12th International Command and Control Research and Technology Symposium

"Adapting C2 to the 21st Century"

Enterprise SOAs for the convergence of Battle Management and Resource Management systems

David Lincourt and Hans Peukert

David Lincourt
Vice President, Field Services
SAP for Defense
SAP Labs Canada
45 O'Connor Street, Suite 600
Ottawa, ON Canada K1P 1A4

T: 902.488.7956
F: 902.434.7821

Enterprise SOAs for the convergence of Battle Management and Resource Management systems

Abstract

In an age where many defense organizations are adopting Service Oriented Architectures, we have observed the convergence of Battle Management and Resource Management systems. Today, many defense organizations either use the ADatP-3 messaging or the MIP information exchange data model replication standards for exchanging data. Consequently, the same software capabilities are often duplicated in both domains. At CWID 2006 and 2007, the Mission Capability Package (MCP) data of the NATO Response Forces NRF 9/10 were maintained within a trial system in multi-security / multi-national federated environment using ADatP-3, MIP, and web services. Specifically, the provision of organizational and resource data to battle management systems from resource management systems, and process integration between resource management and battle management systems. In the future, Battle Management systems will be able to invoke the appropriate web services to obtain the up-to-date relevant information from resource management systems. This paper will provide insights on lessons learned and a roadmap to defining Enterprise Services to enhance the ability to provide solutions that enhance Commanders at all levels the ability to collaborate and disseminate information among communities of interest (COIs) in a net-centric environment while providing agility to the warfighter.

Introduction

In many parts of the world, defense organizations are transforming themselves to better address the realities of today's geo-political environment. As Dr Albert and Dr Hayes noted in Power to the Edge: "Agility is arguably one of the most important characteristics of successful Information Age organizations. Agile organizations do not just happen. They are the result of an organizational structure, command and control approach, concepts of operation, supporting systems, and personnel that have a synergistic mix of the right characteristics." (Alberts & Hayes, 2005, p. 123) This transformation to achieve agility is exhibited by changes in three axes:

- Concept of Operations – defense forces are adopting the concepts of net-centric operations and embracing the idea that individual contributors are central to it's success
- Technology – by implementing and adopting the information and data grid. In essence, the pervasiveness of networking and computing technologies allows these new concepts of operation to be technically realized.
- Organizations – Many defense forces have adopted a modular force structure. As well, organizations that have traditionally been garrison based are now deploying outside of their national boundaries in joint and coalition operations. As such, mission capability packages can be readily composed to meet the need. In other

words, the monolithic organizational structures are no longer appropriate or workable.

The defense ecosystem is highly complex and includes participants from many different segments. Today's operations most often are conducted in a joint and coalition environment where members bring to the area of operation complementary capabilities that when put together form a total mission capability package. Further, many governmental and non-governmental organizations are involved (e.g. Red Cross / Red Crescent, World Food Program, Médecins Sans Frontières, etc). On the industry side – "suppliers on the battlefield" is a very common occurrence. From providing infrastructure management, security services, or even comforts from home (e.g. Burger King, Pizza Hut, and Tim Hortons at the Kandahar airfield in Afghanistan). We are observing that defense organizations are contracting for capability rather than procuring and sustaining the weapon system along its life-cycle. They are outsourcing the complexity of the process to the private sector. Examples include Performance Based Logistics (PBL) for Joint Strike Fighter and the Airbus A400M. Further, the weapon system is also a process participant by sharing health monitoring data. This requires a new interaction model for the process participants in this complex and fluid defense ecosystem.

Empowering the "Strategic Corporal"

"Power to the edge is about changing the way individuals, organizations, and systems relate to one another and work. Power to the edge involves the empowerment of individuals at the edge of an organization." (Alberts & Hayes, 2005, p. 5) The Strategic Corporal (General Krulak, 1999) is a metaphor was developed in the late 90's by then Commandant of the USMC – General Krulak. It typifies the every day soldier, sailor, airman, airwomen, and civilian within a defense organization – in commercial language, it's the information worker. These individuals – in their day-to-day activities have the ability to impact the outcomes of larger operations – or endeavors. In other words… they are today's "Corporal Radar O'Reilly" of the popular American TV show M*A*S*H. They bring "power to the edge".

