Utilising SOA in defence logistics

The logistics function within the defence arena presents distinct and complex challenges which can be mitigated through the adoption of a SOA architecture

April 2010

Defence logistics have multiple touch points with logistics systems operated by civilian and quasi-civilian organisations, and must be able to operate effectively, rapidly and transparently with these systems. However, as defence logistics approach the battlespace, the capabilities and needs change: communication lines become less predictable, physical drop points for reprovisioning and carrying out in-field repairs may be moving in real time. Further complications are introduced through the sheer scale of maintaining a successful operation, with the need to maintain supplies of items ranging from personal supplies of rations, razors, mail from home and so on, through armaments and ammunition to the likes of lorries, tanks and helicopters. Such complexities cannot be allowed to compromise the supply chain and the logistics flows: today's battlespace requires an end-to-end approach to processing supply needs and providing the logistics to fulfil these. Cost remains a major issue and, as such, battlespace logistics must also ensure that all actions are financially optimised, while kept in balance with the real time critical needs of the assets in the battlespace itself.

Clive Longbottom
Quocirca Ltd
Tel : +44 118 948 3360 ext 200
Email: Clive.Longbottom@Quocirca.com

Bob Tarzey
Quocirca Ltd
Tel: +44 1753 855 794
Email: Bob.Tarzey@Quocirca.com

Utilising SOA in defence logistics

Using open standards to enable defence logistics to operate effectively in a rapidly changing environment

The defence environment presents a set of distinct and complex issues when it comes to logistics in the battlespace. The range of items required in an ongoing operation ranges from the very small and relatively fragile, such as rations, through to the very large and less fragile, such as tanks and heavy machinery spares. However, integration with civilian organisations is a key requirement, and a mix of commercial and home-grown systems used here adds further complexities to an already difficult environment. Using SOA to underpin logistics processes can help address many of the associated problems, such as:

- **Ensuring granularity of response:**
  The battlespace requires rapid response in many cases as replacement parts and a continual provision of consumables including food, water, ammunition and small armaments are required. However, wherever possible, logistics have to be aggregated to ensure that items are not being supplied at too high a cost - both at a pure monetary level and also at a risk level, as supply chains to the battlespace will have their own risks to contend with.
- **Creating and maintaining a battlespace logistics capability:**
  No battlespace situation can be sustainable unless there is a capability to maintain suitable logistical support. Having the wrong assets in place, or having assets that are missing key components, will not just compromise a battlespace capability, it could lead to the loss of a strategic position or capability.
- **Using just-in-time in a real time response environment:**
  Building up large quantities of items in a battlespace is not recommended. Not only does it lead to poor inventory management and the probability of assets not being available where they are needed within a reasonable period of time, but it also opens up problems around the security of the assets themselves. If the inventory is compromised, either through theft or through damage incurred by enemy action, then it is lost. Better to keep the assets away from the threat zone, but be able to get the assets to where they are needed rapidly and effectively.
- **Enabling micro-distribution sites for rapid response:**
  In an active battlespace environment, it will be necessary to ensure that certain items are continually provisioned, for example ammunition and rations. These sites may need to move as the battlespace changes, and large stocks of items will either compromise the depot's capability to move rapidly, or will just have to be left behind or destroyed as the depot moves. By keeping small, front-line sites provisioned from a larger behind-the-lines depot, such more immediate needs can be effectively managed.
- **Monitoring of equipment for proactive logistics:**
  Larger assets, as well as items such as communication equipment, can often be continually monitored to warn of an incipient problem, or to show the root cause of an existing problem. Through the use of remote monitoring, asset utilisation can be maximised, and failure requiring complete removal of assets can be minimised, with the logistics chain providing spares support on-demand as required.
- **Shared logistics with other defence forces needs to be managed in a secure manner:**
  Few battlespaces exist where it is one single party in an operation against another single party. Formal or loose coalitions of friendly groups, often involving in-theatre teams of military, police or private security assets are far more the norm, and a means of ensuring that logistics capabilities are not overlapping and that supply chains are not overly redundant is an important consideration.
- **Integration with existing civilian logistics systems:**
  Much of a supply chain's contents will be supplied from purely civilian or quasi-civilian suppliers. Military systems must be capable of providing information into these systems and receiving information from them in a manner which makes the whole set of logistics processes more effective, flexible and supportive of the needs of the battlespace.

Conclusions

Logistics in a defence environment has to embrace standard commercial systems, yet also needs to be able to deal with the specific issues arising from conditions at the front line of the battlespace. The use of a SOA architecture enables the rapid exchange of information required to ensure that massive inventories of equipment are not kept in multiple large distribution depots, yet also ensure that items are available within the short timescales necessary within such a dynamic environment.

1. Introduction

Although the issue of defence logistics has been around for as long as battles have been fought, the scale and complexity of the logistics systems has increased exponentially as conflicts have become aggregations of allied forces interacting with civilian and non-governmental groups attempting to respond to the rapidly changing needs within the battlespace itself.

Although technology has been brought to bear and has enabled rapid communication across a single supply chain application, this is proving to not be enough. The use of different applications within a single force's supply chain, and the need to pass information rapidly and effectively up and down a complete chain of different groups means that monolithic standalone applications are now becoming more of a hindrance than a help in the logistics arena.

What is needed is a different approach: one that combines open standards, interoperability and flexibility in a secure architecture, while still allowing the various groups within the existing logistics chain to continue to participate with minimal changes to their existing systems.

The best approach to this is through the use of a services oriented architecture (SOA). Here, functionality is made available as services that can be called as required. Core functions can be shared across boundaries in a completely standardised manner, while security can be implemented at a highly granular level that enables different participants in the chain to have different access rights to information at different times. Existing applications can have their functionality surfaced as web services that can be peer items within the SOA environment, so maximising existing investments and enabling external parties to rapidly integrate their systems into the overall SOA-based logistics chain. Efficiency and effectiveness can be massively improved, and improvements in flexibility enable better response to the rapidly changing needs of front-line forces in today's battlespaces.

This report looks at the background of how defence logistics has reached the point it has, how this presents major issues to the effectiveness of a battlespace and how SOA can provide a platform for short and longer term needs. The report will be of interest to both military and civilian personnel involved in any aspect of defence logistics.

2. Background

Logistics is generally a mature market, with commercial systems being used heavily in many standard environments, such as manufacturing, retail, and business-to-business (B2B) supplies. Improvements over the past decade or so have concentrated on areas such as just-in-time deliveries, container and transport space utilisation optimisation, in-cloud B2B transactions and so on.

However, the defence markets have tended to stay outside of the reach of such improvements: existing logistics solutions have been created built on proprietary approaches, and any exchange of information between these systems and logistics systems used by civilian suppliers has tended to be based on either fully manual transcription or on highly specialised semi-automated systems. This can lead to slow response times, and also to transcription errors leading to the ordering and delivery of the wrong item, or of the right item to the wrong place.

While it cannot be argued that the battlespace should move to the usage of commercial logistics systems, the use of many of the commercial best practices need to be brought in to play, and flexible, standardised approaches will need to be introduced so that the intricacies and complexities of such a specialised environment can be effectively dealt with, and that the total defence logistics chain can be made more flexible, effective and cost optimised. Monolithic, bespoke systems do not have the flexibility or openness to deal with the complexities of today's logistics needs. A more open approach is required - one that is typified by a standardised service oriented architecture (SOA), based around the federated usage of a series of enterprise service buses (ESBs)

The scale and range of defence logistics is vast. Troops need not only a continuous supply of military equipment, including uniforms, armaments, ammunition and ancillary equipment, but also need rations as well as personal supplies such as mail and parcels from home. The battlespace commanders will need new assets to be delivered as required, which may range from medium-sized armaments through to tanks and helicopters. Battlespace engineers will require a capability for the rapid supply of a complex mix of spares to replace items that have either failed or been damaged in the field. On top of this, casualties may also need to be evacuated: high priority cases may have access to dedicated medevac resources, but many more may have a dependency on sharing their evacuation needs with existing transport being used within the logistics chains.

