Aardvark Newsletter

#9

In this Issue:

Our Sponsors

Please join LinkedIn group: Aardvark Roost

Please visit http://www.aardvarkaoc.co.za/History/Aardvark%20History%20V3.pdf for **an update of the History of EW in South Africa. Please send your comments to Dave Howie (davidh@ansys.co.za).**

Events

10th Little Crow Conference

SAAB EDS sponsored a very successful Little Crow conference on the 7th August. This conference and social event were attended by more than 80 delegates.

Aardvark Newsletter #9

11th Little Crow Conference

The date and venues for next half-day conference is:

- Little Crow #11: 17th November at building 22, CSIR, Pretoria.

The conference will have a technology theme and the presenters will be Col George Muller (SSO Air Ops Technology), Nelis Willers, Willie Nel, Jacques Cilliers and Ignus Swart on the topics of:

- EW: Current & Future – A technology perspective.
- Aircraft Vulnerability Analysis by Modelling and Simulation.
- Radar (Details TBD).
- Radar Cross Section (RCS) - Recent advances in the local capability.
- Collaboration opportunities for EW & IW for next generation warfare and defence.

Please register with Annatjie Orsmond, AOC@csir.co.za, fax 012 841 2455 or telephone 012 841 4861 before the 10th November 2014.

Annual General Meeting (AGM)

No dedicated AGM is planned for 2014, but instead, the Board will give an abbreviated feedback of the achievements for the year as well as activities during the last Little Crow conference on the 17th November.

International Events

51st Annual AOC International Symposium and Convention: 6 – 9 Oct 2014, Washington DC, USA.

The theme will be: *Electromagnetic Spectrum Operations in Contested and Permissive Environments*

Automatic Identification System (AIS) and Maritime Domain Awareness (MDA)

The third in a four part series of technical AIS articles.

By Ernie Batty, Technical Director at IMIS Global

AIS use cases

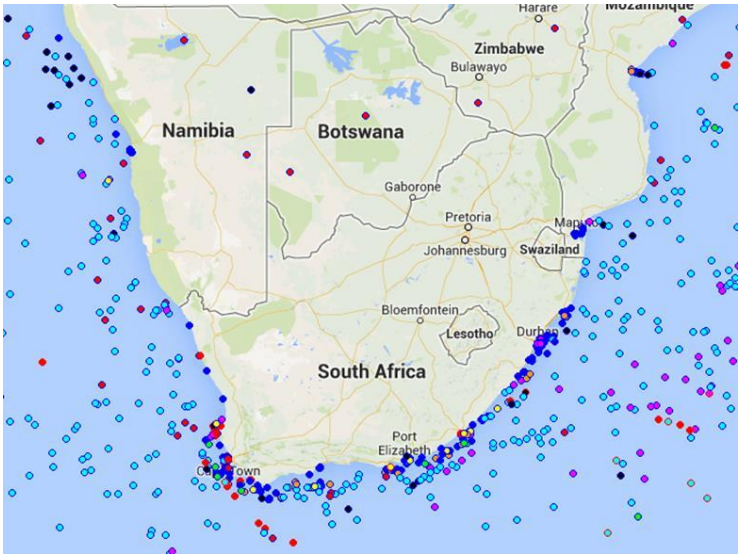
AIS is NOT secret / secure / proprietary!

Governments such as New Zealand have outsourced all national governmental (including security and maritime safety focused) AIS data collection (satellite and terrestrial), processing, storage, reporting and display services to third party service suppliers such as IMIS Global limited while retaining the data fusion on the Common Operating Picture (COP) as an in-house capability.

Due to the open nature of AIS, many consumers of AIS data (security, safety, environmental and commercial entities) have come to realise that purchasing AIS data and network services from third party specialist technology and service providers is attractive thereby eliminating capital and life cycle costs, increasing the number of unique features available to the operators, adding significant scale (100's of operators can connect at the same time from anywhere using the public Internet and encrypted links and capable of viewing >100,000 AIS targets) and ensuring that the AIS systems and sub-systems remain fully compliant with the latest AIS centric specifications that change on a regular basis.

The maritime Automatic Identification System (AIS) is an open and published standard. The AIS data is broadcast without encryption and can be collected, processed, stored, reported on and displayed by anyone with the correct and commercially available applications. AIS is, however, part of every national Maritime Domain Awareness (MDA) strategy and often includes both Terrestrial AIS data (T-AIS) and Satellite AIS data (S-AIS).

