Letters to the Editor

This letter was received in response to a membership reaffirmation. If you agree—or disagree—with the author, please forward your comments to: aess.technical@ieee.org. We want to hear from you.

— Evelyn Hilt

Editors:

Thank you for the letter. It was much appreciated. I will contact you whenever needed. I want to comment on the "Aerospace and Electronic Systems Magazine," p.11. I may think that the format and layout of the magazine is really attractive. As the marketing window of your society, I see it as critical that this magazine should reflect the lively stages. I think the format of the publication has much to do with this.

I am working in the field of inertial navigation (at the university and industry) with industry experience in military aircraft systems. I would happily present suggestions and help where I can to maybe improve the magazine. I am still busy with my PhD, so my time is limited, but say where I can help and I will see what I can do.

Regards,

Franck C. Plessis

Barry C. Breen, Vice President-Conferences
Ira G. Weinstein, Associate Vice President-Conferences

PLACE
Corego, Germany

CONTACT
P. Wells, +361 (0646-2618)
P.1.646.4-2618
wells@bgs.com

Dayton, OH

R.L. Delsing, (937) 255-5055 Ext. 3
(513) 850-4-1250
rdelsing@wspcnet.com

Cleveland, OH

C.J. Pfeifer, (216) 881-8406
pfeifer@asme.org

http://www.asee.org

Milwaukee, WI

P.4.810-2-444
pfeifer@asme.org

http://www.ams.com

Adelaide, Australia

A. C. Jackson, (61) 8-8379-4422
+61 8 8379 4422
r устройства@acs.org.au

http://www.ams.org

Tulsa, OK

A. C. Jackson, (61) 881-444
+61 8 8379 4422
r устройства@acs.org.au

http://www.ams.org

Madison, WI

A. C. Jackson, (61) 881-338
+61 8 8379 338
r устройства@acs.org.au

http://www.ams.org

Praque, Czech Republic

M. Stackhouse, (02) 253-550
+61 8 8379 338
r устройства@acs.org.au

http://www.ams.org

Miami, FL

A. C. Jackson, (61) 881-444
+61 8 8379 4422
r устройства@acs.org.au

http://www.ams.org

St. Paul, MN

A. C. Jackson, (61) 881-444
+61 8 8379 4422
r устройства@acs.org.au

http://www.ams.org

Amsterdam, Netherlands

A. C. Jackson, (61) 881-444
+61 8 8379 4422
r устройства@acs.org.au

http://www.ams.org

Phnom Penh, Cambodia

A. C. Jackson, (61) 881-444
+61 8 8379 4422
r устройства@acs.org.au

http://www.ams.org

Miami, FL

A. C. Jackson, (61) 881-444
+61 8 8379 4422
r устройства@acs.org.au

http://www.ams.org

St. Petersburg, Russia

A. C. Jackson, (61) 881-444
+61 8 8379 4422
r устройства@acs.org.au

http://www.ams.org

Elsharafer, Netherlands

A. C. Jackson, (61) 881-444
+61 8 8379 4422
r устройства@acs.org.au

http://www.ams.org

Montreal, Canada

A. C. Jackson, (61) 881-444
+61 8 8379 4422
r устройства@acs.org.au

http://www.ams.org

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

Column ........................................................................ 3


Articles .........................................................................

♦ SAR for Disaster Management ..................................... 4
  R.K. Sharma, B.S. Kumar,
  N.M. Desai & V.R. Gujraty

♦ Distance Estimation in the 60 GHz Band ...................... 10
  F. Kuroki, Y. Wagatsuma & T. Yoneyama

♦ Dynamic Signature Forgery Assessment and Signal Strength Perception ......................... 13
  S. Elliott & A. Hunt

♦ Along-Track Interferometry for Ground Moving Target Indication ......................... 19
  E. Chapin & C.W. Chen

♦ ISRO Programmable Digital Waveform Generator ......................... 25
  S. Gangele, N.M. Desai, R.S. Kumar,
  J.G. Vachhani & V.R. Gujraty

♦ Monitoring Ball Grid Array Solder Joints 24 × 7 ............. 31
  J.P. Hofmeister, J.B. Judkins, D. Goodman,
  T.A. Tracy & N.N. Roth

Engineering of an Observatory on the Far Side of the Moon ........................................... Insert
  M. Kayton

News & Information ....................................................

Nathanson Award to Marina Sabrina Greco ................................................................. 3
IEEE-NANO 2008 in Texas ......................................................................................... 46
Carnahan Security Technology 2008 in Prague ......................................................... 47
SAR for Disaster Management

In the last couple of years, an indigenous Airborne Synthetic Aperture Radar for Disaster Management (DMSAR) has been under development at SAC / ISRO, as a capacity building measure for evolving an effective Disaster Management Support (DMS) System in India. Synthetic Aperture Radar (SAR) has an unique role to play in the mapping and monitoring of large areas affected by natural disasters, especially floods, owing to its unique capability to see through clouds as well as all-weather imaging capability. DMSAR is presently mounted on-board Beechcraft B-200 aircraft and will be subsequently carried on a jet class aircraft and utilized for estimating the extent of damage over large areas (>50 - 75 Km) and also assess the effectiveness of the relief measures undertaken during disasters like floods. Considering the unique application requirements of disaster management, one of the major essential and critical requirements is the generation and availability of DMSAR images in real- or near-real-time with very fast turn-around times. DMSAR image generation involves complex signal processing of the acquired raw data, involving data decompression, two-dimensional SAR processing, motion sensing and compensation tasks, and image mosaicing on display as well as storage of processed SAR images on suitable recording media.

Distance Estimation at 60 GHz Band

An FM-CW radar front-end was fabricated in an integrated manner at 60 GHz by using the NRD guide. Main emphasis was placed on compactness in size and high-precision operation in performance. The fabricated radar consists of an FM Gunn oscillator, a balanced mixer, and a planar antenna fed by leaky NRD guide with a mechanically beam-scanning performance. All circuit components and the antenna were contained in a compact housing of 170 x 140 mm in area and 25 mm in thickness, and thus, a thin type of millimeter-wave radar front-end was successfully developed. Moreover, an error of distance estimation was measured to be less than 0.7 m.

Dynamic Signature Forgery and Signature Strength Perception Assessment

Dynamic signature verification has many challenges associated with the creation of the impostor dataset. The literature discusses several ways of determining the impostor signature provider, but this takes a different approach - that of the opportunistic forger and his or her relationship to the genuine signature holder. This examines the accuracy with which an opportunistic forger assesses the various traits of the genuine signature, and whether the genuine signature holder believes that his or her signature is easy to forge.

Along-Track Interferometry for Ground Moving Target Indication

Synthetic aperture radar (SAR) along-track interferometry (ATI) has been used extensively to measure ocean surface currents. Given its ability to measure small velocities (~10 cm/s) of relatively radar-dark water surfaces, there is great potential that this technique can be adapted for ground moving target indication (GMTI) applications, particularly as a method for detecting very slow targets with small radar cross-sections. Herein, we describe preliminary results from an ATI GMTI experiment.

ISRO’s Programmable Digital Waveform Generator

One of the major and common requirements for all active microwave sensors is generation of the transmit modulation signal-like chirp/LFM signal, MSK, etc., which can be generated by analog or digital means. With the increasing demands of sidebandwidth, longer duration chirp signals in radar systems, digital signal generation, and processing has emerged as a preferred alternative. Design and development of programmable and generic Digital Waveform Generator (DWG) system based on Xilinx Virtex XCV600 FPGA and high-speed DAC is carried out at the Space Applications Center. ISRO is to generate required transmit chirp signal of high time-bandwidth product (~ 1000) for ISO’s microwave radar sensor missions. This gives a detailed description of the design requirements, implementation details, salient performance features, and test results of this programmable and generic Digital Waveform Generator (DWG).

Monitoring Ball Grid Array Solder Joints 24 x 7

As FPGA density and overall usage increases, there is a corresponding and growing need to monitor these solder joint networks. Prior to the introduction of a first sensor, SJ BIST™ (SJ Built-in-Self-Test™), there were no known methods for detecting faults in the solder joint networks of fully-programmed, operational Field Programmable Gate Arrays (FPGAs). Because SJ BIST™ requires over 100 mW at 3.3 V to test 8 FPGA pins, we introduce SJ Monitor™, a lower-power design (less than 5.0 mW) to provide 24/7 health monitoring of selected I/O pins; the complementary form SJ Monitor™ can be used to monitor the pins of powered FPGAs. SJ Monitor™ is able to detect all solder joint network faults that last at least as long as 15 ms and which are at least as low as 100 S2 with no false alarms. This capability allows for detection of faults before they begin to exhibit intermittent failures, which, in turn, facilitates condition-based maintenance to reduce failures during critical missions.

