<table>
<thead>
<tr>
<th>MEETING</th>
<th>DATE</th>
<th>PLACE</th>
<th>CONTACT</th>
</tr>
</thead>
<tbody>
<tr>
<td>(ICNS)</td>
<td>25-24 May 2007</td>
<td>Monterey, CA</td>
<td>T. Blair, (732) 528-7734</td>
</tr>
<tr>
<td>Radar Resolution, Noise Estimation, and Other GNSS Remarks on the</td>
<td>2007 IEEE/ION Position, Location and Navigation System</td>
<td>St. Petersburg, Russia</td>
<td>G. Schmidt, 617-284-3411</td>
</tr>
<tr>
<td>Back of an Envelope: A Tribute to Fred Dunn</td>
<td>4-8 June 2007</td>
<td>Pisa, Italy</td>
<td>Patrick Woodhead, <a href="mailto:p.w@dstl.gov">p.w@dstl.gov</a></td>
</tr>
<tr>
<td>2007 3rd International Conference on Recent Advances in Space</td>
<td>14-16 June 2007</td>
<td>Istanbul, Turkey</td>
<td>S. Baturer, +90 212 663 2400 x 6355</td>
</tr>
<tr>
<td>Technologies RAST - 2007</td>
<td>18-21 June 2007</td>
<td>Aberdeen, Scotland</td>
<td>V. Silvey, +44 1224 530 429</td>
</tr>
<tr>
<td>2007 10th International Conference on Information Theory</td>
<td>9-12 July 2007</td>
<td>Quebec, QC, Canada</td>
<td>A. J. Scott, (604) 273-5600</td>
</tr>
<tr>
<td>(ICIT 2007)</td>
<td>17-20 September 2007</td>
<td>Baltimore, MD</td>
<td>W. Reznik, +44 0300 2624 2624</td>
</tr>
<tr>
<td>2007 European Microwave Conference (EuRAD)</td>
<td>15-18 October 2007</td>
<td>Edinburgh, UK</td>
<td>E. Benson, +44 (0) 1415 563 989</td>
</tr>
<tr>
<td>2007 AESS BuJ Meeting</td>
<td>17-18 October 2007</td>
<td>Edinburgh, UK</td>
<td>T. Stratton, +61 38 6356</td>
</tr>
<tr>
<td>2007 IEEE/ION Position, Location and Navigation Symposium</td>
<td>21-25 October 2007</td>
<td>Dallas, TX</td>
<td>J.C. Gonda, (703) 488-2772</td>
</tr>
<tr>
<td>(PANS)</td>
<td>5-8 May 2008</td>
<td>Monterey, CA</td>
<td>L. Buzza, (351) 365-9885, tel. 105</td>
</tr>
<tr>
<td>2006 IEEE/ION Position, Location and Navigation Symposium</td>
<td>26-29 May 2008</td>
<td>Rome, Italy</td>
<td>N. J. Littlejohn, +44 207 358 9991</td>
</tr>
<tr>
<td>2008 15th IEEE/ION Position, Location and Navigation Symposium</td>
<td>26-28 May 2008</td>
<td>St. Petersburg, Russia</td>
<td>E. Benson, +44 (0) 1415 563 989</td>
</tr>
<tr>
<td>2008 Oceans 2008</td>
<td>8-11 September 2007</td>
<td>Salt Lake City, UT</td>
<td>E. Benson, +44 (0) 1415 563 989</td>
</tr>
<tr>
<td>2008 Oceans 2008</td>
<td>4-5 November 2007</td>
<td>Ottawa, Canada</td>
<td>E. Benson, +44 (0) 1415 563 989</td>
</tr>
<tr>
<td>2008 Oceans 2008</td>
<td>22 November 2007</td>
<td>London, UK</td>
<td>E. Benson, +44 (0) 1415 563 989</td>
</tr>
<tr>
<td>2008 Oceans 2008</td>
<td>14-16 June 2007</td>
<td>Istanbul, Turkey</td>
<td>W. Reznik, +44 0300 2624 2624</td>
</tr>
<tr>
<td>2008 Oceans 2008</td>
<td>11-13 September 2007</td>
<td>Baltimore, MD</td>
<td>W. Reznik, +44 0300 2624 2624</td>
</tr>
</tbody>
</table>

In This Issue – Technically ......................................................... 2

Articles
◆ Secure Access System Using Signature Verification over Tablet PC .................................................. 3
◆ Safety of Cooperative Collision Avoidance for Unmanned Aircraft ..................................................... 9
  A.D. Zeitlin & M.P. McLaughlin
◆ Power Options for Wireless Sensor Networks .................................................................................. 14
  B.C. Norman
◆ Software Reuse: A Safety-Critical Primer .......................................................................................... 18
  J. Wlad
◆ Fiber-Optic Gyros & Quartz Accelerometers for Motion Control ......................................................... 23
  V.S. Lobanov, N.V. Tarasenko, D.N. Shulga, V.N. Zboroshenko & V.P. Fedotov
◆ Virtual Perimeter Security (VPS) in a Physical Protection System ..................................................... 30
  B.C. Norman & D.G. Adams
◆ VDL Mode E Receiver Performance Measurements ......................................................................... 34
  E. Studenberg

Columns
◆ AESS Radar Systems Panel — H. Griffiths ..................................................................................... 39
◆ What is a Panel? — — Recognize Your Peers — E.H. Hirt ............................................................ 41

News & Information
Radar 2006 Moves to Rome, Italy ........................................................................................................ 40
IEEE AESS Society Organization ..................................................................................................... 42
Fred Daum Tribute Takes the Shape of a Conference ..................................................................... 43
Distinguished Lecturers .................................................................................................................. 44
Ottawa Hosts the 2007 Carnahan Conference ............................................................................... 45
Distinguished Tutorials Program .................................................................................................. 46
Radar 2007 to be held in Scotland .................................................................................................. 47
Membership Application ................................................................................................................ 48
Directory ........................................................................................................................................ 49
Meetings ........................................................................................................................................ 50
Inside Back Cover
Back Cover
Secure Access System Using Signature Verification over Tablet PC

Low-cost portable devices capable of capturing signature signals are being increasingly used. Additionally, the social and legal acceptance of the written signature for authentication purposes is opening a range of new applications. We describe a highly versatile and scalable prototype for Web-based secure access using signature verification. The proposed architecture can be easily extended to work with different kinds of sensors and large-scale databases. Several remarks are also given on security and privacy of network-based signature verification.

Safety of Cooperative Collision Avoidance for Unmanned Aircraft

For Unmanned Aircraft to be routinely used in civil airspace, an effective collision avoidance function is one area deemed essential for safe operation. Like manned aircraft, avoiding collisions with transponder-equipped, or “cooperative” traffic is among the primary hazards.

This paper discusses the necessity of developing various models of environmental and system components in the collision avoidance functional chain. Potential sensitivities and shortcomings of the TCAS collision avoidance system for unmanned aircraft are discussed.

The analysis method of fast-time simulation can develop a rich sample of collision encounter events from the numerous statistical distributions. This provides an established means to demonstrate system compliance with safety targets, when they are established.

Power Options for Wireless Sensor Networks

To combat the security threats of the 21st century it is increasingly necessary to protect ever-remote terrain with wireless sensor surveillance. These systems must be self-sustaining to ensure they are constantly operational. Sandia developed a software simulation tool to validate a variety of renewable energy sources for commercial needs. While this software is heavily used in industry it has yet to be fully applied to wireless sensor networks. Based on simulated solar energy yields two different solar energy systems were designed, built, and deployed to the field. In the time since the solar energy power supplies were deployed, zero hours have been spent on maintenance and it was not necessary to replace a single battery.

Software Reuse: A Safety-Critical Primer

Numerous standards exist to assist software developers in producing higher quality software products. The International Standards Organization (e.g., ISO 9001) and the Software Engineering Institute Capability Maturity Model provide good foundations upon which to improve software development processes and quality. These standards are not often used to develop safety-critical software although some organizations have successfully used SEI-CMM to develop mission critical software. Organizations who sponsor or develop guidance for development of safety-critical software include the US DoD, the United Kingdom Ministry of Defence, the International Electrotechnical Commission (IEC), the Institute for Electrical and Electronics Engineers (IEEE), the Motor Industry Software Reliability Association (MISRA), and RTCA, Inc., (formerly the Radio Technical Commission for Aeronautics).

Fiber-Optic Gyros & Quartz Accelerometers for Motion Control

In article the opportunity of use strapdown inertial navigation system (SINS) on the base of fiber-optic gyrosopes and quartz accelerometers corrected from star sensors and satellite navigation equipment (SNE) for perspective interplanetary spacecrafts motion control on phases of interplanetary trajectory insertion, trajectory correction, and braking during transition to Mars orbit is investigated. Results of onboard control complex accuracy characteristics estimation are presented at the given dynamic spacecraft scheme which is taking into account the liquid oscillations in tanks and structure elements elasticity. At modelling the errors of measuring devices installation, errors of SINS initial alignment and instrumental errors of SINS sensitive elements, variation of control engines parameters were taken into account. The structure of the developed complex of imitation modelling of interplanetary spacecraft controlled motion is resulted. Estimations of active flight legs realization accuracy were received by a method of statistical modelling of spacecraft controlled motion.

VDL Mode E Receiver Performance Measurements

VDL Mode E is a digital communications system proposed as a worldwide standard for replacement of the existing analog AM voice system used for VHF aeronautical communications. It provides a needed increase in voice channel capacity as well as offering a digital data link for CPDLC with the high integrity and low latency needed for time-critical ATC messages.

This report summarizes results of measurements of proposed minimum requirements for an aeronautical receiver for VDL Mode E. A software defined radio (SDR) currently used in Commercial Air Transport communications was used for the tests.

Virtual Perimeter Security (VPS) in a Physical Protection System

There is a need to provide response force personnel with advanced warning of intruder activity in rough terrain outside the traditional facility perimeter. Often the land surrounding a high consequence facility is remote and difficult to sensor with conventional long-range detection systems. In order to combat this difficult problem, Sandia has investigated, developed, and fielded a wireless sensor network that demonstrated the value of providing advanced information of adversary activities. The project used wireless technologies to detect and assess intruders in remote “un-engineered” terrain around a fixed facility. In the time since the wireless intrusion detection system was fielded, minimal time has been spent on maintenance and no batteries required replacement. Sandia’s wireless sensor network provides advanced warning of intruder activities and its installation will improve the security posture of a facility.
Secure Access System Using
Signature Verification over Tablet PC

Fernando Alonso-Fernandez, Julian Fierrez-Aguilar,
Javier Ortega-Garcia & Joaquin Gonzalez-Rodriguez
Universidad Autonoma de Madrid

ABSTRACT

Low-cost portable devices capable of capturing signature signals are being increasingly used. Additionally, the social and legal acceptance of the written signature for authentication purposes is opening a range of new applications. We describe a highly versatile and scalable prototype for Web-based secure access using signature verification. The proposed architecture can be easily extended to work with different kinds of sensors and large-scale databases. Several remarks are also given on security and privacy of network-based signature verification.

INTRODUCTION

Personal authentication in our networking society is becoming a crucial issue [1]. In this environment, there is a recent trend in using measures of physiological or behavioral traits for person authentication, which is also referred to as biometric authentication. Biometrics provides more security and convenience than traditional authentication methods which rely in what you know (such as a password) or what you have (such as an ID card) [2]. Within biometrics, signature verification has been an intense field of study due to its social and legal acceptance [3, 4].

In this paper, we present a prototype for Web-based secure access using signature verification. The increasing use of low-cost portable devices capable of capturing signature signals such as Tablet PCs, mobile telephones or PDAs is resulting in a growing demand of signature-based authentication applications. Our prototype uses a Tablet PC for signature acquisition [5] but it can be easily extended to other signature acquisition devices as well.

WEB-BASED SECURE ACCESS
USING SIGNATURE VERIFICATION

The global architecture of our prototype is shown in Figure 1. A signature verification server manages the verification process. This server communicates with a web server, which manages the communication with the user terminal using the HTTP protocol through a network. In our prototype, the user terminal is a Tablet PC and both the web server and the signature verification server are installed in a standard PC that communicates with the Tablet PC thorough a LAN.

The proposed architecture is highly versatile. User terminal can be any device capable of capturing on-line signatures, from cheap digitizing tablets to more expensive Tablet PCs [5]. It is also highly scalable, since we can use powerful servers capable of managing several transactions in parallel, not only HTTP-based but using any other secured or unsecured protocols. Table 1 summarizes several applications that can use the proposed architecture.

This architecture can also be adapted to work in other situations such as:

- The signature verification server has low storing capacity. Users can be provided with a smartcard with its statistical model stored in it [6]. This approach saves considerable hard disk space in the central server and avoids the statistical models being stolen by a hacker or accidentally deleted by system administrators. On the contrary, the statistical model has to be transferred through a network and thus they can be intercepted by other users if no encryption or secure connection is used.

- The signature verification server has low processing capacity. The user terminal can then be allowed to perform the verification process, notifying the central server the acceptance/rejection decision. This approach saves considerable processing power in the signature verification server and reduces the amount of data to be transferred. In addition, the user templates are never transmitted, so they cannot be intercepted. On the other hand, we

Reference of this work was handled by R.C. McMillan.
Manuscript received December 16, 2005; revised June 16, 2006.
Released for publication September 30, 2006.

Author's Current Address:
0885/6985/07/ USA $25.00 © 2007 IEEE
**Fig. 1. Global architecture of the implemented prototype**

**Table 1. Applications of a network-based signature verification system**

<table>
<thead>
<tr>
<th>Applications</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>e-banking</td>
<td>Access to bank account</td>
</tr>
<tr>
<td>e-commerce</td>
<td>Secure transactions in Internet</td>
</tr>
<tr>
<td>Login</td>
<td>Secure access to home/office computer, LAN, Web account, mobile telephone, laptop, PDA, etc.</td>
</tr>
<tr>
<td>POS (Point-of-Sale)</td>
<td>Secure payment with credit card, verifying customers before charging their credit cards</td>
</tr>
<tr>
<td>Physical Access Control</td>
<td>Secure access to restricted areas</td>
</tr>
<tr>
<td>Medical records management</td>
<td>Secure access to medical records. Only authorized users are allowed to get access</td>
</tr>
<tr>
<td>e-Government</td>
<td>Secure operations such as ID card or driver license renovation, income tax return submissions, etc.</td>
</tr>
<tr>
<td>Electronic data security</td>
<td>Access and encryption of sensitive data</td>
</tr>
</tbody>
</table>

need to ensure that only authorized terminals notify acceptance/rejection decisions.

**USER ENROLMENT**

The next steps are performed in order to enroll a user in the system:

- The user is first authorized by an administrator in the signature verification server. A username and a temporary password are assigned to the user. This ensures that only desired users have authorization to use the signature-based verification system.

- Second, the user is requested to provide five signatures. These five signatures are used to generate a statistical model which characterizes the identity of the user [7]. The statistical model is generated in our prototype using the coordinate trajectories and pressure signals provided by the Tablet PC [5]. Technical details of the algorithm for statistical model generation can be found in [8, 9]. In our system, the user can provide its five signatures remotely with a downloadable application by using the temporary password assigned in the previous step. This scheme provides high flexibility. If a more secure environment is needed, another option is to enroll the users only in the presence of an administrator.

In order to account for the time variability of the signature signals, the five signatures used for enrollment are provided in two different sessions separated by a certain amount of time, typically 1 to 3 days. In addition, the statistical model of the user is updated along time by using the signature acquired in the last successful access.

**THE SIGNATURE VERIFICATION SERVER**

The signature verification server manages the verification process. It receives the requests for verification and decides if the user is accepted or not. In Figure 2 we can see the main window of our signature verification server. It shows the last
transactions that have been realized, which are also stored on a log file. It also allows us to perform the following actions:

- **User authorization**, as described in the previous section.

- **User management**. The next information is available for each enrolled user: name, date of the last successful access, number of unsuccessful accesses since the last successful access, and block status. If a user accumulates a certain number of continuous unsuccessful accesses, he/she is blocked. In Figure 3 we can see the user management window.

- **System management**. This module has the following options: storage place of the user’s data, unsuccessful accesses allowed to the users, communication settings of the signature verification server, storage place of the log file, rules for updating the statistical models of a user, etc.

It is supposed that only authorized administrators have access to the signature verification server.

**USAGE OF THE WEB-BASED SECURE ACCESS CLIENT**

Once enrolled in the system, the user has access to the proper URL using its terminal. Figure 4 shows the main window of our prototype, where the username and a signature realization are requested. If the user is accepted, he/she will be allowed to access his account. If not, an appropriate message will indicate that he/she has been rejected.

**SECURING A NETWORK-BASED SIGNATURE VERIFICATION SYSTEM**

A discussion of issues and concerns related to the design of a secure fingerprint recognition system is addressed in [10]. Some of these concerns also apply in the case of signature verification systems.

When designing a recognition system, we have to decide whether it is going to operate in verification or identification mode [1]. In verification mode, an individual who desires to be recognized claims an identity, and the system compares the captured biometric data with the biometric template corresponding to the claimed identity. In identification mode, the system recognizes an individual by comparing the captured biometric data with the templates of all the users stored in the system. If the number of users is large, verification mode is recommended unless identification is strictly necessary.