The AIS protocols, data contents and network requirements are clearly defined in the ITU-R.M 1371-4, IEC 61162-1, IALA A-124 Recommendations, IEC 62320-1 and the IEC 62320-2 documents. The challenges with collection, processing, storage and display of this AIS data are primarily concerned with volume and scale. There are >130K vessels transmitting AIS data around the world at any one time at a rate of +/-10K messages per second. The S-AIS service providers serve +/-350 messages per second collected from space. Terrestrial systems surrounding South Africa track +/-1,000 vessels at any one time. For strategic purposes, the start and end of voyages of any particular vessel passing through the South African areas of interest is also desirable adding a further data collection, processing, storage, reporting and display load.



All AIS data is available to anyone with the resources to establish the infrastructure or is able to purchase the data from the S-AIS service providers. AIS is **NOT** secret, secure and / or proprietary.

AIS does allow end-to-end encrypted messages to be carried for various uses (messaging and secure position reporting). This does not require the AIS network to be secure since the message is encrypted (AES 128 bit encryption is used) within the published AIS message specifications.

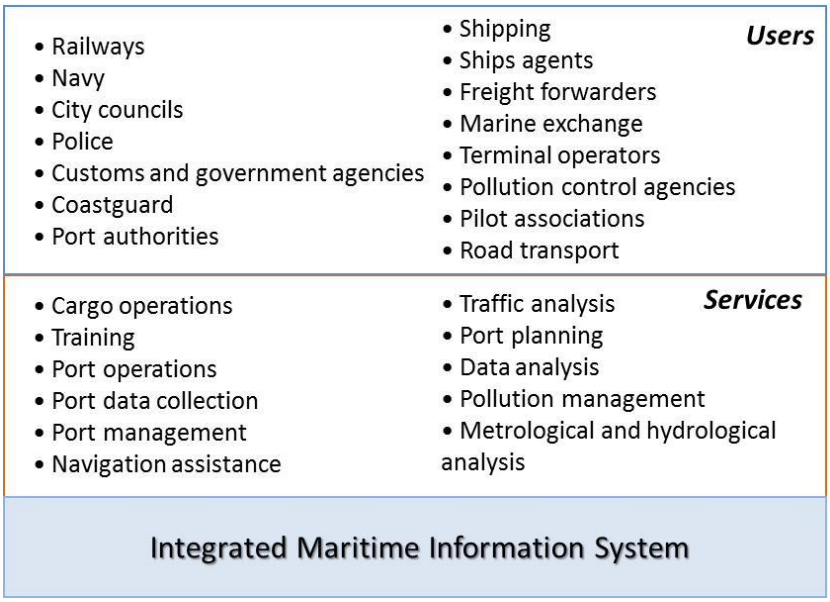
The security, safety, environmental and commercial entities AIS data consumers then add value to the AIS data through data fusion (Radar, Long Range Identification and Tracking (LRIT), Optical, Earth-observation satellites, other asset tracking systems, asset databases) and proprietary reporting tools.

Typical uses of AIS data

AIS data has four primary uses that affects all within the maritime environment:

1. Safety
2. Security
3. Commercial
4. Environmental

The graphic shows the potential of AIS to the various stakeholders (the graphic obtained from the European Union (EU) VTMIS project). These uses are expanded on below.



Safety

When the AIS technology was conceived and proposed, safety was the prime goal. It is officially described as an aid to navigation. The primary safety application is collision avoidance. This can be between vessels, between vessel and land and also between vessels and other floating objects such as buoys (and other Aids to Navigation (AtoN) systems), oil platforms and energy generating systems (surface and sub-surface) that share the same maritime environment.

The primary benefit is the volume of accurate identity, positional and navigational data shared between systems fitted with AIS. This makes significantly more accurate and sensitive systems (decision making and navigational) available to the mariner on board the vessel as well as the shore side Vessel Traffic Service (VTS) systems.

Security

The AIS transmission of a number of unique vessel identity parameters (MMSI, IMO number, Call Sign, Name, Length and width) along with accurate, GPS derived positional and timing information has provided the security authorities with a powerful tool in the maritime surveillance environment. This has now reached the point where a vessel *without* an AIS signature is viewed as a vessel that requires further investigation.

This has given rise to the need for AIS message validation, vessel data validation, data fusion and AIS and vessel data trend analysis. Real time AIS data analysis appliances are available that examine the AIS data stream and attach metadata to the AIS message that indicates the validity of that particular AIS message based on many different message, data, timing and data trend parameters.

The AIS Security Appliances are installed as part of an AIS network and also between AIS networks and VTS and similar systems ensuring that all AIS data used is flagged as trusted / low risk data or as high risk and requiring further attention.

Commercial

Commercial users use AIS data for applications such as port planning, arrivals and departure management, ship reporting validation and fuel management.

