SDR AT ASTRIUM: PART II
FROM DEFENCE TO CIVIL APPLICATIONS

Taj A. Sturman (Astrium Limited, Portsmouth, Hampshire, UK; taj.sturman@uk4.astrium.eads.net); Mark D.J. Bowyer (Astrium Limited, Portsmouth, Hampshire, UK; mark.bowyer@uk4.astrium.eads.net), and Neil R. Petfield (Astrium Limited, Portsmouth, Hampshire, UK; neil.petfield@uk4.astrium.eads.net).

ABSTRACT

High level aspects of security and Information Assurance (IA) in relation to Software Defined Radio (SDR) are raised in this paper. This paper forms Part II of a two-part series which describes some of the SDR work undertaken at Astrium. Astrium have been involved in SDR for about ten years; part of this effort has culminated in the generation of the UK`s military satellite communication (MILSATCOM) SDR modem, the Paradigm Modem (PM) – the first production MILSATCOM SDR modem of its sort in Europe.

A particular emphasis is placed in this paper on some of the security design issues relevant to TETRA (TErrestrial Trunked RAdio) which is a digital trunked radio system that is very popular with European emergency services. Some security features of TETRA are considered with a view to address pertinent issues for the incorporation of one of Astrium`s commercial-off-the-shelf (COTS) SDR platforms in the rapid resolution of a civil crisis requiring international support.

KEYWORDS

SDR Security, Information Assurance, Defence/Civil Applications, TETRA Security, Waveforms, Transceivers.

1. INTRODUCTION

This paper forms Part II of a two-part series; part I [1] provides some association of the modem with space and aviation, and specifically, aspects of security with respect to SDR are not mentioned.

Astrium have developed an SDR modem with IA provision for applicability to the UK MILSATCOM service. This pioneering system utilises the JTRS` Software Communication Architecture (SCA) v2.2 with security partitioning. A high-level description of the modem is provided in [1], and due to the flexibility and portability inherent to SDR, it has given rise to a range of COTS SDR platforms, some features of which are described in Part I of this two-part series.

1.1 The SDR Concept

The SDR concept essentially gives rise to a flexible radio platform whereby, in principle, software modifications to the system are possible giving rise to a broad range of different waveforms. Part I provides a description of SDR in the broader context including the notions of Cognitive Radio (CR) and Dynamic Spectrum Allocation (DSA).

1.2 Security Provisioning SDR

SDR provides numerous benefits including reconfigurability and portability. The notion of reconfigurability is taken to mean that, given the same platform services, the corresponding platform is capable of hosting multiple waveforms. The notion of portability is taken to mean that, given the same waveform software, the corresponding waveform can operate on multiple platforms. These benefits have associated IA hazards.

The National Security Agency (NSA) defines IA as the set of "measures intended to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation" [2]. These five features, availability, integrity, authentication, confidentiality, and non-repudiation are the backbone of protecting information resources.

When considering security within the environment of a reconfigurable system with degrees of flexibility in the communication architecture, the scope of security for a given system includes:

- Software
  - Architecture
  - Modules
- Firmware
- Hardware
- Application
- Standardisation
- Optimisation techniques.

These aspects of security provisioning need to be extended to encompass its network (s). In addition, the flexibility needs to ensure trusted software and it needs to be put into

Proceeding of the SDR 07 Technical Conference and Product Exposition. Copyright © 2007 SDR Forum. All Rights Reserved

context of ITAR. Furthermore, aspects of certification and qualification become important.

1.3 Organisation of Paper

This paper is divided into essentially six sections with Section 1 being the introduction. Section 2 addresses SDR with security provision and seeks to illustrate the additional complexity arising from the security augmentation to the SCA. The notions of IA provisioning are considered in Section 3, which includes an illustration of the partitioning of the Security Services and Countermeasures model with information states; the significance of a secure operating system is illustrated.

SDR certification is raised in Section 4, an issue which is particularly significant for the enabling of full software portability between various SDRs, particularly within a military environment. These issues are put into context in Section 5 which considers the support of a natural disaster through the use of an international military bridging network supporting blue-light services (e.g. fire, ambulance, police and cost guard). Finally, Section 6 summarises this paper.