The "Strategic Corporal" requires understandable contextually relevant actionable knowledge:

- Understandable - capable of being understood or interpreted
- Contextually relevant - in a manner dependent on context (the set of facts or circumstances that surround a situation or event) and having a bearing on or connection with the subject at issue
- Actionable – that they can act upon
- Knowledge – data > information > knowledge

Knowledge is critical for decision making and to rapidly and effectively proceed through Boyd's OODA Loop (Boyd, 1995).

This is regardless of the IT systems that is being used and the user interface or device. Their device of choice is highly depended on the required interaction model, their role, and their operating environment that is the most appropriate. Examples of the user interface include web front end, electronic interactive forms, voice, widgets, office applications (e.g. Microsoft Office), RSS feeds, Podcasts, GIS, or other specialized user interfaces. It is about making sound decision and to self-synchronize with other "strategic corporals".

While the technology enablers are critical, more importantly is the ability to connect strategic corporals with other strategic corporals in order to create understandable contextually relevant actionable knowledge into a "Community of Interest" (ADatP-34 Vol 2, para. 3.3.5). Metcalfe's law states that "the value of a telecommunications network is proportional to the square of the number of users of the system" ("Metcalfe's law", 2007). A seemingly simple but very powerful illustration of Metcalfe's Law can be found in the "Indian Fisherman" story that was recently published in the Washington Post (Sullivan, 2006). While the fishing techniques have not changed, the balance of power between the actors has considerably been revolutionized. In the past, "Rajan said that before he got his first cell phone a few years ago, he used to arrive at port with a load of fish and hope for the best. The wholesaler on the dock knew that Rajan's un-iced catch wouldn't last long in the fiery Indian sun. So, Rajan said, he was forced to take whatever price was offered – without having any idea whether dealers in the next port were offering twice as much." Now that the fisherman – a strategic corporal – is connected via a camera equipped cell phone to a network of fellow fisherman and buyers, he can find fish with greater knowledge and negotiate the catch with various buyers while still at large. In essence, agility was obtained by adopting new technology, applying the net-centric concept of operations and a modular organizational structure.

Another critical component of the network is what has been dubbed the "internet of things". The strategic corporal will now be able to go beyond the any-time and any-place interaction dimensions. Through recent technological breakthroughs, their reach now includes insight from the physical world. Examples include health monitoring of aircraft systems, asset visibility using RFID technology as well as many other types of sensors and devices. As indicated in ITU's 2005 Internet of Thing Report, "connections will multiply and create an entirely new dynamic network of networks" ("ITU Internet", 2005, p. 2).

As seen in the "Indian Fisherman" story, agility is elusive without the appropriate IT to support operations in the dynamic defense ecosystem. There still exist great divides between the Battle Management and the Resource Management communities. In most cases this is artificial and amplified by the different security classifications of these IT systems and networks. In the end, it's really about the same "thing" viewed from different perspectives. The Mission Capability Package is in reality the common ground between these communities. Each community plans and executes their functions based on their perspective of Mission Capability Packages. As such, a common and unified perspective towards Mission Capability Packages is required to fulfill the objective of true interoperability. Today, IT systems are not designed to work together, data exchange

formats are complex and inconsistent vocabulary exist to describe resources. Consequently, misunderstanding of what, where and when resources are needed, assumptions made on the status of critical resources and inappropriate prioritization of support resources. This leads to wasteful micro-management at all levels and the disempowering of the “strategic corporals”.

NATO CWID 2005 & 2006

SAP participated in the Coalition Warrior Interoperability Demonstration (CWID) exercises in 2005 and 2006, conducted by NATO Allied Command Transformation (ACT). The annual CWID event is where the international community can test new and evolving command and control technologies designed to meet NATO standards and protocols. Using a simulated scenario – based on the NATO Response Force (NRF) military command structure – they illustrated the ability of Resource Management to seamlessly integrate with Battle Management systems used by military forces, enabling the rapid transfer of mission-critical information.