Security Threats in Wireless Sensor Networks

Wireless Sensor Network (WSN) is an emerging field. These are normally designed to perform a set of high level information processing tasks; for example, detection, tracking, or classification. Different application areas of WSNs are Environmental Monitoring, Industrial Sensing and Diagnostics, Infrastructure Protection, Battlefield Awareness, Context Aware Computing, etc. From application areas of WSN, it has been observed that ensuring security and privacy is one of the highest priorities for Wireless Sensor Network Systems. Information in the network must be protected from attackers.

Attackers may devise different types of security threats to make the WSN system unstable. Herein, we have identified different security threats possible for a Sensor Net Setting. Effort has been made to model the threats mathematically. Future scope of the work has also been outlined.

---

**Engineering of an Observatory on the Far Side of the Moon**

Insert
FROM THE EDITOR-IN-CHIEF

**IEEE A&E Systems & IEEE Transactions on A&ES**

Many readers may not be aware of the span of subjects published by this society, especially in our *Transactions*, nor are they cognizant of the definite distinctions between the offerings published in these publications. *Transactions* publishes significantly technical material related to our field of interest that is thoroughly peer-reviewed prior to publication. [Our field of interest is printed in every issue of both publications on the inside front cover.] *Transactions* accepts both articles and correspondence, and is published quarterly. Later this year (with the cooperation of the authors) *Systems* plans to provide (as an insert) a sample of material suitable only for the *Transactions* to whet your appetite. Titles of several articles currently being prepared for publication are listed to give you the type and breadth of *Transactions* typical contents. For more details go to the AESS website. All material published is archival and is included in our annual index to publications.

*Systems* issues monthly; it is our agent for bringing you a pleasurable read of short articles, allowing you to stay current on technical topics of interest or to broaden your knowledge of a subject. It serves as the archival journal for IEEE AESS Society activities. It has a strict policy of no mathematical expressions in text.

Extensive articles covering one subject, historical pieces, and series of articles related to one subject are carried as removable inserts, whereas our *Tutorials* and extensive outstanding writings are issued as a separate publication (part two of an issue) to insure that everyone receives them. We make it a practice to send selected issues to every IEEE Student Branch.

All AESS publications are coordinated by the IEEE AESS Publications Board. Comments on our policies are welcome; please address them to the VP-Publications.

— Evelyn Hirt

These are actual titles from our *Transactions*. Each issue's contents are posted on the Society website shortly after issue – try browsing the complete contents. You may wish to become a subscriber – paper or electronic. If so, go to the IEEE website and click on the Aerospace & Electronic Systems Society publication for details.

- Geometric Voting Algorithm for Star Trackers
- Multi-Objective Approach to GNSS Code Discriminator Design
- Carrier Loop Architectures for Tracking Weak GPS Signals
- Fusion of Distributed Extended Forgetting Factor RLS State Estimators
- Position Error Bound for UWB Localization in Dense Cluttered Environments
- Cooperative Task Scheduling for Networked Uninhabited Air Vehicles
- Signature Search Time Evaluation in Flat File Databases
- Cost-Equivalencing Discretization of a Class of Bang-Bang Guidance Laws
- Hybrid Discriminative/Class-Specific Classifier for Narrowband Signals
- Assignment Costs for Multiple Sensor Track-to-Track Association
- Hierarchical Path Computation Approach for Large Graphs
- GLRT Subspace Detection for Range and Doppler Distributed Targets

**The 2007 Fred Nathanson Memorial Radar Award**

Dr. Maria Sabrina Greco was recently awarded the 2007 *Fred Nathanson Memorial Radar Award* "for contributions to signal processing, estimation, and detection theory." The purpose of this award is to grant international recognition for outstanding contributions to the radar art by young IEEE/AESS members. Dr. Greco has been an Assistant Professor at the “Ingegneria dell’Informazione” of the University of Pisa, Italy, since 2001. She received her award at the 2008 IEEE Radar Conference, May 26-30, 2008, Rome, Italy.

(Award details on the AESS website.)
SAR for Disaster Management

Ritesh Kumar Sharma, B. Saravana Kumar, Nilesh M. Desai & V.R. Gujrati
Indian Space Research Organisation (ISRO)

ABSTRACT

In the last couple of years, an indigenous Airborne Synthetic Aperture Radar for Disaster Management (DMSAR) has been under development at SAC / ISRO, as a capacity building measure for evolving an effective Disaster Management Support (DMS) System in India. Synthetic Aperture Radar (SAR) has an unique role to play in the mapping and monitoring of large areas affected by natural disasters, especially floods, owing to its unique capability to see through clouds as well as all-weather imaging capability. DMSAR is presently mounted on-board Beechcraft B-200 aircraft and will be subsequently carried on a jet class aircraft and utilized for estimating the extent of damage over large areas (50 - 75 Km) and also assess the effectiveness of the relief measures undertaken during disasters like floods.

Considering the unique application requirements of disaster management, one of the major essential and critical requirements is the generation and availability of DMSAR images in real- or near-real-time with very fast turn-around times. DMSAR image generation involves complex signal processing of the acquired raw data, involving data decompression, two-dimensional SAR processing, motion sensing and compensation tasks, and image mosaicing on display as well as storage of processed SAR images on suitable recording media.

PROEM

A Near-Real-Time SAR Processor (NRTP) has been built at SAC / ISRO to meet the varied and complex near-real-time SAR processing requirements of various DMSAR operating modes. It is a generic full-fledged hardware SAR processor based on Commercial-Off-The-Shelf (COTS) multiprocessor Analog Devices TigerSHARC TS101S DSP plug-in boards on a Compact PCI (cPCI) platform. NRTP SAR Processor consists of a Range Processor, a Pre-processor for motion sensing computations and Motion Compensation, Azimuth Block processor, and the post-processor. The input ingest to NRTP range processor is done through a recorder replay unit and the data are distributed for range compression to multiple DSPs on a round-robin basis. The range compressed data are fed to the Pre-Processor unit which carries out pre- and post-Doppler Centroid Estimations, velocity / PRF slaving, azimuth interpolation, and resampling of data before storing and feeding to Azimuth Processor consisting of sixteen 4 DSP clusters. The azimuth block processor performs phase compensation, Range Cell Migration correction (RCMC), and Azimuth processing. Here, the data blocks of 1K range gates subswath x 16K azimuth PRF lines are distributed to each 4-DSP cluster, which carries out complete azimuth processing of one block of data. The post-processing module performs geometric and radiometric corrections, sub-block image mosaicing, and image rotation and generates the precision image product. A cPCI Pentium P3 Single Board Computer (SBC) performs the overall control and coordination tasks for the various DSP clusters and other interfaces. The current NRTP configuration necessitates about 72 TigerSHARC TS101 DSP's (a 250 MHz for full swath near-real-time DMSAR processing. The NRTP is housed in a single 14-Slot 7U cPCI chassis, which contains 6 DSP boards, weighs 25 Kgs, and consumes about 600 Watts average power. The complete software development for the DSPs has been carried out in VisualDSP++ and VC++. The hardware configuration, DSP benchmarking, and software development for various constituent modules have already been completed. NRTP has been utilized in the Lab to generate DMSAR images for the test flights conducted during 2006-2007. Although current NRTP is able to generate DMSAR images at 25-30 times real-time (RT) rate, the code and algorithm optimization efforts are underway to
speed up the product turn-around time to at least 10 times RT rate, for all the DMSAR resolution modes using new generation TS2011 DSPs. Present NR 171 has been operationalised for pre- and post-monsoon DMSAR flights carried out in 2007 in flood-prone states of India. Moreover, a scaled-down 48-DSP hardware configuration is also deployed as a Quick Look SAR Processor (QLP) on-board the aircraft to produce real-time limited swath (25-50 Kms) fall resolution (3m / 5m / 10m / 30m) and 30m resolution full swath DMSAR images. QLP is being regularly utilized in all DMSAR prototype flights carried out since December 2005 and is an operational constituent unit of DMSAR.

This mainly gives the performance test results and the image products generated using NRTP and QLP for various DMSAR prototype and calibration flights conducted during the last year. It also describes the design requirements, algorithmic and DSP architecture details, and salient performance features of these DMSAR processors.

INTRODUCTION

Disaster Management SAR is an indigenous system to provide the support to India’s Disaster Management Support (DMS) program. This SAR system is performing a vital role in natural disasters mainly in case of floods where it is able to produce the imagery and maps of the affected areas in cloudy weather as well as night conditions which makes it advantageous over optical sensors. Since in the monsoon period, the atmosphere is fully covered with the clouds, therefore it is very useful to use microwave sensors instead of optical because microwaves can penetrate through clouds. Therefore having the capability of active microwave sensors on-board in the Beechcraft B-200 aircraft, DMSAR is fulfilling the nation’s disaster management requirements.

This system transmits the microwave pulse and receives the back-scattered signal. Coherent processing is applied to generate the High Resolution Synthetic Aperture Radar (SAR) images from these returned signals. The processing is characterized by enormous data volume, complex signal processing algorithms, very high computing power, and difficult control requirements. The generation of off-line High Resolution SAR data products using software-based precision SAR processors involves either considerably large product turn-around time or super-computing machine power.