2. SDR WITH SECURITY PROVISION

SDR`s flexibility is achieved by abstracting and thereby partitioning functionality to enable the end physical waveform to be separated from the mechanism which enables it to occur. The underpinning aspect of this mechanism of abstraction is the actual hardware and firmware aspects which realise the physical waveform; an illustration of the waveform abstraction and system bandwidth is provided in Figure 1.

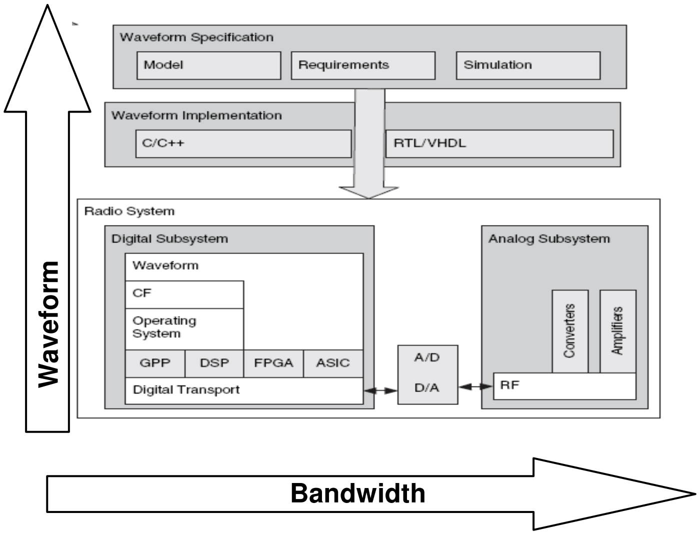

Figure 1: Waveform and Bandwidth abstraction [3]

2.1 Military/Secure SDR

The notions of Security need to be integrated for military SDR. This is particularly relevant for SDR Certification, as the certification process is a means of gaining greater consistency in the application of IT security criteria to hardware, software and firmware. The scope of vulnerability, which has increased due to the very nature of SDR, requires assessment within a given SDR security environment, in order to ensure that SDR Certification is undertaken in an applicable context of operation; issues to be addressed include:

- Threat
- Likelihood
- Vulnerability
- Impact
- Risk
- Residual risk.

This effort needs to be undertaken in conjunction with definitions of scenarios and interoperability requirements in order to yield a system security policy. In the provisioning of a Secure SDR, the notion of waveform/bandwidth abstraction represented in Figure 1 needs augmentation of the system security policy to enable a modem with data separation such as Astrium`s PM; Figure 2 provides an illustration of this concept.

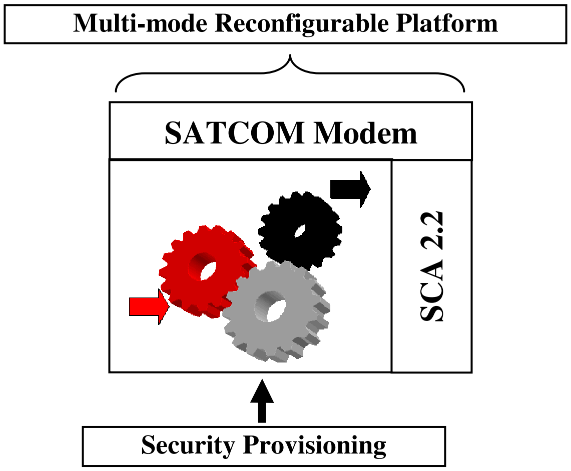

Figure 2: Representation of data separation within the PM

Assurance is significantly more difficult to provision for SDR than it is for traditional hardware-based radios. Once a hardware radio design has been certified to meet functional and security requirements, users can be confident that radios from the production line will meet the requirements through the radio's lifetime. Tampering with radios is possible, but it can only be done to one radio at a time. The adversary must have physical contact with the radio and technical expertise.

However, SDR changes the threat because software updates can modify multiple radios simultaneously. Therefore, physical contact is not necessary because harmful code can be inserted during the development process or during remote software downloads.