Typically, developers and integrators of systems and applications are not the producers of hardware and core software. Several factors should be taken into account when choosing hardware and software components: choose proven hardware and software technology; check standards
compliance with platforms or operating systems; evaluate cost versus performance trade-off; ask for available support; etc. An SDK is usually supplied by the vendors, but system designers will usually have to develop specific applications for managing the enrollment, managing the storage and retrieval of templates and information, setting up the system options, etc.

A policy of how to deal with users with bad quality signatures has to be defined. In signature-based verification this is related to users whose signature is easy to imitate. An attended enrollment can deal with this problem, forcing users to provide signatures which are not easy to imitate, but this may result in future false rejection alarms. It is said that the security of the entire system is only as good as the weakest “password,” so users with simple signatures may compromise the security of the overall application.

System administration is an important issue. The administrator may instruct users and make them familiar with the signature acquisition device. He is also in charge of the state of the acquisition devices if the verification is made in a supervised scenario. Monitoring the system log is also an important task to find out if the system is being subjected to attacks. A threat model for the system has to be defined and the system has to be guarded against them. The threat model has to be based on what needs to be protected and from whom. The typical threats in a verification system are the following:

- **Denial of Service (DoS):** the system is damaged so legitimate users can no longer access it.
- **Circumvention:** illegitimate users gain access to the system.
- **Repudiation:** a legitimate user denies having accessed the system.
- **Covert acquisition:** trait samples of a legitimate user are obtained without his knowledge and subsequently used for illegitimate access.
- **Collusion:** illegitimate access by means of special super-users who are allowed to bypass the verification stage.
- **Coercion:** a genuine user is forced to access the system.

In Figure 5 we can see the main modules and dataflow paths in a signature verification system. The eight possible attack points marked are: 1) Scanner, 2) Channel between the scanner and the feature extractor, 3) Feature extractor, 4) Channel between the feature extractor and the matcher, 5) Matcher, 6) Database, 7) Channel between the database and the matcher, 8) Channel between the matcher and the application requesting verification.

Note that attacks 2, 4, 7, and 8 are launched against communications channels and are collectively called “replay” attacks. Signals in these channels can be intercepted and used at a later time. Attacks 1, 3, 5, and 6 are launched against system modules and are called Trojan horse attacks. A Trojan
horse program can disguise itself as the module and bypass the true module, submitting false signals. For example, a Trojan horse program can perform a circumvention or denial-of-service (DoS) attack by always generating an acceptance or rejection decision in the matcher, respectively. Also, the sensor can be destroyed in a denial-of-service (DoS) attack.

It is very important that the feature extractor, matcher, and database reside at a secure and trusted location. The scanner should implement some security capabilities (e.g.: encryption). Also, a mechanism of trust should be established between the components of the system.

Mutual identification can be achieved by embedding a shared secret (e.g.: a key for a cryptographic algorithm) or by using a Certificate Authority (CA – an independent third party that everyone trusts and whose responsibility is to issue certificates).

**PRIVACY ISSUES**

Privacy is the ability to lead one’s own life free from intrusions, to remain anonymous, and to control access to one’s own personal information [2]. It is widely accepted that biometric identifiers provide positive person recognition better than conventional technologies (token-based or knowledge-based). But several arguments and objections are given against biometric recognition: hygiene of biometric scanners that require contact; negative connotations associated with some biometrics used in criminal investigation (DNA, fingerprint, face); inference of information from biological measurements; linkage of biometric information between different applications, allowing to track individuals, either with or without permission; acquisition of biometric samples without knowledge of the person, allowing covert recognition of

---

**Fig. 4. Main window of our Web-based secure access prototype**

**Fig. 5. Design of a signature verification system.**

The possible security attack points are marked with numbers from 1 to 8
people; etc. The abuse of biometric information is an open issue that should be addressed by governments, industry, and organizations. Unless a consensus is reached, citizens may be reluctant to provide biometric measurements and to use biometric recognition systems.

One way to deal with some of the associated privacy problems is the use of systems with the information in a decentralized place over which the individual has complete control. For example, a smartcard can be issued with the template of the user stored in it [6]. Even more, as the computational power of smartcards is continuously increasing, it will be possible to implement the verification step inside the card in a match-on-card architecture. The card will only have to deliver the accept/reject decision. In that case, neither the template of the user nor the acquired biometric samples are sent to any centralized application.

**CONCLUSIONS**

A prototype for Web-based secure access using signature verification has been described. The proposed architecture ensures high versatility and scalability. The signature verification server, which manages the verification process, is capable of communicating with a variety of sensors through several kinds of networks using standard protocols such as HTTP. It can be customized depending on factors such as: allowed number of users, cost of the acquisition sensors, network used in the access, storing or processing capacity of the signature verification server, etc.

Several issues have to be taken into account when designing a network-based signature verification system: mode of operation (verification or identification), selection of hardware and software components, policy with users with bad quality signatures, administration of the system, definition of a threat model, detection of attacks and implementation of a mechanism of trust between components of the system. Privacy issues have to be also considered when designing a system based on biometric information.

**ACKNOWLEDGEMENTS**

This work has been supported by BBVA, BioSecure NoE and the TIC2003-08382-C05-01 project of the Spanish Ministry of Science and Technology. F. A.-F. and J. F.-A. thank Consejería de Educacion de la Comunidad de Madrid and Fondo Social Europeo for supporting their PhD studies.

**REFERENCES**


Safety of Cooperative Collision Avoidance for Unmanned Aircraft

Andrew D. Zeitlin & Michael P. McLaughlin
MITRE Corporation

ABSTRACT

For Unmanned Aircraft to be routinely used in civil airspace, an effective collision avoidance function is one area deemed essential for safe operation. Like manned aircraft, avoiding collisions with transponder-equipped, or “cooperative” traffic is among the primary hazards.

This paper discusses the necessity of developing various models of environmental and system components in the collision avoidance functional chain. Potential sensitivities and shortcomings of the TCAS collision avoidance system for unmanned aircraft are discussed.

The analysis method of fast-time simulation can develop a rich sample of collision encounter events from the numerous statistical distributions. This provides an established means to demonstrate system compliance with safety targets, when they are established.

INTRODUCTION

Development of Unmanned Aircraft Systems (UAS) is proceeding at a rapid pace, and Government and Industry alike are envisioning numerous uses, aside from battlefield support. There is great pressure to achieve access to the national airspace, but at present no means comparable to those used for manned aircraft are in place. A conspicuous need is to provide protection against midair collision. Manned aircraft utilize a variety of avoidance capabilities, both by the pilot and onboard systems. Some of those aircraft, primarily passenger and cargo carriers, utilize the Traffic Alert and Collision Avoidance System (TCAS II), as a part of their overall safety provision. It is not surprising that TCAS is mentioned as a candidate for use aboard UAS.

Concepts and requirements for operating UAS in civil airspace are in the formative stage, and any role for TCAS must be carefully examined within the broader picture of UAS safety.

The UAS safety case needs to address all of the same hazards that are dealt with by manned aircraft. These include not only cooperative targets, but also non-cooperative traffic, terrain and obstacles, severe weather, and terrestrial features. The TCAS system addresses only transponder-equipped (cooperative) traffic, and does so only when airborne, beginning about 500 feet above the ground. For UAS, a system dealing with this traffic would represent only part of a more comprehensive collision avoidance requirement, whose surveillance system might include a suite of sensors for the various hazard types.

This paper presents the work performed to date from the MITRE research program that is examining the suitability of TCAS for use with UAS. The results will be closely coordinated with industry and government activities, particularly within the RTCA SC-203 standards committee Sense & Avoid Working Group.

CONSIDERING TCAS OPERATION FOR UAS

TCAS was designed prior to UAS technology, so its performance was matched to the operations of manned aircraft which were expected to install it, namely air carriers [1]. This section discusses some aspects of TCAS design that may not be well suited for UAS usage.

Surveillance System

The TCAS surveillance system interrogates nearby transponders using Mode C and Mode S formats on 1030 MHz, and receives replies. It uses antennas mounted on the top and bottom of the aircraft, of which one antenna has direction-finding capability. The transmit power and receiver sensitivity are designed to assure a surveillance range of 14 nm, which is sufficient to establish a timely track when two 600-kt aircraft are approaching head-on, and leave 30 seconds for the Resolution Advisory (RA) and the resulting maneuver. For UAS, where maximum airspeeds should be far less, it should be possible to reduce the surveillance range from the UAS and still detect a target with an equivalent warning time. On the other hand, the warning time parameter
is based on a presumed avoidance maneuver of a certain magnitude. If the UAS cannot achieve that maneuver (discussed below), then additional warning time or other measures may need to be taken to provide the equivalent avoidance capability. This would negate any attempts to reduce the surveillance range.

Response to Resolution Advisories

The surveillance system also provides target data to the TCAS Traffic display. In the cockpit, this display presents a graphical representation of nearby traffic, showing the range, bearing, and relative altitude of the traffic. A pilot-operated control may be used to adjust the range around own aircraft that is displayed, and to show only traffic above or below own aircraft (as well as co-altitude). These controls often are used to reduce clutter, such as during a climbing or descending phase of flight, when traffic at other altitudes might obscure the traffic pertinent to collision avoidance. In the UAS application, the traffic information could be linked to the remote pilot. It could be displayed with heading-up orientation as in the manned cockpit, or it could be adjusted to a North-up orientation using a separate navigation input for own heading. If the surveillance range is reduced as suggested above, the situational awareness benefits of the display would be correspondingly reduced.

For manned TCAS operation, the provision of the Traffic display is meant to build confidence in the system so that its RAs are trusted, and it provides part of the traffic situational awareness picture that pilots desire, supplemented by other information such as see-and-avoid and the radio “party line.” A UAS concept should define the intended means of all aspects of safety provision, and may depart from the role TCAS plays in manned cockpits.

TCAS issues RAs only in the vertical dimension. It is able to form stacks on nearby aircraft and estimate the proximity and rates of range and altitude for each one. The TCAS logic determines the minimum vertical maneuver that will achieve a specified miss distance at the closest point of approach. Its projection is based upon an expectation of pilot delay time and acceleration in achieving the indicated vertical rate. Moreover, pilots are trained not to maneuver laterally based on TCAS traffic information, as the bearing information that it derives for targets is not sufficiently accurate to be trusted for this purpose. For some encounter geometries, it may be difficult to select the correct lateral maneuver from this dynamic display of relative position, especially since pilots are not trained in this skill, as controllers are (for absolute position data).

For the UAS application, if a remote pilot must notice the RA and command an avoidance maneuver, the delays in so doing could be greater than in the manned cockpit. The evaluations of TCAS safety [2] that led to its approval were predicated upon a prompt response, both to initial RAs and even more promptly and vigorously to any subsequent strengthening (for example, “Increase Climb”) or sense reversal (Table 1). For UAS, delays could be considerably greater if communication latencies add time before the

<table>
<thead>
<tr>
<th>RA Type</th>
<th>Delay(s)</th>
<th>Acceleration (g)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial</td>
<td>5</td>
<td>0.25</td>
</tr>
<tr>
<td>Strengthening</td>
<td>2.5</td>
<td>0.35</td>
</tr>
<tr>
<td>Sense Reversal</td>
<td>2.5</td>
<td>0.35</td>
</tr>
</tbody>
</table>

**Table 1. Expected TCAS RA Response Parameters**

recognization of the event (for downlink latency) and to maneuvering the aircraft (for uplink command latency). The UAS concept must specify the remote pilot tasking and resulting workload, the displays, the training requirements, and the decision process before a firm assessment of this delay can be made.

**Could the TCAS RA threshold simply be enlarged to compensate for extra delay?** This approach might succeed for linear collision encounters, but may not affect the warning time for encounters in which a maneuver causes a late encroachment of the protected volume of airspace. Also, the parameters of TCAS were set so as to provide an acceptable tradeoff between achieving safety versus minimizing nuisance alerts from aircraft that were sufficiently separated. A larger protected volume would tend to declare more threats in the latter category and would unbalance the trade. We expect to look for fruitful logic modifications in later efforts.

**Could TCAS RAs be executed autonomously by the UAS vehicle?** This option holds some attraction because it eliminates the communication delays to the pilot and back to the vehicle; it eliminates any reliance on the link operating during the short but critical interval between RA and closest approach; and it eliminates the pilot decision delay and human errors. A safety evaluation would need to consider two sources of errors that could lead to hazardous maneuvers. The first is a system fault that leads to an incorrect RA. The second is a barometric altimetry error for the target aircraft. Altimetry systems, particularly on small aircraft, have a recognized range of inaccuracy. TCAS logic accounts for this error to some extent by the size of its vertical thresholds; but a fundamental tenet of the original TCAS approval was the high probability of the pilot mitigating such a consequence by looking for the target, cued by the traffic display, and rejecting any RA maneuver that seemed clearly wrong. If a UAS design attempts to substitute another sensor that “sees” the target like a pilot, it must either involve the remote pilot in the decision (negating some of the advantages cited above), or develop and implement a decision logic that considers both the TCAS RA and the “visual” sensor input.

*While visual acquisition would be unlikely to help when flying in Instrument Meteorological Conditions, targets with low-quality altimetry systems rarely fly in those conditions.*
Collision Encounter Model

When TCAS was first considered for introduction into the airspace, MITRE constructed a collision encounter model that has become the basis for similar models worldwide. The US model examined moderately close two-aircraft encounters from a variety of terminal airspace locations. The ground radar data was interpolated and smoothed to form tracks, and the qualifying track pairs were characterized in several ways:

- The vertical character of the geometry was expressed in combinations of the two aircraft’s profiles, chosen from:
  
  level
  
  vertical rate
  
  vertical rate, leveling off
  
  level, changing to vertical rate.

- Distribution of vertical rates, including realistic probabilities for transitions from one rate to another;

- Distributions of transitions from rate to level and level to rate;

- Horizontal and vertical separation at the three-dimensional point of closest approach (CPA);

- Whether a crossing of altitudes occurred during the 30 s before or 10 s after CPA; and

- The altitude region of the encounter (TCAS logic parameters vary by altitude).

This model has been used with Monte Carlo fast-time simulation to evaluate each version of TCAS collision avoidance logic. For each such evaluation, a large number of encounters are simulated covering all of the geometry classes and vertical separations (Figure 1). Using a surveillance model for measurement noise and a pilot response model of maneuvering in response to an RA, each encounter is repeated, modeling the separation both with and without TCAS.

Any maneuvers resulting from a TCAS RA can change the separation at CPA, and these are recorded. The Monte Carlo method repeats the nominal encounter many times, drawing specific values of variables from separate distributions. This repetition provides a representative sample drawn from the enormous set of possible combinations. Finally, all the results are combined by weighting them over the proportions corresponding to the traffic observed in the airspace.

Fig. 1. Encounter generation for simulation

The model statistics, drawn from manned operations, would vary for UAS operations.

- Many types of UAS missions have been proposed [3]. Some of these could contain flight profiles very different from conventional manned flight; for example, loitering or patrolling a contained area. The altitude mix also could differ from that used for the airspace model, so that encounter probabilities would fall into different altitude bands.

- UAS vehicle flight dynamics span a wide range of values [4]. Some of these differ greatly from manned aircraft; for example, in speed and horizontal or vertical maneuverability. Some UAS exhibit vertical motion, and can hover.

Fig. 2. Time to Achieve 700 feet with limited climb

Some UAS vehicles are limited in their climb or descend performance. To illustrate the effect of these limits on collision avoidance, Figure 2 presents the calculated time to vertically maneuver from level flight at 0.25g acceleration (the same expected as a manned aircraft using TCAS), to climb or
descend at various maximum vertical rates and achieve a 700 foot vertical separation. This displacement is the value used by TCAS at very high altitudes (i.e., above FL410), and the last value (1500 feet/minute) is the vertical rate expected by the TCAS logic. Although that great a displacement is not required to avoid a collision, the value reflects an allowance for barometric altimetry errors. The figure shows that the maneuver time more than doubles if the vertical rate cannot exceed 600 feet/minute.

When applying the modeling and simulation techniques to UAS operations, the results will only be as good as the underlying assumptions. For fidelity of the results, the particular UAS system concept must be specified and then reflected in the model. Some of the primary issues are:

- Is the UAS remotely piloted in all respects, including collision avoidance, or does it have the ability to maneuver autonomously?

- Are there predictable paths for vehicle failure conditions, such as for a lost control link?

- Is the UAS maneuverability during an avoidance maneuver variable, such as by altitude, weight, temperature, or regime of flight?

The encounter model has served as a basis for TCAS design, since the logic necessarily must involve trades between collision protection and operational acceptability – notably, minimizing nuisance alerts. For TCAS, the threat detection parameters – warning time, acceleration buffer, and vertical alert and separation thresholds – were chosen in part by testing results for the observed “normal” traffic and ensuring that the nuisance alarm rate was tolerably low. At the same time, the detection parameters had to provide sufficient time to alert, maneuver, and avoid a real collision with very high probability. When making similar trades for a UAS, it is not enough to provide the surveillance and alerting for a real collision. The UAS and the manned traffic both need to co-exist without excessive disruption from the alerting system.

The surveillance model must be consistent with the specific system used onboard the UAS. TCAS standards specify its surveillance performance; it is possible that limitations such as vehicle size or power may lead to differences in this function. If different antenna technology is used, variations in field of view could arise. This must be modeled, so that the appropriate encounters (or segments of some encounters) are not incorrectly portrayed as being properly detected by the system. This issue involves the geometric characteristics of UAS-specific mission profiles.