One of the essential requirements for a Disaster Management SAR (DMSAR) is the availability of processed data with a real- or near-real-time product turn-around time. In view of this, the design and development of a full-fledged high throughput processor to process SAR data, and display the images in real-time has been developed. This Quick Look Processor (QLP) unit is placed on-board and able to produce limited swath (25-50 Kms) full resolution (3m / 5m / 10m >30m) and 30 m resolution full swath DMSAR images in real-time. QLP is a 48 TS101S DSP processor configuration. It also displays the annotation parameters below the image and is being regularly utilized in DMSAR flights carried out since December 2005.

Since the airborne SAR is very much affected by the air turbulence and motion errors, it is mandatory to incorporate additional motion compensation tasks for the generation of high precision SAR images. Hence, a Near-Real-Time SAR Processor (NRTP) Unit has been developed, comprising 72

Table 1. Specifications of generic QLP / NRTP

<table>
<thead>
<tr>
<th>Parameter</th>
<th>DMSAR Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resolution</td>
<td>1m / 3m / 5m / 10m / 30m</td>
</tr>
<tr>
<td>No of range gates</td>
<td>16K</td>
</tr>
<tr>
<td>Input data interface</td>
<td></td>
</tr>
<tr>
<td>QLP</td>
<td>16 bit LVDS</td>
</tr>
<tr>
<td>NRTP</td>
<td>@ 7.8125 MHz</td>
</tr>
<tr>
<td>Implementation</td>
<td>RAID / JBOD, DLT, IIDD</td>
</tr>
<tr>
<td></td>
<td>Xilinx FPGA</td>
</tr>
<tr>
<td></td>
<td>Xilinx Virtex-11</td>
</tr>
<tr>
<td>Range Processor</td>
<td></td>
</tr>
<tr>
<td>Range FFT Size</td>
<td>16K</td>
</tr>
<tr>
<td>Number of DSPs</td>
<td>4 (QLP) / 8 (NRTP)</td>
</tr>
<tr>
<td>(TS101S / TS201S)</td>
<td></td>
</tr>
<tr>
<td>Azimuth Processor</td>
<td></td>
</tr>
<tr>
<td>Number of DSP's</td>
<td>44 (QLP) / 64 (NRTP)</td>
</tr>
<tr>
<td>(TS101S / TS201S)</td>
<td></td>
</tr>
<tr>
<td>Doppler bandwidth</td>
<td>160 Hz</td>
</tr>
<tr>
<td>Quick Look image size</td>
<td>1024 × 1024 Pixels</td>
</tr>
<tr>
<td>Scrolling</td>
<td></td>
</tr>
<tr>
<td>Host Processor and Housing</td>
<td>PIII L 1.6 GHz SBC,</td>
</tr>
<tr>
<td></td>
<td>14 Slot -9U ePCI Chassis</td>
</tr>
<tr>
<td>Processed data storage</td>
<td>SDLT / IIDD</td>
</tr>
<tr>
<td>Display monitor</td>
<td>19&quot; TFT / LCD</td>
</tr>
<tr>
<td>Weight and Power</td>
<td>25 Kgs, 600 W (Typical)</td>
</tr>
</tbody>
</table>
TS101S DSP processors, with a capability to generate the images at 25-30 times Real-Time (RT) rate. The upgraded version of this processor will have product turn-around time of better than 10 times RT rate.

**QLP / NRTP CONFIGURATION**

The QLP / NRTP operates in the following modes:

- *Quick Look processor on-board the aircraft* to produce real-time full / limited swath SAR images; and

**Fig. 1. QLP / NRTP Processing Algorithm**

- *On-ground Near-Real-Time*, high precision full swath SAR processor (NRTP)

Major specifications of QLP / NRTP are given in Table 1.

**QLP / NRTP PROCESSING ALGORITHM**

The frequency domain Range Doppler (RD) algorithm is employed for Range and Azimuth compression in both QLP and NRTP configurations for DMSAR. On-board motion compensation tasks like V / PRF slaving, antenna stabilization, etc., are not performed in the DMSAR hardware system owing to operational constraints. Moreover, the aircraft undergoes random turbulences due to the harsh environment it operates in, which introduces motion errors in the acquired SAR data. These motion compensation tasks are incorporated in the Near-Real-Time Processor (NRTP) to generate high precision SAR images. Figure 1 gives the processing algorithm for QLP and additional motion compensation tasks required for NRTP are also shown.

After range compression using FFT-based fast convolution, antenna pattern correction, The estimation and
slaving operation, azimuth processing is carried out in subapertures. It involves phase compensation, data slaving, azimuth FFT, frequency domain RCM correction (RCMC), image detection, multi-look, interpolation in azimuth direction, and final mosaicing operation along with slant-range to ground-range conversion and north-referencing.

**QLP / NRTP ARCHITECTURE**

The generic configuration of QLP / NRTP, shown in Figure 2, is a mix of COTS boards containing VLSI / FPGA signal processors and programmable multiple DSP processors. The major functional hardware constituents are as follows:

- Input Ingest module,
- Range Processing module,
- Azimuth Processing / Motion compensation module, and
- Post-Processing module.

The input ingest module provides an appropriate interface to receive the formatted raw SAR data from the data acquisition subsystem or Data Recording system (DRS). Additionally, it extracts the raw data (sync detection and header stripping) from the formatted data stream. The input raw SAR data is available to the QLP as two 8-bit wide parallel channels (I and Q Channels). For NRTP, the RAID recorder data is replayed at a slower rate. After raw data extraction and reformatting, the input ingest module distributes the reformatted data to the range processing unit via link ports for further processing. Additionally, BAQ decoder is also implemented in the input ingest module, in case the raw SAR data is BAQ-compressed. The BAQ decoder, sync checker, and link port interface logic to DSP are implemented using a Xilinx Virtex-11 FPGA.

The Range Signal Processor, Azimuth Signal Processor, and Post-Processor are built using fully programmable Floating-Point DSPs (Analog Devices TigerSHARC TS101S / 201S processor). Commercial-Off-The-Shelf (COTS) DSP plug-in boards on a Compact PCI (cPCI) platform are used for the purpose. Each COTS board consists of eight TigerSHARC (TS101S / TS201S) processors. Additional processor density per board can be achieved by populating the two PMC (PCI Mezzanine Card) sites with two, four processor PMC modules. Thus, a processor density of 16 processors per board can be achieved. About four to six fully populated boards are required to perform SAR processing of DMSAR data.

Overall, the current NRTP configuration necessitates about 72 TigerSHARC TS101 DSPs (~ 250 MHz for full
swath near-real-time DMSAR processing. The NRTP is housed in a single 14-Slot 9U cPCI chassis, which contains 6 DSP boards, weighs 25 Kgs, and consumes about 600 Watts average power. The complete software development for the DSPs has been carried out in Analog Devices VisualDSP++ and VC++. The hardware configuration, DSP benchmarking, and software development for various constituent modules have already been completed. NRTP has been utilized in the Lab to generate DMSAR images for the test flights conducted during 2006-2007.

QLP / NRTP TEST RESULTS AND DMSAR IMAGES

Quick Look Processor (QLP), which is equipped with the facilities to provide all the annotation as well as the browse images in real-time, is carried on-board as DMSAR constituents. NRTP is presently utilized in the Lab and generates precision SAR images in Near-Real-Time. Subsequently, it will also be carried on-board DMSAR. In 2007, NRTP was operationalised for pre- and post-monsoon DMSAR flights in flood-prone states of India. During these flights, data was acquired over different regions. These data were processed with QLP / NRTP. Figures 3, 4, and 5 show some of these images. These images are also utilized to create inundation maps of flood-prone areas.

Simultaneously, DMSAR test and calibration flights were carried out over Bagodam (near Ahmedabad) calibration site in Gujarat. These calibration images have been processed with NRTP and the resultant image quality parameters are shown in Table 2. Figure 6 shows the point target responses and calibration site images of the deployed corner reflectors for different calibration runs.

CONCLUSION

DMSAR is envisaged as a critical and necessary technical support tool for India's Disaster Management Support Programme (DMSP). The design and development of on-board and ground segment SAR Processors for DMSAR also pose considerable challenges considering the operational requirements of airborne systems in disaster scenarios. For DMSAR flood-mapping applications, real- or near-real-time image generation and inundation map generation for water level extraction is very critical for damage assessment and planning of relief measures. The Quick Look SAR Processor (QLP) on-board the aircraft also has great utility during flood-mapping sessions, as it can be utilized to identify flooded areas for subsequent precision image generation. This describes the design requirements, algorithmic and Multi-DSP architecture details, and salient performance features of QLP and NRTP SAR Processors for ISRO's DMSAR. These QLP / NRTP developments also directly feed into our continuing efforts for the development of NRTP / QLP systems for RISAT-1 SAR ground segments.