2.2 Hardware Limitations on Security

It is also worth noting that the hardware will again impose limitation on what security mechanisms can be employed. Thus when using a platform for new waveforms it is easier to design the waveform security measures to fit the hardware available.

It becomes harder to adapt certain hardware security features to support legacy secure waveforms where the waveforms demand similar security features but at different points in the waveform processing. It is not implementing something that will work but implementing something that works and can be evaluated by the appropriate government IA authority. Designing this aspect of the implementation is as challenging, if not more so, as the signal processing aspects of the waveforms.

3. IA PROVISIONING

IA provisioning requires Security Assessments and Evaluations which are not so straightforward to generalise. The scope of IA includes applications, services and bit-ways; this is shown in Figure 3.

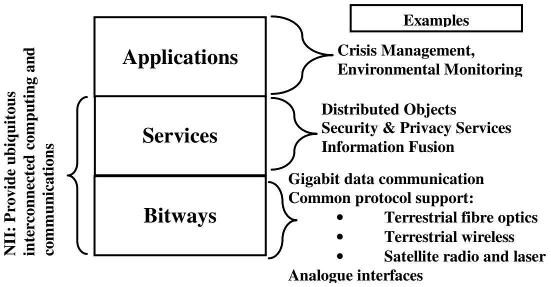
Examples
Applications
Crisis Management, Environmental Monitoring
Services
Distributed Objects
Security & Privacy Services
Information Fusion
Bitways
Gigabit data communication
Common protocol support:
• Terrestrial fibre optics
• Terrestrial wireless
• Satellite radio and laser
Analogue interfaces
NII: Provide ubiquitous interconnected computing and communications

Figure 3: Three-layer architecture for the NII (Modified from [4])

In addition to realising the security policy, the fundamental design goals of an implementation of the reference monitor concept are that it be:

- Tamper-proof (cannot be maliciously changed or modified)
- Nonbypassable (subjects cannot avoid the access control decisions)
- Verifiable (it is correct and implementation of the security policy can be demonstrated).

A modified variant of the Network Centric Operations Industry Consortium (NCOIC) partitioning of security services and countermeasures with Information States [5] is provided in Figure 4. The modification presented in Figure 4 to the original diagram is the indication of Information Classification, such as Unclassified (U/C), Restricted (R), Secret (S), Top Secret (TS), to name four cases.

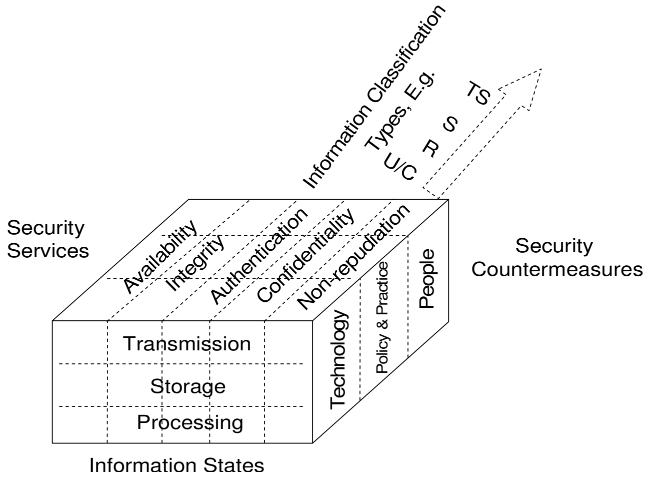

Figure 4: Partitioning of Security Services/ countermeasures with Information States (Modified from [5])

3.1 SELinux

Nearly all operating systems implement some form of a reference monitor and can be characterised in terms of subjects, objects, and security policy rules. Operating systems have two forms of access control: discretionary access control (DAC) and mandatory access control (MAC).

Standard Linux security is a form of DAC security [6]. SELinux adds a flexible, configurable MAC to Linux. DAC has a fundamental weakness in that it is subject to a variety of malicious software attacks. MAC is a way to avoid these weaknesses. Most MAC features implemented so far are a form of multilevel security modelled after governmental classification controls.

