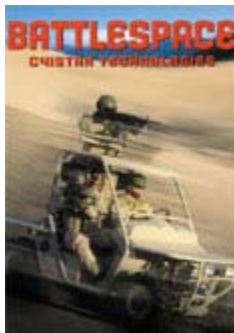


BATTLESPACE**BATTLESPACE
ONLINE****BATTLESPACE**
NEWS[Home](#) | [News Updates](#) | [In This Issue](#) | [Company Directory](#) | [About Us](#) | [Subscribe](#)

▶ BATTLESPACE update & BATTLESPACE email alert service is sponsored by **DRS Technologies Inc.**

▶ Free e-mail exhibition news service, [Register here!](#)

**EUROPEAN NEWS**Page | [1](#)|[2](#)|[3](#)|[4](#)|[5](#)|[6](#)|**ISSN 1416-300X Volume 7, Issue 2 June/July 2004****GKN TO SELL AgustaWestland STAKE – NO DEAL WITH BOEING**

20 May 04. GKN (London:GKN.L - News) said on Thursday it was in talks to pull out of helicopter maker AgustaWestland by selling its half stake to Italian partner Finmeccanica (Milan:SIFI.MI - News).

GKN's stake in the world's second largest helicopter maker by revenues has been estimated at £800-900m(\$1.41-\$1.59bn) by analysts, some of whom say Finmeccanica could pay more as the deal would give it total control.

"It is now timely to advise shareholders that negotiations are in progress concerning the possible sale of GKN's 50 percent shareholding in AgustaWestland to Finmeccanica," Chairman David Lees said in a statement for GKN's annual general meeting.

"A further announcement will be made when appropriate," he said. A deal should be sealed by the end of June, a source close to the operation told Reuters.

A Finmeccanica spokesman declined to elaborate on the possible sale, which was mooted in a Goldman Sachs research report more than a week earlier. Comments by Lees, including an outlook for a year-on-year fall in half-year underlying profit, hit GKN shares, which fell more than six percent. Lees said group pre-tax profit before goodwill and exceptional items in the first half of 2004 was likely to be "somewhat below" that of last year. The shares were off 2.17 percent at 214 1/2 pence as of 1054 GMT, while the FTSE 100 index (London:^FTSE

A Finmeccanica spokesman declined to elaborate on the possible AgustaWestland stake purchase, which was mooted in a Goldman Sachs research report more than a week earlier. Finmeccanica is expected to have access to funds for such a deal after saying last month it would sell part of its stake in semiconductor maker STMicroelectronics (Milan:STM.MI - News; Paris:STM.PA - News) worth more than €3bn. GKN's Lees made no comment on how GKN might use the proceeds from a sale.

Later GKN announced that the company had walked away from talks to buy U.S. manufacturing plants from Boeing Co (NYSE:BA - News) seen by analysts to be worth up to \$3bn, a source close to the negotiations told Reuters on Thursday.

The UK engineering firm bought a U.S. plant from Boeing in 2001 but a mooted purchase of Boeing's facilities in Wichita, Kansas, proved too large, the source said.

Advertisers**THALES**

Featured video presentation.
Oxley

Associated Sites

army-technology.com
▶ [Click here](#)

naval-technology.com
▶ [Click here](#)

airforce-technology.com
▶ [Click here](#)

aerospace-technology.com
▶ [Click here](#)

"They (GKN) have declined to submit a proposal," he told Reuters. "Size was an issue," he added, noting Boeing was interested in selling the Wichita plant together with two in Oklahoma. A GKN spokesman declined to comment. (Source: Reuters)

Comment: At last the sale of the AgustaWestland stake becomes public after much speculation. Originally conceived with GKN Defence as the 'third (defence) leg' of its business to complement automotive and CHEP pallets (since sold to Brambles), GKN is now concentrating its efforts on its wholly-owned new aerospace division and automotive engineering and exiting defence after a period stretching nearly 100 years. The company was never happy with a 50% stake and Westland is more likely to thrive under Finmeccanica in the longer term, how this affects the UK plants will become clear in due course, but, given the record of the present government, little move will be made to preserve this important source of IP and R&D.