The remote pilot response to a TCAS RA presents an important subject in need of study by human factors experts. The UAS concept for any particular implementation may be among diverse possibilities, including pilot training, experience, workload, displays for both flight dynamics, navigation, mission performance (e.g., surveillance of the ground), communications by data link, and finally, collision avoidance. The suite of displays may not resemble those found on manned aircraft, and in any event, the different situation suggests that there will be differences in piloting performance.

Experience with TCAS in manned aircraft found variations in how pilots used the system and responded to RAs. When it was first introduced, there was a pronounced tendency to over- or under-shoot the intended vertical rate until experience was gained making the avoidance maneuver. For UAS pilots, performance could be better or worse depending on many factors: the displays and controls, their experience piloting the UA, and the ability to make the maneuver without the actual onboard visual scene or experiencing the dynamic sensory effects of aircraft motion.

If there is a risk of pilots ignoring the TCAS RA in preference to other information and maneuvering in a different manner, that hazard must be taken very seriously. In encounters between two TCAS-equipped aircraft, the respective RA maneuver senses are coordinated, and safety is contingent upon cooperating by not maneuvering opposite to the displayed sense.

Some concepts envision a single pilot controlling more than one UAS simultaneously. The questions of workload and confusion will need to be studied and compared to the experience for manned aircraft. This could change the probabilities of some hazards and even could create new ones.

The preceding discussion presumed that a remote pilot would respond to RAs. If instead the UAS was able to maneuver autonomously, other issues arise. One of these is informing the pilot of that maneuver so that he can act appropriately, both during and immediately after the maneuver. Another is defining exactly what the pilot can and cannot control during the avoidance maneuver, when and how that reverts to “normal” capability, and how the pilot is informed of these changes. It would be undesirable to have the pilot taking some action that undermines the avoidance. It also would be misleading to have the pilot conclude the vehicle was non-responsive to his inputs due to some failure, when in fact it was correctly performing an autonomous avoidance maneuver.

SIMULATION RESULTS

The first results examined the sensitivity of TCAS safety to incremental delay. This might be incurred if a remote pilot must respond to RAs, and particularly so if communication delays are significant. Figures 3 and 4 present the Risk Ratio for various incremental delays above those normally modeled for a manned aircraft using TCAS. Figure 3 gives the data for a UAS with TCAS in conflict with a manned TCAS aircraft. Figure 4 shows a UAS with TCAS in conflict with a non-TCAS aircraft. Each data point represents the full set of encounters for the US airspace model, i.e., what was previously a complete safety simulation. These results show
that safety is very sensitive to any incremental delay. For example, 5 seconds of additional delay would approximately double the risk in each case.

**FUTURE SAFETY EVALUATION**

Forthcoming simulations will explore the sensitivities to limited climb and descend performance, and will begin the investigation of some mission characteristics and their effect on collision encounter statistics.

Ultimately, to evaluate the safety of a prospective vehicle, mission, and operational concept, all of the models comprising the simulated inputs, collision avoidance system performance, and pilot and vehicle response, will need to reflect the proposed usage.

**CONCLUSIONS**

The foreseen scope of UAS operations is broad. The safety evaluations must be comprehensive and specific to the system and certain elements of the operation.

The maneuvering characteristics of some UAS vehicles could severely degrade the safety obtained from TCAS, as its logic is presently designed.

If a remote pilot is to be the means of responding to RAS, the communication link and the pilot response characteristics are both sensitive elements in the safety calculation.

The Monte Carlo safety simulations used to evaluate TCAS performance in an airspace must accurately model various aspects of the system. Work must be undertaken to properly characterize sensor performance, human performance, vehicle maneuver dynamics, and encounter characteristics. This last model will depend strongly upon the type of mission profiles to be flown, and the airspace traffic characteristics.

**REFERENCES**


**DISCLAIMER**

[1] Work performed by The MITRE Corporation was produced for the US Government under Contract DTF-A01-01-C-00001 and is subject to Federal Aviation Administration Acquisition Management System Clause 3.5-13, Rights In Data-General, Alt. III and Alt. IV (October 1996).

[2] The contents of this document reflect the views of the author and The MITRE Corporation and do not necessarily reflect the views of the FAA or the DoT. Neither the Federal Aviation Administration nor the Department of Transportation makes any warranty or guarantee, expressed or implied, concerning the content or accuracy of these views.
Power Options for Wireless Sensor Networks

Bradley C. Norman
Sandia National Laboratories

ABSTRACT

To combat the security threats of the 21st century it is increasingly necessary to protect ever-remote terrain with wireless sensor surveillance. These systems must be self-sustaining to ensure they are constantly operational. Sandia developed a software simulation tool to validate a variety of renewable energy sources for commercial needs. While this software is heavily used in industry it has yet to be fully applied to wireless sensor networks. Based on simulated solar energy yields two different solar energy systems were designed, built, and deployed to the field. In the time since the solar energy power supplies were deployed, zero hours have been spent on maintenance and it was not necessary to replace a single battery.

INTRODUCTION

Photovoltaic (PV) power supplies for use with wireless sensor networks were designed and implemented by Sandia National Laboratories. Advanced photovoltaics (PV) coupled with rechargeable batteries, provide continuous power for both the wireless sensors and remotely located video assessment equipment. The PV power supply is scalable in size, depending on the system energy requirements and the expected solar resource at the intended geographical location. A PV system performance model was used to optimize both the solar array size and the required battery capacity for each application. Several design objectives were addressed, including: long-term autonomous operation, smaller batteries, and lower cost sensor networks.

The PV performance model used to optimize the system design provided an accurate simulation of the expected energy available from the array of solar cells. Simulations include detailed performance characteristics of the high-performance solar cells and provide hourly estimates for voltage, current, and power from the array. The National Solar Radiation Database provided hourly solar resource and meteorological conditions based on thirty year averages for each site considered. Different PV array orientations (horizontal, vertical, tilted) significantly influence the annual energy available, therefore different possibilities are being considered in the simulation. The system design goals were to have enough PV energy available to fully recharge the battery during typical sunny days, and to have sufficient battery capacity to ensure 24-hour operation during extended periods of stormy weather. A detailed energy balance was conducted to account for the expected load (power) profile of the system, as well as parasitic energy losses in the system components. Successfully achieving the system design goals resulted in a power supply which provided independent operation and dramatically reduced the need for battery maintenance or replacement.

POWER SOURCE SELECTION

Wireless intrusion detection and assessment equipment is typically deployed in locations where utility-based power is unavailable. Historical solar and climate data from the US National Solar Radiation Database and the US National Oceanic and Atmospheric Administration information, combined with the equipment’s continuous power load, allows for selection of a power supply concept. The concept may be a single energy-scavenging device (solar, wind, hydro) combined with traditional battery energy storage, or may require a combination of multiple energy scavenging devices.

WIRELESS INTRUSION DETECTION EQUIPMENT

Sensor Node Equipment Definition

Sandia National Laboratories has deployed wireless intrusion detection sensor node units which are capable of powering a 1.3Watt, 12 Volt Direct Current (DC) continuous load in Albuquerque, New Mexico. The solar power supplies are large enough to provide power to externally connected monostatic microwave sensors, active infrared beam-break sensors, seismic sensors, and magnetometers, as well as a long-haul wireless radio. The sensor nodes transmit detection events along with state-of-health messages to a command center receiver located several miles away.

Author's Current Address:
B.C. Norman, Senior Member of Technical Staff, Sandia National Laboratories, PO Box 5800-0780, Albuquerque, NM 87185, USA.
Based on a presentation at Carahuan 2006.
0985/89/07/ USA $25.00 © 2007 IEEE
Fig. 1. Deployed Wireless Intrusion Detection Sensor

Figure 1 shows a sensor node with a solar panel and lead-acid battery supplying power to monostatic microwave sensors, seismic sensors, and a long haul-wireless radio. This sensor node unit was deployed approximately three miles from the command center.

Sensor Node Power Supply Model

Solar panels that are rated for this amount of power are somewhat difficult to find in industry. Due to a rather limited market, the sensor node’s power supply was built around a single 10 W (rated) photovoltaic panel. The solar arrays deployed as part of this project are constructed with durable glass covers with metal frames.

Since the solar panel was already selected, the modeling and simulating was somewhat constrained. The following section will calculate power outputs for the sensor node’s PV power supply under a variety of conditions and installed in a variety of locations.

Sandia’s Photovoltaic Modeling Tool

Sandia developed a modeling tool that was validated by industry and is now commercially available [1]. The model utilizes model specific solar panels and thirty years of historical data to build an empirical model of the photovoltaic power supply. This simulation tool is different than others on the market since it uses “real” solar panels from manufacturers to build the empirical model. Other simulation tools use only the label or the solar panel’s surface area to estimate power output. Often there are differences in conversion efficiencies and output voltage levels from manufacturer to manufacturer. Since model specific solar panels are used to populate the simulation database, the modeling tool is often less cumbersome and more accurate than generic simulation tools.

Sensor Node Simulation

The sensor node’s (SN) photovoltaic power supply was simulated in twelve locations throughout the United States to validate its performance in these environments. With only a single exception, the Pacific Northwest Rain Forest, the solar panels were able to provide at least 1 W of continuous power to the sensor node for the entire year. Figure 2 shows the results of this analysis.

Fig. 2. Average available energy for solar array power units located in Albuquerque, Nevada, and the US Pacific Northwest. The panel was facing south and sloped at 35°

Fig. 3. Average continuous output power for a SN unit located in Albuquerque, NM. The panel was facing south and sloped at 35°

The SN solar (or PV) energy-power supply works well and has required no maintenance during its time in the field. The small PV-power supply supports a continuously connected load of 1.3W. The SN utilizes a 12 V, 12 Amp-hour, sealed lead-acid battery to store the solar energy during the day and releases the energy back to the SN at night. In the future, thin-film cells may be incorporated into the packaging of the SN. Figure 3 shows the continuous...
power load a solar panel can support when installed in Albuquerque, NM.

**Solar Array Output versus Orientation**

The following analysis provided estimates of the daily average energy available (Wh) for each month of the year for three different array orientations (horizontal, vertical, latitude tilt angle). For varying application sizes, the energy values determined for the 100-cm² array can be scaled up or down in proportion to the array area and to the cell efficiency. Figure 4 illustrates the influence of array orientation and season on the daily energy for one site, Albuquerque, NM. Calculated daily average energy available from a 100-cm² array of silicon solar cells oriented three different ways is also shown.

**WIRELESS ASSESSMENT EQUIPMENT**

**Assessment Node Equipment Definition**

The wireless assessment equipment Sandia National Laboratories deployed in 2005, utilized Internet Protocol (IP) based imagers and high-end commercial off-the-shelf, ad-hoc, mobile radios to transmit snapshot and streaming images several miles in rugged mountainous terrain. The photovoltaic power supplies were designed to provide 30W of continuous load DC power during all seasons when it was installed in Albuquerque, NM, as shown in Figure 5. Simulation results suggest that the solar energy system is suitable to provide at least 30W of power in most locations throughout the entire US.

The video assessment photovoltaic power supply utilized four Shell Solar SQ75W panels and two lead-acid batteries capable of supplying enough energy for 48 hours to compensate for extreme periods of low solar radiation. The design of this system was calculated and validated until performance was acceptable. The calculations were performed with the same simulation tool [3].

The solar panels have a total rated value of 300W, however, the panels typically only deliver this amount of power under ideal solar radiation levels. Dust and dirt on the panels, incidence angle with regards toward the sun, seasonal radiation levels, and the age of the panels all affect the power output of the solar panels. In addition to these factors, there are also inefficiencies when charging the batteries and when alternating current (AC) power is required to power equipment. These effects make this solar panel array capable of supporting a substantially smaller continuous power load.

**Simulated and Actual Performance Results**

Figure 6 shows simulated power output for the photovoltaic and lead-acid battery power supply when deployed in Albuquerque, NM. Since August 2005, when the units were installed, they operated well including a week of poor weather conditions when there was two feet of snow as well as times with heavy rain.

**OTHER RENEWABLE POWER RESOURCES**

Sandia National Laboratories deployed this wireless sensor network in the desert of the southwestern United States. This particular area of the United States boasts an abundance of solar energy for harvest. Due to the constant presence of solar energy, other power sources are not necessary, nor are they feasible. For example, hydropower is virtually nonexistent in the southwestern desert; therefore it would be impractical to consider hydro energy as a power source in this environment.

Although solar arrays worked well to power this wireless sensor network, there are other sources of renewable power that may need to be considered in some deployment locations. Two other popular ways to generate renewable energy are through harvesting water and wind energy by converting their kinetic energy into electrical energy. These power sources are sometimes used in combination with solar power. The renewable energy industry calls power supplies, that harness more than one type of renewable energy source, a hybrid system. However they may be also be used as stand-alone systems with proper design.
Fig. 6. Power output for unit located in Albuquerque, NM with the solar arrays panels facing south at 35° and 90° slopes

Hydro Electric Power

Hydropower (waterpower) harnesses the energy of moving or falling water. This is usually achieved in the form of hydroelectricity. Today there are several small (350-1,200W) commercial-off-the-shelf (COTS) units that can be installed in streams and rivers. Since water is relatively predictable there is a decreased need for an energy storage media, such as batteries. In addition, there is often little to no environmental impact as water flow is relatively undisturbed with the introduction of these small devices.

The small physical size of a hydroelectric generator allows for installation of semi-covert video assessment and detection equipment. Water is a fantastic source of renewable energy and should be investigated when there are continuously flowing streams and rivers in a deployment area.

Wind Power for Wireless Equipment

Wind is also an excellent source of energy as it contains a significant amount of kinetic energy that can be relatively easily harvested to power wireless sensor network equipment. Large commercial wind generation facilities are typically connected to utility power as wind is difficult to predict and has a large variation in the amount of energy it can output. Due to the unpredictable power output a large battery bank is required to store energy during non-windy conditions. Wind is not ideal as a stand-alone power system, however, it is often very successful when used to supplement power output from solat panel arrays.

CONCLUSIONS

A well-designed power supply and intelligent power management can result in long-term autonomous operation, smaller batteries, minimize maintenance, and lead to lower cost wireless sensor networks. Power management is extremely important when equipment must be self-powered and last for years without maintenance.

REFERENCES


[2] Maui Solar Energy Software Corporation, 810 Haiku Road, #113, Box 1101, Haiku, HI 96708, USA.
Software Reuse:
A Safety-Critical Primer

Joseph Wlad
LynuxWorks, Inc.

ABSTRACT

Numerous standards exist to assist software developers in producing higher quality software products. The International Standards Organization (e.g., ISO 9001) and the Software Engineering Institute Capability Maturity Model provide good foundations upon which to improve software development processes and quality. These standards are not often used to develop safety-critical software although some organizations have successfully used SEI-CMM to develop mission critical software. Organizations who sponsor or develop guidance for development of safety-critical software include the US DoD, the United Kingdom Ministry of Defence, the International Electrotechnical Commission (IEC), the Institute for Electrical and Electronics Engineers (IEEE), the Motor Industry Software Reliability Association (MISRA), and RTCA, Inc., (formerly the Radio Technical Commission for Aeronautics).

RTCA/DO-178B

RTCA, Inc. developed RTCA/DO-178B as a guidance document that recognizes the various degrees to which software functions may impact safety. The first versions of DO-178 were produced in the 1980s and the latest version was published in 1992. While the FAA does not mandate or enforce the use of DO-178B to comply with safety standards for software development, it encourages its use by making compliance with other standards seemingly more arduous.

At the system level, Federal Aviation Requirements and System Operational Requirements are inputs to the system safety assessment process. Here in systems such as automatic pilots, decisions about hardware platforms, software usage, redundancy, and outcomes of given failure modes will have a direct impact on software design and verification efforts. Likewise, limitations on software design and verification may cause changes to the system design or assessment process. The outcome of a system safety assessment is a determination of failure conditions and the impact of those failure conditions on the safety of the aircraft and its passengers. Once the system failure conditions are known as well as how latent software defects may affect aircraft safety, then the level of rigor required in the software verification process can then be determined.

FAA CERTIFICATION PROCESS

The certification process for commercial aircraft is such that systems are certified together on the aircraft platform through a series of flight tests. Flight-testing is the final stage of testing during certification of aircraft systems. Prior to the flight test phase, there will likely be a series of integration tests that take place in a laboratory environment. Certification credit for both hardware and software is accumulated over time during laboratory and flight-testing. Configurations of both hardware and software are monitored closely so any change impact to certification credit is minimized. Since there is such a strong coupling between hardware and software configuration, historically, final certification credit is given to the system and not a given hardware or software version.

Recent developments within the FAA have now opened the door to certification acceptance of software independent of a hardware platform. This notion of Reusable Software Components promises economic benefits to those that make use of the FAA's guidance. In order to fully appreciate the concept of Reusable Software Components, it is useful to review the RTCA/DO-178B guidance document in more detail.

RTCA DO-178B BACKGROUND

The level of effort to comply with the objectives of DO-178B will vary based on software criticality (which is related to how latent software defects can contribute to a failure condition). The level of effort is also proportional to the size of the software under consideration. RTCA DO-178B defines five software levels, each related directly to the failure condition that can result from anomalous
Table 1. DO-178B Software Levels

<table>
<thead>
<tr>
<th>Failure Condition</th>
<th>Software Level</th>
<th>Number of Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catastrophic</td>
<td>Level A</td>
<td>66</td>
</tr>
<tr>
<td>Hazardous / Severe - Major</td>
<td>Level B</td>
<td>65</td>
</tr>
<tr>
<td>Major</td>
<td>Level C</td>
<td>57</td>
</tr>
<tr>
<td>Minor</td>
<td>Level D</td>
<td>28</td>
</tr>
</tbody>
</table>

behavior of the software. In Table 1 are the failure conditions, the five DO-178B software levels as well as the number of objectives required to satisfy the requirements of each level.