In order to expedite data exchange between the Resource Management system and Battle Management systems, we used interfaces that are both compliant with Allied Data Publication-3 (ADatP-3), the NATO standard format for data exchange, and in accordance with the data model of the Multilateral Interoperability Programme (MIP). Interfaces between Resource Management system and the NATO Functional Area Services (FAS) were also enabled.

It became readily apparent that similar data that exists in both Resource Management systems and Battle Management systems are exploited across a number of processes. For example:

- Contributing actionable knowledge to the commander’s conference by reporting about the status of all respective resources, be it the operational structure, personnel, or materiel
- Providing the current personnel and materiel information to the NATO Allied Deployment and Movement System (ADAMS) as initial data and to various command and control information systems on a daily basis
- Processing logistic assistance request (LOGASREQ) messages and providing corresponding logistic assistance response (LOGASRESP) messages
- Importing air tasking orders (ATOs) – according to the Integrated Command and Control (ICC) software. The ATO was sent to the Resource Management system for further maintenance planning. Filter techniques have been used so only the relevant logistical data is being extracted and only this data was be transmitted to the Resource Management system.
- Leveraging information and ensuring resource transparency across various IT security domains. From unclassified via one-way diode to national secret and from unclassified via encrypted tunnel to mission secret. A business information warehouse with additional defense key performance indicators was used to provide actionable knowledge.

While these demonstrators were highly successful, they highlighted some challenges that need to be overcome in today's environment:

- ADatP-3 - point-to-point, not robust, difficult to enhance
- MIP - standardized data model, lower bandwidth, offline capable, complex

The Need for an Enterprise SOA

There is a profound need to go further than the machine-to-machine rigid interaction model. The "Indian Fisherman" story exploits simple and readily available COTS technology. Defense organizations have not kept pace with the introduction of such disruptive technologies. The current generation of strategic corporals has however been immersed in this environment. In their private life, they make use of podcasts, peer-to-peer networking, sensors information in their vehicles, Wikis for knowledge sharing, host their own blogs, etc to enrich the network. And only through their resourcefulness in their professional life they are much closer to "Radar O'Reily" than we would imagine. Conflicts today exemplify that through these technologies, the enemy has learned to exploit the power of Metcalf's Law to their great advantage and consequently the erosion of our information superiority.

The need to respond rapidly to operational demands, support new strategies, and improve the overall user experience is driving IT organizations within defense forces to search for new ways to improve interoperability at a lower cost. A Service Oriented Architecture is a technical framework for rapidly building software applications that use services available from a network like the Web. Applications in SOA are designed to use Web services as the standard means to communicate well-defined information with an array of other applications. As such, SOAs enable defense forces to assemble loosely coupled applications from web services distributed over a connected infrastructure. But web services by themselves are not sufficient. As we described in our paper from last year (Lincourt & Peukert, 2006), the fundamental premise of an Enterprise SOA (formerly called Enterprise Services Architecture) is the abstraction of process activities or events, modeled as enterprise services, from the actual functionality of enterprise applications. Aggregating Web services into defense-level enterprise services provides more meaningful building blocks for the task of automating coalition-scale defense scenarios. Enterprise services allow coalition members to efficiently develop composite applications, defined as applications that compose functionality and information from existing systems to support new defense processes or scenarios. All enterprise services communicate using Web services standards, can be described in a central repository, and are created and managed.

We have observed that the commercial sector and military organizations have embraced the concept of Enterprise Services Communities. The Enterprise Services Community is a flexible framework for defining enterprise services with the input and feedback of the ecosystem. The framework is designed to support diverse definition models and levels of cooperation within the community. The value of the Enterprise Services Community lies in its ability to directly impact the business requirements and technical architecture of the

net-centric platform by fostering targeted, business-driven feedback from the Community.

In a military setting, the Enterprise SOA paradigm provides a framework to network seemingly disparate application components in innovative ways by assembling services. All the participants on the grid may ultimately move into a world of consisting of Service Consumer & Service Provider. Depending of their role they will become either Service Consumer or Service Provider or both. Each "Service Provider" will provide a Service which is described and published at a service registry. The service consumer will search the Service in a service registry and invoke the service provider when ever or where ever needed. This occurs in a pre-defined process or even ad-hoc to allow strategic corporals the ability to address unforeseen situations. As Major Q. exemplified in her depiction of the "Wounded Soldier" story ("Net-Centric", 2005). The central strategic corporal books the surgery, arrange for medical evacuation and triggers the personnel replacement process. "Is this soldier a medic, an admin assistant, a transporter or a personnel clerk?" ("Net-Centric", 2005). In essence, she indicated that "even the smallest unit can pull what ever data they need, when ever they needed from where ever they are…" ("Net-Centric", 2005).