"The sheer quantity and range of different items that need to be dealt with in defence logistics dwarfs the majority of supply chains in the commercial space"

With defence logistics, many issues come to the fore. For a start, the sheer quantity and range of different items that need to be dealt with dwarfs the majority of supply chains in the commercial space. The variability in how such items need to be handled is also an issue: for example, rations for troops may be specialised and be in a form that can be stored for years and packed in containers that can be handled roughly, or they may be perishable and fragile supplies such as fresh vegetables and meat. Any system that aggregates such supplies into one "bucket" will tend to create a logistics nightmare where certain goods do not reach their destination as expected. The environmental needs of certain assets may need to be specially dealt with so that it meets the specific conditions of its point of use, and this may mean that changes are required to the item as it moves down the supply chain. The innate dynamics of a battlespace situation means that the requirements for logistics may also be changing, in as much as the types of supplies required and the point of delivery may be changing. Even relatively major distribution points in the battlespace may need to be mobile.

To get to the battlespace, the logistics feed starts from the component supplier, which may well be a standard civilian commercial entity, or may be a specialised defence contractor, but still operating as part of a civilian organisation. These components may need to be assembled, often by another civilian entity, and the assemblages need to be put together as a final item - or as a super-assembly that is required by the point of delivery. Up until this point, the items under consideration will generally still be in a non-aggressive theatre, and the main issues being dealt with will be information security and speed of fulfilment. Much of the logistics being carried out here will be relatively standard, and commercial systems may well be used to manage the flow of goods and information.

From this point, the assets may well be under the control of a fully militarised system. The assemblages and items that have been delivered from the civilian groups will be aggregated at specific depots, either in the military group's home country, or at bases in friendly countries closer to the envisaged point of need. From here, the items may well be repackaged and be sent to in-theatre depots ready for distribution. In these depots, the items will be broken down ready to move to the point of need itself. Even at this point, the overall delivery may still be as an aggregated collection of items that are required by a group of different battlespace points. These items are then delivered to a forward point final depot, from where the items are delivered directly to the point of need.

Throughout this chain, new items may be added, assemblages built upon and items removed as required for delivery or use by the depot where the items are being dealt with.

Although the logistics processes need to be better formalised to ensure that automation and efficiencies are improved, it is also apparent that the systems have to be massively flexible and capable of integrating with a raft of other standardised and non-standardised systems. Therefore, any defence logistics solution chosen cannot be prescriptive or proscriptive in how it lays down its technological capabilities: whatever is chosen as a system must be capable of being flexible now and in the future. Quocirca believes that the only approach that provides a suitable flexible and open, yet secure, platform for managing defence logistics is one based on SOA, built on open standards but configured to provide the granularity of information sharing and security demanded by defence logistics.

This report is a partner report to "Standardised Battlefield SOA", which gives more depth on the concepts of a SOA architecture itself. This report looks specifically at the needs of the battlespace, but lays the foundation for an overall need for a unifying platform across defence environments. The report can be read and downloaded freely here: http://www.quocirca.com/reports/22/standardised-battlefield-soa. A section from this report describing SOA in more detail is contained within this report as Appendix A.

3. Defence logistics

Main findings:

- **Although defence logistics have been around for a long time, much can be done to provide better efficiencies and greater effectiveness.**
- **Changes in the manner in which modern warfare is waged means that different logistical approaches have to be looked at.**
- **The need to interoperate with other military, quasi-military and non-military groups means that a pre- or pro-scriptive approach cannot be taken.**

The need for defence logistics goes back to ancient times. "Scorched earth" tactics were used by many a general to prevent attacking forces living off the land, so stressing their supply chain and minimising their capabilities to maintain a full military campaign. Successful campaigns have invariably been supported by well thought out and implemented logistics. For example, Alexander the Great could not have created his empire without ensuring that his armies were well supplied by a series of highly dynamic logistics. As he invaded and consolidated new territories, Alexander ensured that new central supply depots were rapidly built and manned, so keeping his supply chains relatively short.

Napoleon and Hitler both managed their supply chain logistics well in the major parts of their successful campaigns, but came undone where longer chains were involved. Napoleon lost in Egypt and in Russia as his supply chains became too long for rapid responses to be made, and Hitler's campaign was fatally impacted through the lack of his logistics capabilities to manage the issues of the Russian Front through a hard winter.

In more modern times, the US struggled with the need for a highly dynamic logistics capability in 1960's Vietnam, where the "front line" was no longer definable, and troops and assets were distributed over large areas with a need to be continually mobile. It was during this conflict that the helicopter proved itself as a battlespace logistics vehicle: its rapid means of getting in and out of a battlespace meant that it could supply small groups of troops effectively. However, such logistics are not cheap, and it did not take long for the Vietcong to realise that a helicopter could be brought down from the skies just as easily (if not more so) as a vehicle convoy could be stopped on the ground - and that such an attack could have far greater impact than attacking a convoy.

The Gulf Wars of the 1990s and 2000s have also shown how a more guerrilla-style conflict can lead to logistic issues, with the need for assets to be moved from one part of a country to another in short order. The mixed logistics operations employed here have shown the various strengths and weaknesses of each approach, when faced with insurgents capable of employing improvised explosive devices (IEDs) against road traffic, and rocket propelled grenades (RPGs) and surface to air missiles (SAMs) against helicopters. Increasingly, the logistics function has become just as much part of the battlespace, requiring its own defence support functions and also planning for how best to get mixed supplies in and out of a hostile environment.

"Napoleon and Hitler both managed their supply chain logistics well in the major parts of their successful campaigns, but came undone where longer chains were involved"

In its simplest form, a defence logistics process is shown in Figure 1. Here, original parts are manufactured which are then either built into assemblies directly or are supplied to another commercial entity who adds value through further assemblage. These items are then sent through to a centralised storage depot, from where items are then shipped closer to the point of need. From these distribution centres, items are shipped to battlespace distribution depots and are then provided to the front line as required. Defence procurement, in this case, is involved in the ordering of any additional items that are required between the main depots and the suppliers. In other cases, procurement will be involved at the initial contract stages, but in a battlespace situation it is far more likely that procurement will have a more passive role, mainly in ensuring that items are on the existing preferred list and that costs are being kept under some semblance of control.

Simple defence logistics

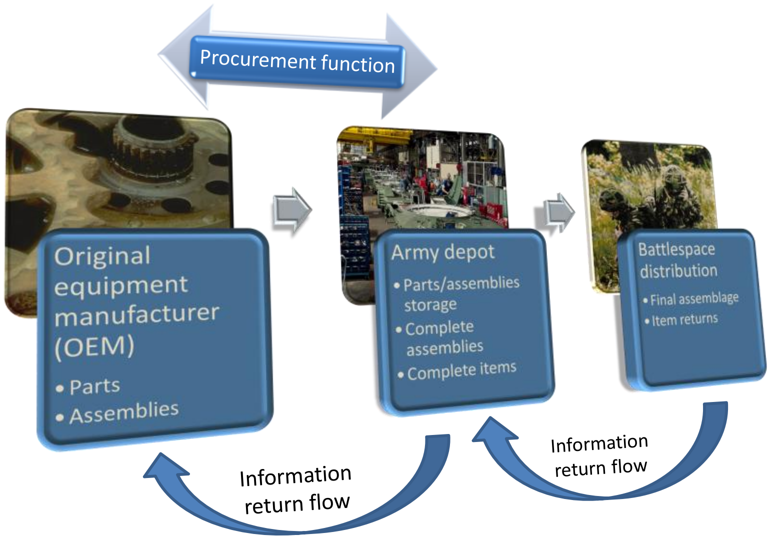

Figure 1: Simple defence logistics

To ensure that the whole logistics chain can be kept fully optimised, any issues with items anywhere need to be captured and information has to flow back up the chain so that suitable actions can be taken.

What is battlespace logistics management?

"The necessity of accurate and rapid reporting against a set of events across the whole of the chain has to be taken into account"

Battlespace logistics management can be split down into three different types: theatre support, external support and systems support. Theatre support is the provision of items needed within a theatre operation, and is provided at a low level of granularity. For example, theatre support may be focused on ensuring that uniforms are provided: this will not be of the order of tens or even hundreds of uniforms, but in getting thousands of uniforms to the theatre of operations. External support tends to be provided within the theatre itself, but is provided either by the host nation's military logistics or via in-theatre civilian logistics teams (via agreements such as the DoD's Wartime Host Nation Support (WHNS) approach). In the vast majority of modern battlespaces, theatre and external support will be provided by civilian commercial entities. Systems support, which is taken as being focused on weapons systems and other battlespace military assets, will be supported by more "trusted" logistics capabilities, generally provided by a mix of the military and the direct supplier.