ATLAS CONSORTIUM –MEETING THE DII CHALLENGE

25 Apr 04. Martin Southgate, Managing Director of the EDS-led Atlas Consortium bidding for the multi-billion MoD DII infrastructure requirement gave BATTLESPACE an update on the progress of its bid. There are now two consortia bidding, the Atlas consortium and the Radian consortium led by CSC. (We will give a Radian update in a later issue)

The complexity and risk outlined by Southgate and his team explains the reluctance of Lockheed Martin to join the final bidding teams.

"The DII bid is divided into three sections:

1. A Deployed Demonstrator which will come into service 6-12 months after contract award expected in the first quarter of 2005.
2. The Battlespace equipment allocations
3. The remaining Corporate applications.

In addition to EDS and Fujitsu Services, Atlas also includes three other key members: Cogent Defence and Security Networks, General Dynamics United Kingdom Limited and LogicaCMG. No one single Atlas member company will account for a majority of the workload, in accordance with the MoD's procurement criteria.

Under the Atlas banner, the five companies bring together a unique combination of skills, experience and capabilities in successfully delivering major public sector and military projects in the UK and worldwide.

Southgate told BATTLESPACE, "Atlas is one of the most distinguished, capable and experienced teams ever assembled for this type of undertaking. DII is a huge and challenging assignment, which very few organisations are capable of meeting. "We support the MoD's assessment that diversity of supply - and avoiding single point of failure - is imperative to the success of this procurement."

"DII is a business to battlefield concept," Southgate continued, "The Atlas team recognise the complexities of wiring up a huge variety of systems into a seamless information infrastructure. In addition we get paid on results so if the system does not work,

we do not get paid!" The existing JOCS and PJOCS Command and Control infrastructure contracts currently managed by EDS will eventually be absorbed into DII with new hardware as will other projects.

DII will enable the MoD to better to exploit its information assets for both operational and business purposes. At present the Department and the Armed Forces operate a wide variety of information systems acquired piecemeal over a number of years. This not only leads to inefficiencies in the conduct of Departmental business processes, and obstacles to meeting e-Government targets and legislative requirements, but also hampers the ability of the Services to operate together as they are increasingly required to do in the modern strategic environment.

One huge challenge facing the teams is the management of bandwidth and the priority given to users. As the system includes an ability for the armed forces to contact home by kiosk phone, surf the web and send emails, the bandwidth provisions for DII require prioritizing of traffic to favour defence applications over civilian 'chat'. In addition Atlas has recognised the requirement for Crypto and security on what is essentially a system 'wide open for hacking', thus the inclusion of EADS's Cogent segment with its wide knowledge of crypto systems already utilised on the UK Bowman programme.

The numbers are huge, 170,000 access systems from handheld thru laptop to rugged computers meeting the requirement of 300,000 users. The exact breakdown of numbers of different systems has yet to be decided but Atlas told BATTLESPACE that they will range from handheld PDAs to high powered rugged computers.

The aim of the DII programme, currently in its assessment phase, is to update and merge individual information systems to provide all staff with a common platform for business applications, enabling many current paper-based processes to be replaced by equivalent electronic services.

SECURING ISTAR SYSTEMS WITH RECONFIGURABLE TECHNOLOGY

Paul Parkinson
Senior Systems Architect, Wind River

Brian Taylor
European Programme Manager, OEM Partnership

Abstract.

This article outlines the potential for reconfigurable technology in Intelligence Surveillance & Reconnaissance (ISTAR) systems including the prevention of reverse engineering, and introduces new techniques for improving security, interoperability and field upgradeability.

Introduction

Intelligence Surveillance Target Acquisition and Reconnaissance (ISTAR) is increasingly becoming a system of systems, with each system building upon the lessons learned for the previous one deployed. The fusion of the data provided from these many

different sources is being used to get inside the opponents decision cycle, enabling our own forces to have superior intelligence available to make decisions upon. As a result, there is a massive push towards multi-role Unmanned Air Vehicle (UAV) platforms, ranging from low orbit theatre satellite platforms through, multi-sensor reconnaissance platforms to all out combat capable platforms.

