A Model-based Architecture for Tactical Systems of Systems Management

Régis Dumond

DGA
7-9 allée des Mathurins
92221 Bagneux CEDEX FRANCE

regis.dumond@dga.defense.gouv.fr

**Nicolas Farcet,
Marc Slimani, Jean-Luc Garnier,
Marie Ludwig, Maurice Israel**

THALES LAND & JOINT SYSTEMS
146, boulevard de Valmy
92704 Colombes CEDEX FRANCE

nicolas.farcet@fr.thalesgroup.com

ABSTRACT

This paper presents an architectural approach to manage systems of systems. This approach leverages models at various steps in the lifecycle of the system of systems, especially during planning and operation.

1 INTRODUCTION

1.1 Foreword

Knowing the current and forecasted state of a Systems of Systems (SoS) within its global operational and technical context, there is a need for functionalities that makes possible to undertake corrective and preventive actions at any of the levels in order to keep it running for the success of the operation objectives. These functionalities are referred to as Systems of Systems Management (SOSM), also called System Management (SM) in the remaining of this document.

When a System providing a capability fails:

- The SM allows getting the same capability from another system.
- Or if this system is not available anymore, the SM can insert in the SoS a new system supporting this same capability.
- Or if the capability cannot be maintained or obtained from the available systems, the SM reconfigures the failing SoS towards a degraded mode.

Additionally, the SM allows transforming the internal SoS organisation in terms of people, services and platforms to fit mission evolutions.

The implementation of the SM relies on a mesh of Autonomic Management Units (AMUs). Each AMU leverages a knowledge base to carry out management tasks such as supervision over the AMU responsibility area, handling system failures, reconfiguring resources based on new threats or commander intent updates, and collaborating with other AMUs for resource sharing. The AMU knowledge base comprises the current state and topology of the SoS and the Policies to be applied depending on operational and technical events.

The promoted solution is to implement the knowledge base with formal models. Models are produced at design time and modified during the rest of SoS lifecycle (planning, operations). They are embedded within the SoS, and used during operations. When a new system is to be dynamically added –as in a plug & fight approach–, an operator can drag and drop the system definition into the SoS Model and accordingly insert the new system into the SoS organisation. The model-based environment enables the validation of the addition with respect to the management policies (safety, security, etc.) before deciding to apply it onto the real SoS. Upon application, AMU generates all technical information required to reconfigure the resources impacted by this addition.

This paper presents the state of our reflection and the status of our prototyping activities.

1.2 SoS definition and characterization

A System of Systems (SoS) as defined by Mark W. Maier [1] presents five main features: (1) Operational Independence of the Elements: Each system composing the SoS can separately operate; (2) Managerial Independence of the Elements: Systems have an independent design and acquisition process; (3) Evolutionary Development: The SoS is dynamically formed, systems are added or removed; (4) Emergent Behaviour: The capabilities of the SoS are more than the sum of capabilities of the systems which compose it; (5) Geographic Distribution: The geographic extent means systems interactions are based on information and should rely on a Network.

Some issues can be drawn from these five points. From Maier's points (1) and (2), the SoS may be composed from heterogeneous systems with different design and technologies. These systems may have not been designed for a particular SoS, yet they are expected to collaborate; (3) The SoS must be set up by connecting up systems each other in a flexible manner. It can happen that systems are removed from or added to SoS during its operation; (4) A SoS brings emergent capabilities as well as undesirable behaviour which must be mastered; (5) The reliability of communication and interoperability are crucial points of SoS as capabilities are geographically distributed.

1.3 SoS dynamicity

To address these issues, dynamicity can be considered as a fundamental property of SoS, in particular for SoS composed of mobile platforms. Dynamicity is present in different aspects of the SoS: *when the SoS is set up* in an incremental way, connecting the systems then assembling the capabilities of systems; *during the planning* of a SoS where a platform can be replaced by another one with identical or similar capabilities; *during deployment and operations* where platforms may be added or removed; due to an occurring event the SoS organisation may require to change;

A SoS can acquire a part of this dynamicity with a design applying the Service-Oriented Architecture (SOA) pattern. "*In SOA, services are the mechanism by which needs and capabilities are brought together*", OASIS SOA Reference Model [2] says. The offered capabilities of systems are represented as services. These services can dynamically be discovered and connected, hence forming or modifying operational workflows during runtime. This approach does not require a complete rework of legacy systems. It has been proven that the legacy systems can be upgraded to exhibit services and make them available on a network. Here the SoS is related to the Net-Centric Operations (NCO) concept, where systems are connected to a network in order to make their capabilities or information available and visible to others. Hence a system may access via the network to the capability (represented by services) exposed by another system. This brings issues such as the right to use, the accessibility and the availability of services and more generally the relationships management across systems. In the context of SoS, these relationships are generally organized into consistent collaborations or Communities of Interest (COI).

The organisation of a SoS may vary even when composed of an identified set of systems. This

organisation may change during runtime due to events or new orientation of the mission. A SoS organisation can be of several types such as structured (hierarchical way: an aircraft carrier with its aircrafts and its escort) or unstructured (cooperative way: the worldwide Air Traffic Management with airline aircrafts and ground centres). These organisations such as COIs should match the human organisations gathered for the goal of a mission. COIs are groups of collaborating entities with a common mission interest and information needs. COIs are usually autonomous units inserted in a SoS organization combining hierarchical command and cross-COI interactions. In such an organization, a COI is a unit of subsidiarity set up with a goal, with specific operational capabilities built from collaborating members (i.e. entities and/or sub-COIs), with an initial allocation of information and communication channels to support these collaborations. COIs are set up in conjunction with the SoS. They can be permanent (during the whole mission or operation time of the SoS) or expedient (during a lapse of time, just for a particular task of the mission). The COIs may mix these different types: hierarchical or cooperative, and, expedient or permanent. A SoS may hosts several COIs.

A set of systems does not necessarily form a SoS. The SoS exists if it is possible to combine capabilities, which then translate into services workflow. The COIs are enabled by networking services and operators according to the expected capabilities and the roles supporting these capabilities.

Because of this organizational flexibility brought by SOA and COI paradigms, when the SoS is set up and running, it shall be monitored and controlled because it may dynamically evolve and the emergence of new capabilities could come along with undesired effects. The evolution of SoS therefore need to be closely managed during operations.