Existing approaches

Since 2001, the US Department of Defense (DoD) has used a procurement approach called Performance Based Logistics (PBL). With PBL, civilian logistics operators are paid based on a guaranteed level of performance and system capability, rather than on the number of items bought. This therefore puts the onus on the civilian logistics company to ensure that the logistics are fine tuned, minimising inventory and enabling non-functioning items to be rapidly turned around and returned into the battlespace. Invariably, the PBL drives logistics companies and original equipment suppliers to work closely together to ensure that supplies and logistics are closely linked in how they operate together. For those working in the systems support environment, PBL has led to marked improvements in asset availability, in cost control of inventory and in battlespace readiness and availability of key assets.

The US Army also uses the Logistics Civil Augmentation Process (LOGCAP), which enables civilian contract logistics capabilities to be utilised for the support of auxiliary logistics, with the US Air Force and the US Navy having equivalent agreements, the Air Force Contract Augmentation Program (AFCAP) and the Construction Capabilities Program (CONCAP) respectively.

Similarly, the UK Ministry of Defence (MOD) uses its Contractor Logistics Support (CLS) system. Under this exists the Contractors on Deployed Operations program (CONDO), which looks at how civilian contractors can provide support to military logistics.

Similar approaches exist within the vast majority of modern defence teams, meaning that the logistics chains are a complex mix of differing systems with little commonality in function, in data structure or in standards.

Baselining battlespace logistics

For optimised logistics, the mantra is "observe, orient, decide, act". Battlespace intelligence is required to provide the baseline against which the logistics process starts. If a non-active battlespace condition is used as the starting point, logisticians will need to know what kinds of assets will need to be deployed, in what order, how many of each and when. Getting everything to the right place at the right time, often with the utmost secrecy, means that standard usage of mass logistics is often unusable, and highly specialised systems, such as aircraft drops, concealed provisioning and so on are required.

Once the assets are on the ground, many of them will need to be deployed to primary active positions ready for use. However, each active deployment will still require a backup system of spares and supplies positioned near enough to the active assets to give rapid support, yet centralised enough so as not to spread the support structure too thin across an active battlespace. These backup systems must, however, be fully supported themselves, so as to be secure and protected against capture or damage by enemy action.

Once the battlespace becomes active, the condition and location of the assets will become highly dynamic, and new field intelligence information will begin to come in on the status of assets and the components within them. Field logisticians then need to be able to respond rapidly to the changing status of the battlespace, ensuring that spares and supplies are rapidly deployed and redeployed as needed, second guessing the needs of the forces, and also ensuring that supplies and spares are not left in positions where they are of little use, where they are at risk of being destroyed or of being captured by opposition forces.

For many battlespace assets, proactive logistics can help to ensure that assets remain in an active condition for the greatest amount of time possible. Through the use of general purpose sensor architecture (GPSA), the performance and status of components within, for example, armoured vehicles, helicopters and weapons systems can be monitored in real time. If a tank is found to be running light on fuel, it can be pulled out from the battlefield and sent to the right supply depot for refuelling, ensuring a rapid return to availability. A helicopter with an oil pressure problem can be pulled out and sent to the nearest position where a suitable spare is available, ensuring that a repair can be carried out rapidly and safely, returning the helicopter to readiness as soon as possible. The focus here is to maintain active condition of assets as much as possible through constant monitoring of consumables status and for the possibility of component or assembly failure.

Civilian sector best practice

The practice of maintenance, repair and operations (MRO) is well known in the civilian space, and best practices already exist in how best to manage the flows of spares and resources to ensure that maintenance and repairs are carried out in the most effective manner. For example, processes exist to evaluate whether it is more cost effective to attempt a repair in the field or to request a return to base (RTB); whether a set of replacement sub-assemblies should be sent to attempt a repair, or just send a swap-out asset; and whether a replacement item can be sent out for field replacement by the user, or whether a skilled resource will need to be sent to effect the replacement. Although the battlespace does introduce specific issues (e.g. few civilian MRO operations will involve having to repair items under enemy fire), Quocirca recommends that defence logistics specialists do look at how geolocational, isochronic and least cost pathways are used in the civilian MRO logistics space to ensure optimised operations.

Even taking care of logistics and ensuring that a battlespace is kept supplied with the items it needs is still not enough in ensuring an effective battlespace capability. For example, asset reconciliation is needed: were items requested actually delivered, and if not, have they gone astray to a different location, or were they mislaid or stolen? In all of these cases, where was the last known place the assets were logged, and where are other assets situated that can be used to meet the needs of the original requirement? The necessity of accurate and rapid reporting against a set of events across the whole of the chain has to be taken into account.

Complexities of mixed environments

Adding to the problem is the need to work in a mixed environment. Although NATO and the UN have pushed hard for standardisation of items across different defence forces, this has not been pushed into how logistics are managed. Therefore, even though there is now general standardisation across areas such as the calibre of small arms ammunition and in certain vehicle and other asset spares, it is not always easy for one group in a battlespace to ascertain whether items that they need are available locally from a friendly group, or whether the items will have to be brought in from a more central depot away from the battlespace. If the latter is chosen when the items are available more locally, not only is the process less effective than it should be, but the effectiveness of the whole battlespace may be compromised. Even where a degree of visibility is possible, other problems can get in the way. For example, one defence force may have a catalogue number for a certain item that is different to the catalogue number used by another force. Therefore, even though items may be available locally in the battlespace, the requesting force may not realise that this is the case, and so have to go for a slower and less effective centralised logistics request and supply process.

The whole set of logistics processes are dependent on information and physical items being able to flow in both directions - both downstream towards the battlespace and upstream towards the supplier. Logisticians have to be able to gain an immediate view of where items are and what demands are being placed, and to pull everything together to ensure that demands are met in the most optimum manner - balancing immediate need, logistics capability, item availability and cost of supply against cost of non-supply.

When the issues of modern defence logistics are examined, it becomes obvious that there is a strong need for a more flexible and dynamic architecture to underpin activities. This architecture is available using web services in a service oriented architecture (SOA) model. To fully understand how SOA can help, it is important to look at the problems that defence forces are currently facing with their logistics in real situations.

"For many battlespace assets, proactive logistics can help to ensure that assets remain in an active condition for the greatest amount of time possible"

4. Challenges within existing approaches

Main findings:

- **Extended supply lines and lines requiring aggregation of items across a broad geography leads to a need for greater monitoring and control.**
- **Gaps in the logistics chain caused by the lack of interoperability between different systems not only causes process inefficiencies, but can have a detrimental impact directly on the battlespace.**
- **Lack of common data models can lead to wasted resource in supplying the wrong item to the battlespace.**

The main issues that occur across a traditional defence logistics capability include:

- Lack of integration between diverse systems.
- Lack of visibility across the whole chain, including the lack of capability to monitor and report against activities to ensure the requisite knowledge of where items are and how quickly they can be sourced to a different area.
- Breaks in informational flows up and down the chain.
- Lack of correct configuration of items for the environment.
- Errors introduced in transcription between various systems.
- Speed of response constraints introduced through breaks in automation capabilities.
- Lack of commonality between item identification across multiple systems.
- Maximising efficiencies across multiple logistics choices, maintaining effectiveness of supply at optimum cost.

The best way to take a complete look at the issues involved is to take a real-life example. For this, Afghanistan provides a suitable case. As an active battlespace with multiple active fronts and a guerrilla-style war being fought, Afghanistan typifies the sort of problems increasingly faced by logisticians in modern warfare. The International Security Assistance Force (ISAF) was set up by the UN in 2001 under the Bonn Agreement, and provides a force that is split across 5 regional areas of command.

