WHITEPAPER

Interoperable Open Architecture (IOA)

MOD AND DOD - ARCHITECTING FOR INTEROPERABILITY

OVERVIEW

Architecting systems and system-of-systems while satisfying the combined attributes of performance, scalability and reliability is hard. Adding non-functional requirements of interoperability, flexibility, modularity, and portability make the problem even more difficult. So imagine the challenge defense procurement agencies like the DoD and MOD have taken on in recent initiatives, whereby they plan to do exactly this – but not for just one procurement requirement, but across all future procurements for systems. Furthermore, this goal is not just for systems of a similar type but also for different mission specific systems that need, want and use similar data. There is a radical shift in defense procurement thinking; instead of the systems integrator, the DoD and MOD are starting to define the reusable Systems-of-Systems Architecture (SoSA) of electronic and software systems they wish to procure. By taking architectural ownership of this common part of the System of Systems (SoS), they seek to evolve the market towards real open market competition for the functional sub-systems; they are seeking to do this by defining a fully Interoperable Open Architecture (IOA).

To be clear, this is not simply **the same everywhere** OA initiative. To be meaningfully interoperable, different systems built at different times, with different hardware, different software architectures, different technologies, and different uses of the data and system information must be readily and meaningfully integratable. Furthermore, this is also not government led integration. A tier 1 system Integrator still takes responsibility for integrating all the sub-systems together and for implementing the IOA – but against a architectural specification governed by the DoD or MOD. The key technical objective that enables this commercial market change is the drive towards interoperability, taking one of the historically key objectives of Open Architecture, which industry has continuously failed to deliver, and making it the Key Performance Parameter (KPP).

The goals are to reduce the cost of system procurement, both up front and, importantly, through life. Delivering greater agility to the warfighter and significantly decreasing turnaround time between war-fighter change requests and delivery. Programs that stand to reap these rewards through their adoption of IOA principles as outlined in the whitepaper include the DoD UCS (UAS Control Segment), defining a common architecture for unmanned control stations, and the MOD GVA (Generic Vehicle Architecture), defining a common architecture for armored vehicles.

IOA is the natural progression of Open Architecture (OA) principles into defense procurement strategy across procurements of systems of a similar type. At the 2011 DSei event you could not pass a major system integrators booth or public presentation without hearing the Open Architecture claim for their products. But Open Architecture is meant to deliver specific benefits – interoperability is perhaps the most important. For over 10 years defense procurement agencies have been asking for Open Architecture solutions from their supply chains, and all they have got is a tick box exercise for the adoption of open standards, open systems (modularity and integratability) and COTS technologies. All of these are components of an OA, but unless they are brought together within an open infrastructure, as we will describe herein, the full benefits of Open Architecture cannot accrue to the DoD or MOD, nor, more importantly, to the warfighter. Industry has not delivered the open infrastructure. Patience has run out.

WHAT IS INTEROPERABILITY?

Interoperability has become a loaded term in the defense industry. It has been used and abused, confused and confabulated with many other terms. So before we proceed we should be clear what the term means. This is best achieved by defining the terms that are often used interchangeably with interoperability when they should not be. Also given that these terms are often used to imply commercial benefits through the adoption of technical functionality, we should also clarify what commercial benefits could be attributed to a system architected with the technical attribute. The following table pulls together definitions from many sources. Unfortunately industry has defined and redefined these terms so many times that no one coherent and agreed definition set exists. So this table is to be used to understand RTI's use of these terms as we have come to understand them through 10+ years of defense industry engagement.