As an interesting example of a commercial application, commodity traders use the current position of oil and LNG tankers of interest as an input to their daily trading position. Since the position, route and historical routes of each tanker is also known and can be easily plotted over time (extending to months and years if required), strategic decisions can be made by commodity traders with significant additional information.

Environmental

Large environmentally sensitive maritime areas are being protected by being declared as a Marine Protected Area (MPA). These areas need to be monitored to ensure that vessels do not enter the area or where this is allowed, the vessels are monitored for infringements such as exceeding a Speed Over Ground (SOG) limit. Some of the MPAs being protected are large and include the Australian Great Barrier Reef (GBR). The GBR is managed by the Great Barrier Reef Marine Park Authority (http://www.gbrmpa.gov.au/) and one of the tools that could be used by the Great Barrier Reef Marine Park Authority is the standards compliant **MariWeb** AIS network supplied by IMIS Global Limited to the Australian Maritime Safety Authority (AMSA).

The ability to use the vessels' AIS signature to determine which vessels have spilt oil or polluted the sea in other ways is gaining wide acceptance. The European Union has the Safe Sea project in place (http://ec.europa.eu/idabc/en/document/2282/5926.html).

Conclusion

In the next and final article in this series, we will look at the future of AIS.

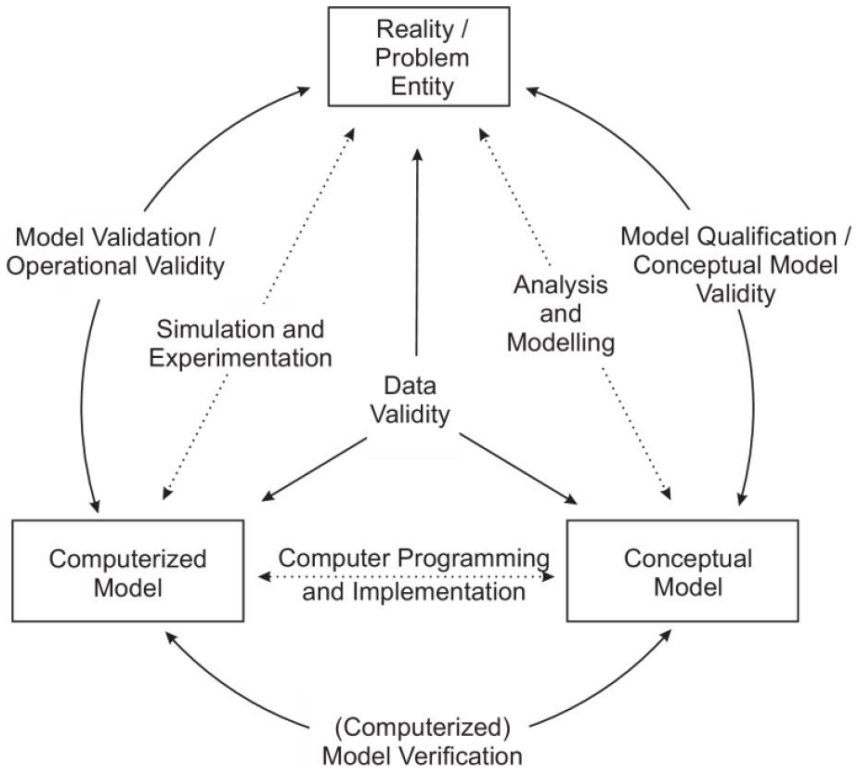
Should you wish to know more about AIS technology, the Hosted **MariWeb** service and the **MariWeb** Security Appliance technology please do not hesitate to contact IMIS Global (www.imisglobal.com).

Research Papers

The Validation of an Infrared Simulation System

Alta de Waal, Cornelius J. Willers, J.H.S Roodt and Azwitamisi E. Mudau - Defence, Peace, Safety and Security (DPSS), CSIR, South Africa, Waikato Institute of Technology – New Zealand.

A commonly-used term in the simulation domain is ‘validation, verification and accreditation’ (VVA). When analysing simulation predictions for the purpose of system solution development and decision-making, one key question persists: “What confidence can I have in the simulation and its results? ” Knowing the validation status of a simulation system is critical to express confidence in the simulation. A practical validation procedure must be simple and done in the regular course of work. A well-known and acknowledged validation model by Schlesinger depicts the interaction between three entities: Reality, Conceptual Model and Computer Model, and three processes: Analysis & Modelling, Programming and Verification, and Evaluation and Validation.



