

EMC² - Arrowhead synergies

Prof. Jerker Delsing
Luleå University of Technology

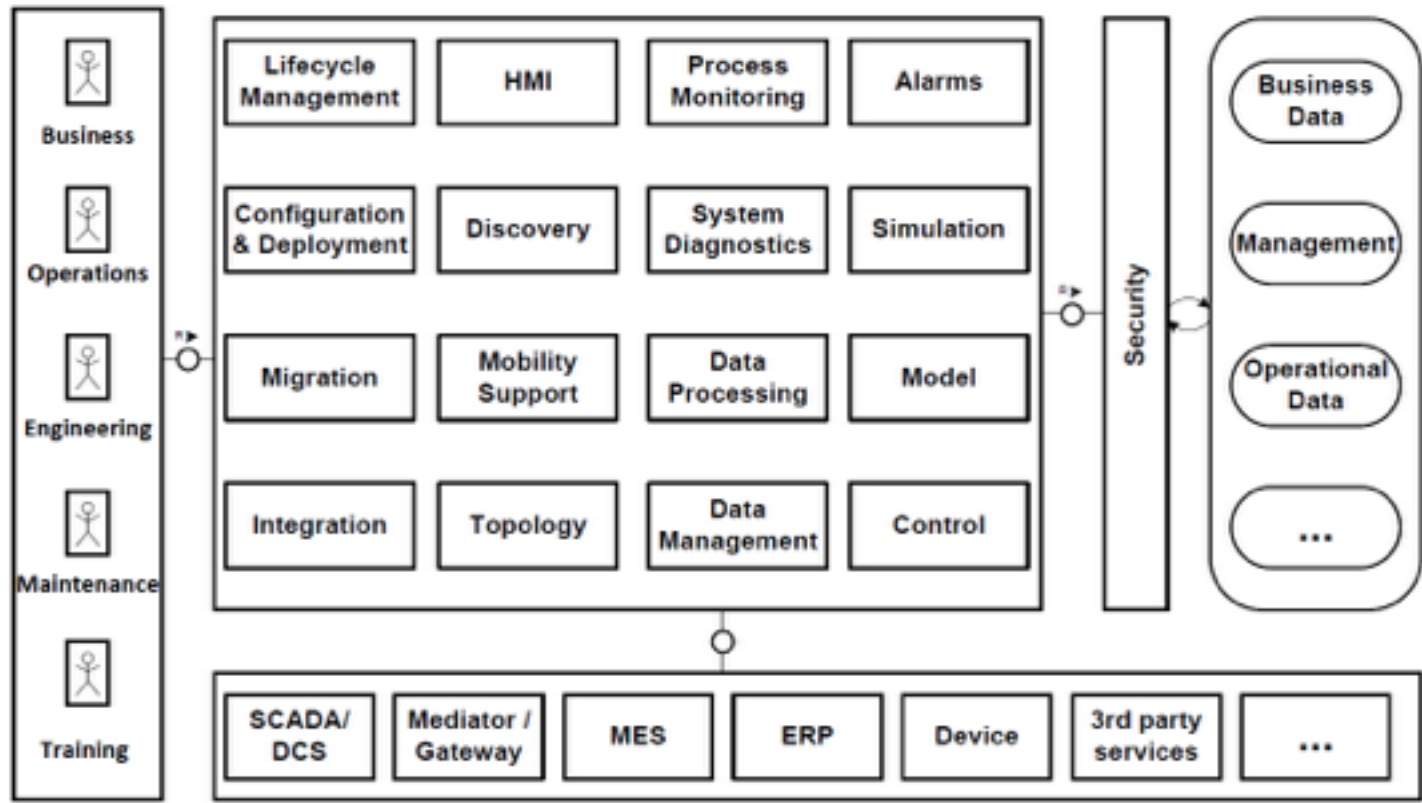


- Service interface architecture for multi-critical applications executed on Multicore processors
 - Realtime
 - Security
 - Safety and Fault tolerant



IMC-AESOP Architecture

IMC-AESOP: Architecture for Service-Oriented Process - Monitoring and Control
Seventh Framework Programme (FP7) Theme ICT - Information and Communication Technologies
Grant agreement no. 256662 | Project Co-ordinator: Armando Walter Colombo | Schneider Electric Automation GmbH