1.4 SoS description

This dynamicity requires a management of the SoS during its whole lifecycle from the manufactory to the theatre of operations. The starting point is the description of Systems in a formal and standardised way. This is the purpose of Architecture Description Frameworks such as DoDAF [3], MODAF [4] and others. This allows describing the systems in terms of interfaces, capabilities and offered services. The SoS is designed according to various modelling viewpoints such as the required capabilities, the expected emergent behaviours, or the operational workflows based on services. From this design activity, the SoS typology is defined. The SoS typology is the logical description of the SoS according to Operational, System, and Service architecture levels.

The SoS typology is instantiated during operations planning in a physical configuration suited for the operations. It is possible to prepare several configurations from one typology. Indeed, several Systems could enable identical capabilities but the resulting SoS may differ in terms of performance (size, power, speed, autonomy…). The result of this preparation activity is the identification of candidate SoS configurations. At the moment the Architecture Description Frameworks provide very limited support to describe SoS configurations. Moreover, these frameworks lack the formalism and precise semantics required for these configuration descriptions.

When a mission is planned and a SoS is to be set up, the suitable configurations are retrieved from the SoS Configurations and valued against the mission goal and desirable effects. The selected configurations become the SoS Nomenclature for the planned mission. At this point, the information in the SoS Nomenclature will allow setting up and then maintaining the SoS during the different phases of the mission. In particular, the proper configuration needs to be applied during a subset or the full SoS deployment. Moreover, depending on mission phases, other configurations from the Nomenclature might need to be applied in order to maintain and maximize SoS capabilities. As seen before, the SoS shall remain evolvable during operations. Therefore the SoS Nomenclature has to embed the multiple configurations needed for mission goals and coping for unexpected events during the operations.

2 MANAGEMENT OF SYSTEMS OF SYSTEMS

From the previous observations, we can draw that the is a need for managing configurations during the SoS lifecycle, in particular during operations where a SoS is set up and running. The idea is to provide a set of functionalities that retains, maximises, optimises and maintains the SoS capabilities while events may occur. These functionalities are referred to as Systems of Systems Management (SOSM), also called System Management (SM) in the remaining of this document. The Systems of Systems Management organization can be distributed on the systems of the SoS or can be centralised on one specific system. It can manage a system or a set of systems depending on the organisation which has been configured. It can manage the systems internally and across the SoS. The present paper focuses on SoS-wide management aspects, i.e. the management of systems interactions.

The expected capabilities of Systems of Systems Management are identified hereafter.

- At design-time, define a SoS Typology: A typology is a validated logical description of the SoS fitting a range of operational capabilities. The SoS typology comprises operational, system, and technical aspects.

- At plan-time, define a SoS Nomenclature: A SoS nomenclature comprises various SoS configurations prepared for the operations. Configurations describe instantiated SoS topologies with allocated resources. These SoS topologies are validated in terms of consistency, interoperability, safety, and security according to the SoS typology. Moreover, these SoS topologies are validated in terms of resource allocation, deployment, and parameterization.

- At deployment-time, sets up the proper SoS configuration by connecting the systems and configuring the resources according to the target SoS topology. During this phase, the SM performs the Networking of System Capabilities by connecting systems in a smooth sequence.

- Instantiates and controls transformations of the SoS topology: A SoS comprises a structured set of resources and capabilities whose organisation may change during the SoS Lifecycle (e.g. the SoS may host several COIs). The SM sets up and controls dependencies within and between the COIs.

- Maintain the SoS in a known and valid state with respect to policies in terms of consistency and interoperability, safety, security, health, performance, resource optimization, and requested operational capabilities. This validation is done in real-time by actively checking the SoS state against the expected SoS configuration. On the reverse way, the SoS state is being actively controlled so as to remain within the expected configuration.

- Contributes to the interoperability within a SoS: A SoS is composed of heterogeneous Systems with different Acquisition process. The SM provides an overall configuration management of the SoS during the runtime. Hence it can control whether a system is connectable or not.

- Provides the situational awareness with information about system and operational capabilities, in particular concerning availability, safety, security, health, performance, and resource optimization within the SoS. Depending on the C2 level, the SoS might need to be managed as a whole. Therefore the SM compiles the status of all levels of management and pictures an overall status of the SoS capabilities.

- Enables sharing of Capabilities across platforms: A participant in a NCO may use a system or operational capability which is not provided by its own platform or COI. Moreover, the SM supports change of management responsibility, such as horizontal delegation and subsidiarity (i.e. delegation along the command chain) for resources and system capabilities. Therefore, SM can be seen as the

enabler of a more flexible C2 architecture.

- Provides a forecast of system and operational capabilities availability: The SoS needs a means to anticipate unavailability of Systems and their replacement. E.g., the SM monitors the energy and ammunition consumption of Systems as well as their warning thresholds and checks these measurements against the expectations along the plan of operations. This implies that SM needs to embed some knowledge about the plan of operation.

- Provides C2 operator with Supervision and Reconfiguration means to support command and control of the System operations at various levels of SoS organization. The SM Supervision and Reconfiguration may be operated according to three modes: Automatic (system self-management with no human interaction), Decision Support (human-based system management helped by the SM: analysis indicators, policy checks, selected configuration candidates, etc.) and Manual (human-based).

The aforementioned capabilities bring two major yet contradictory properties for a SoS: resilience and adaptability. Knowing the current and forecasted state of the SoS, it is possible to undertake corrective and preventive actions in order to keep it running flawlessly and contributing optimally to the operational capabilities. When a System providing a capability fails, the SM allows getting the same capability from another system. Or if this capability is not available anymore, the SM can insert in the SoS a new system providing this capability. And additionally; the SM allows transforming the internal organisation of the SoS to fit mission changes in terms of people, services and systems. By gathering all the information of the SoS in a shared and continually updated model, the SM also enables a total knowledge and control of the SoS architecture, and thus of the information flows that are set between the Systems.

