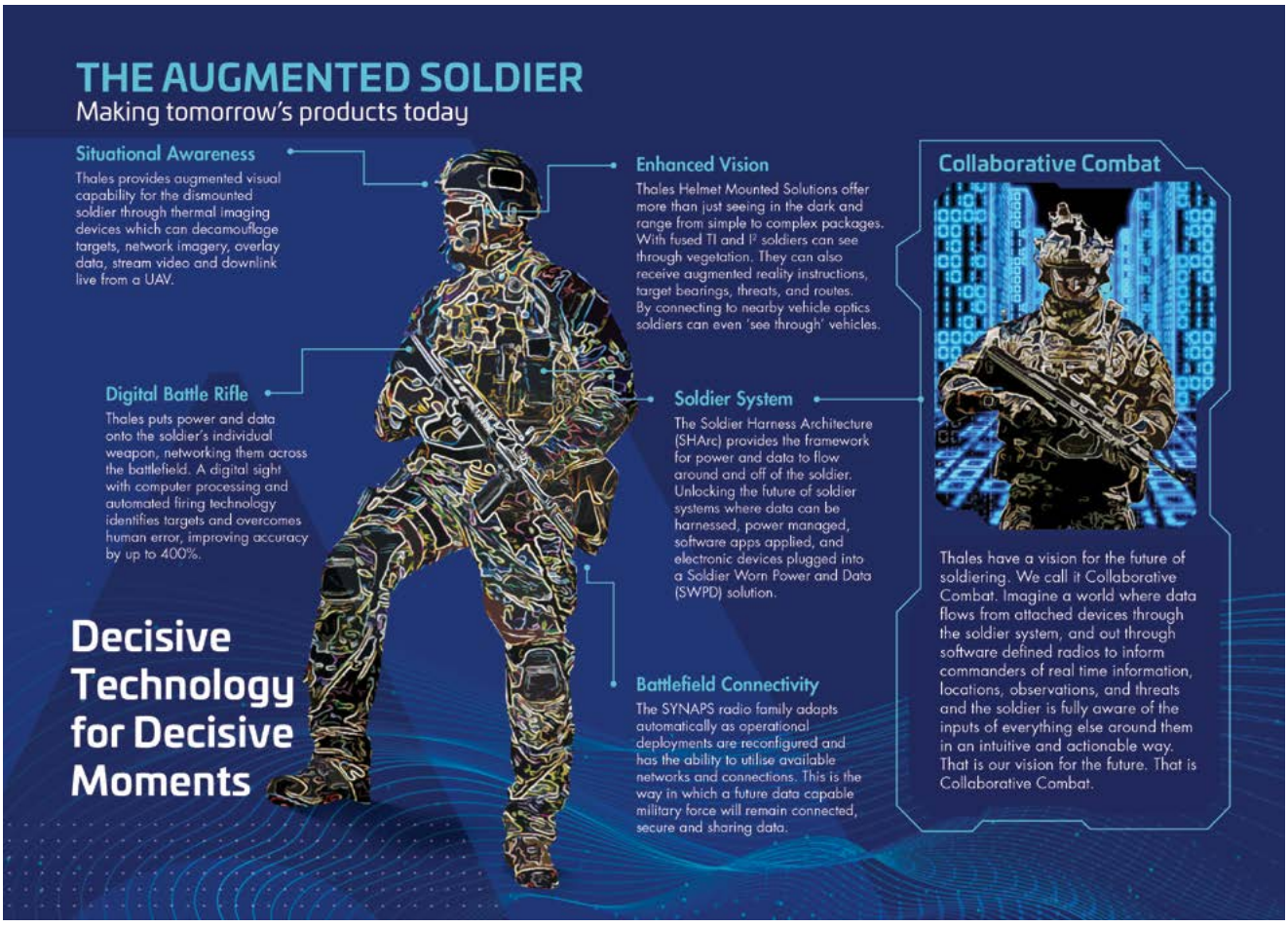
The augmented soldier

John Foley and Paul Clark

In order to realise the future potential of shared data on the battlefield Thales Soldier Systems Architects know that the first step on that journey may very well be the most important. Get it right and you can significantly improve your soldier's capability, augmenting their effect on the ground, but get it wrong and you are just adding burden to an already burdened warrior.