TERM	TECHNICAL DEFINITION	RELATION TO INTEROPERABILITY & COMMERCIAL CONTEXT
Interoperability	Using services (providing and accepting) to enable diverse components to effectively operate together	Key requirement: the ability to combine diverse, multi-vendor components without requiring any changes (software or hardware)
Integratability	Creating a functioning whole system	Often overlooked: up-front costs; in-the-field upgrade costs; and the fact that integratability does not imply interoperability
Replaceability	One thing or person taking the place of another especially as a substitute or successor.	While a replaceable sub-system is an asset, it does not imply that the replaced system can be enhanced or altered in any way – in fact its more likely it has to remain identical in functionality.
Interchangeability	To put each of (two things) in the place of the other, or to be used in place of each other.	An improvement on replaceability because the sub-systems are likely to be able to behave differently based upon the system the sub-system is placed into. But this system context usually has to be pre-determined and fixed ahead of development time.
Extensibility	The ability to add new components, subsystems, and capabilities to a system.	There is no limit on the domino effect of change requests needed across the rest of the system to integrate the new sub-system. Nor does it imply that the new system can meaningfully exchange information with any sub-system already in the system.
Componentization	A software package, service or module that encapsulates a set of related functions that communicates via defined interfaces.	A valuable building block in software architectures, but its interfaces are not necessarily openly defined for interoperability and can still end up delivering stovepiped systems.
Modularity	Clarifies the functional blocks of a system, separating capability into modules.	Improves maintainability but makes no claims for interoperability as interfaces can be closed and proprietary.
Portability	The ability of something, usually a software application, to be readily moved from one environment to another, usually due to a common platform.	While this aids re-use of the application it has no association with interoperability of the application with other applications in the environment it has been moved into. It only facilitates integratability with the platform
Open System	Provides for 'some' level of system capability that exhibits interoperability, portability and use of open standards.	There is no standard to which the level of openness is defined, nor to what interoperability relates.

Table 1. Definition of Terms

When reviewing this list, it becomes clear that qualification of almost every term is needed to be sure the reader correctly understands the writers intent.

INTEROPERABILITY AS A KEY SYSTEM OF SYSTEMS ATTRIBUTE

Interoperability is being brought to the top line as a deliverable requirement, and to ensure they get it, the DoD and MOD are mandating the architecture of the systems they wish to procure – not just for the next system but, with a common systems architecture across all systems of a similar type (combat vehicles, Unmanned Control Systems, etc.) that they plan to procure.

By mandating, managing, and verifying interoperability, the MOD and DoD seek to more closely align the defense market with the operation of open commercial markets. The most important commercial market benefit sought is open market competition for sub-system supply. Defense procurement seeks to foster investment ahead of specified requirement, driving differentiation through cost and innovation, and most importantly of all, building agility into the procurement process so that the warfighter is better served with more capability, delivered more rapidly, with increased update cycles to stay at the forefront of the technology war. The core technology enabling tenet of this approach is the development of a common system of system architecture that satisfies the systems non-functional requirements. But commonality alone is insufficient to reap the agility and commercial benefits sought, because it does not necessarily facilitate the integration of new innovative capabilities with older 'common' functionality or explicitly identify the legitimate points of variation.

To ensure these benefits are received the MOD and DOD are mandating an Interoperable Open Architecture.

WHAT IS IOA?

It is a SoSA based upon open standards that delivers interoperability among sub-systems and applications built and procured at different times. Open Standards allow defense procurement agencies to mandate architecture, not a list of potentially tyrannical suppliers. Arguably previous OA's did this and still did not achieve interoperability in the supplied systems. Both the MOD and DoD, in independent program developments, identified that the key to achieving this final critical step is to control the data. Both selected to use a system of systems data modeling approach. Technologies can be mapped, fundamental understanding of the system information cannot. Historically it is inferred and discovered

during integration and the cost of isolating this inference per integration activity has been seen through ever escalating costs as system scale increases – and every system grows in scale and complexity over time.

But defining a SoSA through its data creates a need for a data-centric middleware open standard. Otherwise when the first SoS is procured and the tier 1 System integrator uses an OA compliant Open Standard from supplier X, then Supplier X is hooked into the sub-system supply chain and has to be mandated for the next system procurement. To be an appropriate Open Standard for SoS integration the standards body has to mandate both a wire protocol (for integratability) and programming interface (for portability). However, while this provides the basis for an interoperable OA, it is still insufficient. Communication and connectivity may have been openly standardized, but the meaning of the information flow has not. Both the DoD with the UCS program and the MOD with the GVA program are seeking to be able to address this issue by defining a System Data Dictionary (SDD) that defines content and context of the data that is communicated around the SoS – it is not a wire protocol but rather a full specification of the data and its meaning which can then be instantiated appropriately on different technologies to exchange information. Included in this SDD is a set of meta-data that defines the semantic information associated with every piece of data, this semantic data contextualizes it or allows it to be re-contextualized to the application using it. (see section Interoperability in IOA below).