Outside of the main conurbations, the population tends to be tribal, and the major tribal leaders maintain their own militia. However, these groups often come together with a view of fighting a common foe: in the current battlespace scenario, the coalition forces are viewed as the enemy, by some from a religious viewpoint and by others as a threat to their commercial activities, in growing opium poppies and trading drugs, guns and people. The insurgents are well supplied with rockets, small arms, mortars and IEDs, so both air and land operations are hazardous. As of February 2010, there were around 86,000 coalition troops in theatre, from 42 different countries with continuous rotation. Added to this, the Afghan National Army (ANA) comprises of some 100,000 personnel, and another 100,000 in the Afghan National Police (ANP). Over 90% of ISAF activities are undertaken in conjunction with the ANA.

Afghanistan:

Area: 652,000 km² (landlocked)
Borders: Pakistan, China, Iran, Tajikistan, Turkmenistan, Uzbekistan
Elevation: 260-7,500m
Temperature: -52.5°- +51°C
Climate: Mainly arid
Infrastructure: Main roads metalled, others mainly dirt tracks

For logisticians, getting equipment into Afghanistan is no easy task. Although Bagram airbase can be used by large supply aircraft (e.g. C-5 Galaxy, C-17 Globemaster and Boeing 747), the airbase is not deemed as secure against ground-to-air missile attack. Therefore, much logistics is carried out as a mixed sea/land operation. 75% of goods are landed at Karachi in Pakistan, from where they are then shipped by land convoy 1,700km to Bagram, having to cross the Khyber Pass. As a strategic bottleneck, the Taliban has focused on trying to gain control of the Khyber Pass and, to remove the Khyber Pass as a critical weak link in the supply chain, US logisticians have also been using an alternative route through Chaman in Pakistan through to Kandahar in Afghanistan. However, this route is also now coming under increasing pressure from insurgents. Even without direct contact, the capability for insurgents to blow up strategic bridges can effectively close supply routes for days on end, and leave supply convoys in critical positions while repairs are made. It is expected that Russia will now agree to open up a new route through its land, using rail routes to get non-military supplies through to Kazakhstan then through Uzbekistan to reach Afghanistan. Russia is also expected to provide enhanced support for the Russian helicopters and vehicles used by the Afghan forces.

For the existing routes, even while the convoys are in Pakistan, attacks by the Taliban cannot be discounted, and even attacks by groups of thieves are relatively commonplace. Once in Afghanistan, planned and co-ordinated attacks by insurgents are far more likely. Local drivers, highly paid to drive tankers and lorries over the Pass, have been known to also be under the pay of the Taliban and will work to sabotage the convoy, or to abandon the vehicle in the middle of the road and make a run for it when trouble starts.

This all makes for a constant problem for logisticians. Supplies from the NATO forces have to be suitably aggregated at shipping ports to fill a ship enough to make a sea-borne delivery effective. The balance of speed of response against cost and risk has to be calculated: the need for a tank to have a track replaced may require faster delivery of spares than can be managed by placing the replacement track on a boat, getting it to Pakistan, loading it onto a vehicle and driving it 1,700 km through difficult terrain. However, such a heavy item will cost a lot to fly in by transporter and from a central base to then use a Chinook helicopter to get the track to where it is required. Contextual knowledge is needed: is the existing track fixable? How important is it that the tank be made serviceable again and in what timescale? Can a temporary fix be implemented until the spare can be made available?

Another issue is in configuring assets to be suitable for the environment. As well as the standard configuration of whether this is to be a troop carrier, a cargo, a medevac or other kind of helicopter, it is necessary to make a decision as to how the helicopter will need to be set up for its use in theatre. Is a helicopter being supplied into the mountains, where low temperatures are a major issue, or into the plains, where dust is a bigger issue? What type of blades should be fitted - ones for maximum speed or maximum lift? What sort of grease is needed - thick to deal with large temperature changes or thin for a more stable temperature range? What types of air filter need to be fixed, and how often will they need to be changed? What types of auxiliary batteries need to be fitted? Some of these decisions can be made back in major depots, others may have to be left until the helicopter is already in theatre.

"The US military uses around 1.8b rounds of small arms ammunition per annum, with the majority being used in Iraq and Afghanistan"

When it comes to one of the most used and required supplies - small arms ammunition - the US military uses around 1.8b rounds per annum in total, with the majority being used in Iraq and Afghanistan. The rate of usage is so high, and the issues with supply direct from the US so problematic, that deals have had to be set up with Israel (and the UK has an agreement with Pakistan) for the provision of ammunition to help meet demand. The need to get ammunition to forces on the ground at a suitable rate cannot be underestimated. A ground force can only carry so much ammunition with it, yet when it comes to be under fire, will use up its supplies rapidly. Ground-based resupply will not always be possible, and air-based resupply will have to be resorted to. However, the presence of helicopters tends to draw enemy fire, and these assets must then also be protected, either by troops in the helicopters themselves, by helicopter gunship support for strafing and targeted cover, or by air fighter and bomber support to provide sufficient bombardment to subjugate the attacking force for as long as is necessary to enable the resupply to take place.

Even so, problems can still arise at the point of supply. In 2008, a $300m contract signed with Miami-based AEY Inc was suspended when the ammunition supplied was found to be 40 year old Chinese stock in a poor state, rather than the Hungarian stock promised. Then, at the point of usage, things can go wrong. It is suspected that many of the Afghan military and police forces being trained and armed by the coalition forces are providing their guns and ammunition directly to the Taliban. Certainly, US ammunition has been found on the bodies of insurgents. However, it is incumbent on the ISAF to ensure that the 200,000 Afghans involved in the ANA and ANP are suitably provisioned so that they can be fully trained and involved in the transition to handing over an increasing responsibility in the running of the country.

What we see in Afghanistan is a major mix of different groups, from the various defence teams that constitute the coalition forces, through groups that have to be viewed with a degree of circumspection, such as the Afghani military and security forces, through civilian groups that will include Western supply and logistics companies and local individuals employed to drive vehicles and act as interpreters and local factotums. Different technological systems will be in place, different assets with different capabilities will need to be supplied and kept in service. Information flows across the theatre and back to major depots and tactical headquarters will need to be maintained. All of this has to be done to maintain operations across multiple fronts, in a generally hostile environment against a guerrilla opposition force.

Flexibility is required, and existing systems must be reviewed as to their efficacy in supporting this new type of battlespace situation.

5. SOA and service bus in defence logistics

Main findings:

- **Interoperability has to be seen as the main issue for defence logistics: security of information flows and the need to enable and disable access to supply chain processes has to be covered.**
- **A flexible, functional approach, where existing technologies can be used in a multi-modal model provides the optimum, least cost/greatest flexibility end result.**
- **Any solution chosen has to be able to deal with a mix of high and low bandwidth environments.**

Defence logistics will involve information and physical item flows up and down a complex environment. Unlike the standard commercial sector, this environment will include a mix of commercial civilian and defence systems, each of which will have its own set of inputs and outputs. However, the necessity for speed dictates that information flows in both directions have to be in near real time, and manual interventions must be kept to an absolute minimum.

A defence logistics environment will also have other constraints on how it can all work together. At the battlespace environment, the network system will be a mix of very low, low and higher bandwidths, and will be subject to constant issues as parts of the network are destroyed, fixed or redeployed. Within itself, the maintenance of network capability is a logistics issue, with the supply of network kit being a high priority in a space where information flows can define who will gain pre-eminence in a battlespace condition.

Likewise, hard-coded connectors between one system and another should also be avoided, as this will prevent either side from making changes to their system as and when required without it having a possible impact on the other partner's capabilities. In particular, hard coding impacts the capability to rapidly include and exclude groups in to the logistics chain. A local logistics company may need to be included at one stage, but as soon as the group is perceived to have been compromised (e.g. drivers having been bribed or otherwise coerced by local insurgents), any access the group has to the logistics system will need to be effectively removed.