In this new era of the "Internet of Things (IoT)" there can be no doubt that the substantial use of digital services will be of real benefit to dismounted soldiers – augmenting what they already do so well through training, team work, and personal mastery of their craft. Just how much data flows up and down (and sideways) between different types of soldier remains an area of open debate. Different Armies will adopt different detailed implementations to suit their own Concepts of Use/Employment (CONUSE/CONEMP), but each of these implementations will need to evolve rapidly if they are to remain relevant as technology progresses and as users find new ways of exploiting emerging capabilities to augment what current capabilities they already have.

Thales are already exploiting a number of areas in which increased access and sharing of data will significantly augment capability. Some of these areas to be exploited fall within the services category provided by software programmes, with Artificial Intelligence (AI)



harvesting vast amounts of data, even Big Data, in order to support decision making. However other areas are more immediately tangible and immediately necessary and include connectivity, processing, situational awareness, accuracy/lethality, and enhanced 'vision'. At Thales we have a name for this connected, data sharing world; we call it 'Collaborative Combat'.

However none of these areas of enhancement or digital augmentation are possible without the well-considered implementation, from the start, of a Digital Soldier System. The clear message that is emerging is the paramount requirement for flexibility in both how the system is implemented and how it can be expanded to allow for continuous growth, where flexibility and expansion mean:

- **Flexibility:** Users need the ability to adapt the system implementation to suit their specific needs and specific mission
- **Expansion:** We live in an era of constant technology advance, systems must cater for this.

Who Gets it?

The scale of Digital Soldier deployment has often been questioned with some implementations being seen as a "Commander " only system. This approach centres on the immediate and obvious benefits of digitising some of the traditional Command & Control (C2) functions, especially mapping, and whilst this offers a 'quick win', failing to also digitise the individual soldier seriously constrains the range of possible benefits.

Given the potential for distraction the extent to which each soldier may access data does need to be carefully considered but they are all important elements of the fighting system from Company, Platoon, Section and down to the individual Fire Team. Tracking key data from each of them can be used to optimise the way that system operates. The 'quick win' approach may see this data as being just individual location, possibly implemented as part of the radio, but this misses out on all the emerging benefits of our growing IoT culture which is rapidly digitising all aspects of our modern life in order to provide a beneficial stream of "services".

Along with all the Situational Awareness (SA) data there will be real benefit in collating an ever increasing range of logistic and status data, such as battery charge states, battery condition, water, user health data, weapon status, and ammunition holdings to name but a few. This data can be seamlessly flowed upwards and used to inform transparent logistic services and command decisions in a manner which greatly reduces commander cognitive burden.

The ability to develop and exploit this stream of data-based services requires the initial Digital Soldier implementation to be open to the addition of future functionality and future devices. This in turn requires the initial Power & Data hub ("the hub") to be designed and engineered to cater for expansion. It therefore needs to be "intelligent" enough, as well as 'open' and scalable, to allow for numerous future software upgrades and substantial increase in services, which are inevitable given current technology trends.

One of the biggest risks to achieving full Digital Soldier capability is the temptation, against cost, time, and other pressures, to focus on Quick Wins and fail to cater for growth. The first procurement of a 'Digital Soldier System' must consider:

- **Design for Growth:** Initial implementation must "own" the responsibility for future growth.
- **Open Interfaces:** Agreement on appropriate common interface standards is critical.
- **"Intelligent hub":** The ability to host major software upgrades offers real growth potential.
- **Integration processes:** System Integrators need to be able to implement major upgrades.

How Much Does Power Weigh?