The common approach to achieving this goal is to build a System Data Dictionary (often referred to as a Data Model) which encapsulates not only the language for speaking between applications and sub-systems, but also the semantic meaning of the data. For example, lets take track data, i.e. the location of an air vehicle. If we take the height information, does one system measure from sea level or just the distance above ground? Is it in km or miles? Is a negative measure valid? But it's even more than that, like the human mind, a sub-system needs context. Who is telling me this? Where did the data originate? How old is it? What happens if I miss an update? Does the first time I see a track have any special meaning? What makes a track stale, and should I care? How fast are the updates? How much of the data update history should be available? There are many such behaviors that to date have been implicitly specified and only partially understood when systems are integrated. Common errors that result are duplicated tracks, incomplete or conflicting data, inefficient use of compute resources, domino-style system integration challenges when integrating additional capability and no gains in system interoperability. The context contributes to the semantic understanding of the data and provides a means to evaluate the veracity and utility of the data. When systems work upon a common semantic data model and not a bunch of syntactic messages they can start to become truly interoperable.

Some Open System programs have been focused on portability of applications. However while they will deliver cost benefits in the first program, they will find as the functionality of one application or sub-system evolves, or requirements change, or new capability is inserted, that portability is not interoperability. Introducing different capabilities and features, while made easy to host and run by the common platform for portability, will have a cascading domino effect of costly change requests through the SoS.
Instead, advanced programs have recognized that application

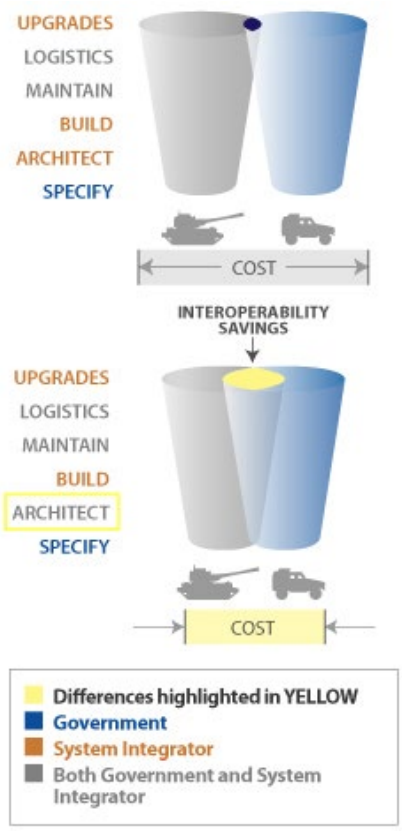

Figure 1. Procurement Savings Through Change of Responsibility for System Architecture is the Key Change IOA Promotes

portability is a goal, but that system-level interoperability is the higher order functionality that is needed.

MANAGEMENT OF SYSTEM STATE THROUGH THE DATA

To achieve system-level interoperability defense procurement are recognizing that the system state needs to be maintained in the architecture infrastructure and not within applications or in a specific sub-system. In fact the entire system state has to be made explicit within the IOA by every connected functional sub-system or application. This decouples not only the communication between subsystems, but also the state information.

There are three guiding prinicples to achieving Data-Led Interoperability:

1. All data (that is to be exchanged) is rigorously defined (with semantics), described, documented and available.

2. Data exists in the SoS fully independently of any application or function. Data is managed by the infrastructure.

3. That data repository, which could be fully distributed and serverless (an architecture which the open standards OMG Data Distribution Service (DDS) middleware facilitates), is the single authoritative source of state information in the SoS.

Now any subsystem or application can obtain state information from the software infrastructure rather than from another subsystem or application, thereby reducing coupling and removing stovepipes. We see this in evidence by the wide use of databases as a central 'cache' of state. Their use has been very effective in enabling client application to get, view, and manipulate the data and its state without the need for full system connectivity. However, this implementation approach is really only practical for data-at-rest. For distributed, non-homogeneous real-time systems a central repository of state information is impractical and not implementable. What is needed is a fully distributed, real time bus that maintains state of data-in-motion.

INTEROPERABILITY IN IOA

To achieve a fully interoperable SoSA, you need to achieve 3 levels of interoperability:

- Technical Interoperability
  - Bits and bytes are exchanged in an unambiguous manner via a set of standardized communication protocols
- Syntactic Interoperability
  - A common data format is defined for the unambiguous sharing of information
- Semantic Interoperability
  - The meaning of data is exchanged through a common information model and the meaning of information is unambiguously defined and shared

Note, semantic interoperability is not common practice today, it is this focus on the data semantics that will facilitate the drive towards interoperability.