The only realistic way in which to ensure that a highly flexible and dynamic logistics solution can be put in place is to use a bus approach. Here, all connectivity is dealt with through a unified capability (see Figure 2). Any function within a system can be connected to the unifying SOA backbone through the provision of a connector. For many commercial systems, such connectors will already be available; for other, more proprietary systems, a connector can generally be created in a short time scale. The idea is to create a method in which any system can talk to any other system by using the capabilities of the connector and the unifying SOA environment. A main part of an effective SOA implementation therefore has to be a backbone, or an enterprise service bus (ESB). In this manner, logistics solutions within the defence organisation's control connect through to the bus, and the bus provides secure and highly functional transport and translation of data through to the individual connectors where data is required to flow through to those parts of the logistics environment that is outside of their control. Therefore, any compromise of security can be dealt with easily and rapidly by revoking the external connection. Also, each connection can have its own definable capabilities, such that, for example, a defence partner can have access to a greater depth and breadth of information than commercial suppliers.

SOA in defence logistics

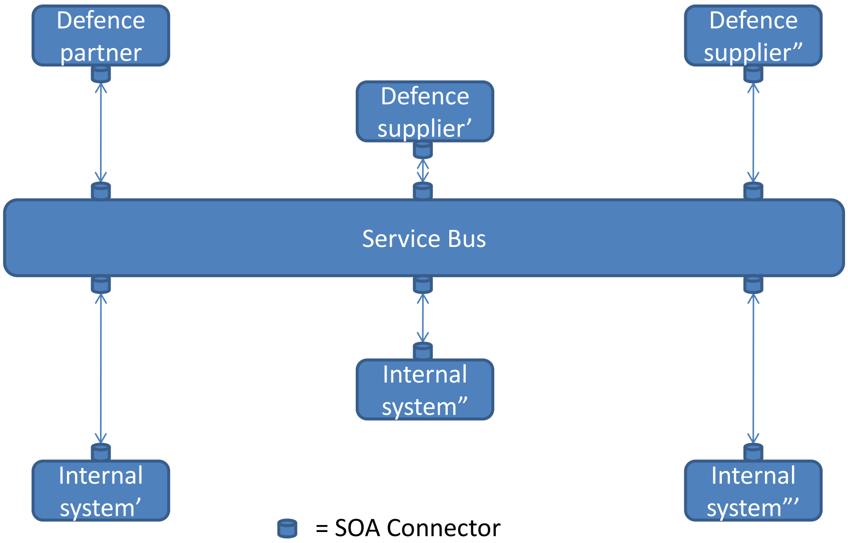

Figure 2: Service bus in defence logistics

Indeed, SOA provides the best way for defence logistics to operate. Functional components of existing applications can be surfaced as discrete capabilities that can be used as core centralised points of reference within the chain. For example, one member of the chain could create a master data model, and could "own" this database on behalf of the other members of the chain. Whenever any member of the chain wants to refer to an item in the chain, they use this master data as a reference point, and the security of how other databases interact with this can be controlled via SOA and the service bus. In this way, everyone operates against a single item description - manual matching of one group's catalogue number against another group's different catalogue number is not required: simple look-ups against the master data model can be carried out ensuring full commonality of reference across the whole chain.

Even where such cooperation is not feasible, the service bus and SOA approach provides a means of information exchange on a far more formal and efficient basis than is found in the disparate systems of today. By defining a "service", the data structure required for this service to take inputs and provide outputs will have to be codified. Functions within existing applications can therefore be connected to the service bus: information can be structured such that the application sees no difference between the incoming data stream from the service bus and its normal mode of operation, and information can be taken from the application for use within the more flexible SOA environment. As the service matures, its information needs may change, and all that will need changing is the service connector between the service and the enterprise bus being used in the defence logistics chain.

In Figure 3, the different needs of example stages in the logistics chain can be seen. Within the commercial sector, it will often be the case that connectors will be available to interface with the standard commercial logistics systems in place. Even with older systems, or even home-grown systems, it is generally relatively easy to create the requisite connectors that can either provide the business logic required to make the system a full peer part of the logistics chain or, at a bare minimum, ensure that information feeds are transposed in both directions to meet the needs of both the application and the general logistics chain itself. Once we come into the defence realm, however, we may need to create specific connectors that can deal with existing systems that ensure specific security needs are met, or that reflect the specialised nature of the capabilities of a battlespace.

Interfacing defence logistics

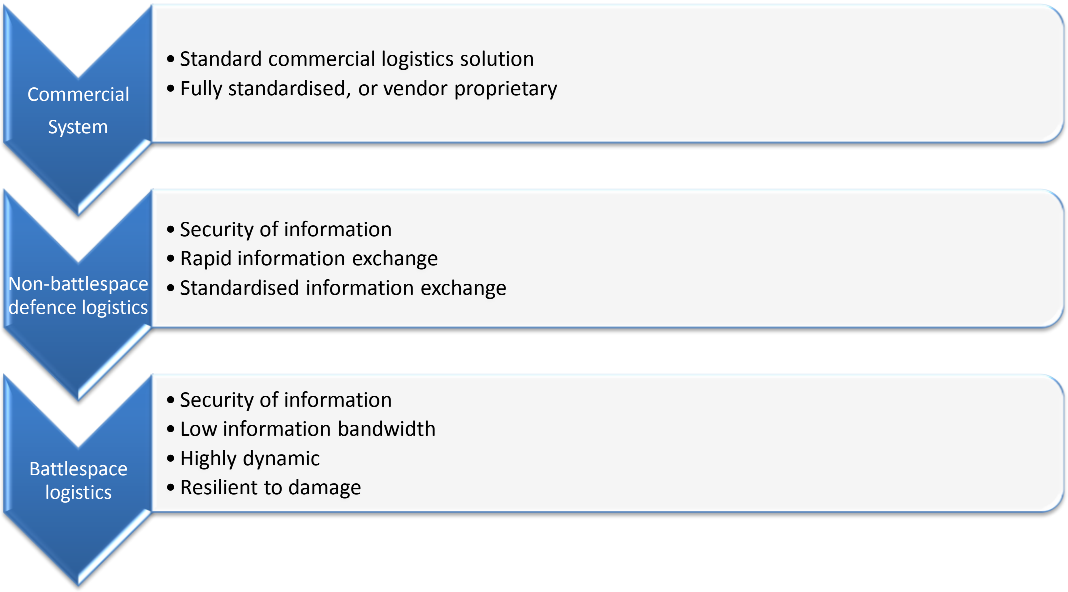

Figure 3: interfacing defence logistics

Figure 4 shows how logistics within the battlespace itself may be needed. Increasingly, battlespace assets will be heavily monitored via sensors, and any anomalous activity will trigger alerts that can be picked up by systems around the battlespace. RFID, or other near field systems within the assets, can send small amounts of data to a meshed communications environment based on WiFi, 3G/EDGE/GPRS or UWB systems that can then feed information back to a more centralised environment via resilient redundant wired systems.

Such an approach can ensure that any asset in the battlespace can be continuously monitored for failure at both a component and an overall asset level. In this manner, the overheating of, for example, a cooling system within a tank caused by the clogging of an air filter by dust can be seen before it becomes too much of an issue. Low-bandwidth hardened meshed WiFi systems can continuously monitor systems in the battlespace itself, feeding back to front-line wired systems, which will, in themselves, integrate with the greater supply chain back to logistics centres and suppliers. At the same time as the tank commander is informed of a possible problem, events can be initiated that identify where the nearest spare filter is, and how it can be brought closer to the active battlespace. The filter, the tank and the engineer required to fit it can then be brought together in a less dangerous position outside of the battlespace and the filter can be changed, enabling the tank to be redeployed back into the battlespace. Without the capability to monitor at a granular level and to integrate information flows across a range of different systems, it would be far more likely that the tank would suffer a more catastrophic failure in the battlespace itself, endangering its crew and compromising the battlespace situation. In this case, the use of SOA at the tank level through GPSA, integrated through federated ESBs to other parts of the logistics chain, ensures that equipment is kept working as needed.