The human user sits at the heart of the "Digital Soldier" and this must be absolutely recognised in the way it is implemented. All soldier-related propositions pay at least lip-service to the importance of Size, Weight, and Power (SWAP) but often it is used as a starting point and many fail to follow it through to delivery. SWAP needs to be a priority metric against which unsuitable implementations are rejected.

Unlike size and weight, power consumption is not often acknowledge in context and yet high power demand immediately translates into excessive loads and major logistic demands in the course of a Battle Field Mission (BFM); the metric against which new soldier equipment is often measured. The UK FIST procurement programme (2003-2009) pioneered the approach of adding in the weight of batteries needed through the BFM to the static weight of the devices on offer to gain a 'real world' view of the 'cost' of introducing new equipment.

The SWAP considerations for a Digital Soldier System are:

- **Size and Weight:** The P&D hub must be acceptably small and light.
- **Power:** The power consumption of the hub must translate to an acceptable battery load.

The Hidden Weight of Data

The Digitised Soldier is nothing without data and the more that you are sharing the more bandwidth is required to move it around. Having lots of data bandwidth is always good, both on the man and between dispersed soldiers, but it comes at a price. This is especially true when sharing data between users where high data rates require substantial radio spectrum allocation (not always available) and consequently high power consumption to achieve useful ranges. Using hopping or MANET radios on the soldier does not overcome this fundamental problem since these invariably consume lots of power routing data through multiple hops.

The benefits of a Digital Soldier arise primarily from the ability to exchange and share data seamlessly in the

The Thales SHArc showing the hub attached to two batteries, a tactical radio, and other connector points with other data enabled but currently unattached devices in a stored position.

background to inform and support a range of Digital Services. In this case the vast majority of soldier systems only require very modest data payloads which can be supported on a very lean, low power radio net.

The radio power consumption required to support the Digital Soldier is a key element of the overall power budget and therefore the user weight budget. The ability to exchange video drives radio nets to high power consumption. Some video transfer is definitely required, especially in this era of remote unmanned platforms, but care needs to be taken in how this is implemented and in ensuring it does not result in over-specification of the basic soldier net and therefore a significant load increase for each user just carrying batteries for their radio(s). High data rates on the man are less problematic but again they do drive increased power consumption and real consideration needs to be given to precisely what services they are supporting. How much time should a dismounted soldier spend viewing video?

The key consideration for data carriage is:

- **Data Bandwidth:** "There is no free lunch". High data rates = extra soldier battery load.

Harnessing the Beast of Burden – Human Integration

The implementation of a Digital system on the soldier creates the need for a series of power and data links to be located around the body in order to connect the dispersed devices to the central hub. Typically this is done using conventional shielded cables. Most current soldier systems specify the use of USB and this in itself mandates that every device must have a direct link to the hub, so increasing digitisation drives an increase in cables. Alternative power and data transfer media are being assessed for soldier use but it is a very demanding requirement and some form of conventional cables are likely to remain the solution for some time.

Cables and Soldiers do not mix. The Digital Soldier System must provide a robust, flexible, snag-free approach to distributing power and data around the user. There is also a need to provide a sensible, comfortable, safe location around the user for both the hub itself and for the central battery or batteries. These are intensely human-centric tasks. They need to recognise and accommodate the variation in user sizes and in user roles and circumstances. For the Digital Soldier system to be acceptable to the user it needs to be designed as a complete package which provides not only the central electronic hub and associated cables but also the means for physically integrating this to the user themselves along with all their other necessary equipment.

In designing the Soldier Harness Architecture (SHArc) Thales have addressed these issues first and foremost, offering all the flexibility of an "Integrated-On" design (which it is) with the robustness and hidden cabling of an "Integrated-In" system, along with a novel means to allow

rapid transitions between protection 'dress states'. The SHArc has evolved through extensive experience where the most important element of integration is:

- **Human Physical Integration:** This aspect is just as critical as electronic/software integration.
- **Human Cognitive Integration:** As minimal as possible, and tailored to meet user needs.