DO-178B describes the process objectives for each phase of a defined software life-cycle. This life-cycle generally follows the waterfall model of software development, but most developers can use any software development model and still comply with the DO-178B objectives. The DO-178B processes are:

- Planning Process;
- Development Process;
- Requirements Process;
- Design Process;
- Coding and Integration Process;
- Testing and Verification Process;
- Configuration Management Process; and
- Quality Assurance Process.

Each process has inputs, outputs, and transition criteria that assist the development team in moving from one phase to the next. Descriptions of evidence are needed to show compliance with each DO-178B objective. The verification processes will result in the creation of a large set of artifacts (mostly documents) that will be reviewed by the certification authorities or their representatives. Table 2 provides a list of DO-178B planning and verification documents that must be produced as part of the verification effort.

The PSAC is the “contract” between the certification authority and the developer. It defines what the applicant intends to certify and describes the processes and tools that will be used during the certification effort. This document is reviewed and approved by the certification authority or its representatives. The other documents that are actively reviewed and approved are the Software Accomplishments Summary (SAS) and the Software Configuration Index (SCI). The SAS is a summary of the DO-178B verification process as viewed against the original plan (PSAC) and the SCI defines the exact configuration of all software, tools, and documentation used during the certification process. As can be appreciated, verification to all DO-178B objectives is a costly and labor-intensive process. The next section provides some background on certification costs when addressing DO-178B requirements.

Software Economics
A common question asked by software managers is:
“What does it cost to certify a line of software to
RTCA/DO-178B? Intuitively, it would seem that it is much more costly to certify software to Level A rather than Level C given that Level C has only 57 objectives and Level A has 66 objectives. But experience has shown that the difference in cost between Level A and Level C is not that great. This is evidenced by the fact that all the deliverables defined in Table 2 are required both for Level A and Level C software. In fact the software planning and software development objectives under DO-178B for Level A and C are identical. The differences between Level A and Level C from a verification perspective include the requirements, design, testing, and analysis processes. Level A verification adds in the requirement of independence for some objectives (where the development and verification efforts are accomplished by different persons). These added activities can indeed add engineering labor to the certification effort; however, the added cost is likely to be a small percentage of the total certification effort.

Where Level A certification can get expensive is usually through the certification scrutiny an applicant will face when all verification efforts are complete. Convincing an auditor or host of auditors that have the responsibility to “sign off” on software where loss of life could result from failures can be challenging if the applicant has not adequately addressed the planning, requirements, and verification processes. Audits can result in added activities that extend project schedules and increase costs.

Useful Metrics

Costs of DO-178B certification vary greatly depending on engineering expertise and code size. One has often heard of the “multi-million dollar” answer when asking the cost of certification of any software to DO-178B, regardless of size. So, how do we more accurately predict the effort required?

There are a number of ways to scope the level of effort required for DO-178B certification. One useful way to scope the effort is to examine the size of artifacts from previous certification efforts. A useful metric is to plan on 2-4 requirements per function or one requirement for every 5-10 lines of code. Each requirement will need to be tested, resulting in one test file for every 2-4 requirements. The requirements, design, code, and test artifacts will need to be reviewed via checklists. Additionally, the artifacts need to be linked to show traceability between requirements, design, code, and tests/results.

To assess a cost for all this effort means that one must estimate the engineering labor required for each of these activities. How long does it take an engineer to produce a requirement from existing source code? One way to find the answer is to ask the engineers to estimate the effort for each activity (it is presumed that the engineer is very familiar with the software and design). One would then repeat this process for each of the other activities defined below (design, tests, reviews, etc.).

Experience has shown that the cost of certification per line of code can range from $50 to $100 depending on the cost of labor in a given organization. That would mean that certification of 100,000 lines of code could range from $5 million to $10 million. These estimates are only guidelines that must be substantiated and corroborated by detailed analysis of the source code, engineering judgment, and compensation for risk factors such as certification experience, use of language features, and relationship with certification authorities among other things.

Given the heavy expense involved in DO-178B verification, use of an accepted Reusable Software Component can help reduce both certification costs and risk.

THE PAYOFF: RSC

Previously, it was stated that Level A certification is more costly and risky from a project perspective because of the auditing obstacles faced by potential applicants. Once Level A certification is achieved, an applicant will work hard not to disturb the certification credit. This can be challenging because with software, change is inevitable, leading one to open up the “Pandora’s Box” of certification credit. So, how does one make changes without affecting certification credit that has been granted previously? The answer lies in the concept of the Reusable Software Component.

Recall that DO-178B certification credit is granted only when software is installed in a target system and verified both in the laboratory and on the aircraft. This means that each time software is redeployed on new hardware, one must re-verify the software on an aircraft platform. The FAA’s recently released guidance on RSC now allows for “acceptance” of software independent of a hardware platform enabling developers to take certification credit on one project and apply it to future projects. This applies to components such as operating systems and networking protocols that can be reused (in unadulterated form) across hardware platforms.

In order to take advantage of reuse, the software component indeed needs to be reusable; that is it should not be adulterated when moved to other hardware platforms. This can be challenging for software components such as an operating system where dependencies on hardware make it difficult to create a hardware-agnostic configuration. LynuxWorks, Inc. (www.lynxworks.com), has successfully developed a time and space partitioned operating system component that has been accepted by the FAA as a Reusable Software Component. This means that developers can take credit for previously verified DO-178B objectives without the added cost of risk of re-verification or audits. The next section provides a background on AC 20-148 and how developers can achieve RSC acceptance.

AC 20-148 Background

This advisory circular describes a process by which one can gain FAA acceptance of a software component that can be used in subsequent certification efforts without requiring re-verification activities or additional audits by certification authorities. Use of the RSC guidance results in an acceptance
letter from the FAA, which enables future users of the software component to employ the RSC in their projects saving time and money.

The RSC advisory circular assumes use of DO-178B as the basis for software certification. The goal is to obtain full or partial credit for as many objectives as possible so they can be reused later. This occurs in two phases: 1) the first-time approval; and 2) subsequent or follow-on use of an accepted RSC. The initial approval of an RSC works largely the same as any software approval today. One must certify the RSC to meet DO-178B objectives using a standard Type Certificate, Supplemental Type Certificate or Technical Standard Order process. Ultimately the approval will be on a given aircraft platform which then results in an acceptance letter from the FAA provided no safety issues with the RSC are found.

During the first-time approval, more planning and effort is required to meet the guidance objectives of the RSC. The actors in the RSC process are the RSC developer and the Integrator. The RSC developer declares intent to produce an RSC in a PSAC that is submitted and approved by the certification authority. The following considerations must also be addressed:

- Detail plans for satisfying each applicable RTCA/DO-178B objective;
- Identify which objectives the RSC will satisfy and which objectives it will partially satisfy;
- Clearly state an agreement to develop the RSC for reuse in future projects;
- State the intent to comply with AC 20-148;
- Define the failure conditions, safety features, protection mechanisms, architecture, limitations, software levels, interface specifications, and intended use of the RSC; and
- Describe the proposed certification liaison process (including communication and coordination focal points) to all involved stakeholders (FAA and integrator).

For each DO-178B objective, the RSC developer will need to provide a table that outlines each objective, its description, the amount of credit being sought, any assumptions, the means of compliance and what, if any, activities remain for the integrator of the RSC. This table will look very similar to a traceability matrix, but it will have added information for the subsequent users describing what other verification activities remain to retain certification credit or to fulfill any partially achieved objectives.

Because DO-178B is written assuming software integration tests will be done as part of the verification process, it is impossible for an RSC to take 100% credit for all DO-178B objectives because an RSC developer cannot make concrete assumptions about future applications that will use the RSC. There will always be activities for follow-on integrators. These may include the following:

- Data coupling analysis;
- Control coupling analysis;
- Timing analysis;
- Memory analysis;
- Software integration testing;
- Hardware-software integration testing; and
- Robustness testing of RSC functions, including safety and protection features.

In order to facilitate the reuse process for future integrators, the RSC developer should provide guidance to the integrator on how to fulfill the remaining objectives and activities. The RSC developer should provide information in a datasheet such as:

- RSC functions;
- RSC Limitations and Assumptions;
- Analysis of potential safety concerns and mitigation strategy;
- Configuration and Characteristics;
- Supporting data; and
- Open Problem reports.

Additionally, the RSC developer will provide the integrator with the so-called type design data meaning software requirements data, design description, source code, executable object code, Software Configuration Index, and Software Accomplishments Summary. Moreover, the RSC developer should provide information on how to interface to the RSC, test and verification procedures and, in the case of a partitioned operating system, provide memory margin and timing margin analyses.

An RSC in the form of a time and space partitioned operating system such as LynxWorks’ LynxOS-178 presents unique challenges because its approval means that subsequent users are able to run multiple applications on the same platform – some of which may be safety-critical and others which may not be certified at all. Unique here is the
The concept of proven fault containment, a failure in an application such as a web server shall in no way affect the operation of the operating system or a critical function such as a display system. Likewise, use of shared resources should not allow for propagation of failures.

A lot of testing, analysis, and verification is needed to ensure that fault containment is guaranteed. A detailed set of tests and analyses are required to demonstrate resource (device drivers, memory, etc.) partitioning and time partitioning. The integrator will need to rely on data such as a timing margin analysis (a time budget outline of kernel services and critical sections of code), a partitioning analysis (addressing software control coupling, data coupling, and interactions between partitioned components) as well as a stack analysis (an analysis to show that a stack overflow cannot occur under various conditions and inputs). Lastly, the challenge to make an RSC out of an operating system is to make it reusable. This means that it should support more than one CPU architecture and contain no CPU or board-specific functions, otherwise the true value of reuse will be lost.

**Economic Value of the RSC**

The economic value of an RSC lies in its ability to do three things:

- Reduce Engineering Labor;
- Reduce Program Risk; and
- Reduce Cost.

If an RSC is properly verified using the foresight of future use, then it is possible to perform verification to most DO-178B objectives and not have to revisit these activities if the RSC is not modified in future projects. The RSC developer should provide integrators with guidance on how to integrate the RSC into applications and retain certification credit for the RSC. More importantly, the RSC artifacts should provide “educational value” to the integrator that reduces engineering labor. This educational value is provided in the form of written guidance and tests that help the integrator assimilate their application with the RSC in a timely manner. LynuxWorks’ experience is that the educational value of its RSC artifacts provides integrators with a savings of 3-6 months of engineering labor over conventional DO-178B artifacts. This learning economy can be consistently applied in future projects.

An RSC reduces program risk by focusing certification audits where they should be focused: on the DO-178B objectives that remain to be satisfied and the integration of the component into an application. With a standard set of DO-178B artifacts, a certification auditor can examine any part of the artifacts, even those areas that have been examined by someone else. On many occasions, developers who envision low risk with submittal of standard DO-178B artifacts have found themselves the subject of auditors’ qualitative interpretations that result in added explanations, action items, and even additional verification work resulting in a prolonged project schedule. Sadly, an auditor’s job is to scrutinize results closely and aggressively find weaknesses in the verification process, so very often it’s impossible to get through an audit the first time, even if the software has been approved before. The RSC concept avoids this dilemma by focusing the engineering and auditing effort on software integration, not previously verified operating system functions such as message queues. LynuxWorks experience is that the risk value of its RSC artifacts provides integrators with a savings of 6-9 months of engineering project schedule over conventional DO-178B artifacts. This risk economy can be consistently applied in future projects.

Lastly, the value of an RSC is to reduce cost. The concept is simple; an accepted RSC that meets DO-178B saves the integrator the cost of verification for this component. LynuxWorks’ LynxOS-178 operating system comprises approximately 60,000 lines of code. An accepted LynxOS-178 RSC saves integrators tens or hundreds of engineering years of verification effort.

**SUMMARY**

Certification of software for use in safety-critical systems, especially those systems in airborne environments is a costly, risky, and labor-intensive endeavor. Historically, DO-178B verification of software has been done in closed form; that is on a single hardware platform and in a single installation. Each time the software is used on subsequent projects, developers must perform many of the DO-178B verification activities again and often face schedule risk during the audit process. The FAA’s new policy on Reusable Software Components, defined in AC 20-148 allows software components such as operating systems and networking components to be accepted on one project and reused on subsequent projects provided integrators follow the guidance and instructions of the RSC developers. The RSC also brings economic savings to safety-critical developers by reducing project labor, risk, and cost.

**REFERENCES**


Fiber-Optic Gyros & Quartz Accelerometers for Motion Control

V.S. Lobanov, N.V. Tarasenko, D.N. Shulga, V.N. Zboroshenko
FSUE Central Scientific Research Institute of Machine Building (TsNIIMash), &
V.P. Fedotov
FSUE Scientific Production Association named by S.A. Lavochkin

ABSTRACT

In article the opportunity of use strapdown inertial navigation system (SINS) on the base of fiber-optic gyroscopes and quartz accelerometers corrected from star sensors and satellite navigation equipment (SNE) for perspective interplanetary spacecrafts motion control on phases of interplanetary trajectory insertion, trajectory correction, and braking during transition to Mars orbit is investigated. Results of onboard control complex accuracy characteristics estimation are presented at the given dynamic spacecraft scheme which is taking into account the liquid oscillations in tanks and structure elements elasticity. At modelling the errors of measuring devices installation, errors of SINS initial alignment and instrumental errors of SINS sensitive elements, variation of control engines parameters were taken into account. The structure of the developed complex of imitation modelling of interplanetary spacecraft controlled motion is resulted. Estimations of active flight legs realization accuracy were received by a method of statistical modelling of spacecraft controlled motion.

INTRODUCTION

Till now on a leg of spacecraft interplanetary trajectory insertion the onboard control complex (OCC) of spacecraft of scientific purpose provided use of precision inertial system on base of gyrostabilized platform, which materializing starting coordinate system and providing autonomous generation of the set impulse with simultaneous correction of errors of the trajectory, generated by launch vehicle. OCC switched on before start of the launch vehicle, and at that, the corresponding ground equipment should support OCC work.

Decreasing energy-mass characteristics and cost of new generation interplanetary spacecrafts onboard control complex is possible at transition from high-precision gyrostabilized platform to strapdown inertial navigation system (SINS). However, SINS application in the trajectory insertion scheme with OCC pre-start switching on and starting coordinate system construction results, in comparison with gyrostabilized platform, to considerably big errors.

In this connection, realization of trajectory insertion scheme with use of strapdown inertial navigation system (SINS) demands additional navigation information about current motion parameters of spacecraft centre of mass and about spacecraft orientation. Reception of such information is possible due to satellite navigation equipment (SNE) installation aboard spacecraft, or by trajectory measurements data transmission aboard via command radio-link (CRL). The information about spacecraft orientation can be received with use of the star and sun sensors included in OCC structure. The spacecraft insertion to pass trajectory of flight to Mars includes the following stages:

• start and insertion of spacecraft on 200-km a circular basic orbit of an artificial satellite with an inclination 51.8°.

• passive flight within ~4 hours on a basic orbit (~2.8 orbits) with carrying out trajectory measurements from the Earth or definition of spacecraft navigation parameters with SNE help, and construction of base coordinate system with the help of OCC astrodevices;
• the first burn of spacecraft propulsion system (PS) and working through of characteristic velocity impulse \( \Delta V \), for transition to an intermediate orbit with apogee altitude \( \approx 11,000 \) km and perigee altitude \( \approx 230 \) km;

• passive flight on an intermediate orbit within \( \approx 26 \) hours (7 orbits) with carrying out of communication sessions with the Earth with transfer of telemetry information (TMI), trajectory measurements and navigation measurements with help SNE, calculation of the impulse parameters, laying of setting values for second PS burn;

• second burn of spacecraft propulsion system and working through of characteristic velocity impulse \( \Delta V \), for transfer to a hyperbolic trajectory of flying away from the Earth, separation of insertion propulsion system, carrying out of trajectory measurements for definition of parameters of the formed flying away trajectory.

The analysis of ballistics of spacecraft insertion shows on an opportunity of generation of the first acceleration impulse of spacecraft not right after separation with 3-d stage, but approximately through 3 orbits of flight on a basic orbit. This time it is quite enough for normalization of gas-dust conditions around spacecraft up to a level suitable for functioning star sensors. Use of the information of star sensors before execution of acceleration maneuver of spacecraft cardinally changes accuracy requirements to inertial measuring means aside their decrease. On a tentative estimation of allowable accuracy of carried out the addition acceleration maneuvers it is quite enough to have collective drift of gyro devices up to a \( 1^\circ \)/hour. To this requirement satisfies wide enough class of low-cost sensitive elements.

Taking into account accuracy requirements of other flight legs, it had been chosen the device with random drift in start \( 0.36^\circ \)/hour \( (3\sigma) \), constructed on the base of fiber-optic gyroscopes. As the sensitive elements measuring linear acceleration of spacecraft are chosen pendulous quartz accelerometers. The structure considered strapdown inertial block (SIB) includes six fiber-optic gyroscopes and six quartz accelerometers, established on faces of the truncated pyramid.