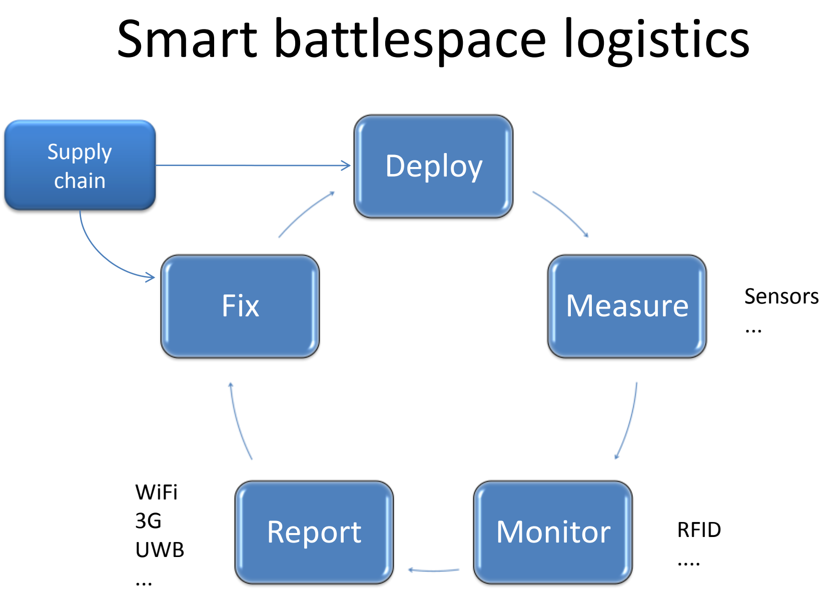

Figure 4: Smart battlespace logistics

Quocirca believes that a SOA approach to defence logistics offers the greatest capabilities to all parties concerned. The logistics chains can be opened up as necessary, while still maintaining full levels of security. Groups and individuals can be added and removed as necessary, and different levels of information access can be provided. Master data models can be implemented across the complete logistics chain, ensuring accuracy of information flows up and down the system. Speed of response and accuracy of supplies are improved. Flexibility is provided for the future, enabling forces to be rapidly deployed across existing and new theatres while still enabling defence logisticians to see the complete picture and to minimise the need for massive oversupply of supplies to try and ensure that no one specific theatre is left under supplied.

6. Use case scenarios

To enable a clearer picture of how SOA can be used within a defence logistics environment, it is best to take a series of different use case scenarios. The idea here is not to give a total factual picture of any real life cases, but to give a high level view of the types of issues defence personnel and defence logistics specialists have to deal with, and how SOA can help in ensuring that such issues can be more rapidly and effectively dealt with.

6.1. Deployment planning

Prior to any defence deployment, there will be a vast amount of information being exchanged between on-the-ground intelligence personnel, command personnel and other defence and civilian groups. Based on this information, decisions will have to be made on how much of what type of assets will need to be deployed across the total battlespace theatre. These decisions will also need to take into account where these assets are already, what state of readiness they are in and also whether the assets are suitable for the conditions the battlespace will present.

For example, a decision to deploy more assets into a desert environment may show that there are sufficient helicopters available in a state of readiness for “standard” use. However, that definition of “standard” may not mean that the helicopter is ready for use in the environment it will need to be deployed into. For example, it is also necessary to ensure that the rotors fitted are suitable to withstand the harsh abrasion of sand in the desert air, and that the air filters in place can deal with the dust and dryness of the environment.

As it is unlikely to be the case that a “standard” configuration helicopter will meet the exact requirements, events need to be triggered to identify where the correct components are being held, identify the most effective transport to get them from where they are to where they need to be, and the correct resources that can rapidly and effectively exchange the existing components for the new components. To add further complexity to this is the question as to where the exchange takes place - at the place where the helicopters are currently, at the target environment, or at some midpoint depot between the two.

SOA helps here in being able to interface between the various tools being used along the logistics chain. The current state and position of the helicopters will be held within the defence group’s own databases, whereas the position of suitable spares will be a mix between existing inventory held by the defence group and the availability of spares from the supplier. The decision as to where the replacement takes place will be dependent on decisions made by the battlespace commanders, and this will impact the decisions that need to be made by logisticians as to the type of transport required to move both the helicopters, the spares and the right skills to the right place at the right time. By using connectors between a service bus and the various applications in use, such interchange of information can be easily carried out - and the right levels of security can be applied as well.

Indeed, by taking a SOA approach, the various functional parts of applications along the logistics chain can be broken down and used as single points of function as required, so reducing functional redundancy and enabling much better optimisation of the whole chain.

6.2. Vehicles out of readiness awaiting spares

In the harsh conditions common to many battlespaces, the failure of small components can mean that assets need to be removed from the battlespace until they can be fixed. Not only does this mean that vital assets are unavailable for a period of time, but often significant amounts of skills and resources are tied up in identifying what the root problem is and then in finding spares, getting them moved to where the asset is and then fixing the problem.

With SOA and smart asset monitoring, many issues can be seen proactively. By the use of sensors in battlespace assets, status information can be fed back to local and central command centres on any issues that could cause an asset to fail. Therefore, prior to the failure happening, the asset can be removed from the battlespace to a point of relative safety.

At the same time, information from the sensors can be used to identify what component is likely to fail, and SOA can then be used to identify where the nearest replacement parts are, along with how best to transport these parts to the battlespace and, if necessary, how best to transport the replaced part either to a point away from the battlespace (for security reasons) or back to the supplier (for examination reasons).

6.3. Asset recall and replacement

The failure of a component is generally due to the specific circumstances surrounding the use of the individual component. However, it can also be that the initial design or manufacture of a component can be defective, which may only become clear once failures start to happen in the battlespace.

In this kind of failure, it is imperative that all assets using the component be serviced as rapidly as possible and the component replaced. However, within a battlespace environment, managing such a massive issue can be highly problematic.

It is necessary to have a full inventory of assets that are currently using the component. This also needs to be cross-referenced with where the assets are - the data for which will generally be held in a completely different database - and can cover assets that are at a central depot, those that are in transit and those that are actively deployed. This information needs to be available across the supply chain, so that front line logisticians, as well as suppliers, can see the scale of the issue and can work together to remedy the problem. It may well be that there are already other components near to hand which could act as a replacement, even if only for a period of time so that some level of readiness can be maintained. However, if it becomes apparent that battlespace readiness will be impacted due to the lack of component availability, a broader search may have to be carried out to identify what other assets can be deployed to the battlespace, by what means and within which timescales. Finally, the delivery of the replacement components to central depots, to in-country distribution points and to the battlespace itself will need to be dealt with. Again, this is a complex mix between the various different types of transport available, the timeliness of delivery required and the cost of each type of transport. The logistics chain will cross over the lines between supplier, the defence group and civilian groups in multiple different ways as the information flows impact the physical chains of component and asset moves. Again, this involves information that is held across multiple different systems, from basic supplier catalogues through supply chain rosters and cargo manifests to battlespace activity records. Only through the use of a SOA approach can such diverse information sources be pulled together and actions taken that ensure that everyone concerned is kept informed of the changing situation.

Within a PBL/CLS environment, managing the complexities of such component recall and replacement issues can heavily impact the profitability of a deal, and it is in the best interests of the supplier to optimise the information and physical supply chains as much as possible.

6.4. Shared spares and supplies

The majority of battlespaces are no longer a situation between two highly defined groups of protagonists. The pattern now is of groups, such as NATO, the UN or a group of allied forces, facing a similar group of antagonists. Information superiority can define who gains the upper hand in any confrontation.

However, each party within the group will have their set of data that they are working against, and will share this data as necessary. Security has to be a priority, and yet the groups have to be able to respond to each others' needs in real time.

Within the logistics environment, this may mean the sharing of spares and components, or even of complete assets. For example, over time, NATO has managed to standardise on many aspects of battlespace assets. Ammunition calibres are now relatively standard, voltages used within equipment have been standardised. Vehicle and other mobile asset spares are becoming more standardised, and even consumables for combatants are being standardised.
This does mean that if an asset has a component failure, the owning party may not have a spare, but an allied force may be better positioned to provide the spare than the owning party's own logistics chain can. Therefore, it is important to enable two-way communication across the various data stores and applications being used by allied forces, such that the overall force readiness is always at an optimal level. No single force is in a position to dictate to other forces how their information communication capabilities should be configured, though. Again, SOA can solve issues across different information schemas and models by enabling the transposition of data at the connector level, taking information flows into and out of systems and reconfiguring them on the fly to meet the needs of other systems. Therefore, each group can continue to use existing systems, but can create a high level of informational fidelity up and down the logistics communication chain.