Simplified version of the Verification and Validation Process [extended from Sargent 1999, Schlesinger 1979]

We developed a systematic procedure where each of these six elements is evaluated, investigated and then quantified in terms of a set of criteria (or model properties). Many techniques exist to perform the validation procedure. They include: comparison with other models, face validity, extreme condition testing, historical data validation and predictive validation - to mention a few. The result is a two-dimensional matrix representing the confidence in validation of each of the criteria (model properties) along each of the verification and validation elements. Depending on the nature of the element, the quantification of each cell in this matrix is done numerically or heuristically Most often literature on validation for simulation systems only provides guidance by means of a theoretical validation framework. This paper briefly describes the procedure used to validate software models in an infrared system simulation, and provides application examples of this process. The discussion includes practical validation techniques, quantification, visualisation, summary reports, and lessons learned during the course of a validation process. The framework presented in this paper is sufficiently general, so that the concepts could be applied to other simulation environments as well.

To obtain this paper, please contact Pieter Botha the Operations Manager, Optronic Sensor Systems, Defence, Peace, Safety and Security, CSIR at PBBotha@csir.co.za

Multi-channel Software Defined Radio Experimental Evaluation and Analysis

J. R. van der Merwe, J. Malan, F. D. V. Maasdorp and W. P. Du Plessis - Defence Peace Safety and Security (DPSS), CSIR, Department of Electrical, Electronic and Computer Engineering , University of Pretoria.

Multi-channel software-defined radios (SDRs) can be utilised as inexpensive prototyping platforms for transceiver arrays. The application for multi-channel prototyping is discussed and measured results of coherent channels for both receiver and transmitter experiments are presented.

This paper concludes that a multichannel transceiver system can be created by combining multiple USRPs. However some precautions need to be implemented to ensure channel coherency and reliability.

SDRs were used in the configuration of two different experiments to prove that multi-channel systems can be developed, with minimal additional RF-component requirements. The experiments minimal setup time, thus showing that SDR is an effective rapid-prototyping platform for a range of applications. SDR is thus considered a valuable tool for research and training on a range of RF systems.

To obtain this paper, please contact Rossouw van der Merwe at JvdMerwe@csir.co.za

Industry News

CSIR

New simulation system helps protect South African air space

The CSIR has more than 50 years of experience with the development of electronic warfare systems for the South African National Defence Force. During 2014 the Enigma 4 system was completed. Enigma 4 is an electronic warfare simulation system, used to simulate radar targets such as aircraft.

The Enigma 4 system is able to simulate signals that would be received by a radar system, as well as detect and characterise the radar signals it receives. If, for example the South African Air Force requires an understanding of how the radar on one of its aircraft behaves under the influence of jamming, the system is used to simulate a realistic target for the aircraft's radar, while also injecting a jamming signal. The performance of the aircraft's radar under these conditions can then be studied.

The technology is used by the South African Air Force and Navy, as well as local and international research institutes.

For more information regarding the Enigma system, please contact Klasie Olivier at KOlivier@csir.co.za

Network emulation platform provides a safe means to test network vulnerabilities

The CSIR has developed a network emulation platform that acts as a testing environment for network and device security. The system is used for cybersecurity training, network modelling and advanced analytics to assist the government departments and private sector.

Networks – particularly those in large organisations or state departments – can easily be exposed to security risks due to poorly configured and unprotected network infrastructure. These security risks can expose the organisations to cyber attacks that may lead to the misuse of resources, allow unauthorised access to confidential data and the introduction of viruses and spyware programs.

Protecting networks against these threats can be extremely difficult, particularly if the different types of threats and the areas of vulnerability are not well-understood. The network emulator provides a platform for the high-fidelity replication of existing or planned networks. It has the capacity to generate real-time, network-aware traffic and to test various aspects of the network such as speed, performance, behaviour and security to determine the areas of greatest vulnerability.

By offering organisations the opportunity to adopt a comprehensive approach to network security, the platform plays an integral part in the evaluation and improvement of South Africa's corporate and government network infrastructure.

For more information please contact Joey Jansen van Vuuren at JJvVuuren@csir.co.za

GEW Technologies

GEW Technologies (PTY) LTD expands its market share in spectrum monitoring

GEW Technologies has recently expanded its global market share in Spectrum Monitoring by being awarded a contract in Sri Lanka to supply a Mobile Spectrum Monitoring system and a static High Frequency Spectrum Monitoring System for the local Telecommunications Regulatory Commission (TRC).