EMC2 requirements



- Service access control
- Service discovery
- Service deployment
- Service composition
- Data aggregator (energy usage com. eff.)
- Resource monitoring
- Disjoining processing units
- Admission control
- Security of reconfiguration
- Process and resource synchronisation
- Intra MPC communication
- Deterministic communication
- Monitoring service
- Gateway service
- Secure boot and update
- Attest of boot and deployment
- Power attacks
- Data encryption
- Encrypted service deployment
- Multiple security domains
- Interference detection
- Memory protection
- Task/service identification
- Resource identification
- Error reporting
- Service encapsulation
- Service artefact id
- Service configuration
- HW and OS adaptability



EMC2 spec. mapping to Arrowhead Framework












- Service access control
 - Service discovery
 - Service deployment
 - Service composition
 - Data aggregator
 - Resource monitoring
 - Disjoining processing units
 - Admission control
 - Security of reconfiguration
 - Process&resource synch
 - Intra MPC communication
 - Deterministic com.
 - Monitoring service
 - Gateway service
- ▶ Authorisation service,
 - ▶ Service registry&discovery
 - ▶ Service Deployment
 - ▶ Orchestration
 - ▶ Meta service registry
 - ▶ ?
 - ▶ ?
 - ▶ Authentication service
 - ▶ Authentication service
 - ▶ ?
 - ▶ HW or Service
 - ▶ ?
 - ▶ Monitoring service-proposed
 - ▶ Arrowhead Framework



EMC2 spec. mapping to Arrowhead Framework



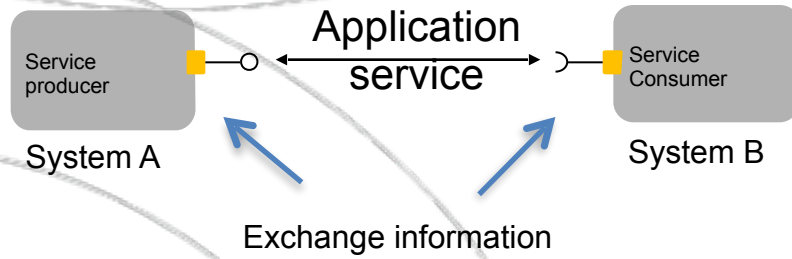
- Secure boot and update  ?
- Attest of boot and deploy.  ?
- Power attacks  ?
- Data encryption  Specified by SOA, CP
- Encrypted service deploy  Deployment authorisation
- Multiple security domains  Authorisation services
- Interference detection  ?
- Memory protection  ?
- Task/service identification  Service registry/discovery
- Resource identification  User system reposi./service
- Error reporting  Event handler system
- Service encapsulation  ?
- Service artefact id  Service registry/discovery
- Service configuration  Config, Orch, Depl System
- HW and OS adaptability  Arrowhead Framework



- SOA technology a brief introduction
 - Material from Arrowhead project

SOA

Services are produced
Services are consumed



SOA Key properties

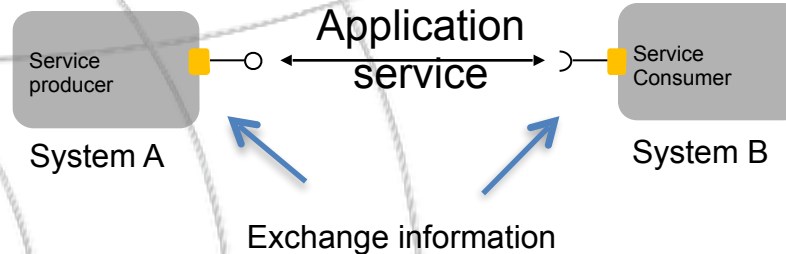
- **Loosely coupled**
 - Autonomy
 - Distributed
 - Owner is responsible and owns the information and decide whom to share to
- **Late binding**
 - Possible to use information anytime by connect to the correct resource at a given time
- **Lookup**
 - Publish and register for notify others about endpoint (how to reach me)
 - Discover others that I comply to (expected/wanted Service Type)

Fundamental approaches in Arrowhead

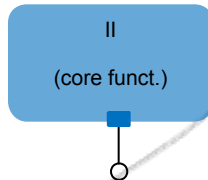
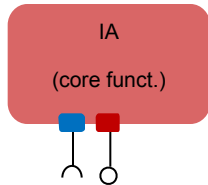
- Information centric
- Information assurance at service exchange level
- Publish subscribe approach -
- Push approach - Pull possible
- Minimal set of mandatory services in a System of Systems

Mandatory services to enable a service exchange

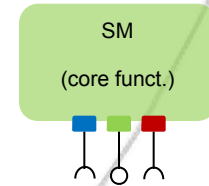
- How to set presence (existence) of the Service in the Framework?
- How to discover Services?
- How to decide which consumer has access right in security level?
- How to control which service instances shall exchange information?