The System Management does not only concern the operations time but the whole lifecycle of the SoS. It starts at design time when the SM functions are defined and implemented and the System is made able to be inserted in a SoS. The information that defines this system must be recorded in a repository. This is the start of the SM. Then before operations, the SM can support the rehearsal. As the SM contains the SoS description, it could be included in the simulation activity in order to check the SoS behaviour with respect to Mission events. After the operations, the SM can provide a log describing all SM actions for logistics. Hence the SM bridges the logistics activity with the operation time. Additionally this log can be used for replaying the mission. The activity of SM can take place in any time of the SoS lifecycle. This allows to get the SM during operation and to enhance logistics activity during and after operation.

At this point, two actors come up: (1) The system manager who leverages system resources and controls system state in order to retain, maximise, optimise and maintain the overall system capabilities; (2) The system user who leverages system capabilities in order to achieve an operational task during a Mission. The separation between these two roles is difficult. There is not a clean break between the System Management and Mission Management. The failure of a System may impact the mission progress. The adding of a new system is a decision of the Mission Management. The System Management needs to know the decisions of the Mission Management when it impacts the SoS composition. The Mission Management needs from the System Management information describing the current or forecast state of the SoS. Moreover, as the System Management provides or forecasts availability status of system capabilities, it should value the current state of a capability against the Mission progress. If it remains only 10 litres of gasoline at 10 kilometres before the destination, the capability of mobility is okay. However if the vehicle is at 100 kilometres before the destination, the capability is down and the logistics should be notified. The SM is the assessment of the capabilities of the SoS with respect to the current state and future tasks.

2.1 SoS Lifecycle considerations & evaluation

The SM activities must be considered through the whole lifecycle of the SoS:

- During the architecture description and the concept development & experimentation:
    - Static and dynamic architecture evaluation.
- During these phases the system behaviour is analysed, including its management. In particular, the fully operational modes and graceful degraded modes are defined.
- The operational behaviour is evaluated on scenarios in order to assess:
    - The relevance against the doctrines and the organisations.
    - The ad-equation regarding the situation, and the effects to be provided.
    - The feasibility of the capabilities considering the constraints (cost, schedule, safety, security, ergonomics, etc).
- During the system experimentation, the management model is validated on the different configurations and the specifications of activities are tested. The requests and complaints, coming from the users and operators, are taken into account to evolve the system through the modification of its constitution, its operating modes, and the management policy.
- During the operation planning, the command and the management operators use the experimentation data to configure the system in order to face the real situation and to achieve the expected effects. The planning phase and the associated management operations are based on libraries of validated use cases and decision aid algorithms in order to estimate the operational activity during its definition.
- During the execution phase, the services of operational activity survey and collection of requests/complaints allow tuning of the resources and the system behaviour according to the contracts of services.

2.2 Autonomy within the System Management Organization

To ensure the best added-value and minimize the interferences of the SM during the operations, the SM processes and organization need to be aligned with those of the Command and Control. A comprehensive study of Command and Control structures and processes for NCO has been done by Jay Bayne (e.g. in [8]).

Our assumption is that SM activities should be organized as a mesh of Autonomic Management Units (AMU). An AMU represents a management capability, acting in support to a C2 capability, able to operate on its area of responsibility, even if parts of the rest of the SoS has become unreachable or damaged.

On its management responsibility area, the AMU operates according to short (i.e. automatic) and long loops (i.e. with human decision involved).

An AMU has hierarchical relationships in the SoS organization:

- Commander intent comes as input to the AMU with associated resources and management

policies

- Reports and supervision synthesis are provided as output

The AMU also has collaborative relationships with other AMU in different command chains. These collaborations can be freely set up (within the boundaries of common management policies) between AMU for e.g. to organize resource sharing during operations.

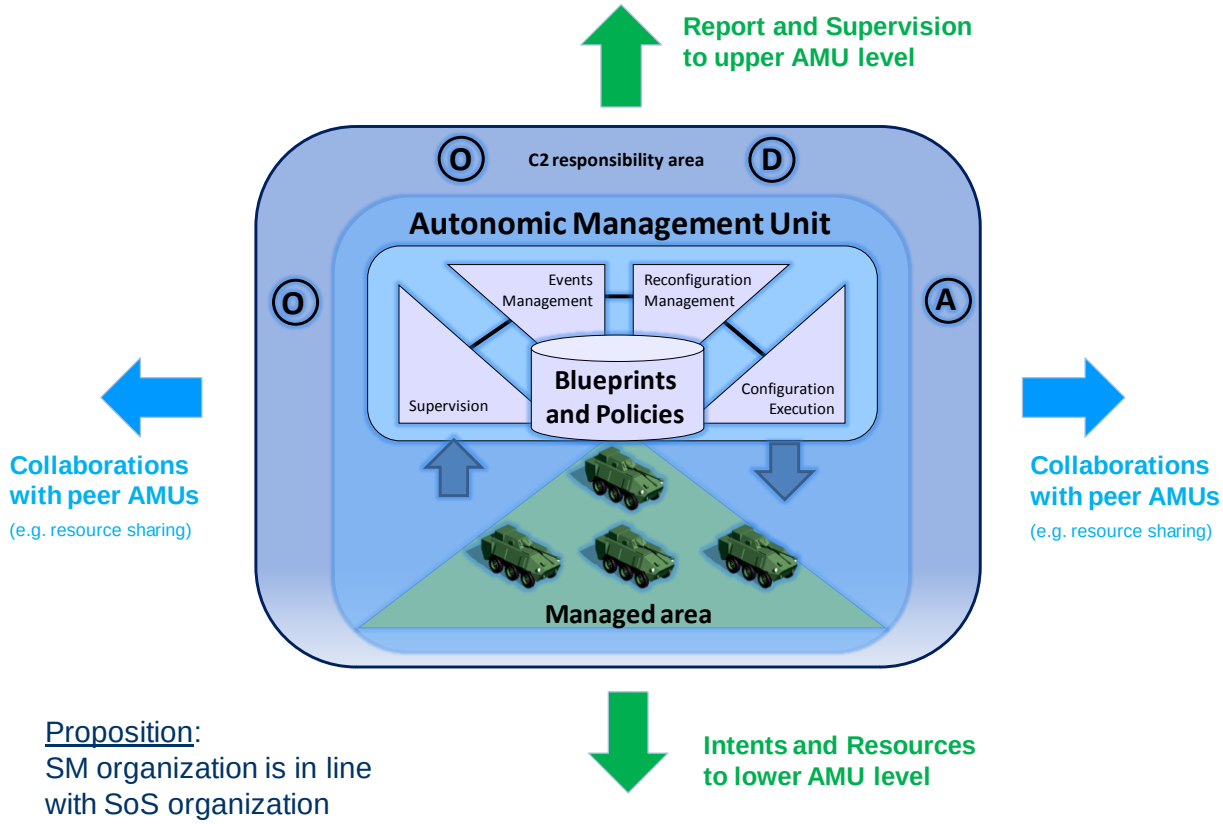

Figure 1 : Autonomic Management Unit (AMU)