ACKNOWLEDGMENTS

The authors thank Dr. R.R. Navalugund (Director, SAC) and Shri S.S. Rana (Deputy Director, MRSA) for their guidance and encouragement to Microwave sensors and SAR-related developmental activities. The authors also wish to acknowledge the contributions of all of their colleagues in MSDPD / MSDG, Scientists / Engineers, and other staff.
members of SAC / ISRO and other ISRO centres involved in the activities related to DMSAR.

REFERENCES

[1] SAC / ISRO Internal report, 2006,
   Quick Look / Near real-time SAR processor
   System for RISAT-1:
   Preliminary Design Review Document.

   Preliminary Design Review Document for Disaster Management SAR (DMSAR).

   A real-time processor for the Danish airborne SAR,

   Synthetic Aperture Radar - Systems and Signal Processing,
   J. Wiley & Sons, USA.

   A Real-Time Airborne SAR processor,
Distance Estimation at 60 GHz Band

Futoshi Kuroki  
*Kure College of Technology*  
Yoshihiko Wagatsuma  
*Tohoku University*  
&  
T. Yoneyama  
*Tohoku Institute of Technology*

**ABSTRACT**

An FM-CW radar front-end was fabricated in an integrated manner at 60 GHz by using the NRD guide. Main emphasis was placed on compactness in size and high-precise operation in performance. The fabricated radar consists of an FM Gunn oscillator, a balanced mixer, and a planar antenna fed by leaky NRD guide with a mechanically beam-scanning performance. All circuit components and the antenna were contained in a compact housing of $170 \times 140$ mm in area and 25 mm in thickness, and thus, a thin type of millimeter-wave radar front-end was successfully developed. Moreover, an error of distance estimation was measured to be less than 0.7 m.

**INTRODUCTION**

Millimeter-wave frequencies have attracted much attention for the construction of novel communication and sensing systems. Actually, several types of millimeter-wave front-ends have been developed by many companies, institutions, and laboratories based on various printed transmission line techniques [1]. The printed transmission lines are suitable for applications in the centimeter frequencies, but they suffer from a lot of transmission losses in the millimeter-wave region.

Another candidate as a transmission medium is the NRD guide, which consists of dielectric strips inserted in a below cut-off parallel metal plate waveguide and features no radiation at curved sections and discontinuities. Indeed, many high performance millimeter-wave front-ends such as an ultra-high speed LAN transceiver [2] and a broad-band transmitter and receiver [3] have been successfully fabricated.

With this in mind, we developed an FM-CW radar front-end for distance estimation at 60 GHz band.

---

**Fig. 1. Structure of NRD guide FM-CW radar front-end**

**Fig. 2. Plane view of NRD guide FM-CW radar front-end**  

**NRD GUIDE FM-CW RADAR**

Figure 1 shows a structure of the NRD guide FM-CW radar, which has a double layered structure. The NRD guide circuit as shown in Figure 2, which consists of an FM Gunn oscillator, two 3-dB directional couplers, a circulator, and a balanced mixer, are installed in the lower layer. A modulated wave is introduced to a leaky NRD guide radiator through a coaxial transition. This leaky NRD guide is an uni-directional radiator because a reflector is set at the right side. A leaky wave is introduced from the lower layer to the upper layer.
Fig. 3. Side-view of NRD guide FM-CW radar front-end

Fig. 4. Structure of NRD guide FM Gunn oscillator

Fig. 5. Measured performance of NRD guide FM Gunn oscillator

through a coupling slit. To scan a main beam, a short plate is
mechanically rotated by a motor as shown in Figure 3.

FM OSCILLATOR AND ANTENNA

In this chapter, characteristics of key components for
FM-CW radar are described. The metal plate separation of
the NRD guide was set at 2.25 mm so as to be less than half a
free space wavelength at 60 GHz. Teflon with a relative
dielectric constant of 2.04 was chosen as a dielectric strip due
to its low loss nature, and its cross-sectional dimensions were
2.25 mm in height and 2.5 mm in width, respectively.

At first, a structure of an FM Gunn oscillator is shown in
Figure 4. A Gunn diode was transversely inserted in an
H-shaped metal block, where a λ/4 choke circuit was
installed in the metal block. A beam-lead type varactor diode
mount was made by glass-Teflon substrate as shown in the
inset of Figure 4, on which electrodes and bias choke circuits
were etched. The diode mount was sandwiched by Teflon
pieces and this was located behind the Gunn oscillator.

Figure 5 shows the measured frequency deviation and output
power of the FM Gunn oscillator. The oscillation frequency
can be tuned at 300 MHz versus the bias voltage of 15 V,
while the oscillation power is 80 mW on average. Next
consideration is concerned with a leaky NRD guide. The
NRD guide has a non-radiating nature, but radiation occurs in an asymmetrical structure for horizontal mid-plane of the NRD guide. An example of the an asymmetrical structure is shown in Figure 6, where the Teflon strip was embedded in a groove made on the metal plate. In this structure, a leaky wave was radiated to the left side due to installation of the reflector, and is introduced to the upper layer as shown in Figure 7.

Figure 8 shows a plane view of the coupling slit. When the short plate was leaned by the motor, the direction of the leaky wave was changed. The measured radiation patterns versus the leaning angle are shown in Figure 9. It is obvious that the direction of the main beam can be controlled at 15° without any degradation of the radiation pattern.

**PERFORMANCE OF NRD GUIDE FM-CW RADAR**

Figure 10 shows a photograph of the fabricated NRD guide FM-CW radar front-end. All circuits components and the antenna was contained in a compact housing of 170 × 140 mm in area and 25 mm in thickness, and thus, a thin type of millimeter-wave radar front-end was successfully developed. The measured distance estimation performance is shown in Figure 11. The precise radar performance can be confirmed because the estimation error was less than 0.7 m for the distance to the target from 5 m to 120 m. Radar performance is summarized in Table 1.

**REFERENCES**


Dynamic Signature Forgery and Signature Strength Perception Assessment

Stephen Elliott & Adam Hunt
Purdue University

ABSTRACT

Dynamic signature verification has many challenges associated with the creation of the impostor dataset. The literature discusses several ways of determining the impostor signature provider, but this takes a different approach – that of the opportunistic forger and his or her relationship to the genuine signature holder. This examines the accuracy with which an opportunistic forger assesses the various traits of the genuine signature, and whether the genuine signature holder believes that his or her signature is easy to forge.

INTRODUCTION

Dynamic signature verification (DSV) has long been used to authenticate individuals based on their signing characteristics, such as speed, pressure, and graphical output. Approaches to DSV have been discussed in detail in the literature. Popular applications, such as document authentication, financial transactions, and paper-based transactions have all, at one time, used the signature to convey the intent to complete a transaction [1, 2]. DSV is a subset of a larger science called biometrics. Biometrics aims to authenticate an individual based on either behavioral or physiological traits, (or a combination of both), including face recognition, iris recognition, and fingerprint recognition, to name a few. Many of these modalities are made up of both behavioral and physiological attributes, with various proportions of each. Within the continuum, the signature is a strong behavioral biometric. The signature’s unique traits make it harder to test and evaluate than some of the other behavioral biometrics, such as voice or face recognition. Challenges to testing and definitively evaluating the signature include the fact that a signature is learned over time (and evolves over time as the owner and his or her handwriting matures), it contains variant measures (such as pressure, speed, etc., that can be changed), can be changed by the owner (depending on the ceremony of the transaction), and may have several versions (for example, at work and home may have different signatures).

A discussion of DSV invariably raises a number of concerns. The first concern is that people acknowledge their failure to sign consistently, and the second is that most people have attempted, irrespective of degree of success, to forge someone’s signature at some time. In fact, a straw poll conducted in a class of 80 undergraduate college students revealed that at least 90% of them have attempted to forge a signature at one time. When asked for more details about the forgery attempt, in the majority of cases, the subject of the attack is someone who is known to the forger (typically a parent or close relative) and the signature is easily available. In these cases, it is more than likely that the forger has had several chances to practice the signature and that the signature is not rigorously checked by the receiver of the document being forged. These two conditions correlate to a low chance of getting caught – this is the scenario of the opportunistic forger.

Another important consideration has to do with whether a genuine signature holder believes that his or her signature is difficult to forge, and whether the imposter also believes that to be the case. The approach, proposed herein, is to understand whether the imposter can actually make well-informed decisions on the measurable variables of the genuine signature. For example: Can the forger determine the speed of the signature, as well as the handedness of the genuine signer? If the forger can determine these most basic of attributes, then he or she might then achieve some level of success to forge some of the additional variables within DSV.