However, such "openness" also has to be flexible. For example, the training of nominally friendly forces could mean that such communication flows are required to maintain the readiness of their own assets. Should these "friendly" forces be seen as a security threat, it may be required that the lines of communication be rapidly shut down. SOA enables this through the use of point connectors from the service bus. Where such a shutdown is required, the single connector can be closed, so cutting out the affected group while maintaining the availability to the systems for all other groups.

6.5. Battlespace logistics

Logistics within the battlespace itself show the greatest complexity. Here, nothing is static: forward deployment points change on a regular basis, assets are in constant motion, failure can be either through component failure or via opponent action. Storing large amounts of inventory in the active battlespace itself is not a viable situation - the inventory is at risk from damage due to enemy action, could be stolen and used by the enemy to shore up its own assets or, at the very least, ties up inventory and costs that may be more useful elsewhere.

Therefore, it is desirable to minimise the inventory at the front line itself, with a hierarchy of just-in-time depots and distribution points being in place. However, these all need to be tied successfully together so that responses can be made in real time, ensuring that asset availability is maximised in the battlespace.

This requires continual monitoring of assets, both locally and remotely. Those using the assets on the ground need to have proactive notification of any possible problems; those away from the direct field also need to be aware of these problems so that advice can be provided on alternative approaches, on when the asset needs to be pulled out or left behind, on how long it will be before a new asset can be provided, or spares delivered so that a fix can be carried out. If the asset is to be pulled out, the user needs to know where to and at what time. They need to know at what point do they hand over the asset, whether they get a replacement, a different replacement, or whether they need to stay with the asset until it is fixed. Others on the ground need to understand the impact that all of this has on them, and what steps are being taken to mitigate any such impact.

With disparate systems, this whole procedure becomes too complex to be viable. Information transcription between systems leads to errors, particularly in life and death situations where speed is seen as being the priority, rather than accuracy. However, manual transcription introduces high degrees of information latency as well, so both speed and accuracy are compromised.

SOA enables disparate systems to be brought together, and the use of an enterprise bus means that information flows can be completely automated, maintaining accuracy and optimising speed. By using sensors within battlespace assets, information and events can be triggered automatically, so freeing up the battlespace personnel to do what they need to be doing - not monitoring their own assets.

7. Conclusions and recommendations

The defence logistics environment is complex and dependent on many links in an extended chain. Existing approaches of using siloed systems and manual transcriptions between internal and external systems lead to errors and to issues in timing which can compromise the capabilities of a battlespace or a complete theatre of operations. The need to rapidly fix and redeploy assets within the active battlespace means that demands on defence logisticians are growing exponentially, and yet political pressure to minimise costs means that oversupply of items is not an option.

The use of SOA enables disparate logistics and supply chain systems to be pulled together in a secure and flexible manner. The need for different military, quasi-military and non-military groups to work together can be enabled, with different parties and individuals being given different levels of informational access dependent on their trusted relationship. If necessary, such access can be rapidly and effectively removed.

SOA also enables existing systems to carry on being utilised. In an environment where cost is a major issue, the capability to completely replace existing systems is not high: SOA enables existing systems to be made available as sets of functions that can be individually used within the overall logistics processes. Therefore, costs can be minimised while capabilities are maximised.

Through using SOA, information flows can be increasingly automated, cutting down on any need for manual intervention and removing transcription errors. The use of a common data model means that errors can be further removed, as system catalogues maintain views of what catalogue numbers refer to what items across the whole chain.

Overall, SOA presents today’s defence logisticians with the lowest cost, highest benefit approach to dealing with existing issues and providing a flexible platform to deal with issues in the future. While still using existing systems, SOA can be implemented to add additional functionality and capability. SOA does not have to be an impacting project: the capabilities can be introduced alongside live systems and defence logisticians, intelligence operatives and finance/procurement personnel can all start to benefit from the additional capabilities provided as systems are brought together, processes become more streamlined and information availability allows for greater visibility and monitoring of where assets are within a total system.

About IBM

IBM is committed to supporting and assisting Defence organisations as they address the challenge of transforming from the industrial to the net-centric age, investing in IBM's Global Defence Industry, a dedicated global team of Defence industry consultants, subject matter experts and solution developers that is focused on helping our clients achieve information superiority. Our Network Centric Operations solutions combine IBM's deep insight into Defence organisations with leading strategic consulting skills and unparalleled technical assets to help our clients forge a new path to more effective, efficient, and responsive operationally relevant capabilities. Our success is accomplished by building strong relationships with our clients and their partners, by completing complex systems integration projects on time and within budget, by providing consulting services, introducing innovative solutions, backed by IBM's extensive research and development capabilities, and underpinned by IBM's broad portfolio of technology offerings. For more information, please contact your IBM client representative, or visit: http://ibm.com/government/defense

REPORT NOTE:
This report has been written independently by Quocirca Ltd to provide an overview of the issues facing organisations seeking to maximise the effectiveness of today's dynamic workforce.

The report draws on Quocirca's extensive knowledge of the technology and business arenas, and provides advice on the approach that organisations should take to create a more effective and efficient environment for future growth.

Quocirca would like to thank IBM for its sponsorship of this report and the IBM customers who have provided their time and help in the preparation of the case studies

About Quocirca

Quocirca is a primary research and analysis company specialising in the business impact of information technology and communications (ITC). With world-wide, native language reach, Quocirca provides in-depth insights into the views of buyers and influencers in large, mid-sized and small organisations. Its analyst team is made up of real-world practitioners with firsthand experience of ITC delivery who continuously research and track the industry and its real usage in the markets.

Through researching perceptions, Quocirca uncovers the real hurdles to technology adoption – the personal and political aspects of an organisation's environment and the pressures of the need for demonstrable business value in any implementation. This capability to uncover and report back on the end-user perceptions in the market enables Quocirca to advise on the realities of technology adoption, not the promises.

Quocirca research is always pragmatic, business orientated and conducted in the context of the bigger picture. ITC has the ability to transform businesses and the processes that drive them, but often fails to do so. Quocirca's mission is to help organisations improve their success rate in process enablement through better levels of understanding and the adoption of the correct technologies at the correct time.

Quocirca has a pro-active primary research programme, regularly surveying users, purchasers and resellers of ITC products and services on emerging, evolving and maturing technologies. Over time, Quocirca has built a picture of long term investment trends, providing invaluable information for the whole of the ITC community.

Quocirca works with global and local providers of ITC products and services to help them deliver on the promise that ITC holds for business. Quocirca's clients include Oracle, Microsoft, IBM, O2, T-Mobile, HP, Xerox, EMC, Symantec and Cisco, along with other large and medium sized vendors, service providers and more specialist firms.

Details of Quocirca's work and the services it offers can be found at http://www.quocirca.com

quocirca

Appendix A: SOA – a proven architecture

Main findings:

- **Open standards provide the means for interoperability between heterogeneous systems.**
- **Complex events need flexible systems to analyse and report on them.**
- **SOA presents a long-term flexible approach to provide a more functional technical architecture.**

The key to creating a platform for communications and data transfer within any environment is to use open standards wherever possible. This enables the easy interchange of information between different systems, and also ensures that processes can be streamlined and more effective.

A service oriented architecture (SOA) is a technical platform based on open standards where applications cease to be the main focus for the provision of solutions to the user. Instead, small discrete functions are created which can be used as required within any process. As a simple example, we can look at the need for a timing component. Within a monolithic application, the code for managing a timed event will be generally built in to the application itself. If there are multiple such applications, you have multiple different means of managing a timed event (see Figure 5). If any one of these has a flaw within it, any dependency between the timing of events that cross the applications will fail. Further, any integration between applications tends to be done via hard coded connections, leading to further complexities. Within the concept of the common operating picture (COP), there may well be many different systems with different timing capabilities built in to them. The possible variances between the timing services could drastically affect situational awareness.