Realization of spacecraft acceleration impulses assumes execution of the first impulse with use only astrocorrection of inertial coordinate system orientation without a laying of command – program information (CPI), and the second leg – with astrocorrection of orientation and with a laying aboard CPI, calculated by results of trajectory measurements or measurements of SNE already during flight. CPI includes the data about the moment of PS burn, velocity increment value, the law of spacecraft orientation change during PS work, and also a set of service parameters providing necessary service operations of a regime. Realization of the second impulse can be carried out as independently, with attraction of SNE measurements, and with the data transferred aboard from ground station. At second impulse generation all insertion errors accumulated before are corrected.

At a stage of interplanetary flight, the regimes of trajectory correction and braking are carried out at transition to an orbit of Mars with the help brake propulsion system (BPS) of spacecraft. The basic command - measuring device in these regimes also is SINS.

Carrying out of SINS correction supposed as follows. On a passive flight leg time intervals choose where there are no operations of executive units of stabilization system. In these

<table>
<thead>
<tr>
<th>Error of realization of characteristic velocity impulse value (in % from required impulse value)</th>
<th>An error of thrust vector orientation relative to set position (degree)</th>
</tr>
</thead>
<tbody>
<tr>
<td>The first impulse at phase of interplanetary trajectory insertion</td>
<td>0.10</td>
</tr>
<tr>
<td>The second impulse at phase of interplanetary trajectory insertion</td>
<td>0.10</td>
</tr>
<tr>
<td>Impulse of a trajectory correction</td>
<td>0.38</td>
</tr>
<tr>
<td>Braking impulse</td>
<td>0.28</td>
</tr>
<tr>
<td>Impulse of an orbit correction</td>
<td>0.43</td>
</tr>
</tbody>
</table>
time intervals the apparent velocity increments by three axes, caused by presence of errors such as “a zero” signal of accelerometers taken readings from SINS. Use of algorithm of averaging of the received measurements on set of the chosen time intervals allows to calculate and enter corrections into SINS algorithms and thus partially to remove an accelerometers error such as “a zero signal” from day to day.

Calibration of gyro units is carried out with the help of the information of astrodynamics on a passive flight leg before carrying out of an active leg. Before the beginning of an active leg, the base coordinate system is formed up with use of astrodynamics, is determined initial quaternion of spacecraft orientation and transferred as a reference mark in SINS. SNE is used on a leg of an interplanetary trajectory insertion for definition of spacecraft position and velocity in an orbit and for the assignment of initial value of position and velocity in SINS.

Necessary accuracies of execution of required characteristic velocity impulses are resulted in Table 1. Let’s consider an opportunity of use corrected from star sensors and SNE SINS on the basis of fiber-optic gyroscopes and quartz accelerometers for motion control of perspective interplanetary spacecraft at phases of interplanetary trajectory insertion, correction of a trajectory and a phase of braking at transition to an orbit of Mars.

Research of accuracy and dynamic characteristics of OCC of perspective interplanetary spacecraft on active phases of flight carried out by a method of mathematical modelling with the help of the developed imitating models of spacecraft controlled motion on considered phases of flight.

**Brief Description of Imitating Modelling Complex**

The imitating modelling complex consists of two imitating models: model of space head part (SHP) controlled motion and model of over-flying module (OM) controlled motion. Imitating models differs by composition and structure of dynamic scheme of spacecraft components, instrumental and algorithmic realization of automatic units of stabilization, structure of executive units (engines of correction), and sequence diagram of OCC works in considered regimes. The structure of imitating models includes the following basic modules:

- model of spacecraft motion (the dynamic scheme);
- SINS model consisting of sensitive elements model, including the kinematic scheme of their installation, models of gyroscopes and accelerometers errors;
- model of propulsion system;
- model of the mid-flight propulsion system actuator (for SHP);
- algorithms of spacecraft stabilization on active flight phases;
- programs – dispatchers realizing sequence diagram of OCC works on active flight phases;
- SINS algorithms (algorithms of processing of strapdown inertial block measurements, calculation of spacecraft orientation);
- model of SINS correction sensors; and
- model of mission task.

The structural flowchart of imitating model is resulted in Figure 1.

**MODELLING RESULTS OF PERSPECTIVE INTERPLANETARY SPACECRAFT SPACE HEAD PART MOTION ON A PHASE OF AN INTERPLANETARY TRAJECTORY INSERTION**

The initial data for imitating model are:
1. Parameters of spacecraft dynamic scheme.

2. The initial data for the block of sensitive elements (SE) of strapdown inertial block:
   - kinematic scheme of SE arrangement relative to the spacecraft body coordinate system; – parameters of SE errors models;
   - attribute of errors modelling on everyone SE;
   - attribute of SE failures.

3. Required value of the increment of apparent velocity vector ΔVreq and sign of used engines, duration of the passive phase before impulse generation, duration of a passive phase between the impulse beginning and construction of base coordinate system, variation of engines aftereffect impulses.


5. Characteristics of used engines.

6. Parameters of automatic units of stabilization.

7. The initial data for definition of SINS initial quaternion errors (errors of base coordinate system construction and errors of the program turn).

8. Requirements of generation of spacecraft correcting impulse accuracy by the module and the direction.

9. The initial data for statistical calculations:
   - sign of statistical calculations carrying out;
   - quantity of realizations.

   The quantity of calculations external cycles for the given mathematical model is equal to quantity of realizations set in initial data. For each realization, it is carried out:
   - calculation of initial quaternion taking into account the errors of base coordinate system construction and the program turn which is used as SINS quaternion initial value;
   - formation of a vector of SINS sensitive elements measurements in view of their given errors models;
   - modelling of SINS algorithms;
   - modelling of the space head part stabilization system work on active and passive flight phases;
   - modelling of engines work;
   - integration of motion equations of the spacecraft centre of mass and relatively centre of mass taking into account the liquid oscillations in tanks according to SHP dynamic scheme;
   - definition of correcting impulse realization error by the module and the direction:

   \[ ΔV = \left( \frac{|V| - |V_{req}|}{|V|} \right) \times 100\% / V_{req} \]

   \[ Δδ = \arccos \frac{V_x}{|V|} \]

   The step of integration of the SHP motion equations selects automatically according to the maximal frequency of oscillator taken into account at modelling. The step of formation of the measurements vector of SINS sensitive elements is equal 0.01 sec. The cycle of OCC work is accepted equal 0.1 sec. In model the delay on one step, equal 0.1 sec is taken into account, at delivery of the information from SINS and on one step at formation of control signals on engines burn and switching-off. At modelling the spacecraft mass change is taken into account at utilization of the actuating fluid.

   In imitating model, the following kinematic scheme of strapdown inertial block is realized:
   - the device has six independent non-coplanar channels of angle measurement and six channels of measurement of an apparent velocity increment;
   - nominal orientation of SE sensitivity axes in angle measurement channels in axes of instrument coordinate system (ICK) on generatrix of cone. The axis of a cone coincides with an axis OX of instrument coordinate system. Projections of sensitivity axes to plane OYZ of ICK form among themselves an angle 60°, at that one of projections coincides with axis OY;
   - nominal orientation of elements in channels of an apparent velocity increment measurement in axes of instrument coordinate system on generatrix of cone.

   As sensitive elements in channels of angular parameters measurement the fiber-optic gyroscope (FOG) without a feedback with the piezoelectric modulator, produced on wholly-fiber technology, is applied.

   As a sensitive element in channels of an apparent velocity increment measurement it is applied pendulous quartz accelerometer with an analog feedback. SINS mass, consisting of six fiber-optic gyroscopes, six quartz accelerometers and the microprocessor is about 2 kg, power
Table 2. Results of statistical modelling of the first active flight phase

<table>
<thead>
<tr>
<th></th>
<th>MO</th>
<th>3 RMSD</th>
<th>MO-3RMSD</th>
<th>MO+3RMSD</th>
<th>Min</th>
<th>Max</th>
</tr>
</thead>
<tbody>
<tr>
<td>$</td>
<td>\Delta V</td>
<td>$, %</td>
<td>0.002</td>
<td>0.042</td>
<td>-0.040</td>
<td>0.044</td>
</tr>
<tr>
<td>$\delta$, deg</td>
<td>0.114</td>
<td>0.066</td>
<td>0.049</td>
<td>0.180</td>
<td>0.081</td>
<td>0.162</td>
</tr>
<tr>
<td>$V_y$, m/sec</td>
<td>-2.435</td>
<td>2.253</td>
<td>-4.688</td>
<td>-0.181</td>
<td>-4.181</td>
<td>-1.308</td>
</tr>
<tr>
<td>$V_z$, m/sec</td>
<td>2.024</td>
<td>1.374</td>
<td>0.650</td>
<td>3.399</td>
<td>1.090</td>
<td>3.188</td>
</tr>
</tbody>
</table>

*Quantity of excesses over $|\Delta V|$ - 0.*
*Quantity of excesses over $\delta$ - 0.*

Table 3. Results of statistical modelling of the second active flight phase

<table>
<thead>
<tr>
<th></th>
<th>MO</th>
<th>3 RMSD</th>
<th>MO-3RMSD</th>
<th>MO+3RMSD</th>
<th>Min</th>
<th>Max</th>
</tr>
</thead>
<tbody>
<tr>
<td>$</td>
<td>\Delta V</td>
<td>$, %</td>
<td>-0.004</td>
<td>0.042</td>
<td>-0.046</td>
<td>0.038</td>
</tr>
<tr>
<td>$\delta$, deg</td>
<td>0.121</td>
<td>0.050</td>
<td>0.071</td>
<td>0.171</td>
<td>0.092</td>
<td>0.152</td>
</tr>
<tr>
<td>$V_y$, m/sec</td>
<td>-2.964</td>
<td>1.889</td>
<td>-4.853</td>
<td>-1.075</td>
<td>-4.255</td>
<td>-1.935</td>
</tr>
<tr>
<td>$V_z$, m/sec</td>
<td>2.261</td>
<td>1.060</td>
<td>1.201</td>
<td>3.321</td>
<td>1.527</td>
<td>3.089</td>
</tr>
</tbody>
</table>

*Quantity of excesses over $|\Delta V|$ - 0.*
*Quantity of excesses over $\delta$ - 0.*

consumption up to 10 Wt. For comparison the gyro-stabilized platform, which is carrying out the same functions, has mass about 30-40 kg and power consumption more than 100 Wt.

Modelling the following SE errors is provided: errors of scale factors, zero bias, errors of sensitivity axes orientation, fluctuation and the errors arising due to discretization of measured parameters values.

For variants of the active phase modelling executed with use SINS without calibration, in model of error the values of error such as “a zero signal” from day to day for gyroscopes and accelerometers are taken into account. In model of strapdown inertial block errors for variants of calculation with calibration the values of errors such as “a zero signal” in run after calibration for gyroscopes and accelerometers are used.

The results of statistical modelling at the first active phase, which executed with SIB use with calibration for a case when all errors in model are set for each realization by random manner are resulted in Table 2, and for the second active phase – in Table 3.

In Tables 2 and 3 and further it is designated:

- **MO** – a mathematical expectation,
- **RMSD** – root-mean-square deviation.

As may be seen from results of statistical computations, accuracy requirements of active phases execution are carried out with a sufficient reserve.

**MODELLING RESULTS OF PERSPECTIVE INTERPLANETARY SPACECRAFT OVER-FLYING MODULE MOTION ON PHASES OF TRAJECTORY CORRECTION AND BRAKING AT TRANSITION TO AN ORBIT OF MARS**

Research of OCC accuracy and dynamic characteristics on phases of a trajectory correction and braking at transition to Mars orbit carried out with the help of imitating model of the over-flying module controlled motion after module
Table 4. Results of statistical modelling of the over-flight trajectory correction phase

<table>
<thead>
<tr>
<th></th>
<th>MO</th>
<th>3RMSD</th>
<th>MO-3RMSD</th>
<th>MO+3RMSD</th>
<th>Min</th>
<th>Max</th>
</tr>
</thead>
<tbody>
<tr>
<td>$</td>
<td>\Delta V</td>
<td>$, %</td>
<td>0.009</td>
<td>0.115</td>
<td>-0.106</td>
<td>0.124</td>
</tr>
<tr>
<td>$\delta$, deg</td>
<td>0.205</td>
<td>0.143</td>
<td>0.062</td>
<td>0.348</td>
<td>0.137</td>
<td>0.291</td>
</tr>
<tr>
<td>$V_y$, m/sec</td>
<td>0.150</td>
<td>0.200</td>
<td>-0.050</td>
<td>0.351</td>
<td>0.090</td>
<td>0.297</td>
</tr>
<tr>
<td>$V_z$, m/sec</td>
<td>0.280</td>
<td>0.192</td>
<td>0.088</td>
<td>0.472</td>
<td>0.187</td>
<td>0.408</td>
</tr>
</tbody>
</table>

*Quantity of excesses over $|\Delta V| < 0$. 
*Quantity of excesses over $\delta - 0$. 

Table 5. Results of statistical modelling of the braking flight phase during transition to Mars orbit

<table>
<thead>
<tr>
<th></th>
<th>MO</th>
<th>3RMSD</th>
<th>MO-3RMSD</th>
<th>MO+3RMSD</th>
<th>Min</th>
<th>Max</th>
</tr>
</thead>
<tbody>
<tr>
<td>$</td>
<td>\Delta V</td>
<td>$, %</td>
<td>-0.002</td>
<td>0.062</td>
<td>-0.064</td>
<td>0.059</td>
</tr>
<tr>
<td>$\delta$, deg</td>
<td>0.143</td>
<td>0.082</td>
<td>0.061</td>
<td>0.225</td>
<td>0.078</td>
<td>0.182</td>
</tr>
<tr>
<td>$V_y$, m/sec</td>
<td>1.945</td>
<td>1.198</td>
<td>0.747</td>
<td>3.144</td>
<td>0.968</td>
<td>2.489</td>
</tr>
<tr>
<td>$V_z$, m/sec</td>
<td>0.288</td>
<td>0.931</td>
<td>-0.643</td>
<td>1.219</td>
<td>-0.199</td>
<td>0.818</td>
</tr>
</tbody>
</table>

*Quantity of excesses over $|\Delta V| < 0$. 
*Quantity of excesses over $\delta - 0$. 

separation from mid-flight propulsion system. In the given imitating model, the over-flying module dynamic scheme, which is taking into account the liquid oscillations in tanks and structure elements elasticity, is used. The developed imitating model can be used for modelling of the over-flying module controlled motion on active phases on a line of flight to Mars, at transition to an orbit of Mars and in an orbit of Mars.

On a line of flight and at transition to Phobos orbit 15 burns of brake propulsion system are planned. From these 15 BPS burns were simulated three most typical phases:

- 1. A phase of the flight trajectory correction;

- 2. Braking phase at transition to Mars orbit; and

- 3. Orbit correction phase.

The first velocity impulse value ~90 m/sec, the second ~800 m/sec, the third ~45 m/sec.

On a passive phase before BPS burn, the base inertial coordinate system with use of the information of sun and star sensor is constructed. Accuracy of base coordinate system construction is determined by errors of measurement and errors of sun and star sensors installation and makes $\approx 5$ angular minutes.

Accuracy requirements for execution of over-flying module active maneuvers are presented in Table 1. The accuracy estimation of active phases was realized by statistical modelling method.

In this case the errors of base coordinate system construction, the errors of engines installation, variation of BPS engines aftereffect impulses, errors of sensitive elements installation relative to the spacecraft body coordinate system, and also all components of instrumental errors of gyros and accelerometers were set in a random way. Also the delays of control signals generation were taken into consideration.
Table 6. Results of statistical modelling of the orbit correction phase

<table>
<thead>
<tr>
<th></th>
<th>MO</th>
<th>3 RMSD</th>
<th>MO-3RMSD</th>
<th>MO+3RMSD</th>
<th>Min</th>
<th>Max</th>
</tr>
</thead>
<tbody>
<tr>
<td>$</td>
<td>\Delta V</td>
<td>$, %</td>
<td>-0.016</td>
<td>0.065</td>
<td>-0.049</td>
<td>0.081</td>
</tr>
<tr>
<td>$\delta$, deg</td>
<td>0.034</td>
<td>0.129</td>
<td>-0.095</td>
<td>0.163</td>
<td>0.006</td>
<td>0.131</td>
</tr>
<tr>
<td>$V_y$, m/sec</td>
<td>0.024</td>
<td>0.108</td>
<td>-0.084</td>
<td>0.131</td>
<td>-0.011</td>
<td>-0.103</td>
</tr>
<tr>
<td>$V_z$, m/sec</td>
<td>0.003</td>
<td>0.007</td>
<td>-0.005</td>
<td>0.010</td>
<td>-0.008</td>
<td>-0.005</td>
</tr>
</tbody>
</table>

Quantity of excesses over $|\Delta V| = 0$.
Quantity of excesses over $\delta = 0$.

25 realizations of the over-flying module motion were simulated at execution of the first, second, and third active flight phases.

The results of statistical modelling of the first active phase executed with using of SINS with calibration for a case, when all errors in model are set for each realization by random way (by random-number generator), are presented in Table 4; in Table 5 for the second active flight phase, and in Table 6 for the third active flight phase.

Results of statistical modelling show that accuracy requirements of active flight phases execution with help braking propulsion system are carried out with a sufficient reserve.