NATO CWID 2007

In CWID 2007 we are demonstrating a service enabled environment where users in Battle Management systems seamlessly interact with other users in Resource Management systems. These Services will be used for a Proof of Concept for a two way integration of Battle Management and Resource Management. They will also demonstrate a data transfer across security domains from a red network to a black network via a gateway. The specific objectives include:

- Initial data transfer from Resource Management to Battle Management
- Ongoing update of the Battle Management systems with real time logistics situation information
- Test and demonstration of the ADatP-3, MIP and Web Services interfaces
- Test and demonstration of the interfaces to NATO LogFAS
- Provide resource information in and across multiple information domains in both directions black-to-red and red-to-black
- Validation of Business Information Warehouse reports

This demonstration will provide significant value to the community:

- High quality reports and automated data entry for J1, J3Org, J4 and J5
- Enabling real time integration of logistic and operational processes between the Battle Management Resource Management systems
- Collaboration with NATO Functional Area Services
- Providing consistent information across security domain boundaries

Preliminary results from the NATO CWID 2007 experience include:

- SAP's Enterprise Services Definition Group provided the necessary guidance for the needed service enablement in a military
- Service definitions are published on a publicly accessible web site
- Process orientation is key to determine what needs to be service enabled
- The way forward is to enable bi-directional interoperability between Resource Management & Battle Management systems across different security domains using commercially available filters and diodes

Additional insights and graphics will be shared during our presentation.

Conclusion

In conclusion, strategic corporals will ultimately become the central focus of transformational activities and interchangeably become service providers and service consumers within an "internet of thing". This occurs when they have understandable contextually relevant actionable knowledge. Collectively, they come together in a net-centric environment where information is shared in pursuit of shared goals, interests, missions, or business processes across security domains. SAP has demonstrated at both NATO CWID 2005 and 2006 that this objective is feasible. Specifically with the support of decentralized Resource Management systems interconnected to a central homeland Resource Management system, and bridge the divide between Resource Management and Battle Management systems by providing organizational and resource data to Battle Management systems. Process integration between Resource Management and Battle Management systems has been successfully demonstrated at NATO CWID 2006. The next generation of integration will be demonstrated with process integration using an Enterprise SOA framework at NATO CWID 2007. This will only be possible through the Community of Interest involvement in Enterprise Services Communities.

References

Alberts, David. S., & Hayes, E. Richard. (2005). *Power to the Edge: Command and Control in the Information Age* (3rd). Washington, DC: DoD Command and Control Research Program.

Allied Data Publication 34 - NATO C3 Technical Architecture - Volume 3 (7.0). : NATO ADatP-34.

Boyd, John. R. (1995, June 19). *The Essence of Winning & Losing.* Retrieved February 15, 2007, from http://www.belisarius.com/modern_business_strategy/boyd/essence/eowl_frameset.htm

General Krulak, Charles. C. (1999, January). The Strategic Corporal: Leadership in the Three Block War. *Marines Magazine*.

Lincourt, David., & Peukert, Hans. (2006). *Towards Shared Awareness and Self-Synchronization in a Coalition Environment*. : 11th ICCRTS.

Metcalfe's law. (13, February 2007). Retrieved February 15, 2007, from http://en.wikipedia.org/wiki/Metcalfe's_Law

ITU Internet Reports 2005: The Internet of Things. (2005). *Executive Summary*: International Telecommunication Union.

Net-Centric Manager: Interview with Major General Marilyn A. Quagliotti. (2005, February 18). [Electronic Version]. *Military Information Technology*

Sullivan, Kevin. (2006, October 15). For India's Traditional Fishermen, Cellphones Deliver a Sea Change [Electronic Version]. *Washington Post Foreign Service*, p. A01.