2.3 Staff cells and System Management

The SM is a means for enhancing the efficiency and effectiveness of the current activities in a staff. The identified support to these staff activities is from a focus on the state of availability of system:

- (2) Intelligence: The SM provides the availability state of capabilities of ISR sensors as well as their current task and position. This allows immediately assessing a request according to the current situational awareness. This improves the tempo of action. A new tasking can be elaborated if needed. If the request corresponds to a current task, the ISR sensor will provide the requester with the information at the end of task.

- (3) Operations: The availability state of capabilities of systems can be coupled with other information in order to produce a situational awareness. A candidate application is the Blue Force Tracking (BFT). By combining SM (capabilities of systems) and BFT (position of systems), it is got a comprehensive own situation report.

- (4) Logistics: While the operations are interested in the availability state of capabilities, the logistics focuses on the technical nature of unavailability (component failure, gas, etc.) as well as the forecast of failure.

- (5) Planning: Planning activity relies on the current and forecasted state of systems. The planning can elaborate the future manoeuvre on the basis of information from operations (what are the systems currently doing?) and from logistics (when will the systems be made available?)

- (6) Communications: All systems connected to the network can notify the Communications with its state. The SM allows monitoring the current state of the network and the healthiness of systems connections.

All these staff cells are networked from the line of contact to the Headquarter. At each level of the hierarchy information are aggregated, then sent to the upper level. And at each level (brigades, divisions, etc.) the staff functions are present. It means several operators supervise the SM with different points of view at different levels.

While at upper levels, operators interest is the state of availability of systems, at lower levels the operators leverage on the capability of configuration and reconfiguration of systems in order to retain the operational capabilities of the systems and the SoS. The supervision of a SoS on the line of contact concentrates all information at operational, system and technical levels regarding the state of systems and SoS. After, this information is split and is of different nature when it is sent out to the different cells. For instance, the information at operational level concerns the operations cell, while those at technical level concern the logistics cell.

2.4 Organization of Autonomic Management Units

The SM Architecture has to match the SoS breakdown and the COIs that populate it. The types of SoS and SM organisations could be unlimited but it can be characterised with properties, which nevertheless define a large scope of type of organisations.

- Firstly, along the command axis, the SoS organization will likely be hierarchical with superior linked to subordinate or cooperative where people and systems collaborate within their respective degrees of freedom.

- Secondly along the temporal axis, the SoS organization can be permanent during a mission or expedient for just a part of the mission.

- Thirdly, along the collaboration axis, the SoS organization is subject to modification during mission due to events, which are of two kinds: planned where collaborations have been planned before the mission or unanticipated such as e.g. opportune collaboration setup for resource sharing.

Combining these dimensions with the staff cells considerations presented before leads to an SM organized as an AMU mesh combining hierarchical and collaborative relationships. Such an AMU mesh is depicted in the Figure 2 below.