CONCLUSIONS

As a result of researches of accuracy and dynamic characteristics of perspective interplanetary spacecrafts controlled motion on active flight phases it is possible to draw the following conclusions:

- The spacecraft onboard control complex of a considered class can be constructed on the basis of corrected SINS with middle class of accuracy which structure includes fiber-optic gyroscopes and quartz accelerometers. Mass, dimensions and power consumption of such SINS much less than similar characteristics INS based on gyrostabilized platform.

- For realization of spacecraft injection on an interplanetary trajectory with necessary accuracy with use SINS, the injection scheme is offered, which is allowing to execute the first impulse of spacecraft acceleration through three orbits after separation from launch vehicle. At the same time, SINS initial alignment can be carried out with sufficient accuracy under indications of star sensors and satellite navigation equipment before the first acceleration impulse execution.

- For increase of active phases execution accuracy, it is offered to realize SINS initial alignment under indications of star sensors before maneuver, and to reduce an error such as “the zero signal” of SINS sensitive elements by correcting signals introduction.

REFERENCES

[1] Kargu, L.I.,
Accuracy of gyrodevices of flying vehicles control systems,

[2] T.Okosi and other authors,
Fiber-optic sensors,

Virtual Perimeter Security (VPS) in a Physical Protection System

Bradley C. Norman & Douglas G. Adams
Sandia National Laboratories

ABSTRACT

There is a need to provide response force personnel with advanced warning of intruder activity in rough terrain outside the traditional facility perimeter. Often the land surrounding a high consequence facility is remote and difficult to sensor with conventional long-range detection systems. In order to combat this difficult problem, Sandia has investigated, developed, and fielded a wireless sensor network that demonstrated the value of providing advanced information of adversary activities. The project used wireless technologies to detect and assess intruders in remote “un-engineered” terrain around a fixed facility. In the time since the wireless intrusion detection system was fielded, minimal time has been spent on maintenance and no batteries required replacement. Sandia’s wireless sensor network provides advanced warning of intruder activities and its installation will improve the security posture of a facility.

INTRODUCTION

Virtual Perimeter Security (VPS) utilizes wireless intrusion sensors and wireless video assessment equipment to enhance existing physical security systems by detecting and assessing intruders beyond the facility boundary. This project has adopted a modular system architecture to provide timely, mission centric event reporting. The system incorporates multiple protocols and various types of hardware which contribute to a robust system. The modular system architecture permits easy integration of future hardware and technology. This advanced architecture allows monitoring and control of sensor and video assessment systems scattered throughout a large facility and interfaces with command and control systems, both internal and external, to a facility.

VPS has defined a three level system architecture to meet its performance specifications. Long-range primary sensors, like radars, may cover most of the perimeter surface area, however, secondary short-range sensors are needed to fill in blind spots and terrain depressions. VPS customized a variety of short-range sensor systems to meet its intrusion detection needs. VPS realized the importance of video assessment in a physical security system, and implemented a solar-powered, high-speed, ad-hoc wireless data network. Each video assessment node is designed to support up to three video cameras and a two-way audio capability.

DESIGN REQUIREMENTS AND GOALS OF VPS

A wireless sensor network is a valuable method to provide early warning before intruders reach the facility’s Perimeter Intrusion Detection and Assessment (PIDAS) fence. It has been suggested the highest value implementation of this capability would be in non-line-of-sight areas (behind hills, in trees, in low areas such as dry river beds, etc.) or along likely avenues of approach.

The VPS application has several attractive features that differ from many other wireless sensor system applications. The system is designed to be fielded on terrain owned by the facility where public access is limited. It was not necessary the demonstrated system be covert and power was provided by solar arrays or batteries. Sandia’s internal analysis suggests there are advantages in deploying a combination of overt and covert equipment to monitor these remote locations. The VPS system also has certain requirements which will be more difficult to satisfy. The system must provide human operators with enough information to enable them to know how to respond. This may be done through multi-modality sensor suites for detection of different types of emanations from the intruder, coupled with visual assessment. The use of sensors with overlapping ranges and both local and system-wide data fusion is important to achieve high detection effectiveness with low nuisance and false alarms.

In addition, VPS systems must be affordable enough to field at the sites, flexible enough to adapt to changing threats, as well as possessing the ability to remotely adjust or
reprogram sensor sensitivities, sensor fusion algorithms, and software. This will enable the VPS system to quickly adapt to changing environmental conditions or threat scenarios and minimize invalid alarms.

**VPS DEPLOYMENT**

Security Experts believe the need for this technology is urgent. Sandia worked diligently to accommodate their wish with a demonstration of a practical operational system. In the fall of 2005 the system was demonstrated and showed how probable locations of intruder access, such as high ground surveillance locations or low profile avenues of approach situated in Non-Line-Of-Sight (NLOS) terrain from the facility could be remotely monitored. A use-case scenario of a likely facility attack focused the demonstration.

The demonstration successfully portrayed how modern wireless communications can effectively relay sensor alarms and useful images from Ethernet-enabled, Internet Protocol (IP) cameras to the Command Center for early assessment of intruders. See Figure 1 for a general VPS concept diagram.

The VPS use-case scenario determined the functional design requirements, including the need to detect and assess intrusions by low profile intruders (e.g., individuals carrying only a rifle) on complex, un-engineered terrain, detect and assess vehicles approaching along roads, and support the security forces in determining temper and intent of the intruders. This demonstration featured non-continuous deployment of limited fields of sensors instead of the continuous ring of sensor fields as originally conceived as a Virtual Perimeter.

Rather than attempting to ensure all approaches to the site are detectable, areas of probable approach, and areas around sensitive remote locations were instrumented. Sensors were placed along vehicle access routes, around areas where people on foot might approach high ground for surveillance, and around possible targets for sabotage. Based on site specific requirements, VPS can be deployed in a continuous detection perimeter or it can be installed in the most probable avenues of approach and add uncertainty to the remote location areas surrounding the facility.

The VPS demonstration was conducted at an undisclosed location on Kirtland Air Force Base (KAFB) in the mountains east of Sandia National Laboratories (SNL). The location was selected due to the extreme terrain and environmental conditions.

VPS utilized hand-emplaced, networked multi-sensor nodes with varying types of sensor transducers and wireless video assessments to aid operators in determining the intent of the detected intruders.

**VPS SYSTEM ARCHITECTURE**

Designers have chosen to divide the system into three separate levels in order to meet the various challenges facing VPS. Each region has its own set of components that are optimized for their operating environment. Figure 2 is a graphical representation of the VPS hardware architecture.

Sensors (or more accurately, transducers) in the field are generally connected to Sensor Nodes (SN, Level 0) which communicate to Cluster Nodes (CN, Level 1), and finally to the site Command Center (CC) communications network at Level 2.
INTRUSION SENSOR EQUIPMENT

Sandia installed a variety of wireless intrusion detection equipment. The sensor equipment includes primarily seismic sensors, however, Passive Infrared (PIR), monostatic microwave, magnetic, and active beam break sensors were also used to detect intruders. Figure 3 shows a typical intrusion detection sensor.

WIRELESS VIDEO ASSESSMENT EQUIPMENT

During the VPS deployment, Sandia connected up to two Ethernet IP cameras per single wireless communications link. However, the system is designed to accommodate more imagers per wireless link, power permitting. Figure 4 shows the deployment terrain and wireless video assessment equipment. Sandia deployed fixed field of regard/view (FOR & FOV) imagers for assessment. This is based on a strict design methodology that pan-tilt-zoom (PTZ) imagers are to be strictly used for surveillance since PTZ imagers cannot gather pre-alarm video assessment. FOV Imagers allow for assessment of intruders who rapidly pass through the detection area.

CHALLENGES FACING THE VPS SYSTEM

There are many challenges presented when implementing a VPS system. Sandia’s experts believe system operators have a tendency to turn off the system if there is an excessive amount of nuisance or false alarms, rates (NAR/FAR) in a physical security system. In general, exterior sensors work best when deployed in controlled environments such as areas between fences, or in gravel beds where vegetation is not allowed to grow. In the VPS environment such controlled conditions will not be available and the systems will be deployed in un-engineered terrain. Thus, it is expected that sensors will have high nuisance and false alarm rates.

(NAR/FAR). Severe weather conditions such as rain, wind, and heat also raise the NAR/FAR levels in external sensors. Sensor fusion and improved sensor algorithms will be utilized to mitigate alarms caused by non-target sources.

Renewable and reliable power is also a major concern for the VPS system as it is designed to be installed beyond the perimeter. The Sandia team presupposes that electrical power will generally be unavailable. The design assumes that any VPS system’s hardware will have to provide power for sensing and assessment elements.

Video imaging assessment during all weather and lighting conditions is a condition that must be met by the assessment equipment. Assessment may be achieved with the use of stand-off assessment systems that look out from the perimeter for much of the VPS assessment capability. However, locations that are out of line of sight will require localized assessment.

VPS systems will need to span large distances, perhaps many kilometers. This has an impact on the number of sensors deployed, the capabilities of assessment systems, and the types of wireless communications.

Sandia desires to have VPS interface with existing systems. In order to be effective, VPS systems must be integrated into the existing command and control infrastructure and concept of operations at a site. This would mean feeding alarm and assessment data into the existing Alarm Communications and Display (AC&D) system, or as a less attractive alternative, providing information to response forces in parallel with the existing AC&D system. Given that VPS equipment is designed to be deployed over large areas, there is a need to have a display system which is capable of
exhibiting a large amount of information in an organized fashion.

**KEY RESULTS FROM THE VPS DEMO**

The VPS system demonstrated the ability to detect and visually assess human and vehicle intrusion at five non-line-of-sight areas. These areas are rather remote and would require significant infrastructure improvements in order to install a more conventional physical protection system.

The system demonstrated a high probability of detection against human “walk-test” intruders during functional testing. In addition, the system was demonstrated to have a high probability of detection against intruding vehicles. Sandia verified its sensor algorithms were able to distinguish footstep from background seismic signal, dramatically reducing false positive alarms or nuisance alarms (NAR) caused by non-target energy sources. VPS also demonstrated the ability to visually assess low-profile intruders in this remote terrain.

The deployed equipment’s wireless communications link was well suited for the transmission of images and sensor alarms from remote non-line-of-sight areas. The maximum demonstrated wireless transmission distance for this data was several kilometers, however, the actual maximum distance may be farther.

The deployed hardware has been operational in the field for a year and is self-powered with integrated tamper detection. During this extended period of time, only minimal maintenance was required. Such maintenance included altering sensor sensitivity based on seasonal changes. In future systems, this maintenance will be able to be performed from a remote location. The system was interfaced with a function commercial-off-the-shelf (COTS) operator interface, Tactical Automated Security System (TASS). However the equipment is capable of being interfaced with most COTS AC&D displays.

**CONCLUSION**

An early warning system such as VPS will allow facilities to protect areas that have never before been easily monitored. The VPS system was designed to provide near real-time assessment of intruders in remote areas around fixed facilities. In addition, the advanced technology implemented in VPS may eventually reduce labor costs associated with a large guard force. VPS demonstrated the ability to detect intrusion attempts by humans and small vehicles in non-LOS areas while maintaining a low nuisance alarm rate (NAR) caused by animals. The intrusion information was displayed in the command center in less than five seconds from the initial detection event. The most important aspect is VPS is designed to be flexible and meet evolving performance, threat, and cost requirements.

**REFERENCES**


VDL Mode E Receiver Performance Measurements

Fred Studenberg
Rockwell Collins, Inc.

ABSTRACT

VDL Mode E is a digital communications system proposed as a worldwide standard for replacement of the existing analog AM voice system used for VHF aeronautical communications. It provides a needed increase in voice channel capacity as well as offering a digital data link for CPDLC with the high integrity and low latency needed for time-critical ATC messages.

This report summarizes results of measurements of proposed minimum requirements for an aeronautical receiver for VDL Mode E. A software defined radio (SDR) currently used in Commercial Air Transport communications was used for the tests.

INTRODUCTION

To solve radio frequency congestion issues and provide high integrity, and guaranteed quality of service (QOS), a replacement is needed for the analog AM system now used worldwide for VHF aeronautical communications.

VDL Mode E [1] is one of several next-generation digital systems being considered by the Future Communications System (FCS) study group as a global standard for a new system operating in the 118-137 MHz aeronautical communications band [2].

VDL Mode E has been included in the list of candidates since it can provide capacity increase, the required voice and data link performance, and is spectrum compatible with the European analog AM system using 8.33 KHz channel spacing. The system can also be efficiently implemented within the 25 kHz channel spacing system used elsewhere in the world, including the United States.

In previous reports, it was shown that a VDL Mode E voice and data link network is scaleable to provide capacity as needed for growth in aeronautical communications beyond the year 2050 [3].

The 8.33 KHz spectrum compatibility of VDL Mode E permits a seamless "drop-in" transition to a modern digital system by the replacement of any 8.33 KHz analog channel with a VDL Mode E digital circuit. In the 25 KHz channel spacing environment, up to 3 individual VDL Mode E channels (6 independent voice or data circuits) can be accommodated in place of one analog AM channel.

Fig. 1. Rockwell Collins VHF-2100

OVERVIEW OF DIGITAL VHF COMMUNICATIONS SYSTEMS

VDL Mode E is a digital TDMA system based on the key parameters and protocols from VDL Mode 3. VDL Mode 3 was developed by the United States FAA, MITRE Corporation, and industry partners. VDL Mode 3 uses a DBPSK waveform with operation on 25 KHz channel spacing. It provides 4 digital circuits per channel with configurations for various combinations of voice and data link circuits.

Multi-mode, FAA TSO approved VHF Communications transceivers that provide VDL Mode 3 capability are now
commercially available. One example is the Rockwell Collins VHF-2100, shown in Figure 1. This software defined radio (SDR) also provides all legacy operating modes such as analog AM voice, VDL Mode A, and VDL Mode 2.

Certification flight tests of the VHF-2100 demonstrated that the VDL Mode 3 system meets and exceeds all performance requirements for range and signal quality [4]. Versions of the VHF-2100 VHF Communications Transceiver are now entering service with major commercial air carriers.

Notwithstanding the unqualified success of the VDL Mode 3 development program, the schedule for implementation of VDL Mode 3 in the US has been delayed to allow the FCS study group to make its recommendations in 2007.

A concern by some stakeholders for the global implementation of VDL Mode 3 is the incompatibility of the required 25 KHz channel waveform with the 8.33 KHz channel spacing now being used in Europe. To accommodate a new VDL Mode 3 channel in that environment, it is necessary to find new frequencies for 3 contiguous 8.33 KHz channels. There is also concern over improvement in capacity with only 33% increase in voice channel capacity in a 25 KHz band compared to 8.33 KHz analog operation (4 vs 3).

VDL Mode E was developed to overcome these concerns by providing operation within an 8.33 KHz channel. By reducing the symbol rate of the VDL Mode 3 D8PSK waveform so it is contained in an 8.33 KHz channel, all the features of VDL Mode 3 are preserved. The reduction in data rate reduces the number of independent voice or data circuits from 4 to 2. However, in a 25 KHz channel, three VDL Mode E channels can provide 6 independent circuits instead of 4 circuits with VDL Mode 3.

MINIMUM OPERATIONAL PERFORMANCE SPECIFICATIONS (MOPS)

The VHF aeronautical communications system was first introduced in 1946 with AM voice operation using 100 KHz channel spacing. Since that time, industry technical standards have been developed and continually revised as technology advances. These standards are necessary to insure compatibility between equipment produced by different manufacturers.

One such set of standards are those prepared by members of RTCA, a United States based technical coordinating body for avionics systems.

RTCA DO-271C contains the Minimum Operational Performance Specifications (MOPS) for VDL Mode 3. The primary specifications for VDL Mode 3 receiver and transmitter physical layer performance are contained in DO-271C, along with suggested test procedures.

When VDL Mode E was developed, it was a requirement for the design that VDL Mode E operation could be provided with only a software update of VDL Mode 3 equipment. This approach would result in the ability to operate with new software defined radios, such as the VHF-2100, and would provide the lowest overall cost of development and validation for VDL Mode E.

Because VDL Mode E was designed as a reduced bit-rate version of VDL Mode 3, the MOPS for VDL Mode 3 transmitter and receiver were scaled as required for operation 8.33 KHz channels.

Tables 1 and 2 show the key characteristics of transmitter and receiver performance for 25 KHz channels (VDL Mode 3) and those proposed for 8.33 KHz channels. (VDL Mode E).

Previous reports have demonstrated that with software-only updates to the multi-mode VHF-2100, the transmitted VDL Mode E waveform can be generated that meets all proposed MOPS for transmitter operation, as shown in Table 1 [1].

The following sections of this report discuss results of recent measurements of key VDL Mode E receiver

<table>
<thead>
<tr>
<th>Transmitter</th>
<th>VDL Mode 3</th>
<th>VDL Mode E</th>
<th>Units</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency Band</td>
<td>118-137 MHz</td>
<td>118-137 MHz</td>
<td>MHz</td>
</tr>
<tr>
<td>Channel Spacing</td>
<td>25</td>
<td>8.33</td>
<td>KHz</td>
</tr>
<tr>
<td>RF Output Power</td>
<td>NLT 15</td>
<td>NLT 15</td>
<td>W</td>
</tr>
<tr>
<td>Frequency Tolerance</td>
<td>±5</td>
<td>±5</td>
<td>PPM</td>
</tr>
<tr>
<td>Waveform Type</td>
<td>D8PSK</td>
<td>D8PSK</td>
<td></td>
</tr>
<tr>
<td>Nyquist Filtering</td>
<td>Raised cosine</td>
<td>Raised cosine</td>
<td></td>
</tr>
<tr>
<td>Excess Bandwidth</td>
<td>α = 0.6</td>
<td>α = 0.3</td>
<td></td>
</tr>
<tr>
<td>Bit Rate</td>
<td>31500</td>
<td>15750</td>
<td>Bits/Sec</td>
</tr>
<tr>
<td>Energy in 1st Adjacent Channel</td>
<td>NMT-18</td>
<td>NMT-18</td>
<td>dBm</td>
</tr>
<tr>
<td>1st Adjacent Channel Bandwidth</td>
<td>16</td>
<td>6.6</td>
<td>KHz</td>
</tr>
<tr>
<td>Symbol Constellation Error (EVM)</td>
<td>NMT6</td>
<td>NMT6</td>
<td>%</td>
</tr>
</tbody>
</table>
requirements using prototype receiver software installed in the VHF-2100.