These platforms can be vulnerable to interception by hostile forces due to their operational role. If these platforms are to utilise leading edge technology, this must be implemented in a manner which cannot be compromised or reverse-engineered by hostile forces. There is also a growing need to perform rapid deployments of new coalitions in response to world events, and field-based configuration and upgradeability will be essential in order to achieve interoperability with other coalition forces.

This paper will consider techniques utilising reconfigurable technology to achieve secure implementations which are resistant to reverse engineering by hostile forces, and effective software destruct sequences to prevent systems from being compromised.

The Dawn of Reconfigurable Computing

Traditionally, the silicon building blocks used to construct embedded systems have fallen into one of three categories. Firstly, the 32bit CPU has proven itself to be a versatile general-purpose processor for process control, but is generally sequential in operation. Second, Digital Signal Processors (DSPs) are optimized for high-performance algorithmic processing, but generally perform dedicated function. Thirdly, Field Programmable Gate Arrays (FPGAs) have been used to implement logic, but recent developments have widened their appeal and application considerably.

The distinction between these silicon building blocks has blurred considerably with the advent of the Platform FPGA. These differ from previous generations of devices in the following ways.

The gate count of Field Programmable Gate Arrays (FPGAs) has increased dramatically in recent years, with the ready availability of devices having two million gates. The massive increase in gate count has unleashed the potential of FPGAs (also known as CPLDs – Complex Programmable Logic Devices), so that now they are no longer devices which can be used solely for interface logic, but can be used as processing subsystems in their own right. The platform FPGAs will continue to evolve in the coming years towards true system-on-a-chip systems, by incorporating CPU and DSP functionality.

These platform FPGAs have the potential to be used for algorithmic operations, but until recently this has not been exploited due to the fact that it is difficult to develop million gate applications in VHDL. However, the ability to program reconfigurable logic from high-level software languages such as C, as well as VHDL, opens up the potential of these devices to further exploitation. This has been illustrated by Xilinx EDA tools ability to generate hardware peripheral & IP definition in VHDL, closely coupled with the automatic generation of the software configuration to support the running of the VxWorks RTOS running on PowerPC processor cores within the FPGA fabric.

Secure ISTAR Implementations

Reconfigurable technology can enable greater security in two key areas. Firstly, they are well suited to the high-computational demands of encryption algorithms; secondly, they can be used to secure the content of classified algorithms within hardware devices.

Triple DES [1] encryption provides a high level of security by encrypting data with three times using three 64bit private encryption keys. This is inherently more secure than single DES encryption, but will take a processor three times longer to compute, because a processor will perform the encryption as 3 sequential steps. The parallelism inherent in an FPGA can be exploited to implement three encryption stages operating in parallel, with the output of one stage being pipelined into the next stage in 64bit words. This acceleration enables data to be passed at higher rates over secure downlinks. For example, a 350MHz PowerPC can Triple DES encrypt a datastream at the rate of 1.2Mbit/s, whereas a lower-power 20MHz FPGA can Triple DES encrypt a datastream at the rate of 22Mbit/s, with each 64bit word being processed in 57 clock cycles [2].

Triple DES encryption can be used to implement a secure TCP/IP implementation as part of an IPSec framework, with the network processing being performed on the PowerPC and the computationally intensive encryption being off-loaded to the FPGA, which acts as a co-processor. The use of IPSec in secure airborne networks was recently discussed by Tingey & Parkinson [3].

Triple DES encryption can also be deployed within the content, known as the "payload", of the FPGA device. In this case, when the "bitstream" is read-out from the FPGA, the DES Triple encryption must be decrypted before it can be decoded. This not only protects the content from being copied blindly & re-used, but also prevents it from being reverse-engineered.

Software Destruct Sequences

Software Destruct capability is desirable option for systems which may be compromised or be captured by hostile forces, for instance UAVs. Current implementations of destruct sequences may or may not provide rapid, complete and irreversible destruction of subsystems. There may be the potential to perform reverse engineering of some hardware designs, especially if they include fixed hardware components such as ASICs.