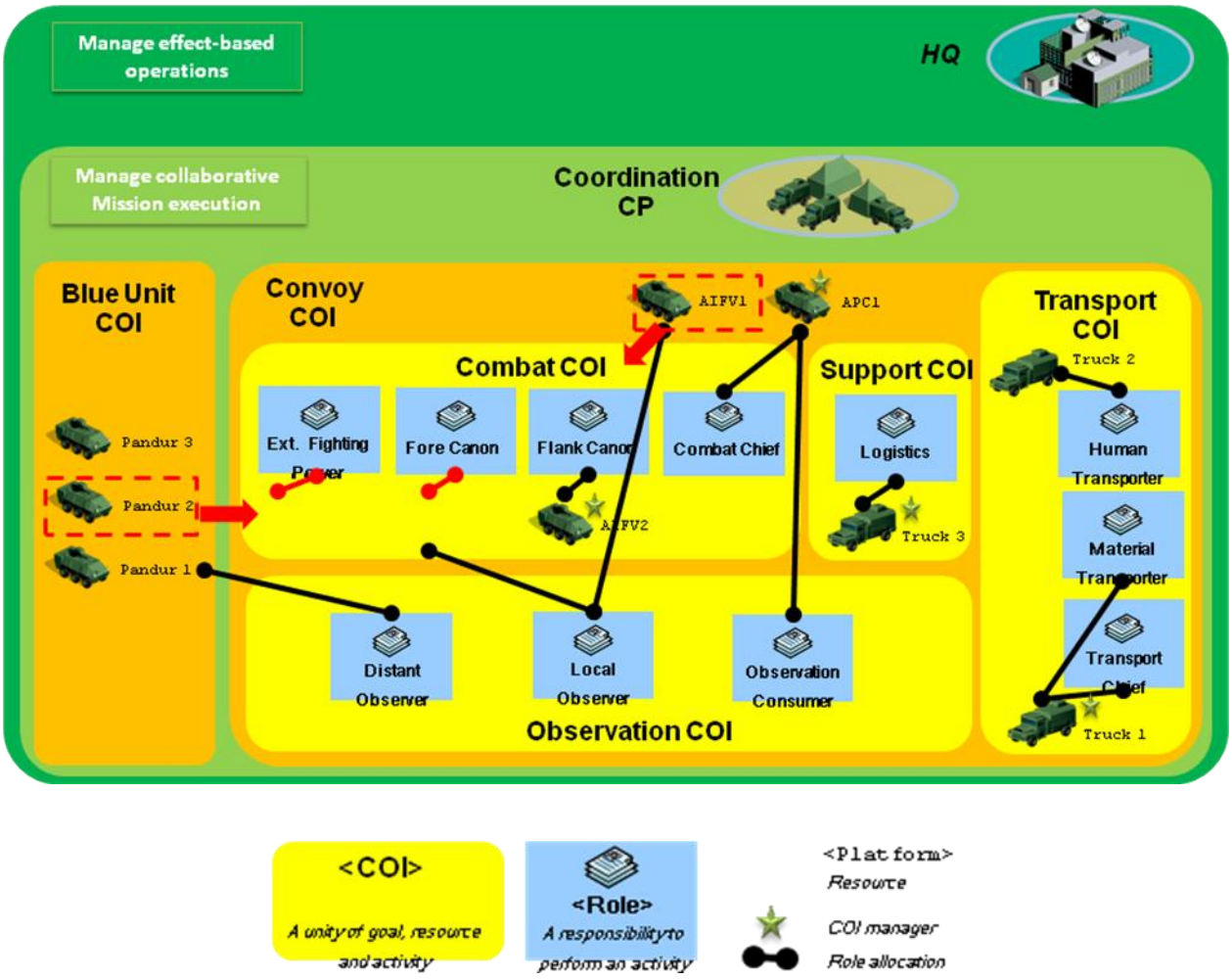

Figure 2: Organization of AMUs

2.5 System Management Services

The system management services and functions are defined as a subset of the C2 activities. High level services are identified to:

- Support the mission (planning and design at the technical level of the command chain, supervision, and decision making),
- Collect the users requests and complaints,
- Manage the security,
- Define, put in place and survey the system configuration,
- Decide on the aspect of maintenance activities,
- Allow simulation and replay.

3 IMPLEMENTATION OF SYSTEM OF SYSTEMS MANAGEMENT

The implementation of the SM relies on an engine which carries out tasks according to events (operator's order, system failure…) and a knowledge base. This knowledge base comprises the current state and composition of the SoS and the Policies to be applied depending on events. This concept was studied in the ASAAC program [5], which provided Guidelines and Standards for an Integrated Modular Avionics System for strike aircraft. In the ASAAC study the SM focuses on the platform and the knowledge base, called blueprint, is a database of parameters. This blueprint is fed in the manufactory. It means all configurations are foreseen once and for all. And there is no action from the operator during the mission. This type of implementation is somewhat limited even completely inefficient when the SM is applied to a SoS. The dynamic nature of SoS makes parameter-based implementation impossible to enable the management of SoS. For managing a SoS, it must be possible to modify its composition (in terms of systems and organisation) in the blueprint and to generate technical data according the new composition and the policies. The promoted solution is the implementation of blueprints with formal models.

The SoS is described with models from different viewpoints. The models are produced from design time and modified during the rest of SoS lifecycle. They are embedded in the SoS, and are executed during operations. When a new system is added, an operator can put this system with a drag and drop in the SoS Model, and place the new system in the SoS organisation. The operator could first test the Model to verify if the adding conforms to the policies (safety, security, etc.) and then execute the Model in runtime. This execution generates all technical parameters to configure the new systems and systems, which are impacted by this adding.

3.1 System of Systems Management Framework

The SM Models decompose into three types of models which are declined at operational, system and technical levels.

- Deployed Management Organisation: This model defines the organisation of the SM in term of interactions between the SM agents on different platforms, the area of responsibility (who is in charge of managing the system) and the centres of management (where are the centres of decision).

- Deployed Management Policies: Any modification or action on the organisation of the SoS have to abide by a set of rules called policies which are of different nature: reconfiguration constraints (some interactions could be forbidden for technical reasons), Safety (innocuousness), Security (some tasks are only assigned to authorised system or people), Doctrine (according a concept of use), Events analysis and propagation (Who should be notified after detection of an event)

- Deployed SoS: The SoS is described at planning time with models. The information are capabilities/services provided by the SoS which are represented by contracts, workflows, interactions between systems of the SoS, systems in the SoS and COI.

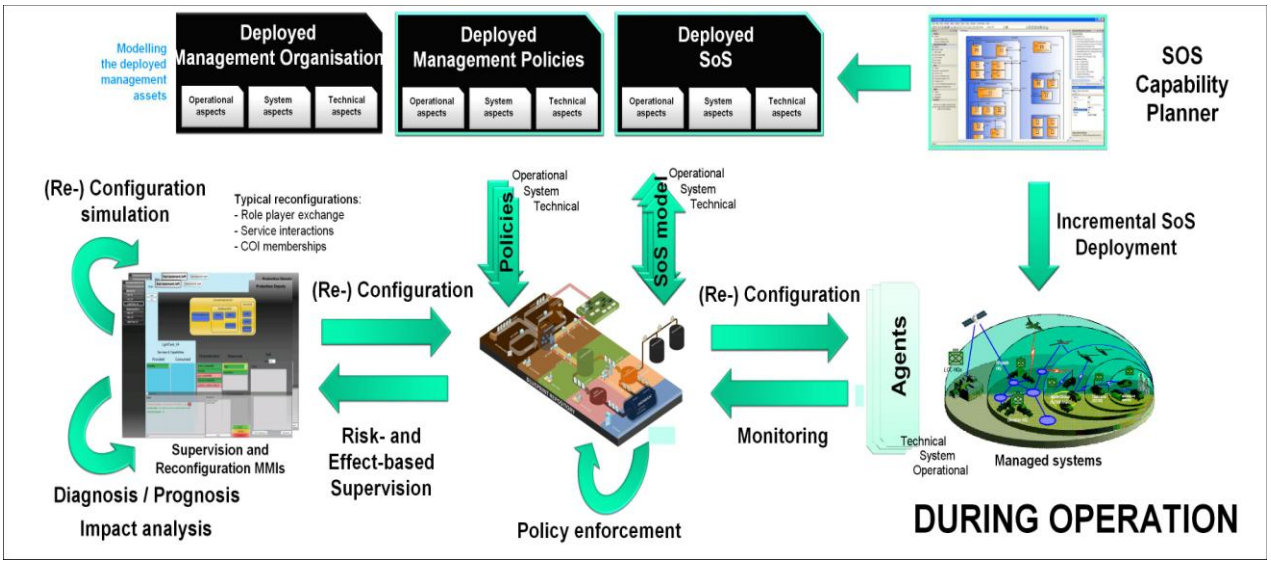

Figure 3: System Management during operation

At planning time, the SoS capability planner generates models of Deployed Management Organisation, Deployed Management Policies and Deployed SoS. These models contain the useful information for setting up the SoS and retaining its capabilities.