**PROTOTYPE VDL MODE E RECEIVER DESIGN**

Software for demodulation of the 15750 bit/sec D8PSK waveform for VDL Mode E was developed for use in the VHF-2100. The demodulator design was based on the VDL Mode 3 demodulator with sampling period adjusted for the 50% reduction in symbol rate. No change due to the reduction in the raised cosine alpha factor was needed since

![Fig. 3. Selectivity Characteristics](image)

**Table 2. Receiver Key Characteristics**

<table>
<thead>
<tr>
<th>Receiver</th>
<th>VDL Mode 3</th>
<th>VDL Mode E</th>
<th>Units</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency Band</td>
<td>118-137</td>
<td>118-137</td>
<td>MHz</td>
</tr>
<tr>
<td>Channel Spacing</td>
<td>25</td>
<td>8.33</td>
<td>KHz</td>
</tr>
<tr>
<td>Sensitivity for .001 Bit Error Rate</td>
<td>NMT-98</td>
<td>NMT-98</td>
<td>dBm</td>
</tr>
<tr>
<td>Frequency Capture Range (Doppler + T × Freq Error)</td>
<td>±967</td>
<td>±967</td>
<td>Hz</td>
</tr>
<tr>
<td>1st Adjacent Channel Rejection</td>
<td>NLT 40</td>
<td>NLT 40</td>
<td>dB</td>
</tr>
<tr>
<td>Co-Channel Interference</td>
<td>NMT 20</td>
<td>NMT 20</td>
<td>dB</td>
</tr>
</tbody>
</table>

**Table 3. Receiver Sensitivity**

<table>
<thead>
<tr>
<th>Mode</th>
<th>Requirement for .001 BER</th>
<th>RF Level for .001 BER</th>
</tr>
</thead>
<tbody>
<tr>
<td>VDL Mode 3</td>
<td>NMT –98 dBm</td>
<td>–101 dBm</td>
</tr>
<tr>
<td>VDL Mode E</td>
<td>NMT –98dBm</td>
<td>–104 dBm</td>
</tr>
</tbody>
</table>

this waveform does not require a matched filter at the receiver.

Because the VHF-2100 provides analog AM operation on 8.33 kHz channels, no change in frequency tuning was necessary to select 8.33 kHz channels.

The receiver bandwidth needed for demodulation was modified from that used for 8.33 KHz AM operation so as to provide more adjacent channel rejection capability. Figure 2 shows an expanded amplitude vs frequency of the VDL Mode E waveform.

This figure shows that the VDL Mode E waveform has a –6 dB response at ± 2625 Hz. A ± 3.0 kHz receiver passband response was selected. This will allow margin for receiver and transmitter frequency errors and maximum Doppler shift on received signals of ± 282 Hz.

Based on an estimate of the energy in the 1st adjacent channel, a rejection of 60 dB was needed at ± 4.0 KHz. Since the VHF-2100 is a software defined radio, all receiver
Table 4. Receiver Adjacent Channel Rejection

<table>
<thead>
<tr>
<th>Mode</th>
<th>Requirement for .001 BER</th>
<th>Measured RF Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>VDL Mode 3</td>
<td>NMT 40 dB</td>
<td>45 dB</td>
</tr>
<tr>
<td>VDL Mode E</td>
<td>NMT 40 dB</td>
<td>46 dB</td>
</tr>
</tbody>
</table>

Selectivity for 8.33 kHz operation is provided by software filters. Figure 3 shows the amplitude and phase response of the software bandpass filter used in the prototype testing. The passband is ± 3.0 kHz with attenuation greater than 65 dB at ± 4.0 kHz.

RECEIVER PERFORMANCE MEASUREMENTS

For all receiver tests to follow, a test frequency of 127.500 MHz was used with an Agilent E4434B generator used to generate the D8PSK waveform.

Receiver Sensitivity
The RF signal level required for .001 bit error rate was determined with the VHF-2100 operating in VDL Mode 3 and then in VDL Mode E.

Table 3 shows the results. As expected, there was a 3 dB improvement with VDL Mode E due to the 50% reduction in receiver bandwidth.

Receiver Adjacent Channel Rejection
The RF signal level of a 1st adjacent channel signal required to degrade a desired −87 dBm on-channel signal to .001 BER was determined with the VHF-2100 operating in VDL Mode 3 and then in VDL Mode E.

For VDL Mode E, adjacent channel rejection tests, the interfering signal was set at ± 8.33 kHz and modulation on the interfering signal was set for FM at 400 Hz FM with a peak deviation of 2625 Hz. This is a direct scaling of the VDL Mode 3 test of 400 Hz FM with a deviation of 5250 Hz.

Table 4 shows that VDL Mode E provided similar performance as VDL Mode 3.

Co-Channel Rejection
The RF signal level of an on-channel channel signal required to degrade a desired −87 dBm on-channel signal to .001 BER was determined with the VHF-2100 operating in VDL Mode 3 and then in VDL Mode E.

For VDL Mode E, the interfering signal was set at ± 8.33 kHz and modulation on the interfering signal was set for FM at 400 Hz FM with a peak deviation of 2625 Hz. This is a direct scaling of the VDL Mode 3 test of 400 Hz FM with a deviation of 5250 Hz.

Table 5 shows that VDL Mode E provided similar performance as VDL Mode 3.

Frequency Error from Doppler and Transmitter Frequency Tolerance Receiver Adjacent Channel Rejection
The frequency offset of a desired signal that did not degrade a desired −87 dBm on-channel signal to .001 BER was determined with the VHF-2100 operating in VDL Mode 3 and then in VDL Mode E.

Table 6. Receiver Frequency Error

<table>
<thead>
<tr>
<th>Mode</th>
<th>Requirement for .001 BER</th>
<th>Measured RF Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>VDL Mode 3</td>
<td>NLT ±967 Hz</td>
<td>±1267 Hz</td>
</tr>
<tr>
<td>VDL Mode E</td>
<td>NLT ±967 Hz</td>
<td>±467 Hz</td>
</tr>
</tbody>
</table>

Table 6 shows that VDL Mode E did not provide the expected performance.

The smaller frequency tolerance than expected was due to the narrow (± 3 kHz) bandpass filter used so as to meet the adjacent channel rejection.

Two options are possible to provide the same performance as VDL Mode 3.

One option is to modify the −6 dB to 60 dB rejection (shape factor) of the VDL Mode E software filter. This approach will trade off adjacent channel rejection for an increase in frequency tolerance. Based on the margin of both measurements with the current configuration, it is possible that a compromise can be reached that still allows meeting both requirements.

A second option is to change the proposed MOPS to use a more rigorous frequency tolerance on airborne transmitters in the system instead of the ±5 PPM limit used for VDL Mode 3. This will only require a frequency capture necessary for Doppler shift (± 242 Hz) plus whatever frequency error is allocated to the transmitters. Based on the prototype
measurements, up to ± 225 Hz frequency tolerance could be tolerated. This is ± 1.6 PPM instead of the existing tolerance of ±5 PPM.

For option two, rather than require a hardware change for a higher stability reference oscillator, a solution that can be implemented in the VHF-2100 software defined radio is to lock the transmitted frequency to the received frequency of the ground station. If the ground station operates with very small frequency tolerance, for instance less than 10 Hz, then the frequency error of an airborne unit locked to this will be no more than ± 1 maximum Doppler shift or about ± 141 Hz. When received by another aircraft moving in the opposite direction, the apparent maximum frequency error will be no more than ± 282 Hz. Locking the transmitted frequency to the ground station is possible since the apparent frequency error (due to Doppler and receiver frequency errors) of the “perfect” received ground station can be used to calculate the offset of the transmitted signal.

This technique can also resolve any performance concerns with the adjacent channel rejection when the adjacent channel signal is not exactly at ± 8.33 kHz (as it is measured in the MOPS test). For instance, with ± 5 PPM allowable error, with Doppler, an adjacent channel transmission can be as close as 8333 - 967 Hz or 7.366 kHz.

CONCLUSIONS

This paper has identified the key receiver MOPS for VDL Mode 3 and presented results of measurements on a prototype software defined radio.

The tests demonstrated the theoretical sensitivity performance improvements was achievable. Because of the 3 dB improvement, the VDL Mode E transmitter power requirement could be reduced from 15 watts to 7.5 watts and still maintain the same link budget as VDL Mode 3.

However, this is not recommended since the lower receiver sensitivity limit of −101 dBm is not likely to be realized in practice due to low level signals entering the antenna from normal aircraft EMI sources. This limits the usable sensitivity since the BER is degraded from the co-channel EMI signals.

The tests also demonstrated that some additional work is needed on defining a software filter with adjacent channel rejection vs frequency error tradeoffs or alternately, decreasing the allowable frequency tolerance for airborne transmitters to about ± 1.5 PPM. With existing software defined radios, this can be accomplished by locking the transmitter to the ground station’s frequency and no hardware change is needed. For new designs, either frequency locking or improved reference oscillator stability could be used.

REFERENCES

[1] Studenberg, Fred, 2004,
   A Digital TDMA System for VHF Aeronautical Communications
   on 8.33 kHz Channels,
   Presented at IEEE 23rd DASC, Salt Lake City.

[2] ITT Industrics,
   Advances Engineering and Sciences Division, 2005,
   Technology Assessment for the Future Aeronautical
   Communications System.

[3] Studenberg, Fred, 2005,
   The Capacity and Performance of a CPDLC System Using
   VDL Mode E,
   Presented at 24th DASC, Washington, DC.

[4] Cyr, Jeff, 2005,
   Results of VDL Mode 3 STC,
   Presented at IEEE 24th DASC, Washington, DC.
AESS Radar Systems Panel

The Radar Systems Panel exists as a special interest group within the AESS. Its active membership consists of some 25 experts on radar, drawn from all over the world. It meets annually, usually at the IEEE Radar Conference held that year. Panel membership is by invitation and anyone wishing to be considered for membership should contact the Chair with details of his or her career and interests. There are other “emeritus” members who are no longer active, but on whose wisdom the panel may wish to draw from time to time.

It has been in existence for at least 35 years, having been established in the late 1960s - early 1970s.

One of the principal functions of the panel is to oversee the series of radar conferences held under IEEE auspices. In the radar domain a regular five-year cycle of International Radar Conferences has been established. This began in 1973 when the Institution of Electrical Engineers held an unclassified radar conference in London. Encouraged by this, the IEE organised the first International Radar Conference in Washington, DC in 1975, and an agreement was forged between the IEE and IEEE to act as co-sponsors of each others’ events, and to adopt a common naming scheme for the conferences – thus the IEE agreed to host RADAR-77 in London and the IEEE’s RADAR-80 would again be in the US.

The success of the 1975 and 1977 conferences was noted with interest by the French professional institution (SEE), who asked to join the new series by conducting the Colloque International sur le Radar in December 1978 in Paris. All three sponsoring societies agreed that a five-year cycle was appropriate to sustain the series.

In the 1980s, the community in India joined by conducting a 1983 conference (but were unable later to sustain their participation), the Japanese Electrical Engineering Society (IEICE) conducted their first conference, and China asked to join the series and conducted the first Chinese International Conference on Radar, in Nanjing in 1986. The Japanese conferences emphasised image processing in more than just radar; in the 1990s they reduced the radar emphasis and participation as a radar conference could not be continued. Subsequently, the Australian community joined the series with their very successful RADAR 2003 in Adelaide, and will now host RADAR-08 as the five-year cycle continues.

In addition to the international series of radar conferences, an IEEE Radar Conference is held each year (except in years when the International Conference is held in the US). These are smaller in scale than the international radar conferences, but provide an important focus for the radar community and its activities.

All of these conferences have benefited by the addition of tutorials to the regular set of presentations and posters. These have proved extremely popular and have also helped ensure the financial success of the conference series. There are plans to make this tutorial material available more widely in electronic format.

One of the panel’s functions is the award each year of the IEEE Nathanson Award; named after Fred Nathanson, who was a much respected radar engineer and author of the classic textbook Radar Principles. The award is made each year to the leading radar engineer worldwide under the age of 40, and is highly-prized. Details of how to make nominations may be obtained from Michael Wicks, whose contact details are given elsewhere.

Another responsibility of the panel is to maintain and update the IEEE Radar Standard Definitions (IEEE Std 686). This has recently been revised since its last update in 1997 and is now undergoing the balloting process. It is indicative of the progress and development of the subject that there have been numerous new definitions, revision of old definitions, and deletion of definitions now considered obsolete.

In summary, the Radar Systems Panel is a lively and international group. It maintains links with the radar activities of other professional bodies worldwide.

– Hugh Griffiths
Chairman
The 2008 IEEE Radar Conference is in the series of radar conferences promoted by the IEEE Aerospace and Electronics Systems Society (http://ewh.ieee.org/soc/aes/).

In continuity with the tradition of IEEE Radar conferences, so far always held in the United States, the radar community will gather next year in Italy, in the city of Rome, the beautiful capital of the ancient Roman Empire.

CONFERENCE TOPICS

The 2008 IEEE Radar Conference will focus on the key aspects of radar theory and applications as listed below. Exploration of new avenues and methodologies of radar signal processing will also be encouraged. Tutorials will be held in a number of fields of radar technology. The Conference will cover all aspects of radar systems for civil, security, and defense applications. Topics to be covered include (but are not limited to):

- Radar Systems, Radar Data and Signal Processing, Waveform Design and Trade-Offs,
- Antenna & Component Technology, Environment and Phenomenology,
- SAR and Weather Radars, Sonar and Merchant Marine Radar,
- Radar Early Warning, Radar Simulation, Dual-Use/Civil Applications,

SUBMISSION

Procedures to submit a paper can be found at www.radarcon2008.org. Submitted summaries must be 1000-1500 words long, final full paper, no more than six pages all inclusive and conforming to the format specified on the RadarCon2008 website listed above. In addition to formal presentations, there will be poster presentations. Authors who believe their papers are better suited to a poster format are requested to so note on their summaries. The poster format provides authors the opportunity to display their paper and to discuss their information with conference participants. Both oral presentation and poster presentation papers will be published in the Proceedings.

BEST STUDENT PAPER AWARDS

There will be a student paper contest. Student authors who appear as first authors in a paper may enter the student paper contest.

IMPORTANT DATES

Submission of Summaries: September 15, 2007
Notification of Acceptance: October 30, 2007
Submission of Full Papers and Registration: January 15, 2008

www.radarcon2008.org
FROM THE EDITOR-IN-CHIEF

What is a Panel? -- Recognize Your Peers

Evelyn H. Hirt

What is a Technical Panel?
When reading the AESS Society Organization (on the next page, 42): Have you ever wondered about the listing for Technical Panels? Within AESS, Technical Panels are coordinated as subsets of Technical Departments by the AESS Vice President-Technical Operations. Technical Departments are groupings of AESS members interested in symposia, papers, and programs featuring specific portions of the technical fields of interest of AESS: [http://www.ieee.org/portal/site/main/site/menuterm]. Technical panels address smaller portions of the technical field of interest of a Department as stated in the listing. Starting with this issue and throughout the year, *Systems* will include reports from AESS Technical Panels to allow you to become more familiar with their activities and needs. If you are interested in becoming involved with an AESS Technical Panel, please contact the panel chair.

Make an Effort to Recognize Your Colleagues or Peers
IEEE and its various organizational units (OUs) present many awards throughout the year. There are diligent efforts to find nominees for these awards but frequently I'm aware of deserving individuals – especially dedicated volunteers – who have never been honored with an IEEE award. If you know of a dedicated individual who deserves to be recognized by the IEEE or one of its OUs, please take a moment to check available IEEE awards: [http://www.ieee.org/portal/site/main/site/menuterm] and nominate that individual for an award appropriate for their contributions.

-- Evelyn Hirt

---

The 10th International Conference on Information Fusion

Quebec, Canada • 9-12 July 2007

Topics:

Theoretical and technical advances in information and knowledge modelling; probabilities and statistics; non-classical set theories; possibilities; evidential and other theories; non-classical logical approaches; graph-based approaches; neural networks; genetic algorithms; artificial life and intelligence; nonlinear estimation and filtering; semiotics and ontologies.

Algorithms and Systems Perception and cognition; detection and tracking; recognition and classification; data association; resource management; image or sensor fusion; database fusion; knowledge-based systems; data mining; distributed systems; system design; measures of performance.

Applications of C4ISR: network-centric warfare; networks and communication; robotics and control; autonomous systems; intelligent transportation systems; navigation, positioning and guidance; economy and finance; surveillance and situation analysis; remote sensing; medical and biological diagnosis; decision support; data acquisition and testing; machine vision and learning; security and safety.