For example, if this were to happen within the targeting cycle, we can see a situation where one system could be analysing an event, and a decision made to eliminate the target with artillery. This analysis system could be using one timing routine, and calculates that a particular type of force should be used to destroy the target. The artillery round to be used needs to hit the target in so many seconds, and explode a fraction of second afterwards. This information may then be handed over to a fire control system, which repeats the calculations within its own systems and then fires the round. If the times were to be calculated as actual times (e.g. 10:04:05 UTC), then any issues with the core timing routines between the two systems would lead to the round being fired at the wrong time, hitting the target at the wrong point (or missing it completely), and/or exploding at the wrong time.

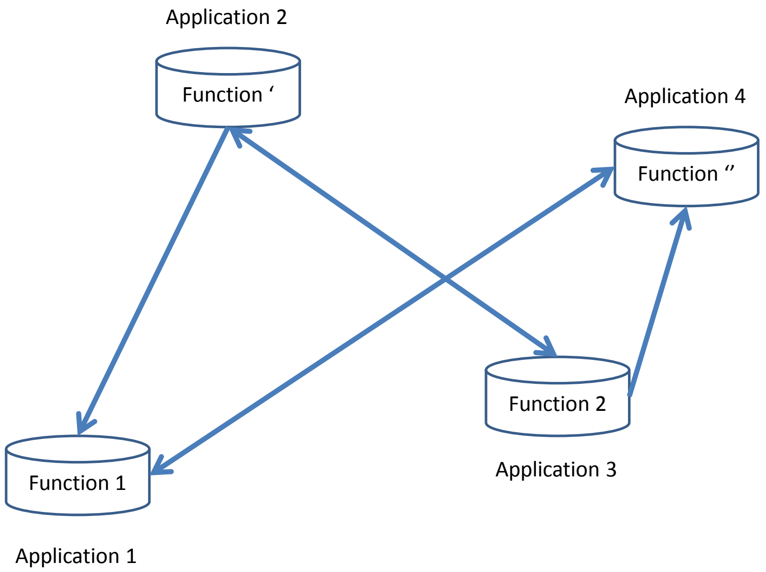

Figure 5: Archetypal application architecture

Now, assume that there is a single timing function. The analysis process needs to use this to calculate the required response. It then passes this information to the fire control system, which then uses the exact same timing routine within its own calculations. Therefore, there cannot be any issues with timing as everything refers to the same routine. Mission effectiveness is optimised, and the communication of events among the various command and front-line personnel involved is improved to ensure greater agility and accuracy in decision-making.

This functional reuse is central to the concept of SOA, and changes the way that the battlespace can be regarded in IT and communication terms.

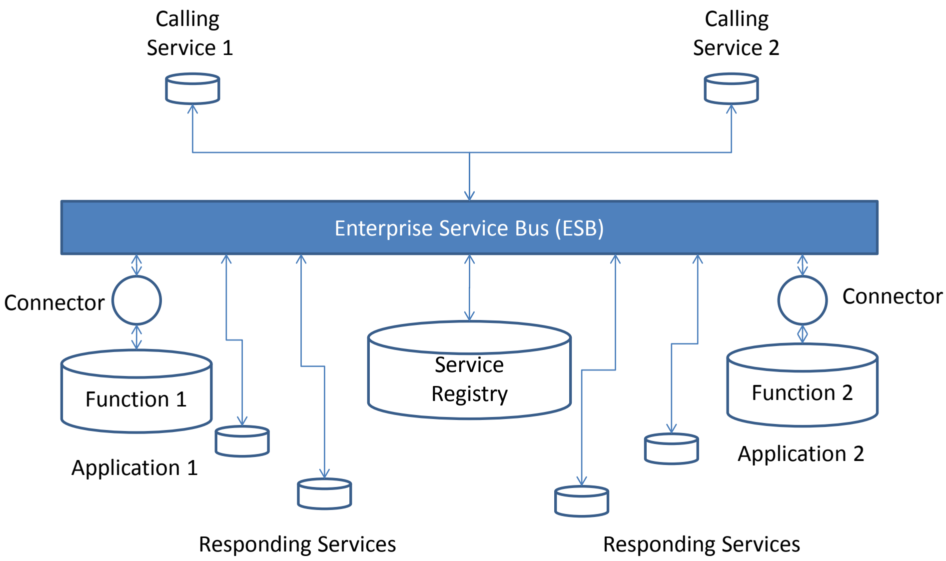

Figure 6: SOA architecture

Each functional component within a SOA is termed a service (often referred to as a "web service"), and can act as both a calling and a responding service. Therefore, in the above example, the timing routine can be called by any other function that requires such granularity of timing within its own event, and the timing routine itself could call, for example, a calendaring service should its own output need to be comparative against a higher level, known datum point (such as a zero time/date event).

For a SOA to operate effectively, it needs a common means of transferring information between the various web services, and from one environment to another. In the majority of cases, this is carried out via an enterprise service bus (ESB), which contains all the functionality required for carrying out such critical tasks (see Figure 6). Therefore, should a responding web service not be available for any reason, the call can be re-routed or held by the ESB functionality so that the call can be effectively serviced.

An ESB also provides other benefits. As a core component within a system, it provides the connection points to other systems. As well as acting as the broker between, for example, one defence group's systems and another, it can also act as a gateway between new web services-based systems and existing monolithic or proprietary applications. Through the use of specific connectors, existing applications can exchange data with the ESB in a manner where the ESB can then serve such information to calling or responding services. Therefore, there is no need to carry out immediate replacements of old systems – this can be carried out when time, money and need dictate.

The reuse of web services is managed through a catalogue of such services. By ensuring that this catalogue is the central point for accessing the web services, re-use is more effective, with developers being able to see what services are already available during their work. Indeed, such catalogues should provide a great deal of information on the capabilities of the service, such as throughput capabilities, how many calls it can service in a given period of time, what inputs it requires and what outputs it provides.

An overall process facilitated by a SOA platform is known as a “composite application”. Here, we still have the concept of an overall application that provides a solution to a specific problem. However, we have a level of granularity within the system that gives greater flexibility. Using our previous example, if a better timing web service is found, it can replace the existing timing web service, and all other services that use this timing service will be automatically upgraded.

A SOA environment also enables data to be dealt with more effectively. For data that is associated with an application, it is often the case that the data is specific to that application, and access to the data has to be carried out through the application itself. If the data is needed by a different application, then hard coding is generally required to carry out extract, transform and load (ETL) activities on the data to move it to the database that the new application uses. However, a SOA can provide direct connectors to databases, creating a means of federating them in such a manner that the movement of the physical data from one database to another is no longer required. Instead, the SOA uses these connectors to dynamically access the data as the composite application requires it. Through this means, action is always carried out against the latest data available and systems are not working against multiple instances of key data.

Within standard commercial environments, SOA has taken off as the main means of providing flexibility within their IT platforms and networks. SOA is now a tested and mature approach, and today’s solutions provide fast response times, highly resilient systems and flexibility to embrace existing systems. Therefore, taking an existing SOA approach as a basis for the design and development of networks within the battlespace means that the proven capabilities and the use of market-based standards will provide a suitable platform for creating a robust interoperable and reliable battlespace information solution.

Security, performance and SOA

Security within a SOA architecture should be viewed as different to that within an archetypical application environment. Whereas, within an application, security can be viewed as being distinct and specific to the application, with data between applications being encrypted, SOA presents more issues. As services are calling and responding to each other, trust models have to be set up and maintained to ensure that only known services are requesting and responding. This requires the setting up of a technical “contract” between services, which needs to be brokered through a trusted environment. Again, as in a standard application-centric environment, all data on the move has to be encrypted, and here the ESB becomes the major means of ensuring that data is maintained in a highly secure yet highly optimised manner. Through these means, each service can be fully secured as a discrete item, opening up connections to other services only as the trusted broker decides that this should be the case. Once the services have been opened up to each other, any information flows are fully secured via encryption and tunnelling (ensuring that point-to-point information flows are maintained, rather than packets of data finding their own way around the network).

Within the technical contracts, a SOA can enforce more than just trust levels. To further drive optimisation of the various infrastructure assets, the contract can define what the performance requirements are. For example, a requesting service may require a single response to its request, and the responding service can therefore be provisioned as a small service utilising only a small proportion of the infrastructure assets in order to meet these needs. A different service may be required to respond to many requests per second or minute, in which case it will need to be provisioned with more of the available resources. All of this can be managed through the use of a technical contract broker.