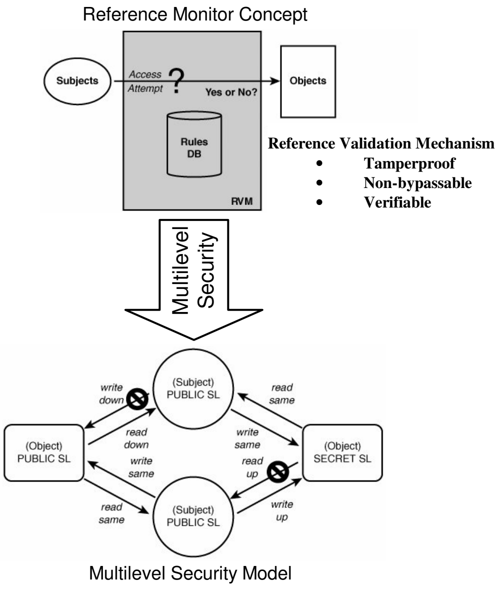

Figure 5: Reference Monitor and Multilevel Security Model [6]

Mandatory Access Control (MAC), where the basis of access controls decisions, was not at the discretion of individual users or even system administrators. This is an implementation of an organizational security policy to control access to objects that could not be affected by the actions of individual programmes; for example, threats on Java are raised in [7].

The funding into the Multi-level Security Model was from the US Military, which focused on protecting the confidentiality of classified government data. In particular, the most common MAC mechanisms implemented to date address the problem of multilevel security, a simplified form of which SELinux is one way of having comprehensive, strong security for Linux.

4. SDR CERTIFICATION

Software certification can provide required levels of assurance. Comprehensive SDR certification could ensure that adversaries cannot circumvent security controls. It should include examination of the SDR device boot procedure and mechanisms to achieve process separation and memory isolation. SDR certification is largely in its infancy – currently the European Defence Agency (EDA) [8] is undertaking an independent appraisal of SDR certification in the absence of US support due to ITAR restrictions. The certification process in the US is undertaken by JTEL, the JTRS Test and Evaluation Laboratory [9].

The SDR Forum has plans to develop protection profiles that could be used in certifications of SDR implementations under the Common Criteria (CC). CC-based [10] certification has a number of valuable characteristics—certifications are internationally accepted and the process is widely viewed as rigorous. The certification process is aimed at verifying the compliance of systems (including networks, devices, testing and evaluation processes) against relevant standards. The qualification process is aimed at verifying the performance of systems against customer's other specifications.

SDR offers the benefit of maximal tactical waveform diversity, that is, SDR enables the ad-hoc reconfiguring of:

- Waveforms
- Networks
- Protocols.

In a military communication system the benefits offered by SDR, in terms of remote flexibility, give rise to new dimensions of threat and vulnerability; figure 6 provides an illustration of protection against an unauthorised security attack. The underpinning notions of SDR need security augmentation to offer robustness to these threats. Therefore, in addition to the SDR implementation, in terms of the SCA and the transceiver API, there is a need to augment the Security API.

Provisioning consistency within the SDR Certification process requires:

- Evaluation criteria
- Evaluation methodology
- Evaluation scheme
- Final Evaluation results.

Figure 7 provides the links to SDR Certification by showing the evaluation context.

Software testing and certification is a critical component of software assurance. SDR users should be advocates for its continued progress, but maturity is still years away. In the interim, both the developers and consumers of SDR technology need to build internal controls to ensure that SDR technology risks are mitigated.