To set up a SoS, the Deployed Management Organisation Models are first executed. The SM agents on the managed systems are interconnected. The operators, roles, area of responsibility, responsibility chains, and management centres are defined within the SoS itself. The SM uses this information to implement management policies.

Once set up, the SM monitors the SoS, which is described with the Deployed SoS Models. These models are information about the system capabilities and architecture. They describe the SoS structure and behaviour in terms of system entities, services, service relationships, COIs, capabilities and roles, etc.

Additionally, the SoS models contain information about the evolving system topology and state. They describe the current topology of entities and service relationships, and the current state of entities and capabilities such as the value of operational properties (such as fuel, position, and ammo) and technical properties (such as the current set of flows within a communication channel and the measured end-to-end QoS on a communication path). Basically, agents probing the system provide the SM with this information. A subset of this information can also be provided in real time by system management operators (when it is not feasible or suitable to use agents, e.g. to record troop fatigue information).

Operators in SM centres supervise the SoS. This supervision allows displaying the current state of the SoS as well as the impact analysis on a diagnosis, which in turn allows a prognosis on the future state of the SoS. A new configuration can be generated and then it can be assessed by simulation and if the result is satisfactory, the new configuration is applied.

When an event occurs, it is analysed against policies for propagating the events in the SM organisation. This event may impact the current SoS organisation, which may require a modification. The SoS models may be modified according to Deployed Management Policies.

Deployed Management Policies are the strategies and corresponding policy rules that govern the system management itself. They are expressed after the system has been designed while avoiding any form of

tight coupling with the target SoS itself. These policies cover:

- Events analysis policies: They define how event occurrence are measured, evaluated based on criteria, correlated one another, and eventually aggregated according to viewpoints. These viewpoints are defined according to risks and effects of immediate importance to management operators.

- Event propagation policies: They define the rules to propagate events from one management centre to another one, according to management responsibility areas and supervision strategy.

- Performance and behaviour policies: beyond the behavioural policies defined at the architectural level during design-time, one can add here performance and behavioural policies specific to an operational context or to a mission.

- Security policies: They define security access control and privacy to SoS services.

- Reconfiguration policies: beyond the structural and behavioural policies defined at the architectural level, one can add here configuration and reconfiguration constraints specific to an operational context or to a mission.

3.2 Status of the prototyping activities

Here are the main prototypes developed.

SM Node

The SM Node is our implementation of the AMU concept (Autonomic Management Unit). There is one SM Node per platform or platform subset having a management responsibility. *One key requirement of the SM organization is to be resilient in the event of the damage or destruction of a subset of the managed system of systems*. The SM Node is therefore designed to enable the autonomous management of its area of responsibility, despite its possible temporary isolation. Corollary, the SM Node is designed to resynchronize itself during re-entry in a SoS after a temporary isolation. Here are its main characteristics:

- In-memory store of all the management models (consistency and validation rules)
- On-the fly persistent storage into an embedded COTS database
- Extensible architecture
    - For SM agents: Service monitoring, Vehicle monitoring, Business Application monitoring and configuration
    - For SM functions and rules add-ins: Analysis indicators evaluation and propagation engine
- Command-based pattern to control concurrent access on the store and synchronization
- Evaluation mode for Reconfiguration Impact Analysis
- SM Node instances synchronization according to their place in the management organization (i.e. responsibility domains)
- Journaling (post-operation replay of management actions on the SoS)
- Runtime evaluation of performance indicators (Implements THALES Research & Technology multi-criteria architecture called “Myriad”)
- Supervision MMI
- Role-based reconfiguration MMI

SM Domain Model, SM Designer

The SM domain model prototype was presented before in this paper. The domain model forms the core knowledge supporting the SM functions, formalized as a model. A documentation generator allows a model-centric approach to defining the domain concepts. Modelling tools have been semi-automatically generated using a meta-tool called DSL Tools (integrated in Microsoft Visual Studio 2008). Here are the main characteristics of these prototypes:

- SoS lifecycle coverage: design-time, plan-time, and operation-time
- Scope of modeling:
  - SoS description (Capabilities, services, COI, platforms…)
  - Policies description
  - SM organization
- SM Designer
  - Covers design-time and plan-time
  - Multi-diagram modeling experience (i.e. modelling according viewpoints)
  - Domain-specific modelling notation
  - Open and mastered code generation

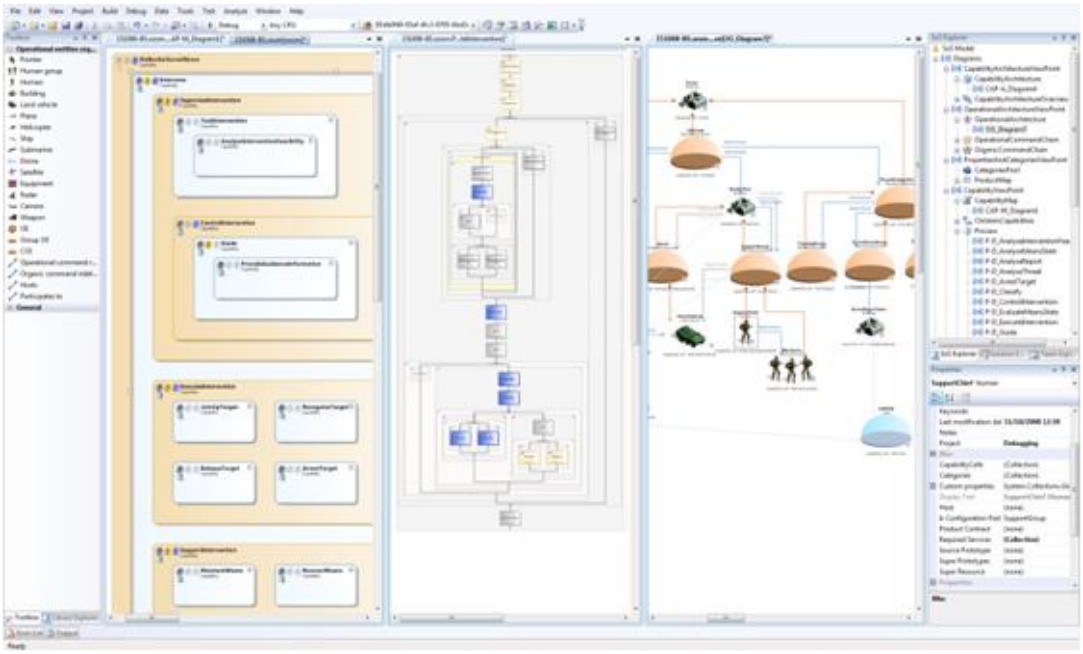

Figure 4: SM Designer

3.3 Experimentations

These prototypes have been assessed on a Convoy scenario, which considers a convoy in charge of delivering some materials to a specific place. The convoy is considered as a COI, which is further subdivided into 2 sub-COIs : Combat and Transport. The first one is assigned to the protection of the second one. The convoy also contains a transverse COI called “Observation” and composed of vehicles belonging to both Combat and Transport COIs, whose role is mainly to provide short range observation