Core services



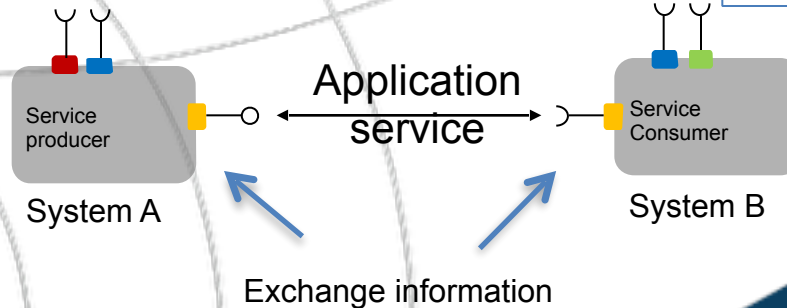
Core Services



IA: (The Information Assurance) core system providing support for secure information exchange. The IA provides authorization, authentication, certificate distribution, security logging and service intrusion functionality

II : (The Information Infrastructure) is the core system mainly in charge of providing support for service registry and service discovery. It also addresses orchestration, software distribution and application control

SM : The System Management (SM) is the core system providing support for Late binding and solving system of system composition. The SM provides logging, monitoring and status functionality. It also addresses network QoS and performance, configuration and policy



Core Arrowhead Framework Service

IA, Information Assurance services

- Authorisation Control
- Authorisation Management
- User and System Registry
- Deployment Authentication

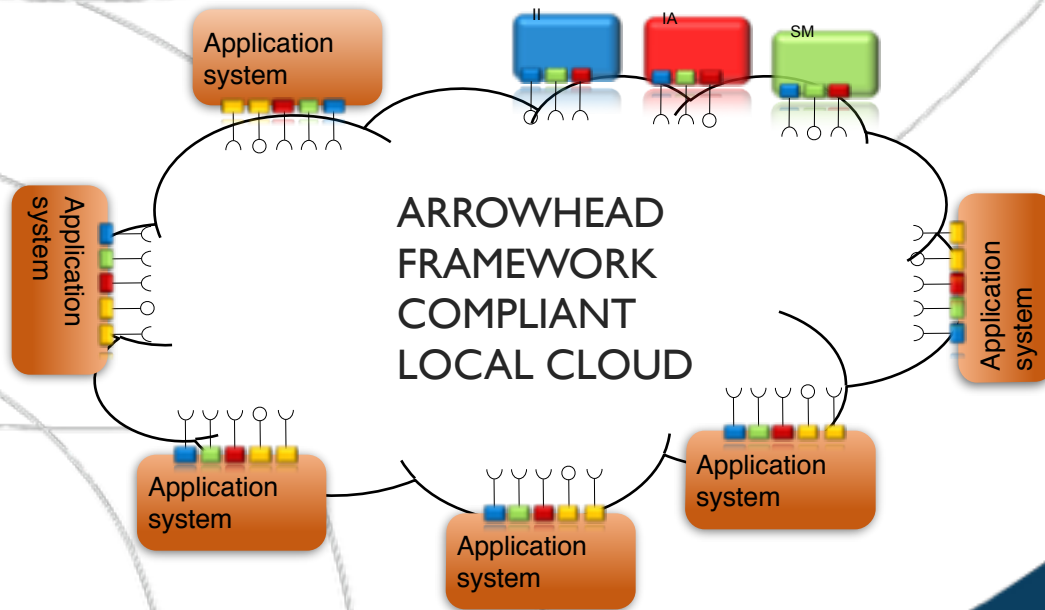
SM, System Management services

- Orchestration
- Orchestration Store
- Orchestration Management
- Meta Service Registry