VARIABLE CHARACTERISTICS OF THE DSV

DSV’s numerous variables are calculated using the input gathered from a digitizer. These variables include x and y (Cartesian) coordinates, pressure (p) or force, and time (t) [3]. This output from the digitizer is used to create the global
<table>
<thead>
<tr>
<th>Study Authors</th>
<th>Type I (FAR)</th>
<th>Error Rates</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Type II</td>
</tr>
<tr>
<td>Achemlal, Mourier, Lorette &amp; Bonnefoy (1986)</td>
<td>11.0%</td>
<td>8.0%</td>
</tr>
<tr>
<td>Beatson (1986)</td>
<td>1.0%</td>
<td>2.0%</td>
</tr>
<tr>
<td>Bechert (1984)</td>
<td>5.0%</td>
<td>5.0%</td>
</tr>
<tr>
<td>Bonnefoy &amp; Lorette (1981)</td>
<td>0.6%</td>
<td></td>
</tr>
<tr>
<td>Bault &amp; Plamondon (1981)</td>
<td>1.2%</td>
<td>1.0%</td>
</tr>
<tr>
<td>Collantier (1984)</td>
<td>3.5%</td>
<td></td>
</tr>
<tr>
<td>Crane &amp; Ostrem (1983)</td>
<td>1.5%</td>
<td>1.5%</td>
</tr>
<tr>
<td>Debruyne (1985)</td>
<td>3.0%</td>
<td>2.0%</td>
</tr>
<tr>
<td>Hale &amp; Pagnini (1980)</td>
<td>1.5%</td>
<td>1.2/2.5%</td>
</tr>
<tr>
<td>Herbst &amp; Liu (1979)</td>
<td>1.7%</td>
<td>0.4%</td>
</tr>
<tr>
<td>Herbst &amp; Liu (1979)</td>
<td>2.4%</td>
<td>3.4%</td>
</tr>
<tr>
<td>Ibrahim &amp; Levrat (1979)</td>
<td>19.0%</td>
<td>5.5%</td>
</tr>
<tr>
<td>Lam &amp; Kamis (1979)</td>
<td>0.0%</td>
<td>2.5%</td>
</tr>
<tr>
<td>Lorette (1983)</td>
<td>6.0%</td>
<td></td>
</tr>
<tr>
<td>Mital, Hin &amp; Leng (1989)</td>
<td>0.0%</td>
<td>0.0%</td>
</tr>
<tr>
<td>Parizeau &amp; Plamondon (1989)</td>
<td>4.0%</td>
<td></td>
</tr>
<tr>
<td>Sato &amp; Kogure (1982)</td>
<td>1.8%</td>
<td>0.0%</td>
</tr>
<tr>
<td>Worthington, Chainer, Williford &amp; Gunderson (1985)</td>
<td>1.8%</td>
<td>0.28-2.33%</td>
</tr>
<tr>
<td>Zimmerman &amp; Varady (1985)</td>
<td>30-50%</td>
<td>4-12%</td>
</tr>
<tr>
<td>Cordella, Foggia, Sanson &amp; Vento</td>
<td>0.03-20.82%</td>
<td>5.7%</td>
</tr>
<tr>
<td>Wirtz (1997)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dimauro, Impedovo &amp; Pirlo (1993)</td>
<td>1.7%</td>
<td>1.2%</td>
</tr>
<tr>
<td>Nalwa (1997)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nalwa (1997)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nalwa (1997)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mingming &amp; Wijesoma (2000)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mingming &amp; Wijesoma (2000)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mingming &amp; Wijesoma (2000)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hamilton, Whelan, McLaren &amp; MacIntyre (1995)</td>
<td>34.0%</td>
<td>26.0%</td>
</tr>
<tr>
<td>Hamilton, Whelan, McLaren &amp; MacIntyre (1995)</td>
<td>22.0%</td>
<td>18.0%</td>
</tr>
<tr>
<td>Hamilton, Whelan, McLaren &amp; MacIntyre (1995)</td>
<td>12.0%</td>
<td>10.0%</td>
</tr>
<tr>
<td>Hamilton, Whelan, McLaren &amp; MacIntyre (1995)</td>
<td>7.0%</td>
<td>6.0%</td>
</tr>
<tr>
<td>Martens &amp; Clausen (1997)</td>
<td>1.5%</td>
<td>1.3%</td>
</tr>
<tr>
<td>Chang, Wang &amp; Suen (1993)</td>
<td>2.0%</td>
<td>2.5%</td>
</tr>
<tr>
<td>Higashino (1992)</td>
<td>8.0%</td>
<td>0.6%</td>
</tr>
<tr>
<td>Minot &amp; Gentrie (1992)</td>
<td>2.0%</td>
<td>4.0%</td>
</tr>
<tr>
<td>Lucas &amp; Damper (1990)</td>
<td>5.6%</td>
<td>4.5%</td>
</tr>
<tr>
<td>Tseng &amp; Huang (2002)</td>
<td>12.5-28.8%</td>
<td>5.0-12.5%</td>
</tr>
<tr>
<td>Lee, Berger &amp; Aviczer (1996)</td>
<td>1.0%</td>
<td>20.0%</td>
</tr>
<tr>
<td>Lee, Berger &amp; Aviczer (1996)</td>
<td>5.0%</td>
<td>20.0%</td>
</tr>
<tr>
<td>Lee, Mohankrishnan &amp; Paulik (1998)</td>
<td>0.9%</td>
<td>0.7%</td>
</tr>
<tr>
<td>Han, Chang, Hsu &amp; Jeng (1999)</td>
<td>4.0%</td>
<td>7.2%</td>
</tr>
<tr>
<td>Komiya &amp; Matsumoto (1999)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cardot, Revenu, Victorri &amp; Revillet (1993)</td>
<td>2.0%</td>
<td>4.0%</td>
</tr>
<tr>
<td>Cardot, Revenu, Victorri &amp; Revillet (1993)</td>
<td>0.9%</td>
<td>7.4%</td>
</tr>
</tbody>
</table>
and local features described in various accounts [4, 5]. These
global and local features, derived from the basic set of data
that a digitizer provides, vary significantly across algorithms.
44 features. In [2], describes the x and y coordinates of the
pen's motion. Also [9], observes that the temporal
“characteristics of the production of an on-line signature are
the key to the signature’s verification” (p. 5). From these
many approaches and features, the number of variables
associated with a dynamic signature can be synthesized to
several major statistical features. These major statistical
features include pressure, time, horizontal, and vertical
components of position, velocity, acceleration, and force, all
measured against time. An alternative approach to
characterizing a signature involves analysis of the “stroke,”
that is, the up and down movements of the pen on the
digitizer. The many dynamic traits collected by the digitizer
during the act of signing are said to make an impostor
signature easier to detect than that of a traditional
paper-based impostor signature.

IMPOSTOR SIGNATURE GENERATION

Impostor datasets are created in numerous ways and have
the effect of changing the respective performances of
algorithms. This change can be done through the different
generation of the impostor signatures. A review of the
literature shows various performance results from several
studies, all of which have different methodologies for
collecting impostor signature datasets. Table 1 outlines the
various studies and their respective error rates (false accept,
false reject, and the equal error rate where appropriate).
The variances in error rates shown in Table 1 (0% to 50%
false accept rate and 0% to 20% false reject rate) can be
explained by a number of factors, one of which has to do
with how an impostor signature dataset is created. [10]’s
study is particularly interesting. This study had a database
consisting of 293 genuine signatures and 540 forgery
signatures from eight individuals. Although the study did not
explain how the forgeries took place (in terms of training,
payment, etc.), eight individuals created the impostor dataset.
[11] study dataset was comprised of 496 original signatures
from 27 people. Each person signed 11 to 20 times. The
database contained 48 forgeries that “fulfill the requirement
on the visual agreement and the dynamic similarity with the
original signature” (p.5). [12] trained the algorithm using
250 signatures per writer; of these 250 signatures, 100 were
authentic signatures and 150 were random forgeries,
classified as the genuine signatures of other writers. [13] used
27 people in their study, with the participants writing their
own signature. The study also used 4 people who imitated
the signatures of these 27 people. Unfortunately, no further
information is provided on the selection of the impostor or on
what knowledge the forgers possessed in order to forge the
signatures.

[11] used genuine signatures from other individuals as
forgeries. In addition, a group of synthesized signatures was
created by distorting real signatures through the addition of
low-level noise and dilation or erosion of the various
structures of the signature. [14] motivated the forgers by
offering a cash reward. [15] examined people’s signatures
over a four-month period to assess variability over time.
In the Signature Verification Competition, genuine signers
created signatures other than their own [16]. In [17], the
author uses a number of different methodologies to generate
the impostor distribution, with the majority of impostors
using some form of practice. In [18], the authors defined
three different levels of forgeries: the simple, statically
skilled, and timed (p. 643). [19] used signatures that “on
casual visual inspection would pass as authentic” (p. 201).
[20] provides three characteristics of forgery: the random
forgery, defined as one that belongs to a different writer of
the signature model; simple forgery, represented by a similar
shape consistency with the genuine signer’s shape; and the
skilled forgery (p. 2).