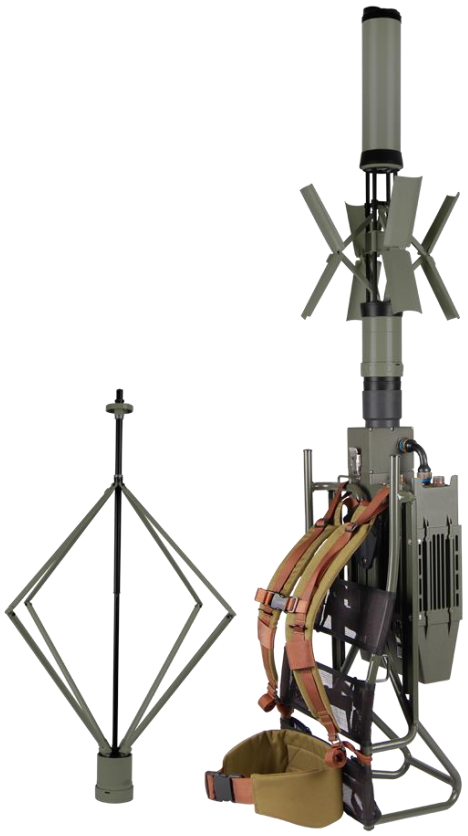
In the Far East, GEW Technologies received a follow-on order expanding its existing Spectrum Monitoring systems in Vietnam. This contract, with the Authority of Radio Frequency Management (ARFM), is to deliver three Control Centres with six Remote Fixed Spectrum Monitoring Systems.

In South Africa, GEW Technologies was selected above five other international competitors in a bid for a National Spectrum Monitoring System for the Independent Communications Authority of South Africa (ICASA). The system will consist of twelve Fixed Remote Spectrum Monitoring systems and one Central Control Station, based in Johannesburg. The remote fixed sites are located in major cities throughout South Africa.

Great interest in GEW Technologies' new multi-role wideband direction finder

GEW Technologies, the South Africa-based Airbus Defence and Space Company who are experts in innovative communications intelligence and security applications, recently launched the MRD7 Multi-role Direction Finder. Great interest in this product has led to sales in various parts of the world.

Modern asymmetric warfare demands equipment suitable for use by rapid deployment troops in order to empower them for such missions. Electronic Warfare has long since been known as a "force multiplier" and the new MRD7 is an example of just this. In a combat scenario, for instance, it would be used by front-line forces to provide real-time information to the battlefield commander on threats detected in the communications bands, along with the location of these emitters. This information would be critical in assessing the enemy order of battle, as well as in directing own forces in order to gain tactical advantage, and to gain control of the spectrum ?)



The MRD7 is an exciting new addition to GEW's extensive range of electronic warfare products. This model has been specifically designed for man-portable and mobile applications where size and weight are critical factors. The MRD7 direction finder provides an extremely wide frequency range of 1 MHz to 6000 MHz, and is a compact, cost-effective and complete solution for full-band direction finding and monitoring purposes. It can successfully be used against modern communication threats such as GSM and TETRA signals.

An important feature of this model is its ability to concurrently monitor signals while performing direction finding. The MRD7 is specifically designed for peacekeeping and low-intensity conflict scenarios.

The MRD7 has been designed for mounted and dismounted deployment in the following operating environments:

- Man on the move – in this mode the equipment is carried on the operator's back and operated via tablet or notebook whilst moving. In this mode the frequency band is 20 MHz to 6000 MHz.
- Man-portable – the equipment is carried to an area and deployed. Full band operations are available with the addition of the HF antenna segment.
- Mobile – the MRD7 is used with a suitable antenna which may be mounted onto vehicles for mobile operations.

"We have noticed the nature of conflict changing to asymmetric warfare and in order to keep abreast of these changes, we have developed the MRD7 to meet client expectations in this environment. We foresee great interest in this equipment," says Mr Carel van der Merwe, Chief Executive Officer of GEW Technologies.

The MRD7 has been designed to operate either in stand-alone mode, or integrated with other MRD7 equipment or even integrated with Tactical Operation Centres. This enables the user to configure a more complete Electronic Warfare solution that includes DF/monitoring and electronic attack.

About GEW Technologies

GEW Technologies (PTY) LTD, an Airbus Defence and Space Company, is a system engineering organization with more than 40 years of market experience in the design and production of sophisticated applications for communication monitoring, direction finding, communication countermeasures, spectrum management and perimeter security.

GEW Technologies is internationally recognised as a leading supplier of comprehensive Electronic Warfare solutions.

Contact details

Tel: +27 12 421 6212
Fax: +27 12 421 6216
E-mail: marketing@gew.co.za
Website: www.gew.co.za

For any inputs/comments on this newsletter, please contact Christo Cloete at ccloete@csir.co.za or 012-841 4485.