Recruiting the Digital Armourer

The Digital Soldier concept, with its analogy to the IoT world, assumes frequent upgrades in both software and attached devices, so that rapid advances in technology can be quickly available to front line users and their digital support services. Systems cannot all be recalled to central depots in order to manage this. They must be designed to be upgraded by suitably trained users. It would be wrong to not emphasise the critical importance of all aspects of maintaining these Digital Soldier systems through life. This will drive personnel, training and Whole Life Cost (WLC) issues and will, ultimately, determine the reliability and availability of the benefits the systems offer.

Digital Soldier Systems will be deployed in large numbers across highly dispersed locations and will require appropriate second line support to maintain both their physical/electronic integrity and their software/firmware upgrades. This will drive a need for the development of new skill sets for a significant number of service personnel. The scale of the transition to Digital Soldier will be far too large to expect existing signals support to "just manage it". Whilst this poses a new challenge it does also mean that Armies will be offering to train recruits in valuable "modern world" software and electronics skills.

The Digital systems need to be designed to ensure that their support is something that can be sensibly managed by a suitably trained soldier, a sort of modern day "armourer" with the tools and skills to maintain digital systems. Equally the design needs to ensure that systems are inherently reliable, that they offer graceful degradation where appropriate and that their maintenance is affordable. Once introduced the Digital Soldier System will be ever present requiring regular whole fleet upgrades. This will require the initial system to have the following characteristics by design:

- **Reliability:** Always critical – and not always easy to ensure with evolving systems.
- **Maintainability:** Must be designed in from the outset – cannot be grafted on later.
- **Support Needs:** Training implications for supporting deployed systems are critical.
- **Upgradable:** Digital Soldier systems must be designed to allow frequent upgrades.

Additionally as electronic devices proliferate on the soldier so too will they across the rest of the battlefield. They will carry, travel in, operate or be co-located with a plethora of electronic systems. What they carry must not degrade the performance of the other systems and in particular must meet demanding Electro-Magnetic Compatibility (EMC) criteria. This is a major challenge – for many reasons. Electronically linking a set of devices located around a soldier immediately poses EMC challenges, which are not easily overcome.

If you then have a philosophy which allows such devices to be moved, replaced, upgraded or added to (as is the case with Digital Soldier) then ensuring that the minimum necessary EMC performance is maintained does become a significant challenge. When you factor in the hard physical life systems worn by soldiers must endure, and the inevitable degradation of the shielding performance, the EMC challenge becomes very significant. Some elements of this challenge can be addressed and minimised by optimum design decisions but much of it will remain to be managed through-life by the Digital Soldier "Integration Authority" (IA) which, in whatever form it is instituted, will absolutely be required in order to control "allowed configurations" from an EMC perspective and to manage the introduction of new elements to the soldier systems and new systems alongside the Digital Soldier.

- **EMC:** Managing what they will carry, travel in, operate or be co-located with and ensuring it all still works as required, the soldier system cannot degrade other electronic systems or itself.

Hackers and Jammers and Bugs, Oh My!

The consequence however of opening up your system for sharing, upgrading and accessing in order to make it relevant in the data-rich, e-battlefield of the future is that you also open it up to a whole host of new threats and risks, the ones that we are all familiar with in the 'online world' in which we now live and increasingly rely on.

All battlefield Digital Systems need to be fully security assessed, both on introduction and through life. Even where such systems are only intended to process "modest" data they still offer a potential attack vector for malicious third parties. Systems deployed on soldiers are especially vulnerable to capture. Systems designed to offer "open interfaces" for ease of upgrade also offer vulnerable avenues of attack. Digital Soldier security is a serious concern which needs to be thoroughly understood before such systems can be widely deployed, otherwise skilled and determined opponents may be able to exploit the vulnerabilities it introduces. Equally being over-zealous in employing security provisions could easily make Digital Soldier Systems both unaffordable and unusable.