PERCEIVED STRENGTH OF SIGNATURE (PSS)

The purpose of this paper is to assess the basic attack on a
signature by an opportunistic forger and to determine the
perceived strength of the signature (PSS). PSS is a concept
that indicates that an opportunistic forger will not forge a
signature that is difficult to forge, as their success at the
point-of-sale may be not as high as the forgery of an easy
signature. This is more the trademark of an opportunistic
forgery than of a more sophisticated attack on the signature,
as outlined in previous research. For this study, an
opportunistic forger is analogous to an opportunistic thief,
that is, one who works on his or her own without any
equipment [21]. This definition is further enhanced by the
absence of occasion to practice forging the signature. The
study outlines a basic truth involving the genuine signature
owner’s perception of the strength of their signature and tries
to understand whether the owner of a genuine signature has
the same or different perception of the signature than that of
the forger.

In order to understand the basic truth of the perceived
strength of the signature, each of the genuine signature
owners was asked for the following information about their
signature:

1. How easy their signature was to forge (rated on
   a Likert scale).
2. How fast or slow they signed their signature
   (rated on a Likert scale from slow to fast).
3. Handedness (right- or left-handed;
   ambidexterity was not an option captured by the
   survey).

The objective in obtaining these three pieces of
information was to assess whether the forger was able to
predict the speed and forgeability of genuine signatures, which was typically centered on the dynamic traits of speed or velocity, time, and graphical outline or complexity of the shape. Furthermore, subjects were asked to sign their name on a digitizer so that feature variables could be extracted to estimate whether there were any correlations between variables and the respective PSS categories.

**Table 2. T-Test for Difficulty Groups**

<table>
<thead>
<tr>
<th>Speed</th>
<th>p-value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.026</td>
</tr>
<tr>
<td>2</td>
<td>0.000</td>
</tr>
<tr>
<td>3</td>
<td>0.107</td>
</tr>
<tr>
<td>4</td>
<td>0.000</td>
</tr>
<tr>
<td>5</td>
<td>0.053</td>
</tr>
</tbody>
</table>

**METHODOLOGY**

In order to assess PSS, two separate groups were organized. The dataset of genuine signatures was collected from consent forms signed by the genuine signature owners. The consent forms were used to maintain a level of ceremony, since the consent form is a document that requires a signature with a level of intent, as opposed to a random signature with no intent. This signature was subsequently used as the target signature. In order to estimate whether any of the dynamic signature verification variables were the same for each group (those who ranked their signature within the same Likert classification), each subject signed his or her name on a digitizer three times. In order to obtain a consistently precise signature, the study utilized an Interlink Electronics ePad-ink Pro™ device, which has 100-400 reports per second and 300 dots per inch [22].

The device was connected to forensic signature software to extract the raw data from the digitizer, but the subjects could not see the signature or the information on the PC monitor as they signed. The digitizer provided an inked display of the signature as the subject signed his or her name. The three signatures were then processed and the resultant variables averaged across the signatures.

The impostor group consisted of individuals other than those who owned the original signatures. Members of the impostor group were asked for information about what they observed while looking at the signed consent form of each individual in the genuine group:

1. How easy the genuine signature was to forge (rated on a Likert scale).
2. How fast or slow was the genuine signature estimated to be made (rated on a Likert scale from slow to fast).
3. What was the handedness of the genuine subject (right- or left-handed; ambidexterity was not an option captured by the survey).

The results were analyzed statistically to determine whether any significant differences existed between the genuine signature owners and the impostors regarding their assessments of the signature.

**RESULTS**

For the genuine dataset, a total of 60 subjects participated, of which 1 was female and 59 were males. Of these 60 subjects, 36 signed the digitizer. The remainder did not sign (or dropped out of the study). This represents a retention rate in the study of 60%. For the impostor dataset, there were 9 individuals who ranked the genuine signatures using the parameters previously described.

A t-test was used to determine whether the mean of the genuine and impostor groups were statistically significant from each other with regards the three questions posed: the rank of the perceived level of difficulty, velocity, and handedness. A level of 0.05 was selected for determining statistical significance. In the study, the data were normally distributed, and there were no outliers. The data were ranked from 1 to 5, with 1 being easy to forge and 5 being difficult to forge.

**Table 3. Signature Speeds**

<table>
<thead>
<tr>
<th>Speed</th>
<th>p-value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.002</td>
</tr>
<tr>
<td>2</td>
<td>0.011</td>
</tr>
<tr>
<td>3</td>
<td>0.060</td>
</tr>
<tr>
<td>No group 4</td>
<td>N/A</td>
</tr>
<tr>
<td>5</td>
<td>0.035</td>
</tr>
</tbody>
</table>

When assessing the PSS, a t-test result shows parallels between genuine subjects and forgers when the level of difficulty was assessed as "neutral." Likewise, the difference in the "very difficult" ranking has a p-value of 0.053. Other categories (levels 1, 2, and 4 in the Likert scale) exhibited significantly different means. It is difficult to determine whether the groups were statistically significant. Further refinement of the question is needed (and will be undertaken...
Table 4. Handedness

<table>
<thead>
<tr>
<th>Handedness</th>
<th>p-value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Left</td>
<td>0.000</td>
</tr>
<tr>
<td>Right</td>
<td>0.000</td>
</tr>
</tbody>
</table>

in a subsequent study) to examine the PSS in more detail. Table 2 outlines the results of the PSS category.

When analyzing speeds (see Table 3, where 1 denotes fast speed and 5 denotes slow speed), both groups had significant differences, except for the neutral standing. Neither group assigned a rank of 4 as a speed.

The results indicate that neither the impostors nor the genuine users could determine the speed of each other’s signatures. This is particularly interesting, as speed (or velocity) is an often used a statistical feature in DSV algorithms.

When analyzing handedness, the impostor group could not consistently determine the handedness of the genuine signature owners. Only 3 out of 8, 37.5%, of the forgers correctly identified a left-handed signature, while 3 of the left-handed signatures were not correctly identified at all. Comparably, 7 of 49 right-handed signatures were correctly identified by all forgers. However, the least accurate results showed that 5 of 8 forgers incorrectly identified a signature as left-handed when it was, in fact, right-handed. These results are represented in Table 4.

The last question posed is whether the dynamic features extracted from the digitizer were similar for each group of the PSS categories. For example: Do those in the easy-to-forge category exhibit the same speed? Is there an underlying dynamic variable within these groups that are selected by impostors as easy to forge?

An Analysis of Variance (ANOVA) test was conducted over all of the individual variables that were extracted from the digitizer. At a = 0.05, none of these variables were significantly different across each difficulty group. For the forger group, the ANOVA showed no significance with these extracted variables and difficulty group. There were some interesting correlations, however; speed was negatively correlated with difficulty (-0.191, with p-value 0.273), as were the number of strokes and difficulty of -0.314. The forger groups had a slightly positive correlation with speed and slightly negative correlation with segments (0.081).

CONCLUSION

The purpose was to assess whether genuine and impostor groups could successfully predict variables that could aid in the successful forgery of the genuine signature. Variables included the perceived strength of the signature, speed, and handedness. The results indicate that genuine signers and impostors did not rank signature within the same strength categories, that the impostors could not determine speed of the genuine signature, and that the impostors could not determine handedness. Furthermore, there were no common characteristics of the signature variables within the groups. Further research should be undertaken to examine whether these attributes change as the forger gains more knowledge about and experience with the signature.

REFERENCES


Establishment of Personalized Templates for Automatic Signature Verification,

[12] W.S. Lee, Mohankrishnan, N. and Paulik, M.,
Improved Segmentation through Dynamic Time Warping For Signature Verification using a Neural Network Classifier,

On-Line Signature Verification using LPC Cepstrum and Neural Networks,
IEEE Transactions on Systems, Man, and Cybernetics,

[14] M. Mingming and Wijesoma, W.,
Automatic On-Line Signature Verification Based on Multiple Models,

[15] P.-C.C. Chin-Chuan Han, Chao-Chih Hsu, and BorShean Jeng,
An on-line signature verification system using multi-template matching approaches,

[16] D-Y. Yeung, H. Chang, Y. Xiong, S. George, R. Kashi, T. Matsumoto and G. Rigolls,
SVC 2004: First International Signature Verification Competition,
presented at First International Conference on Biometric Authentication, ICBA, Hong Kong, China, 2004.

[17] S. Elliott,
A Comparison of On-Line Dynamic Signature Trait Variables vis-A-vis Mobile Computing Devices and Table-Based Digitizers,

[18] L. Lee, Berger, T. and Aviezer, E.,
Reliable On-Line Human Signature Verification Systems,
IEEE Trans. Pattern Analysis Machine,

[19] W. Nelson and Kishon, E.,
Use of Dynamic Features for Signature Verification,
presented at Proceedings IEEE International Conference on Systems, Man, and Cybernetics,

[20] E.J.R. Justino, Bortolozzi, F. and Sabourin, R.,
The Interpersonal and Intrapersonal Variability Influences on Off-Line Signature Verification using HMM,
presented at Proceedings of the XV Brazilian Symposium on Computer Graphics and Image Processing,
SIGGRAPH'02, 2002.

[21] D. Cvccuk, Khojick, J. and V. Matyas,
PIN (& Chip) or signature - beating the cheating?
Bino, Czech Republic, 2005.