information to the convoy and detect potential threat. Finally, a friend "Observation Unit" is present in the area and provides long range observation information. The convoy chief is in charge of synthesizing the information coming from both the Observation COI and the distant Observation Unit.

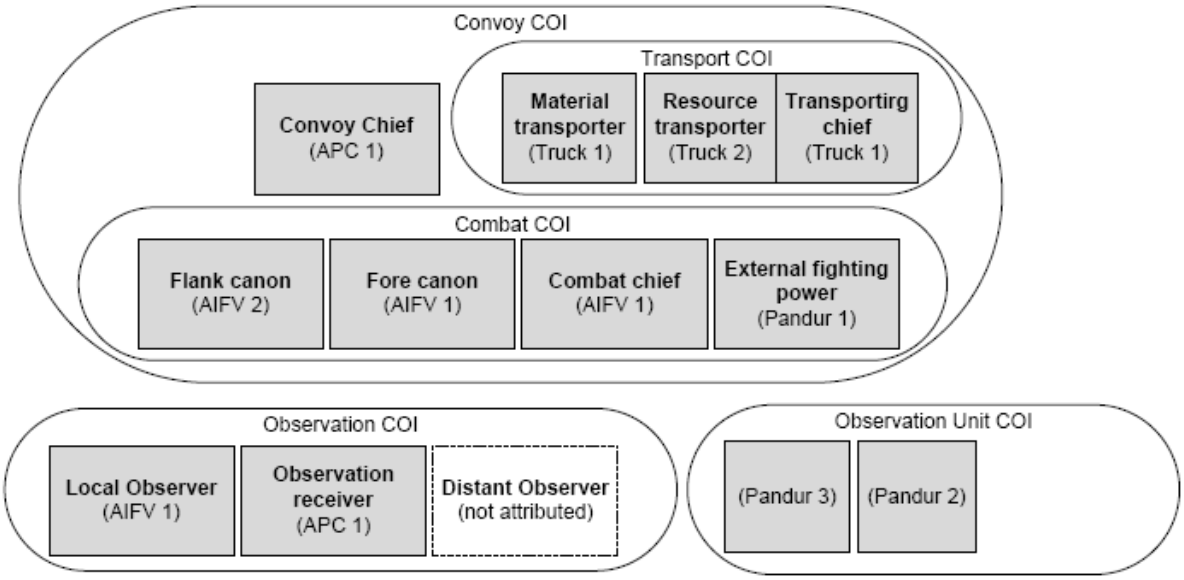

Figure 5: Convoy - Original configuration

During the scenario, an observation equipment and a weapon will break and thus lead two vehicles (AIFV1 and Pandur1) to losing some most of their capabilities. The aim of the experimentation is to assess the proper reassignment of the roles to maintain the global efficiency of all the COIs.