However even if you enable all these capabilities in a SoS you may not achieve an IOA. There is one more key step required. That is to delegate the syntactic and semantic interoperability to a software infrastructure layer, which can be common across every sub-system. Thus interoperability can now be maintained, like the state, at the SoS level and not between 2 or more interoperating applications or sub-systems.

The means of associating interoperability with data and information flows at the system level is to use a data-centric design approach. This is exactly what both UCS and GVA identified and are implementing. If your sub-system cannot speak the system data language you are not interoperable.

IS THE SYSTEM INTEGRATOR READY?

Not really – this is a fundamental shift in procurement strategy and as such will have cultural, organizational as well as technical implications. But that does not mean the System Integrators are unprepared. Some Systems Integrators have been building out their own internal interoperable system of systems capabilities for the same commercial reasons that the MOD and DoD now want them. The difference is that the MOD and DoD need that interoperable environment to be open and common across suppliers of all sizes, whereas the supply chain wants it to be closed and proprietary, for obvious commercial 'lock-in' and through-life program revenue reasons.

The uncomfortable truth is that the System Integrators have been selling and reselling the non-functional component of the SoS's they supply as a highly profitable part of their business and shading the integration costs in order to maximize profits; an expected and entirely appropriate approach given the need to deliver maximum returns to shareholders. But now, the non-functional system architecture will be reduced as a profit center for the supply chain, although they can compete on the efficacy of their implementations. In that context, the supply chain is not commercially ready. Therefore, the MOD and DoD are stepping forward carefully because a commercially healthy supply chain is critical to their operational capability. Of course, private companies with no shareholders to report to are potentially able to move very quickly to take advantage of this shift. The DoD in particular is fostering greater involvement of smaller businesses, perhaps as a means to accelerate this commercial market shift.

In addition the MOD and DoD are still refining and redefining their procurement processes to leverage this new approach. Managing a more open competitive market is an unfamiliar process and will take some considerable time to adopt, leverage and re-organize for.

DRIVERS OF CHANGE

The reason for this change is the economic imperative in combination with the changing warfare environment, spurred on by the more visible rate-of-change gap in technology supply between defense equipment and commercial offerings. Smartphones are a prime example – a few years ago our phone struggled to do much more than text and phone, now they are fully-fledged computers capable of receiving video, tracking location and orientation and even measuring our heartbeat. The open application platform has enabled rapid accessibility of this change in compute capability, and in asymmetric warfare the enemy is using this device quite effectively. But more than that our mobile contracts allow us to upgrade every 12-18 months to a new device with even more capabilities. What's not to like? Contrast this with change requests that take years to bubble up to requirements, expressed to defense procurement and eventually delivered by industry.

But the real driver comes from the warfighter. The one flying his F16 with an iPad on his lap or sitting in his Humvee surrounded by 4-5 screens when one would be enough (both true feedback from the field). That difference is felt in two ways:

1. The individual warfighters' technology expectations, in terms of capability and ease of upgrade, is being set by the commercial market not by the defense industry itself.

2. The enemy is able to access more high tech for less money, and those without defense industries to support them are making effective use of advanced commercial technology and access to information.

We live in a period of unprecedented global peace, we have had over 60 years with few major wars, yet the asymmetric threat has never been greater. The normal government driven impetus to innovate and drive technology forward through defense requirements has been overtaken by the rapid technology cycles of the competitive commercial world. It's also clear that the purse strings are tightening and defense, as with all other government departments, has to tighten the

belt. To do that, something has to change – and that's the procurement process itself.

The middleware, system and data modeling technologies are ready, the open-standards supply chain is ready, and the defense supply chain is up to speed with the technology and is already leveraging it. The only difference going forward will be how integration will be managed – IOA introduces a shift from the current vertical integration strategy to a horizontal one. Everyone has fully open access to the infrastructure. In fact the infrastructure could, and perhaps should, be acquired independently from the system functional components.

The warfighter will gain as they receive more frequent upgrades and new technology insertions in a more agile fashion and at a pace closer to the commercial world, albeit within systems that have to be managed for 20-30 years in deployment.