[22] I. Electronics, 2006,
E-Pad Signature Pad Specification Sheet.
Along-Track Interferometry for Ground Moving Target Indication

Elaine Chapin & Curtis W. Chen
Jet Propulsion Laboratory
California Institute of Technology

ABSTRACT

Synthetic aperture radar (SAR) along-track interferometry (ATI) has been used extensively to measure ocean surface currents. Given its ability to measure small velocities (~10 cm/s) of relatively radar-dark water surfaces, there is great potential that this technique can be adapted for ground moving target indication (GMTI) applications, particularly as a method for detecting very slow targets with small radar cross-sections. Herein, we describe preliminary results from an ATI GMTI experiment.

The SAR data described were collected by the dual-frequency NASA/JPL airborne radar in its standard dual-baseline ATI mode. The radar system imaged a variety of control targets including a pickup truck, sport utility vehicles, passenger cars, a bicycle, and pedestrians over multiple flight passes. The control targets had horizontal velocities of less than 5 m/s. The cross-sections of the targets were not purposely enhanced, although the targets' reflectivities may have been affected by the existence of the GPS equipment used to record the targets' positions. Single-look and multiple-look interferograms processed to the full azimuth resolution were analyzed. In the data processed to date, all of the targets were observed by visual inspection in at least one of the four combinations of dual-frequency, dual-baseline interferometric data. This extremely promising result demonstrates the potential of ATI for GMTI applications.

INTRODUCTION

Along-track interferometry (ATI) is an interferometric synthetic aperture radar (SAR) technique for mapping the line-of-sight velocities of surface targets [1]. Because velocity-measurement accuracies of a few centimeters per second have been achieved in oceanographic contexts with this technique, ATI holds great promise for ground moving target indication (GMTI). The processing algorithms and performance models used for oceanographic applications do not necessarily apply to the case of detecting moving targets amidst clutter, however. In the oceanographic case, the entire ocean surface acts as a single large target moving at a nearly uniform velocity, whereas in the GMTI case, the objective is the detection of dim, discrete targets against a stationary background.

Unlike the widely-used cross-track interferometric SAR techniques that are able to map surface topography by utilizing data acquired from phase centers separated in the elevation or across-track direction on a moving platform, ATI techniques involve the acquisition of data from phase centers that are separated in the direction of the SAR flight path. SAR images formed from these two phase centers are therefore characterized by a temporal baseline equal to the time required for the platform(s) to travel the distance of the along-track offset (i.e., the physical baseline) between the two phase centers. Thus, while stationary elements of the imaged scene contribute identically to the two images, moving targets in the scene exhibit phase shifts between the two images. An interferogram formed from the two complex SAR images consequently depicts surface movements in the imaged scene, and the system can be made very sensitive to small velocities with the use of a long interferometric baseline.

In addition to their sensitivity to low target velocities, ATI systems can also be made very sensitive to targets with low radar reflectivities. This is because the SAR ATI technique makes use of long coherent integration times that reduce the amount of clutter competing with any given target. An unresolved target of interest competes only with the clutter in a single image pixel, so with appropriate SAR resolution,
high signal-to-clutter ratios can be achieved. ATI thus offers the capability of detecting targets too dim to detect by other means. Such long coherent integration times are often not possible with space-time adaptive processing (STAP) techniques in which the coherent processing intervals are limited by sample-support restrictions.

Moreover, ATI techniques are less sensitive to channel mismatch than other GMTI techniques. ATI techniques do not cancel clutter through the complex subtraction of two signals as STAP and displaced phase center antenna (DPCA) techniques do. ATI techniques rely on a conjugate-product operation and involve only two channels, so algorithms for correcting channel bias, topographic effects, etc., are simpler, more efficient computationally, and less demanding of sample support.

While previous ATI experiments relying on oceanographic models have reported anecdotal observations of targets of opportunity or detections of radar-bright targets whose reflectivities were artificially enhanced by retroreflectors [2], little experimental work has addressed the problem of detecting slow, dim, discrete ground targets. To evaluate the suitability of the ATI technique for detecting such objects, we performed a proof-of-concept demonstration utilizing airborne SAR data. Herein, we will describe the experimental setup for the demonstration and the encouraging preliminary analysis and results.

![Fig. 1. Photograph of the NASA DC-8 showing the positions of the AIRSAR antennas used for ATI](image)

**EXPERIMENTAL SETUP**

The radar data discussed were acquired opportunistically as “piggy-back” collections during four routine calibration flights of the NASA/JPL AIRSAR system [3,4] on 26 February 2004, 15 April 2004, 17 September 2004, and 6 December 2004. A total of thirteen passes of data were acquired. During each pass, 40 MHz range-bandwidth stripmap SAR data were collected simultaneously at both C-band and L-band from multiple phase centers separated along the fuselage of the NASA DC-8 platform. Figure 1 shows a photograph of the plane and the locations of the C-band and L-band antennas used for along-track interferometry. The fully processed SAR image data have a range resolution of 3.75 m and an azimuth resolution of 85 cm. The C-band and L-band along-track physical baselines are 1.9 m and 19.8 m, respectively. Typical platform velocities are 200 to 215 m/s, and typical pulse repetition frequencies are 1 kHz. The plane normally flies 8 km above the imaged surface. For twelve of the thirteen passes, the pulse transmissions from the fore antenna were interleaved with the pulse transmission from the aft antenna on a pulse-by-pulse basis while the pulse echoes were received by both antennas for every pulse. This is done simultaneously for both frequencies. The resulting data allow for full-baseline and half-baseline (as well as zero-baseline) interferometric combinations of the phase centers to be synthesized for both frequency bands.

The collections imaged control targets and targets of opportunity moving amidst a relatively radar-dark scene. The experiment was performed in the Mojave Desert south of the NASA/JPL AIRSAR calibration test site at Rosamond Dry Lake and north of Lancaster, California—a rural area with very little vegetation. Ten of the thirteen passes view the background scene from the west with very similar imaging geometries. The remaining passes view the same scene from the east with very similar imaging geometries. The passes were repeated and oriented this way to facilitate signal-to-clutter and signal-to-noise calculations for the control targets which will be done as follow-on work.

A variety of control targets including ordinary passenger cars, sport utility vehicles, a pickup truck, a bicycle, and pedestrians were deployed as control targets. During each pass of radar data, between one and five control targets were imaged. Each control target was equipped with a precision global positioning system (GPS) unit and operated slower than 5 m/s. Figure 2 shows one of the control targets and the character of the scene’s terrain and vegetation. Although the cross-sections of the control targets were not deliberately enhanced, the GPS equipment used to record the control targets’ positions may have increased the targets’ backscatter. All of the control targets operated on paved rural roads. The grid of roads at the test site is approximately aligned.
along-track and across-track, and some control targets were imaged traveling in both directions.

**DATA ANALYSIS**

We have performed a preliminary analysis of four of the passes of radar data, and the initial analysis is very encouraging. The passes' data were processed using JurassicProk, JPL's advanced interferometric SAR processor for airborne data [5]. We have examined the SAR imagery and both single-look and multiple-look interferograms for both the full and the half interferometric baselines at both frequencies. We have processed data to the full available azimuth resolution at the Doppler centroid of the stationary background, although future work may involve evaluating the impact of different azimuth integration times on target detectability. For the slow velocities of the control targets, however, the Doppler spectra of the targets are expected to match the Doppler spectrum of the stationary background fairly well.

Before attempting to develop a target detection algorithm, we have attempted to answer the more basic question of whether a human observer is able to detect the signatures of the moving targets upon visual inspection of the interferometric data. Consequently, our data analysis thus far has consisted primarily of visual inspection of the single-look and multiple-look interferograms. We have used the GPS data of the control targets' positions and velocities at the imaging times to compute the expected positions of the targets in the interferograms, accounting for the apparent shift of the moving targets in the SAR imagery [6].

The motor vehicle targets moving predominantly perpendicular to the flight direction were easily visible in both the C-band and the L-band interferograms. These targets had radial velocities of 2 to 3 m/s, corresponding to multiple cycles of the interferometric phase for the longer along-track baselines. The targets appear at the expected positions in the slant plane data products displaced in azimuth from their nominal GPS positions in proportion to their radial velocities.

Figure 3 shows a sample four-look interferogram containing the control target shown in Figure 2 while it was moving roughly perpendicular to the flight direction. The brightness of the image represents magnitude, which is approximately proportional to the amount of signal energy backscattered to the radar. Agricultural fields and roads are visible in the magnitude imagery. The color superimposed on the brightness image represents the interferometric phase. The blue-green color indicates a constant background phase value for the stationary background scatterers in the scene. Objects with suitable line-of-sight velocities appear as different colored dots. The dots should appear shifted in the along-track direction (vertically in the images) relative to the stationary background. The expected shift can be calculated if the range to the target, the velocity of the radar, and the velocity of the target are known [6]. In Figure 3, the purple dot displaced in azimuth above the road near the center of the image in range is the control target.