Information:

Secretariat: jPdL
Tel: (418) 692-6636; Fax: (418) 692-5587
fusion2007@jpdL.com
IEEE AEROSPACE & ELECTRONIC SYSTEMS SOCIETY ORGANIZATION

OFFICERS

President — James V. Leonard
Executive Vice President — Robert C. Rassa
Secretary — Theodora S. Saunders
Treasurer — George R. Dean
Vice President - Administration — Robert N. Trebits
Vice President - Conferences — Barry C. Breen
Vice President - Education — Robert M. O’Donnell
Vice President - Member Affairs — James Howard
Vice President - Publications — Joel F. Walker
Vice President—Technical Operations — James R. Huddle

ASSOCIATE OFFICERS

Senior Past President — Russell J. Lefever
Junior Past President — Paul E. Gartz
Members-at-Large

1/1/05 To 12/31/07
W. Dale Blair
Jose R. Bolanos
Barry C. Breen
Robert P. Lyons, Jr.
Robert C. Rassa
Cary R. Spitzer
S. Zafar Taqvi
Joel F. Walker

1/1/06 To 12/31/08
Ram Gopal Gupta
Evelyn H. Hirt
William Lyons
Ron T. Ogan
Robert N. Trebits
Iram J. Weinstein
John R. Weyrauch
Shunjun Wu

1/1/07 To 12/31/09
Paul E. Gartz
Hugh D. Griffiths
James Howard
Igor Immovene
James V. Leonard
Marina Ruggieri
Theodora S. Saunders
Peter K. Willett

STANDING COMMITTEES & THEIR CHAIRS

Accomplishments Search — Open
Awards — Erwin C. Gangl
  • M. Barry Carlton Award — Peter K. Willett
  • Harry Rowe Minnow Award — E.H. Hirt
  • Warren D. White Award — Mark Davis
  • Pioneer Award — Erwin C. Gangl
  • Judith Resnik IEEE Field Award — Erwin C. Gangl
Chapters — Ron T. Ogan
Constitution, Organization & Bylaws — Charles H. Gager
Distinguished Lecturers — James R. Huddle
Distinguished Tutorials Program — Saj Durrani
Education — Robert M. O’Donnell
Fellow Evaluation — Fritz Steudel
Fellow Search — Elliot L. Axelland
GOLD Coordinator — Joe Pignotti
History — Henry Oman
International Activities — Hugh D. Griffiths
Nominations — Paul E. Gartz
Professional Activities — M. Cardinal
Public Relations — James R. Huddle
Publications — Joel F. Walker
  • Systems — Evelyn H. Hirt
  • Transactions — Peter K. Willett
  • Tutorials — Lance M. Kaplan
Social Implications - Technical — Open
Standards — Arnold M. Greenspan
Strategic Planning — Paul E. Gartz
Student Activities — Jose R. Bolanos
Transnational Activities — Hugh D. Griffiths

IEEE/AESS Website: http://www.eewh.ieee.org/aes
Please send corrections or omissions for this page to the Secretary

IEEE Publications
  • IEEE Press — George W. Zobrist
  • Journal of Lightwave Technology — D. Chamin & M. Cardinal
  • Transactions on Pattern Analysis & Machine Intelligence — J.R. Harris

IEEE Organizational Units
  • Sensors Council — M. Wicks
  • IEEE-SA, IEEE S80-20 Hardware Interfaces Sub-Committee (RFI and S80-20 Standards) — A. Greenspan
  • IEEE-USA, Communication & Information Technical Policy — Open
  • IEEE-USA, PACE — M. Cardinal
  • IEEE-USA, Research & Development Technical Policy — P. Holmer
  • IEEE-USA, Transportation & Aerospace Technical Policy — P. Holmer
  • PSPACE Magazine Committee — Systems Editor-in-Chief — E.H. Hirt
  • PSPE Transactions Committee — Transactions Editor-in-Chief — P.K. Willett
  • Society on Social Implications of Technology — M. Cardinal

CONFERENCE LIAISONS

• IEEE Aerospace — M. Ruggieri & R.C. Rassa
• IEEE Autotestcon BoD — J. Chapman, W. Downing & D. Wallfhefechtel
• IEEE International Carleton Conf on Security Technology — R.B. Trebits
• IEEE/AIAA Digital Avionics Systems Conf. — C.R. Spitzer & B.C. Breen
• All Radar Conferences — M.E. Davis
• IEEE Position, Location & Navigation Symposium — J.R. Huddle
• International Energy Conversion Engineering — G. Dakemanji

LIAISONS TO NON-IEEE TECHNICAL SOCIETIES

• American Institute of Aeronautics & Astronautics (AIAA) — C.R. Spitzer
• Association of Old Crows (AOC) — E.C. Gangl
• French Institute of Navigation (SIN) — J.R. Huddle
• German Institute of Navigation (DGNV) — J.R. Huddle
• Institution of Electrical Engineers (IET) Radar, Sonar & Navigation (RSN) Professional Networks (PN) — R.T. Hill
• Institute of Navigation (ION) — J.R. Huddle
• International Council on Systems Engineering (INCOSE) — G. Friedman
Radar Resolution, Nonlinear Estimation, and Other Gratuitous Remarks on the Back of an Envelope:
A Tribute to Fred Daum

May 23-24, 2007
Naval Post Graduate School
Monterey, California

Anticipated Sponsors
Georgia Tech Research Institute
IEEE Aerospace and Electronic Systems Society

Frederick E. Daum has worked for Raytheon Company for over 30 years and during those years made significant contributions to the areas of phased array radar systems and nonlinear estimation. Fred has also made numerous contributions through his recognition and interpretation of practical problems such as those associated with finite sensor resolution. Fred is also well known for his uncanny talent to distill a complex problem to a simplified formulation on the back of an envelope. However, Fred is best known for his witty and lucid lectures that have brought us the “3 R’s of radar: resolution, resolution, resolution” and the “particle filter (a.k.a., gas mask).” In honor of Fred’s contributions, a tribute workshop will be held on May 24, 2007 and the workshop will be preceded by a banquet on the evening on May 23.

Call for Papers
Original papers that are related to the broad area of target tracking are sought for this tribute. Papers that address the impacts of limited sensor resolution or nonlinear estimation are of special interest. Papers that address nonlinear filters, particle filters, real-time phased array radar waveform scheduling, radar waveform design, Bayesian discrimination for radar, radar bias calibration, multiple input multiple output (MIMO) radar, radar system engineering are also of interest. Papers that address or utilize fuzzy logic, neural nets, Dempster-Shafer, and wavelets are not of interest. All accepted papers must be presented at the tribute and will be published in the Proceedings of the tribute and IEEE Xplore. Manuscripts in pdf format are to be e-mailed to Lisa Ehrman at: lisa.ehrman@gtri.gatech.edu and Paul Burns at: paul.burns@gtri.gatech.edu.

Call for Tribute Items
Stories with photos and other related items that reflect on Fred's career are sought for the tribute. These will be included in the printed Proceedings and the banquet as time permits. Stories which relate and other items are to be sent to John Gray at: john.e.gray@navy.mil and Darin Dunham at: darin@vectraxx.com.
April 2007

**Distinguished Lecturers Program**

**James R. Huddle, Chair**

All AESS Chapters and IEEE Sections are encouraged to take advantage of the AESS Distinguished Lecturers Program for their regular or special meetings. We have selected an outstanding list of speakers who are experts in their fields. The AES Society will cover up to $500 of the speaker's expenses for travel in North America, with any remaining amount normally covered by the AES Chapter or Section or by the speaker's organization. For travel outside North America, the AES Society will cover half of the speaker's expenses per trip, up to a maximum of $1500. The procedure for obtaining a speaker is as follows: If a Chapter or Section has an interest in inviting one of the speakers, it should first contact the speaker directly in order to obtain his agreement to give the lecture on a particular date. After this is accomplished, and if the Chapter or Section wishes to request financial support from the AESS, it should contact James R. Huddle on (818) 715-3264, F (818) 715-3976, j.huddle@ieee.org at least 30 days before the planned meeting, in order to obtain approval for the financial support. The list of distinguished speakers who have expressed their willingness to speak to Chapters or Sections, along with their organization, topics, and telephone numbers, is given below.

<table>
<thead>
<tr>
<th>Title</th>
<th>Name</th>
<th>Contact Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Control Technology Applied to Aircraft &amp; Automobiles</td>
<td>Dr. Kimio Kanai, National Defense Academy of Japan</td>
<td>81-45-812-1244 (V&amp;F)</td>
</tr>
<tr>
<td>Producer</td>
<td></td>
<td><a href="mailto:k.kimio@mech.biglobe.ne.jp">k.kimio@mech.biglobe.ne.jp</a></td>
</tr>
<tr>
<td>Avionics for Manned Spacecraft</td>
<td>Dr. Myron Kayton, Kayton Engineering Co.</td>
<td>(310) 393-1819</td>
</tr>
<tr>
<td>Evolution of Aircraft Avionics</td>
<td></td>
<td>(310) 393-1261 F</td>
</tr>
<tr>
<td>Navigation: Land, Sea, Air and Space</td>
<td></td>
<td><a href="mailto:m.kayton@ieee.org">m.kayton@ieee.org</a></td>
</tr>
<tr>
<td>One Hundred Years of Inertial Navigation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Practitioner's View of System Engineering</td>
<td>Dr. Hugh D. Griffiths,</td>
<td>+44-20-7679-7310</td>
</tr>
<tr>
<td>Synthetic Aperture Radar</td>
<td>University College, London</td>
<td>+44-20-7388-7325 F</td>
</tr>
<tr>
<td>Bistatic &amp; Multistatic Radar</td>
<td></td>
<td><a href="mailto:h.griffiths@ce.ccl.ac.uk">h.griffiths@ce.ccl.ac.uk</a></td>
</tr>
<tr>
<td>Current Advances in Radar Technology</td>
<td>Robert T. Hill, Consultant and Lecturer</td>
<td>(410) 770-4535 (V&amp;F)</td>
</tr>
<tr>
<td>Evolution of Inertial Navigation</td>
<td>Dr. Itzhak Bar-Itzhack</td>
<td>+ 972-4-829-3196</td>
</tr>
<tr>
<td>Future of Electronic Warfare and Modern Radar Signals</td>
<td>Dr. Richard G. Wiley, Research Associates of Syracuse</td>
<td>(315) 463-2266</td>
</tr>
<tr>
<td>Multisensor Data Fusion</td>
<td>Dr. Pramod Varshney, Syracuse University</td>
<td>(315) 463-8261 F</td>
</tr>
<tr>
<td>National Missile Defense and Early Warning Radars</td>
<td>Larry Chasteen, University of Texas at Dallas</td>
<td>(972) 234-3170;</td>
</tr>
<tr>
<td>Novel Orbits &amp; Satellite Constellations</td>
<td>Dr. Daniele Mortari, Texas A&amp;M University</td>
<td>(972) 883-2799</td>
</tr>
<tr>
<td>Radar — Past, Present and Future</td>
<td>Dr. Eli Brookner, Raytheon</td>
<td>(979) 845-6051 F</td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="mailto:mortari@aero.tamu.edu">mortari@aero.tamu.edu</a></td>
</tr>
<tr>
<td>Radar Communication Systems</td>
<td>Dr. S.H. Durrani, Consulting Engineer</td>
<td>(978) 440-4007</td>
</tr>
<tr>
<td>Satellite Communication Systems</td>
<td></td>
<td>(978) 440-4040 F</td>
</tr>
<tr>
<td>System Engineering for International Development for the 21st Century</td>
<td>Paul Gartz, Boeing Co.</td>
<td>(301) 774-4607 (V&amp;F)</td>
</tr>
<tr>
<td>Target Tracking and Data Fusion: How to Get the Most Out of Your Sensors</td>
<td>Dr. Yaakov Bar-Shalom, Univ. of Connecticut</td>
<td>(860) 486-4823</td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="mailto:ybar@engr.yale.edu">ybar@engr.yale.edu</a></td>
</tr>
</tbody>
</table>

All data on this page is under the purview of James Howard, VP-Member Affairs. Please send all corrections and omissions to him at the address on the inside back cover.
MEETING LOCATION
Hampton Inn Ottawa
100 Coventry Road
Ottawa, Ontario, Canada K1K 4S3
(613) 741.2300 / Toll Free (800) 426-7066

PUBLICATION OF PAPERS
In order to have your completed paper printed in the 2007 IEEE ICCST Proceedings, the author’s paid registration fee must be sent with the paper. Information about this procedure will be provided through the conference website.

ABSTRACTS AND PAPERS
Abstracts ad papers must be in English. Papers will be selected by the Technical Program Committee and authors will be notified. Authors will be responsible for their own travel and related expenses. Authors will pay 50% of the regular registration fee. Abstracts should be submitted to Carnahan Conference 2007.
This international conference is directed toward the research, development, and user aspects of electronic security technology, including principles of operation, applications, and user experiences. It is a forum for the exchange of ideas and dissemination of information regarding new and existing technology, as well as the impact of security-related technology on society.
Participation in the Carnahan Conference also provides a basis for long-range support and assistance to authorities and agendas in the use of technology for security, safety, law enforcement, and emergency response purposes.
Papers are sought which describe recent developments in the following fields:

- Sensor and detection technology, including principles of operation and signal analysis
- Alarm devices, searching aids and systems
- Monitoring, command, control and communication systems
- Computer systems security and privacy
- Information security
- Communication security and privacy, including modulation techniques, spectrum management and encryption
- Biometric identification systems, utilizing voice, handwriting, fingerprints, hand geometry, facial recognition, etc.
- Entry control systems, access delay technology and surveillance
- Counter-terrorism techniques and technology
- Impact on society of security systems and technology
- User experiences of operating security systems including their introduction and testing
- Police and forensic technology
- Cryptology
- Less-than-lethal weapons technology
- Counter-proliferation of weapons of mass destruction
Port and airport security
Emergency management
Network intrusion detection technology and virus protection
Border security
Society News & Information

Calling All Chapters !!!
The Distinguished Tutorials Program

Sajjad H. Durrani

The Distinguished Tutorials Program (DTP) was established in 2006. Many sections have expressed interest and some are currently in touch with Distinguished Instructors (DIs) to schedule a tutorial.

The Distinguished Tutorials Program allows a Section or an AESS Chapter to invite a Distinguished Instructor to give a tutorial at no cost to the hosts. The AESS picks up the travel cost and pays an honorarium. This allows members to benefit from tutorials, normally presented at major conferences that are not available locally, at a date convenient for the hosts.

The Program was approved by the AESS Board of Governors in 2006 and budgeted. Due to the better-than-expected response, funds are available for three or more Tutorials in 2007. Similarly, the program started with five Tutorials with four currently available. Tutorials are as listed. Interested parties should contact the Instructor directly.

Automated Testing
Michael Ellis, Northrop Grumman Corporation,
mtellis@aol.com

GPS and Inertial Data Processing
James Farrell, VIGIL, Inc.,
navaide@comcast.net

Systems Approach to Engineering Projects
Paul Gartz, Boeing Corporation,
p.gartz@ieee.org

Design and Use of Small Satellites in Education
Albert Helfrick, Embry Riddle Aeronautical University,
helfrica@erau.edu

Advances in Radar Technology
Robert Hill, Consultant,
janebobhill@msn.net

Navigation – Land, Air and Space
Myron Kayton, Consulting Engineer,
m.kayton@ieee.org

Space-Time Adaptive Processing for Surveillance Radar System
Michael L. Picciolo, SAIC,
Michael.L.Picciolo@saic.com

Digital Avionics
Cary Spitzer, Consultant,
c.spitzer@avionicon.com

Radar Reflectivity
Robert Trebits, Georgia Tech,
bob.trebits@gmail.com
About the Conference

The latest in the series of the UK's premier radar event returns in October 2007. Radar 2007 will cover all aspects of radar systems for civil, security, and defence applications and will showcase the latest developments in radar technology techniques and signal processing.

Radar 2007 provides a unique opportunity to update your knowledge on the latest developments for all involved in advanced radar systems, from the experienced engineer to new graduates seeking to build a career in this field.

Conference Highlights

- Three days of presentations showcasing the latest worldwide research and development
- A valuable opportunity for you to receive an update on the latest technologies and future challenges facing the radar industry
- A Tutorial day on 15 October – your chance to study a state-of-the-art topic area in greater detail
- An exhibition of the latest, most innovative products and services from key suppliers
- Valuable networking opportunities, including lunch breaks served on the exhibition show floor, a welcome drinks reception, and conference dinner at the prestigious Royal Museum of Scotland

Key Conference Themes

Topics to be covered at Radar 2007 include:

- Dual-Use/Civil Applications
- Radar Systems
- ECCM/ECM
- Advanced Sub-Systems
- Environment
- Processing Techniques
- Emerging Technologies
- Computer Modelling and Simulation

To Register Your Place At This Exciting Conference

Conference registration will be available in April 2007. To register your interest and receive advance information, please contact the organizers on: +44 (0) 1438 765 647 or e-mail: Eventsa3@theiet.org

Main Sponsors: Thales and Selex Sensors and Airborne Systems
Sponsors: BAE Insyte, Raytheon, and UCL

The IEEE Aerospace & Electronic Systems Society (AESS) is a technical sponsor of Radar 2007, one in an ongoing series of International Radar Conferences. The AESS Board of Governors has scheduled its Fall 2007 meeting to coincide with Radar 2007 in Edinburgh.