The central commercial tenet that will deliver the efficiencies is **competition** enabled by DoD and MOD mandated systems **interoperability**.

MANDATING THE INTEGRATION STRATEGY IS CRITICAL

The lesson learnt by defense procurement using OA over the last 10 years or so is that the benefits that should accrue to OA don't happen unless defense procurement also mandates the integration strategy. The traditional ICD/IDD (Interface Control Document/Interface Description Document) have been shown to be insufficient as they only enable syntactic interoperability. The MOD and DoD are starting to define an IOA, and with that they are taking ownership of those parts of the integration strategy that are necessary to ensure the delivery of interoperable SoS's.

But surely this is stepping onto the suppliers' traditional turf? While true, the more forward-looking Systems Integrators are recognizing the economic imperative and are embracing the change. Indeed GVA would not exist today as Def Stan 23-09 unless industry had worked extremely closely with defense procurement to define the line to be drawn between the architecture and integration strategy defined by MOD versus the functional sub-systems delivered by industry. Similarly UCS has been developed with the co-ordination and co-operation and support of industry.

The integration strategy has to encompass:

- Modularization of sub-systems
- Simple update/replacement over time of sub-systems
- Innovation within a sub-system
- Insertion of innovative new sub-systems
- No 'stovepipe' connectivity between any 2 sub-systems
- The ability to 'wrap' and integrate legacy sub-systems not originally built to the new Open Architecture

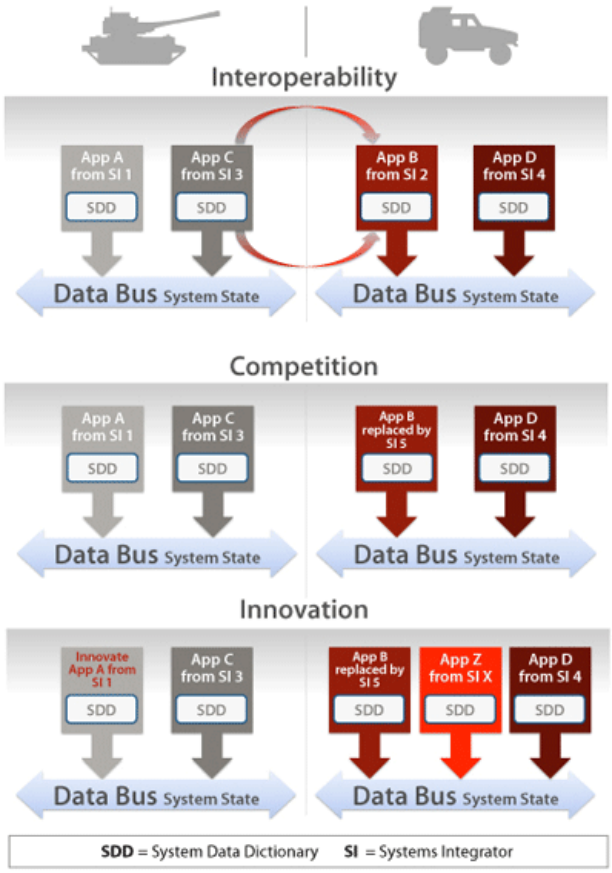

Figure 2. An IOA promotes Interoperability, which leads to Open Market Competition which drives increased Innovation Cycles

SELECTING APPROPRIATE IOA MIDDLEWARE

Unfortunately creating the SDD is insufficient for guaranteeing integration within an Open Architecture. The means to 'speak' the language has to be fully compliant with all the tenets of Open Architecture.

The communication mechanism and SoSA state maintainer selected and mandated under GVA is the OMG (Object Management Group) DDS (Data Distribution Service), which has proven vendor interoperability and for which vendor interoperability is maintained and managed by the OMG. Under UCS much of the test and SDD validation work has been built on DDS. However UCS does not mandate an implementation technology as this is left for the program offices using the UCS architecture to define. This is partially because as an umbrella architecture that is, uniquely, being applied across services (Army, Navy, Air Force) it is beyond the remit of the UCS program to define the implementation approach within any one service.

We started this paper by talking about scalability combined with performance and reliability. It is normal for systems engineers to trade one to get the other two. But this is unacceptable in the defense market. The battlefield scales in an undefined manner, performance saves lives and unreliability costs lives.