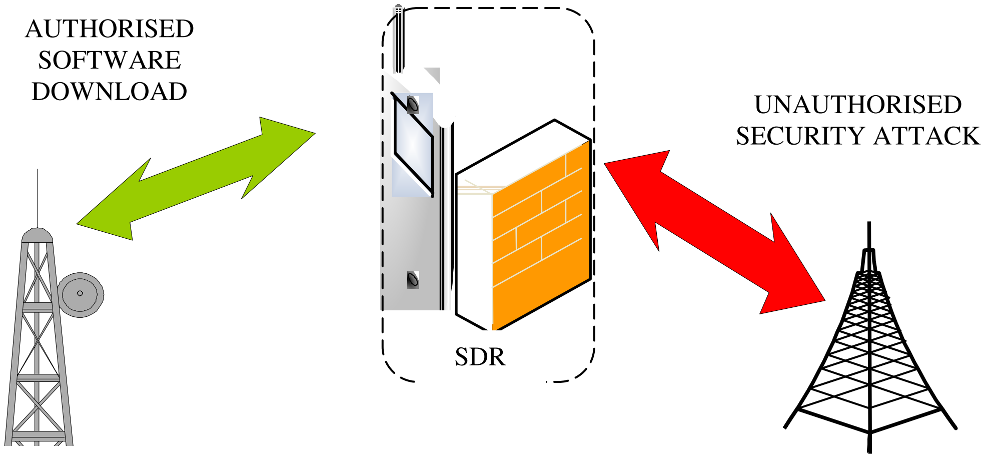

Figure 6: Illustration of Protection against Unauthorised Security Attack

Proceeding of the SDR 07 Technical Conference and Product Exposition. Copyright © 2007 SDR Forum. All Rights Reserved

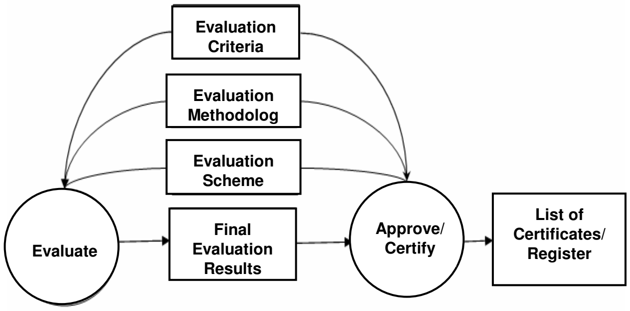

Figure 7: SDR Certification - Evaluation Context [10]

The verification processes for SDR for security will need to encompass the given platform features for the end waveform. Currently, the CC approach is being assessed for applicability into XML. A European Common Architecture based on SCA including security functions and a certification process is aimed at a European common development of a Wideband Network Waveform (WNW) and some other Waveforms (legacy and new) [11]. The goal of achieving an EU WNW will require a robust and flexible platform particularly as many EU states emergency response systems are currently interoperable within a single Member State – this has been observed amongst the various forces called up to intervene in the case of an emergency [12].

5. FROM DEFENCE TO CIVIL

5.1 Bridging

In principle, the bridging process can be made more robust by deploying SDR for porting waveforms from one platform onto another; an illustration of the complexity within defence and the benefits of SDR is provided in Figure 8.

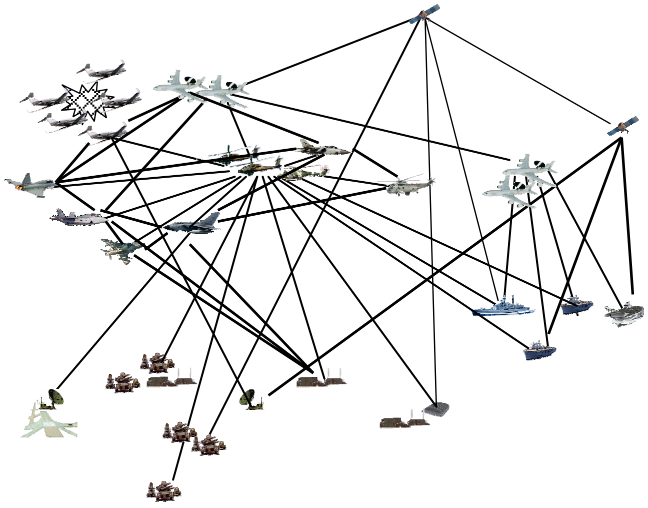

Figure 8: Example Military Waveform Deployment

Considering the complexity represented in Figure 8 with the vulnerability represented in Figure 6 it is clear to see the significance of the Certification process of Figure 7. Various nations have undertaken programmes in SDR specifically due to SDR`s significant flexibility. A recent initiative by the European Union (EU) within its Seventh Framework Programme (FP7) series seeks to identify how the utilisation of SDR can be beneficial in the resolution of a severe national crisis, employing an international effort and the corresponding military backbone [13]. It is envisaged that the scope of the solution would involve the minimal provision of military security but the need for interoperability and portability to enable the waveforms of the various blue-light services to be operational. Within the bounds of a natural crisis, the IA metrics of availability and integrity have been determined as essential [11][12]; clearly the security provisioning changes for a terrorist attack.