Reconfigurable technology may provide the means to achieve rapid and complete destruct sequences in a number of ways. FPGA device can be erased completely, leaving no trace of its original application. This can be implemented in hardware, by asserting a specific signal on these devices, clearing the device in a few hundred microseconds (which may provide an appropriate approach for a manned airborne reconnaissance system).

The 'Software Destruct' sequence can also be performed via programmatic software control, issued from a remote system, which could be used in the case of the capture of a UAV. This can be implemented via a processor running the VxWorks RTOS which is connected to the command & control centre via a secure IP-based network, and can permanently & irreversibly

erase the content of a Xilinx FPGA using PAVE (PLD API for VxWorks Embedded Systems) [4], as shown in figure 1.

Field Upgradeability

Many in-service systems make widespread use of ASICs to implement specific functionality, but as deployed boards are replaced and updated, suppliers are faced with the issue of how to replace ASICs. The initial productions often do not provide enough capacity to replace deployed boards throughout a service lifetime of twenty years or more, and enhancements to the ASIC functionality are often required. It is of course possible to produce another ASIC for this purpose, but the costs of producing a new ASIC can be prohibitive, exceeding a million dollars for even a short ASIC run. There is also the risk that the ASIC produced may fail to meet its design criteria, resulting in another costly re-spin.

FPGAs provide an ideal solution to this problem by providing a platform device which can emulate the ASIC, and can be developed much more quickly than a new ASIC can be fabricated. The FPGA can also be easily reconfigured in the event of the implementation needing to be modified, so these factors combine to provide a low-risk, highly flexible and future-proof replacement.

The reconfigurability of FPGAs also provides the added benefit of providing a means to extend the in-service lifetimes of boards, by providing the means to upgrade the content of FPGAs whilst deployed in the field, as shown in figure 2.

Rapid Deployment & Interoperability

There is also the potential use reconfigurable technology for codecs to perform reconfiguration in the field to assist the rapid deployment and interoperability of coalition forces.

Reconfigurable technology can also be used to achieve rapid field-based upgrades of systems by sharing new encryption keys with coalition forces. This will significantly reduce the time required to achieve interoperability with other coalition members and aids rapid deployment. There is also a side benefit in that platforms can also be reconfigured on the fly to communicate with legacy or incompatible systems of other coalition members (if a suitable codec has been developed). This approach could be used to achieve interoperability between JSTARS and ASTOR.

Conclusions

Reconfigurable technology is now sufficiently mature to warrant incorporation into ISTAR applications. It provides the potential for acceleration of algorithms, increased connectivity and secure communications. This technology also offers benefits to network-centric warfare and C4ISR.

About the Authors

Paul Parkinson BSc CEng MBCS MIEE is a Senior Systems Architect with Wind River in the UK, working with customers in

the Aerospace & Defence markets. Paul's professional interests include Integrated Modular Avionics and airborne radar systems. Paul also has a current UK security clearance held by Trusted Experts.

Brian Taylor is European Programme Manager for OEM Partnership. Brian has extensive experience of reconnaissance and ISTAR systems and was a member of the NATO SOSTAS subcommittee. Brian also has a current UK security clearance held by Trusted Experts.

References

[1] "Data Encryption Standard", Federal Information Processing Standard, FIPS 46-3.

[2] "Acceleration of Triple DES Encryption using Reconfigurable FPGAs", Wind River technical presentation.

[3] P.Tingey & P. Parkinson "Secure Networking for Avionics Networks", Defence Procurement Analysis, Summer 2003.

[4] PAVE (PLD API for VxWorks Embedded Systems, Wind River partner directory. URL <http://www.windriver.com/cgi-bin/partnerships/directory/viewProd.cgi?id=1239&dtype=4>

Page | [1](#) | [2](#) | [3](#) | [4](#) | [5](#) | [6](#) | [Previous Page](#)

[Home](#) | [News Updates](#) | [In This Issue](#) | [Company Directory](#) | [About Us](#) | [Subscribe](#)

Design by [Net Resources](#).