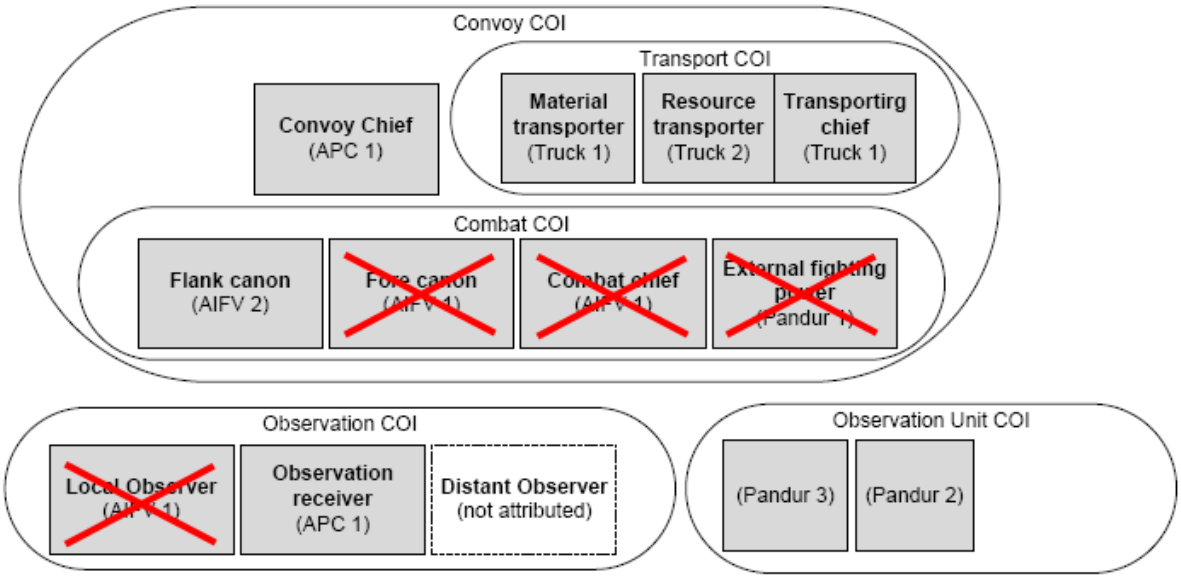

Figure 6: Convoy - Damaged vehicles and impacted roles

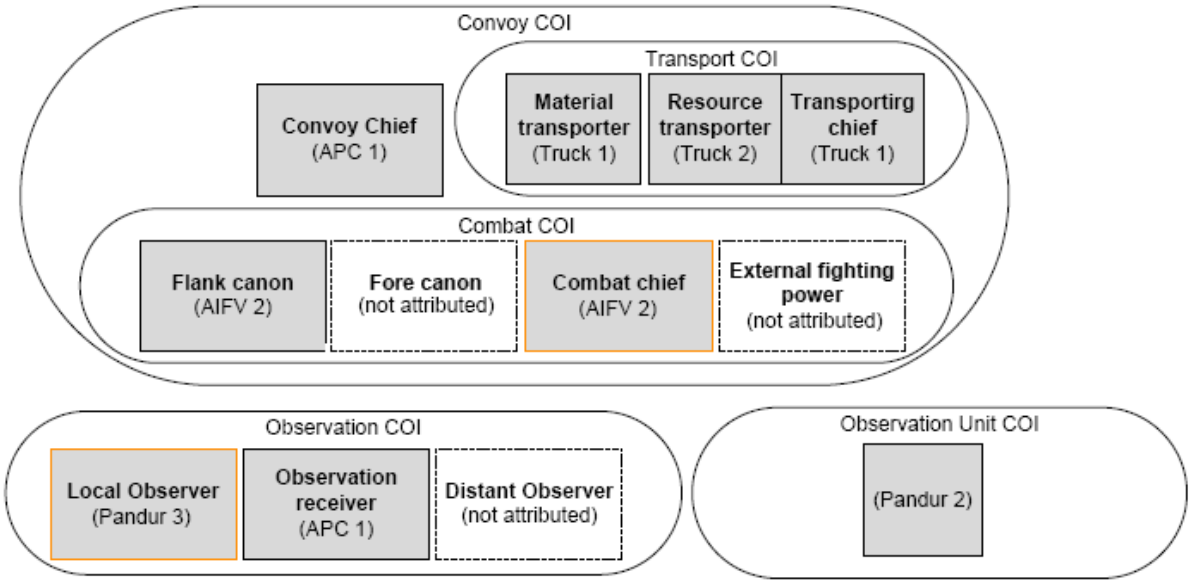

Figure 7: Convoy - Degraded configuration (orange = roles reallocated to new vehicles)

In the degraded configuration presented by Figure 7, the efficiency of the Observation COI is maintained by the reallocation of the Local Observer role to a new actor with similar observation capabilities, Pandur3 from the Observation Unit. The Combat COI however has not been able to reallocate all its roles: the only vehicle with the same combat capabilities as AIFV1 is AIFV2, who cannot play at the same time the role of flank and fore cannons.

4 ONGOING RESEARCH

Model-based SoS Management is still facing issues such as:

- The SoS needs to be described in a comprehensive way drawing from the operational needs and target capabilities, down to a comprehensive description of the SoS technical components. However, in today's situation, architecture frameworks still show some limitations at technical level, and still provide a limited coverage of the SOA paradigm.

- Talking about SOA, which is the key paradigm for NCO, the SOA pattern at tactical level still needs some engineering and operational exploitation investigations. As previously said, the organisation of people, system and services drives the organisation of SM at tactical level. Among others, the centralisation of service directory or its distribution may impact the organisation of SM Node and its model repository.

- The SM to be widespread should converge to current and emerging standards. A candidate is the Service Modelling Language (SML) [6], which enables to describe complex systems and services in XML. An interesting standard for management agents is Netconf, which provides mechanism to install, configure or reconfigure devices and equipments. Netconf is expressed in XML. Moreover, even if not specifically targeting the tactical segment, recommendation and standardization bodies such as ITIL, DMTF, and Tele-Management Forum are active players that need to be watched carefully.

- The current MIP work promotes the JC3IEDM [7] for sharing a common language for the situational awareness. As the SM is nested in the Command & Control Process, it might be worth having SM

attributes in the JC3IEDM.

- The interactions with C2 processes and logistics have to be valued with their related Human Factors issues.

5 CONCLUSION

The SM relies on a comprehensive knowledge of the SoS design in terms of the systems that composed it, the capabilities provided, and the rules it has to abide by. These rules are described in policies. It also relies on the capability to dynamically configure the organisations within the SoS. This knowledge is expressed by models of SoS services and workflows, along with technical data needed to configure sensor resources, processing equipments and communication channels between service producers and users. The management of SoS at tactical level however focuses on system interactions rather than on systems internals. Therefore, the management of SoS needs to interoperate with legacy management of existing systems. During operations, the constant monitoring of system health allows to correct and even prevent failure of capabilities by reconfiguring the relationships between systems. This brings an enhancement to the resilience of the SoS and a valuable support to the command level. The idea developed in this paper is to model the SoS and its expected behavior, then to embed this model into the operational SoS and to keep this model living and up to date during the SoS operations. The SM architecture is thought to be fully distributed, therefore favouring agility and autonomy of management in the event of a system damage or failure. Yet, the hierarchical nature of the management domains still allows consolidating global supervisions at various levels of command, and according to multiple management viewpoints.

6 REFERENCES

[1] Mark W.MAIER, Architecting Principles for Systems-of- Systems, http://www.infoed.com/Open/PAPERS/systems.htm

[2] OASIS Reference Model for Service Oriented Architecture 1.0, 10 February 2006, http://www.oasis-open.org/committees/download.php/19679/soa-rm-cs.pdf

[3] DoDAF 1.5, http://www.defenselink.mil/cio-nii/docs/DoDAF_Volume_I.pdf http://www.defenselink.mil/cio-nii/docs/DoDAF_Volume_II.pdf http://www.defenselink.mil/cio-nii/docs/DoDAF_Volume_III.pdf

[4] MODAF V1.1, http://www.modaf.org.uk/

[5] ASAAC Final Draft of Proposed Guidelines for System Issues Document reference: ASAAC2-GUI-32450-001-CPG, Issue 01, January 2004. http://www.era.co.uk/assc/asaac/4626 Guidelines_vol 1and 2.pdf

[6] Service Modeling Language, http://www.serviceml.org/

[7] Multilateral Interoperability Programme, Joint_C3_Information_Exchange_Data_Model, http://www.mip-site.org/publicsite/04-Baseline_3.0/JC3IEDM-Joint_C3_Information_Exchange_Data_Model/HTML-Browser-ZIP/

[8] Scale-free Enterprise Command & Control – Unified Command Structures -, Jay Bayne, Raymond Paul, 10th International Command and Control Research and Technology Symposium, June 13-16, 2005, McLean, VA, USA