5.2. TETRA

The TETRA standards define certain interfaces for a digital trunked radio system [14]. A fundamental feature and a key requirement from conception, has been the need to design-in security. The range of security features offered is capable of meeting the needs of many types of user, including the public safety community. TETRA has not been designed with just the public safety community in mind although their requirements exceed those of most users. IT security features are relevant to TETRA systems with IP based infrastructures to safeguard the vulnerability to attacks via system gateways etc. End to end encryption is also offered as a feature which allows users to be certain that their confidentiality is assured all the way through a system. An illustration of TETRA authentication by the UK Police IT Office (PITO) [15], now the National Policing Improvement Agency (NPIA) [16], is provided in Figure 9.

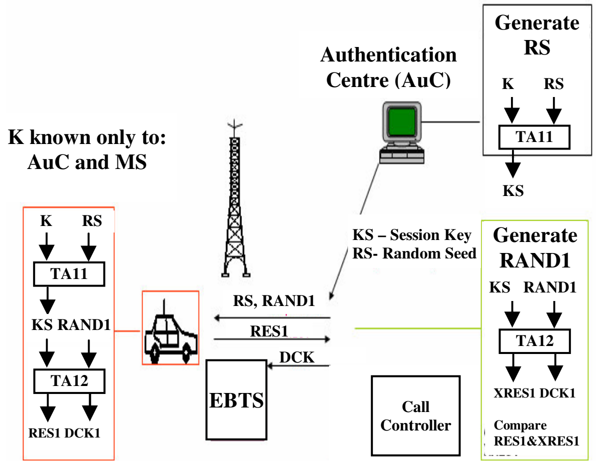

Figure 9: TETRA Authentication Process [15]

5.3 Crisis Support

Presented in Figure 10 is the case where a point-to-point (P2P) bespoke waveform, such as a TETRA/TETRAROL waveform, is being made interoperable with an alternative high-data rate (HDR) waveform. The basis for this form of interoperability is through the use of an SDR platform which supports both types of waveforms achieved through porting.