This area does pose a major challenge for the deployment of the Digital Soldier. There are no "magic bullets" which will just "solve" this problem. Thales, having the benefit of access to major in-house security expertise, have conducted a number of studies into both the threats posed and the potential measures to counter these and are developing a suite of provisions to offer as part of their SHArc Soldier Worn Power& Data (SWPD) system. It is anticipated that Thales will be able to work with potential customers to tailor these security provisions to best meet

their individual needs. As with so many other aspects of Soldier Systems there is no viable "on size fits all" solution.

This is also true of the integral, non-malicious, threat that digital systems may introduce. Digital Soldier systems also bring an additional safety challenge. The use and abuse of new streams of soldier-related data needs to be assessed for its potential impact on the soldier safety case, in a similar manner to that required for security. The adoption of Open Architectures will make the physical integration of new devices simpler, but the management of the information exchange with each new device, and amongst the new set of devices, needs to be considered. Where devices have some safety-related data function they may also need to offer processes to provide the required level of data integrity.

- **Security:** Digital Soldiers must be armed with appropriate and effective security provisions.
- **Safety:** The introduction of each new device and data service must be assessed for its potential impact on the overall Safety Case for the Digital Soldier.

Decisive Technology for Decisive Moments

There are many considerations before fully implementing a Digital Soldier System. Get these right and the whole system will grow and evolve in step with technology and software development continually augmenting and enhancing the soldier's effect on the battlefield and the commander's ability to make decisions. Get it wrong, however, and the whole system quickly becomes irrelevant, costly, and a burden to the users.

There are challenges and implementing digitisation on soldiers does pose some unique problems. The creation of an Integration Authority for any military who controls software upgrades, test and trial of new devices and capabilities, and phase out of old technology, will go a long way towards mitigating many of the worries and new challenges. In any case it is important to identify and address these specific "challenges" at the outset of any Digital Soldier programme so that the resulting implementation can be optimised and avoid subsequent disappointment. Therefore the last consideration to list is:

- **Integration Authority:** Arbitrating authority on the evolution and upgrade of the system.

It is duly noted by the authors that there are no "right answers" in the Soldier System domain and Thales are very willing to discuss tailoring products and solutions to meet specific customer needs. Indeed, Thales have been active in this field for several decades and have used this experience to influence their current product thinking. In so doing the Thales SHArc Soldier Worn Power and Data capability has these vary considerations designed in from concept:

Flexibility, Expansion, Design for Growth, Open Interfaces, "Intelligent hub", Integration processes, Size and Weight, Power, Data Bandwidth, Human Physical Integration, Human Cognitive Integration, Reliability, Maintainability, Support Needs, Upgradable, EMC, Security, Safety, Integration Authority. ■

John Foley is a Thales Senior Expert in the field of Soldier Systems and has been active in this domain continuously since the NATO NIAG Sub-Group 48 Soldier Study in 1993-4. He subsequently led the UK industrial consortium (Pilkington, Racal & Royal Ordnance) which delivered the UK FIST Technology Demonstrator programme for DERA (1998-2000). He was Technical Director for the Thales Team which won and delivered the Cat-A FIST programme (2003-15), which included a comprehensive Main Gate submission on FIST-C4I and subsequently delivered the CLB (Casualty Locator Beacon) UOR which implemented many of its features. He is now fully involved in leading the development of a suite of Thales Soldier System products and in developing a Thales Soldier System Architecture Model which will be used to guide the definition of soldier-related activities and ensure coherence across Thales's multi-national and multi-functional organisational structure.

Paul Clark has been actively involved in the soldier systems field for 10 years since his participation on the UK FIST programme as well as multiple Soldier Systems UOR programmes. Paul was the Thales integration lead for the Weapon As A Platform (WAAP) project as part of the DSTL Delivering Dismounted Effects (DDE) research programme. More recently, he has been responsible for architecting and developing Thales' Soldier Systems product portfolio, ensuring they are suited to the needs of the future digitised soldier.