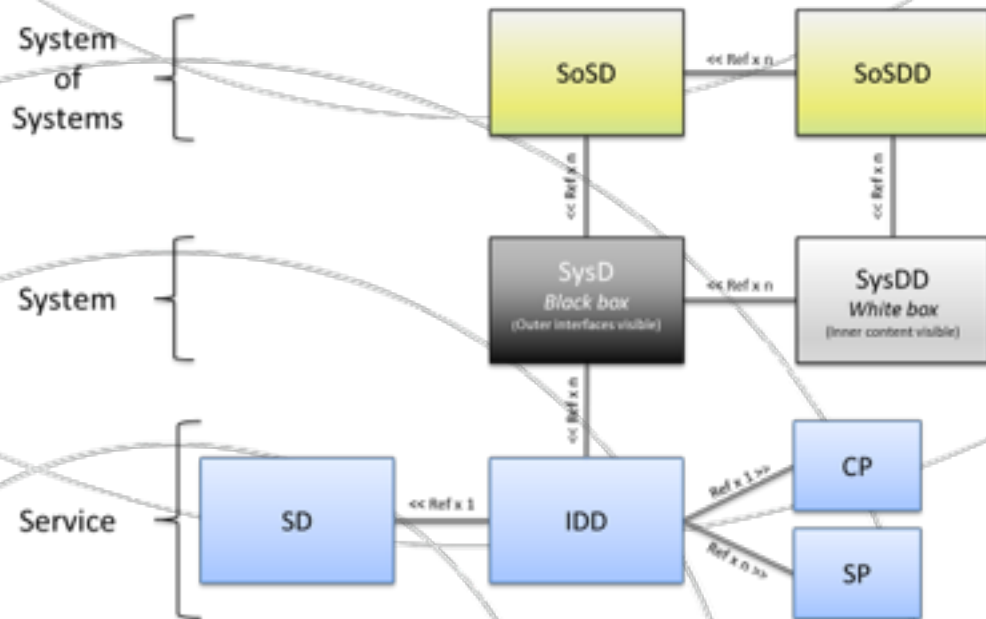
II, Information Infrastructure service

- Service Registry
- User System Repository
- Service Discovery
- Event Handler
- Deployment System