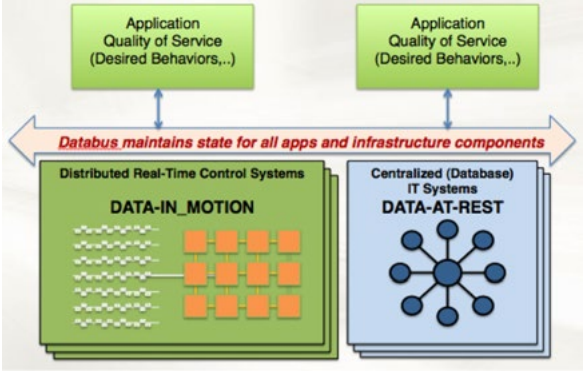

Figure 3. Decoupling System State from Applications and Infrastructure Components is Critical to removing Stovepipes

In a SoS it should be possible for any system or sub-system to fail without bringing down the wider SoS around it. Well-architected implementations of middleware have been built with a guarantee of no single point of failure. Unlike inherently client-server architectures whereby the server dies and all its clients die or suffer reduced capability, a true peer-to-peer implementation of the middleware does not suffer this problem.

The middleware must also inherently support the ability to sustain a data-driven system-of-systems state on the bus; effectively within the dataset on the move between systems at any point in time. Only one open standards based middleware potentially delivers all these attributes: the OMG data Distribution service (DDS). Only one has a proven 8 year plus history of delivering no single point of failure in its DDS implementation – RTI's.

Scalability is primarily achieved by DDS's inherent decoupling of one system from another combined with its systems communication and application-oriented Quality of Service (QoS) capabilities. Each system only talks to the system-wide data bus. It either places data (from the SDD, including the semantic context) onto the bus or pulls it off. Systems talk directly to other systems as defined by their data needs. DDS manages the 'data in motion' and thereby maintains a record of the SoS state and semantic interoperability.

Despite these inherent core characteristics of scalability and reliability, DDS does not sacrifice performance to achieve them. RTI's DDS has been consistently shown to out-perform all other large scale SoS communications open standards middleware (see http://www.rti.com/products/dds/benchmarks-cpp-linux.html), whether its across HF radios, Ethernet, satellite or a proprietary connection type.

Lastly, and perhaps most importantly of all, the OMG manages a process of vendor integration validation, with closely managed control of both the API for portability and the wire protocol for integratability. Thus any sub-system developer can select any DDS supplier based upon their commercial and technical needs. While DDS is standardized the implementations are not, nor are the business terms defined. So the MOD and DoD can safely mandate DDS secure in the knowledge that they are not undermining their own key objective of building competitiveness into their supply chain.

SUMMARY

The economic imperative is driving procurement and system integration innovation in the same way that wars tend to drive technology innovation. However technology has advanced sufficiently to create the foundations of a fundamentally new procurement strategy. IOA promises to meet the demands of the warfighter for more, faster, better systems while reducing costs for initial delivery as well as enhancing the pace of through life upgrades and reducing costs for logistical support.

ABOUT RTI

Real-Time Innovations (RTI) is the largest software framework provider for smart machines and real-world systems. The company's RTI Connext® product enables intelligent architecture by sharing information in real time, making large applications work together as one.

With over 1,500 deployments, RTI software runs the largest power plants in North America, connects perception to control in vehicles, coordinates combat management on US Navy ships, drives a new generation of medical robotics, controls hyperloop and flying cars, and provides 24/7 medical intelligence for hospital patients and emergency victims.

RTI is the best in the world at connecting intelligent, distributed systems. These systems improve medical care, make our roads safer, improve energy use, and protect our freedom.

RTI is the leading vendor of products compliant with the Object Management Group® (OMG) Data Distribution Service™ (DDS) standard. RTI is privately held and headquartered in Sunnyvale, California with regional headquarters in Spain and Singapore.

Download a free 30-day trial of the latest, fully-functional Connext DDS software today: https://www.rti.com/downloads.

Your systems. Working as one.

CORPORATE HEADQUARTERS
232 E. Java Drive, Sunnyvale, CA 94089
Telephone: +1 (408) 990-7400
Fax: +1 (408) 990-7402
info@rti.com

rti.com
rti_software
rtisoftware
company/rti
connextpodcast
rti_software