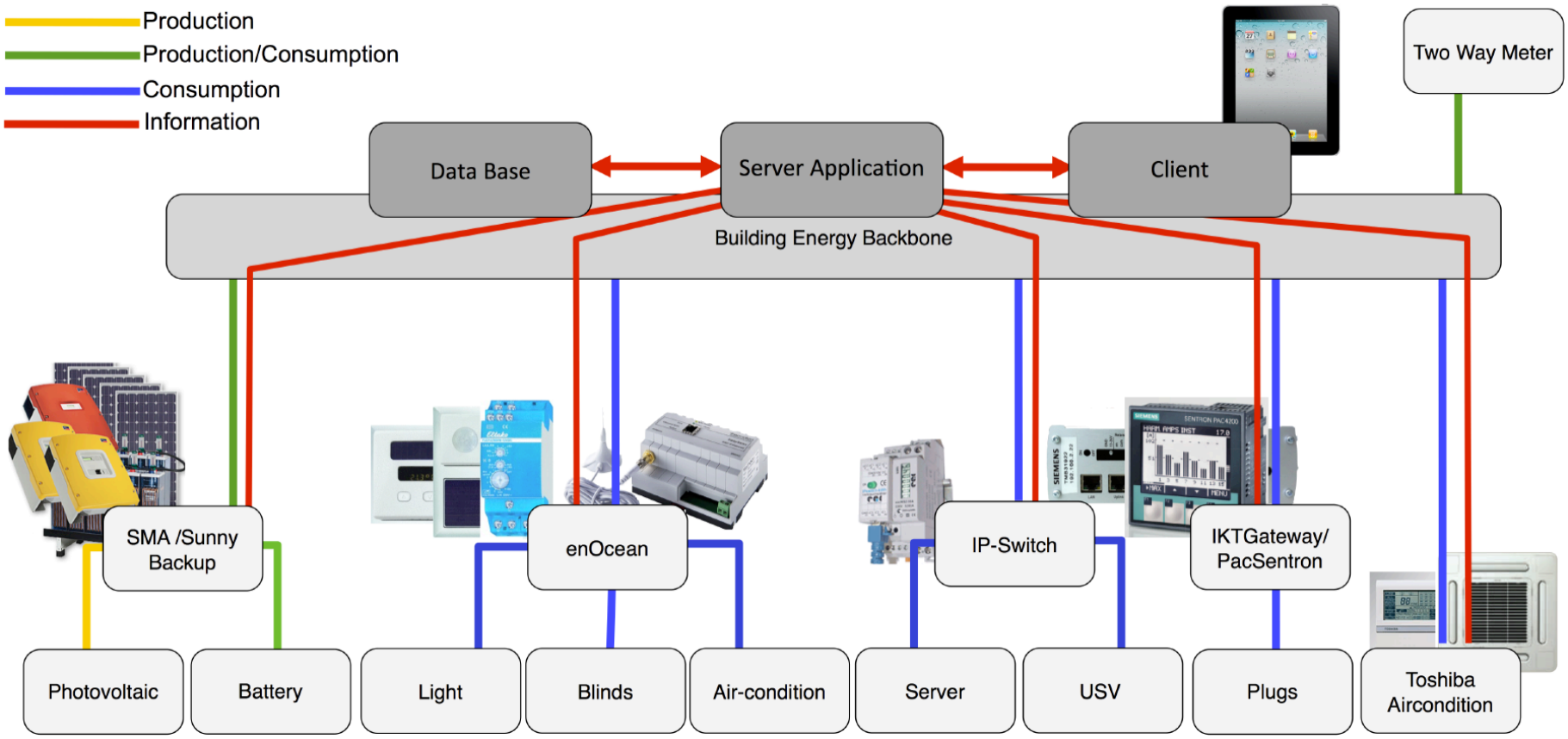


MILS Platform Assurance Case Structure

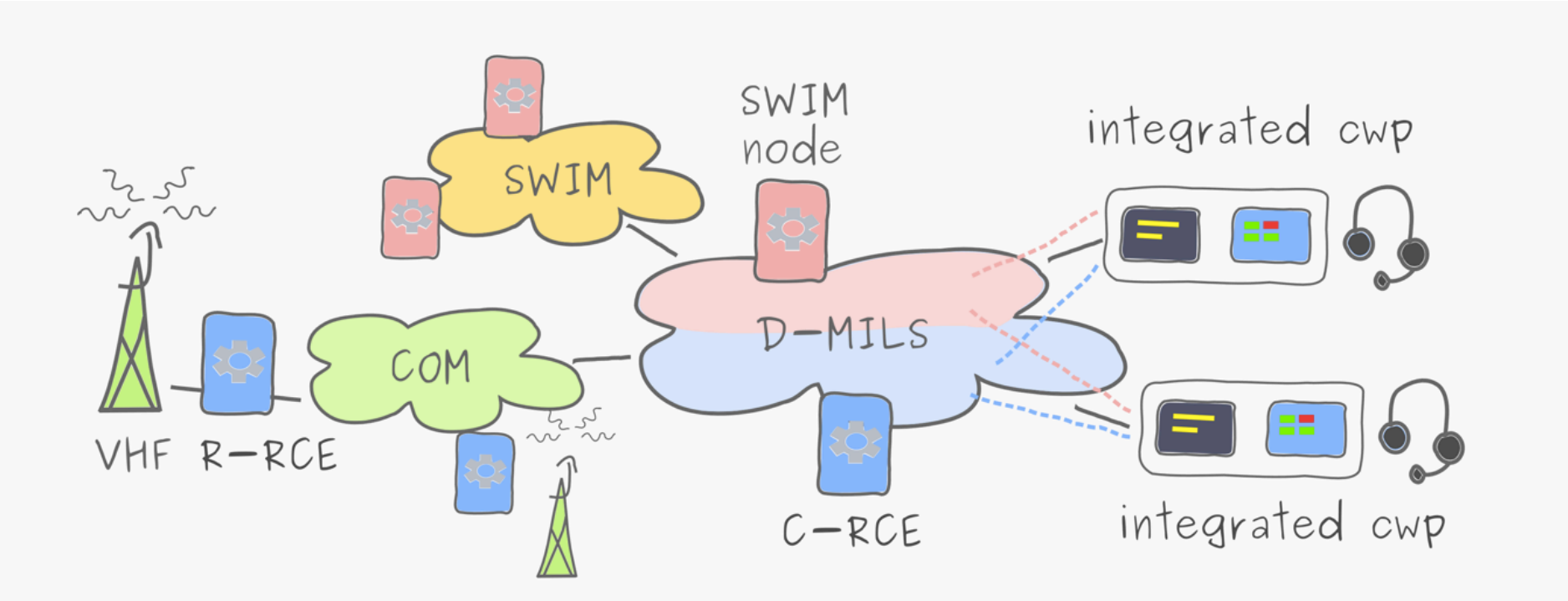
- The D-MILS Platform is composed of three major subsystems: MSK, MNS, MCS
- Assumptions from D-MILS Platform assurance case become goals for the components
- Assured Goals from component assurance cases become evidence for D-MILS Platform sub-cases
- Ground evidence provides the ultimate justification for the assurance case



Demonstrator: fortiss Smart Microgrid



Demonstrator: Frequentis Voice Services



cwp... controller working position
rce...radio control equipment
r-rce...remote rce
c-rce...center rce
swim...system wide information management