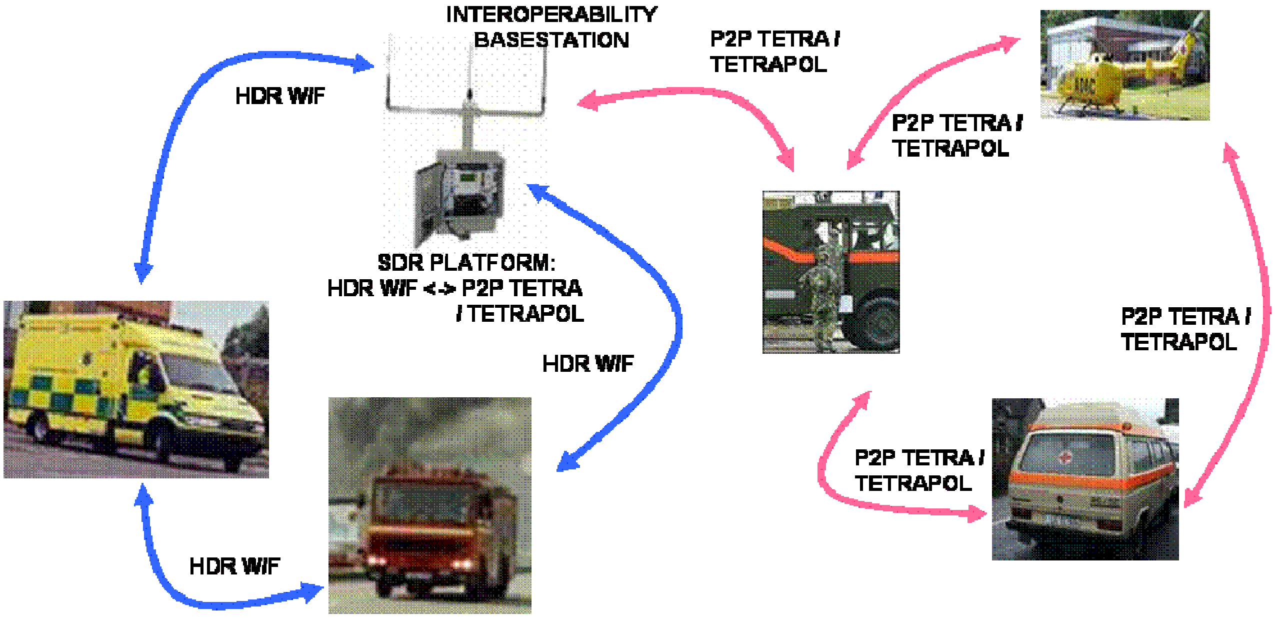

Figure 10: Illustration of HDR-enabled SDR-bridging for international disaster recovery

6. SUMMARY

The inherent flexibility to SDR implies that the platform capabilities can be extended beyond its initial purpose. The original Astrium PM platform was devised using the SCA architecture with appropriate security augmentation for use within a military network for the UK`s MILSATCOM service provision for Skynet 5. Aspects of SDR certification have been considered, a particularly relevant feature for the deployment of a system with the potential for blue-light bridging. It is envisaged that the security mechanisms will need to be modified, depending upon the nature of the emergency – e.g., the IA associated with a natural disaster will be different to that of terrorist attack. It is understood that the IA metrics of availability and integrity, in the context of consistency of information and how it is used, will be key drivers for a natural crisis.

Assessments within various European Member state blue-light operations have revealed interoperability difficulties amongst the various forces called up to intervene in the case of an emergency. This matter within a national scale requires resolving – which can be mitigated by using SDR principles. Furthermore, the provisioning of SDR will enable the expedient establishment of communications required within an international crisis operating joint and multinational interoperability between defence and blue-light communications. An example of HDR-enabled SDR-bridging for international disaster recovery has been considered.

7. REFERENCES

[1] Sturman, T.A., Bowyer, M.D.J. and Petfield, N.J., "SDR at Astrium – Part I: SDR in Space and Aviation", *To Appear* SDRF`07, November 2007.

[2] NSA`s IA Definition, Web-site: http://www.nsa.gov/ia/iaFAQ.cfm?MenuID=10#1

[3] Bard, J. and Kovarik, V., SDR: The Software Communications Architecture, Wiley 2007.

[4] NII Web-site: http://www.eff.org/Infrastructure/nist_frame.html

[5] Network Centric Operations Industry Consortium (NCOIC) Web-site: https://www.ncoic.org/

[6] Mayer, F., MacMillan, K. and Caplan, D., SELinux by Example: Using Security Enhanced Linux, Prentice Hall, July, 2006.

[7] M. Ladue. When Java Was One: Threats from Hostile Byte Code. Proceedings of the 20th National Information Systems Security Conference, 1997.

[8] Gari M., *EDA and SDR Certification*, Sophia Antipolis, February, 2007.

[9] JTEL Web-site: https://jtel.spawar.navy.mil

[10] CCIMB-99-031, *Common Criteria for Information Technology Security Evaluation – Part I: Introduction and general model*, August 1999.

[11] Pereira, J., *Risk, Disaster and Emergency Management*, EC Europa, SMi London June 2007.

[12] Munro, A., Pereira, J. and Fabbri, K., *ICT for Environmental Sustainability and Growth,* Report of the Working Group on Risk, Disaster and Emergency Management, Nov. 2006.

[13] Seventh Framework Programme (FP7) Web-site: http://cordis.europa.eu/fp7/home_en.html

[14] TETRA Web-site: http://www.tetramou.com

[15] Murgatroyd, B., *Introduction to TETRA Security* UK Police IT Organization (PITO); TWC 2005, Frankfurt, Germany.

[16] National Policing Improvement Agency (NPIA) Web-site: http://www.npia.police.uk/

Proceeding of the SDR 07 Technical Conference and Product Exposition. Copyright © 2007 SDR Forum. All Rights Reserved