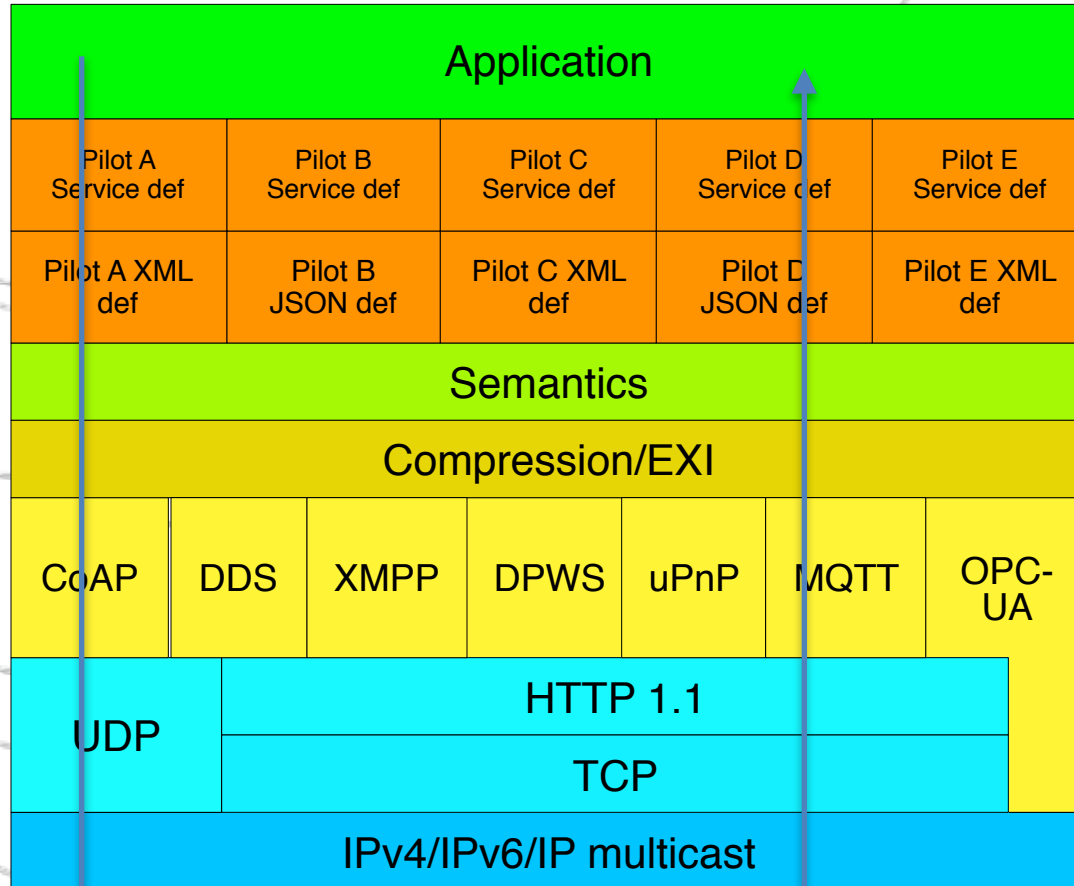
Arrowhead Framework



Documentation structure



SoSD: System-of-Systems Description
 SoSDD: System of Systems Design Description
 SysD: System Description
 SysDD: System Design Description
 SD: Service Description
 IDD: Interface Design Description
 CP: Communication Profile
 SP: Semantic Profile

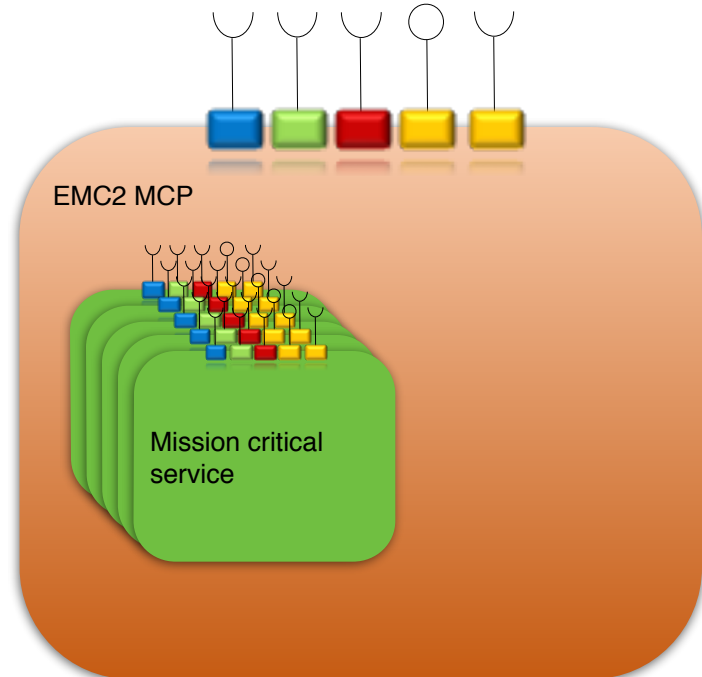
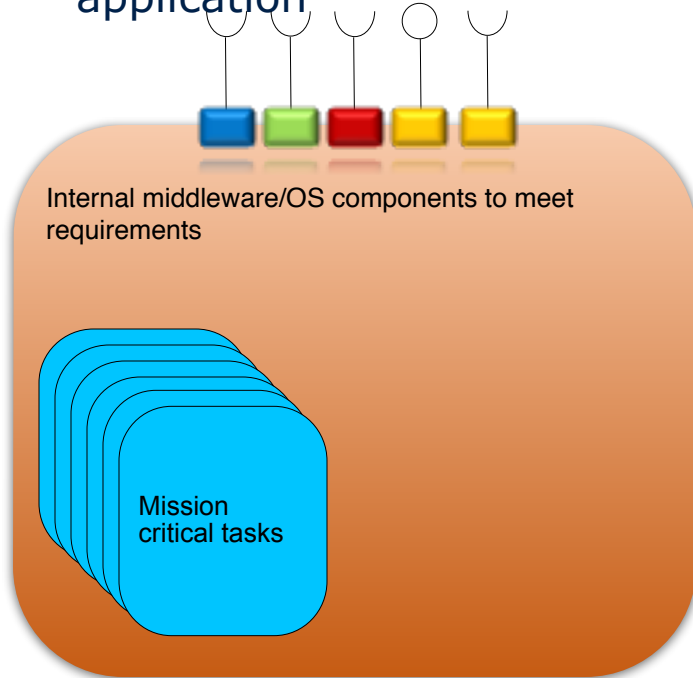




EMC² architectural aspects



- Two possible principles
 - EMC2 service paradigm between any service executed on a single MCP, **a cloud on a chip**.
 - EMC2 services only as a shell to an MCP running multiple application





Conclusion



- Arrowhead results exploited in the EMC2 project
- Still a number of open questions on
 - Real time
 - Security
 - Safety and fault tolerant
- EMC2 service interface architecture by 2017