**Fig. 3. Sample four-look C-Band full-baseline along-track interferogram showing a control target. Increasing range is to the left of the image. The aircraft's flight direction is down the page. The area represented covers 1630 m in range and 1060 m in azimuth.**

**Fig. 4. Single-look interferogram chips centered on the predicted positions of the control target. The upper two images correspond to the C-Band data while the lower two images correspond to the L-Band data. The left two images correspond to the data with half the effective baseline of the two images on the right. Each chip displays 216.5 m in range and 40.625 m in azimuth. For each chip, range increases across the page while platform flight direction is down the page.**
Fig. 5. Full-baseline L-Band interferogram centered at position of a target moving predominantly in azimuth. The area imaged covers 1524 m in range and 1025 m in azimuth. The pickup truck shown in Figures 2, 3, and 4 appears as the orange dot in the upper right corner of the image.

Figure 4 shows C-band and L-band single-look interferograms for both of the non-zero interferometric baselines that can be synthesized because the antenna used for transmit was alternated. Each interferogram is centered at the expected location of the control target shown in Figures 2 and 3. As with Figure 3, the brightness indicates the magnitude, and the color indicates the interferometric phase. The phase offset of the target is different in each of the four cases because of differences in the effective interferometric baseline. The target appears more smeared in the L-band interferograms than in the C-band interferograms. This is likely due to deviations of the target motion from linear, which cause misfocusing of the target in azimuth, and the longer L-band integration period. The coherent integration times for the C-band and L-band data are approximately 2 s and 8 s.

The cars and trucks moving predominantly parallel to the flight direction have much lower radial velocities (e.g., 10 cm/s). They were detectable only in the longest baseline L-band interferogram, the interferometric pair with the highest sensitivity to velocity. These targets appear at the expected positions in the slant plane imagery although they are visibly smeared. Such smearing is expected because the along-track component of the target motion gives rise to a mismatch between the target phase history and the reference phase history used for azimuth compression.

Figures 5 and 6 show an example of a control target, in this case a Subaru Legacy station wagon, moving approximately parallel to the flight direction. For this case, the radial velocity of the target was 11 cm/s although the horizontal velocity of the target was 2 m/s. The target is visible as the purple dot near the center of the four-look interferogram in Figure 5. Figure 6 shows portions of the single-look interferograms for all four interferometric pairs. The target is not detectable in the C-Band interferograms where the ambiguous velocities are 5.9 m/s and 3.0 m/s, respectively, for the half-baseline and full-baseline interferometric pairs. Because the ambiguous velocities for the L-band cases are 2.4 m/s and 1.2 m/s, the target’s phase is more significantly offset from the stationary background making the target visible in the full-baseline L-band data. Comparing Figures 4 and 6, it is clear that the target moving predominantly parallel to the flight track is more smeared than the target moving predominantly perpendicular to the flight track as expected.

Fig. 6. Example of interferograms of a control target moving predominantly in azimuth. The figure is in the same format as Figure 4.

In order to examine the limits to which the ATI technique can afford the detection of slow, dim targets, we also deployed a bicycle and pedestrians as control targets. Figure 7 shows a photograph of a bicycle control target operating during the 15 April 2004 experiment. The target’s GPS equipment is mounted on and in the child carrier.
7 shows a photograph of the bicycle control target. The bicycle was towing a trailer which carried the GPS equipment. Note that parts of the bicycle that were not moving in a nearly linear fashion (e.g., the wheels and pedals) would not be expected to focus well in the SAR data, so the target signature of Figure 7 is likely due to scattering from the aluminum frames of the bicycle and the trailer, from the GPS equipment, and perhaps from the rider’s body. The bicycle had a horizontal velocity of approximately 3 m/s and a radial velocity of 1.5 m/s at the imaging time corresponding to the single-look interferograms shown in Figure 8. Because of the target’s low reflectivity and the relatively coarse range resolution of the radar data, the bicycle does not have a signal-to-clutter ratio sufficient for it to be visible in the multiple-look interferograms. The bicycle target is visible in the single-look interferograms at both C-band and L-band. (Note that spatial averaging does not enhance the detectability of the target because the target occupies only one resolution cell.) The bicycle target is most clearly visible in the C-band full-baseline interferogram because the bicycle’s radial velocity corresponds to an approximately 180° phase offset from the stationary background for this baseline. For this baseline, the bicycle appears as a red dot at the center of the image.

![Bicycle Control Target](image1)

**Fig. 8. Interferogram chips showing the bicycle. The figure format is the same as Figure 4.**

To test the detectability of even slower targets, we also used pedestrians as control targets. Figure 9 shows a photograph of a pedestrian pushing a cart instrumented with high precision GPS equipment. The horizontal velocity of the pedestrian was 1 m/s. The cart consists of a steel frame with upper and lower decks made of wood. The cart may have a strong radar reflection, especially at the L-band wavelength.

![Pedestrian Control Target](image2)

**Fig. 9. Photograph of a pedestrian control target during the 6 December 2004 data collection. The GPS equipment is on the electronics cart because of double-bounce phenomena of the VV-polarized signal associated with the vertical members of the cart frame and the flat horizontal surface of the paved road.**

![Interferograms](image3)

**Fig. 10. L-Band interferograms imaging the pedestrian pushing the electronics cart. The image on the left corresponds to the interferometric pair with the shorter baseline while the image on the right corresponds to the longer baseline. Each interferogram displays 216.5 m in range and 40.625 m in azimuth. For each chip, range increases across the page while platform flight direction is down the page.**

Preliminary results for the pedestrian targets are very encouraging. Figure 10 shows the L-band interferograms imaging the pedestrian pushing the electronics cart. Given the low radial velocities, we only expect to see the pedestrian targets in the L-band interferograms since they have smaller ambiguous velocities. Comparing Figures 7 and 9, the pedestrian target is more smeared in azimuth than the bicycle. The smearing may be caused by nonlinear movements of the target or by a greater degree of internal motion for the human pushing the cart compared with the bicycle. As expected given its small radial velocity, the target is more easily detected in the full-baseline interferogram.

**CONCLUSIONS AND FUTURE WORK**

ATI has potential as a technique to detect ground moving targets with velocities that are too low and cross-sections that...
are too small for other methods. We have conducted an airborne flight test to evaluate this potential. Preliminary analysis of the test data is promising. For this analysis, we formed full resolution interferograms for both available interferometric baselines at both the C-band and L-band frequencies. All of our control targets (cars, sport utility vehicles, a pickup truck, a bicycle, and pedestrians) are detectable upon visual inspection of the interferograms. This result is very encouraging, implying that automated detection may be possible.

The work done thus far is preliminary and does not fully exploit the rich data set or the full capabilities of ATI processing. Only four of the data takes have been evaluated. The processing done on the data thus far has produced the standard oceanographic products. Future algorithmic work includes optimizing the processing to enhance the detection probability and developing detection algorithms. Target and clutter phenomenology will be addressed after the full set of flight lines have been processed and both the control targets and the faster moving targets of opportunity have been evaluated. The processed data will also be used to refine and verify performance models.

Our experiment has revealed the suitability of ATI GMTI for slow, dark targets. This rich data set has given us a peek at what possible future ATI systems, more suitably designed for detecting ground moving targets, may be capable of.

ACKNOWLEDGEMENTS

This work was performed at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration. The authors thank Michael Fitzsimmons, Scott Hensley, Michael Jourdan, Charles Le, Thierry Michel, Charles Morris, Ron Muellerschoen, Paul Rosen, Scott Shaffer, and the JPL AIRSAR group for their help in conducting the airborne experiment and processing the data.

REFERENCES


ISRO’s Programmable Digital Waveform Generator

Shalini Gangele, Nilesh M. Desai, R. Senthil Kumar, J.G. Vachhani & V.R. Gujraty,
Indian Space Research Organisation (ISRO)

ABSTRACT

One of the major and common requirements for all active microwave sensors is generation of the transmit modulation signal-like chirp/LFM signal, MSK, etc., which can be generated by analog or digital means. With the increasing demands of side bandwidth, longer duration chirp signals in radar systems, digital signal generation, and processing has emerged as a preferred alternative. Design and development of programmable and generic Digital Waveform Generator (DWG) system based on Xilinx Virtex XCV600 FPGA and high-speed DAC is carried out at the Space Applications Center. ISRO is to generate required transmit chirp signal of high time-bandwidth product (~1000) for ISO’s microwave radar sensor missions. This gives a detailed description of the design requirements, implementation details, salient performance features, and test results of this programmable and generic Digital Waveform Generator (DWG).

INTRODUCTION

Space Applications Centre, SAC, ISRO, Ahmedabad is involved in the design and development of Microwave Radar Sensors like Synthetic Aperture Radar, Scatterometer, Altimeter, and Radiometer for various civilian satellite and aircraft missions for all-weather imaging of land, and ocean resources. One of the major and common requirements for all active microwave sensors is the generation of the transmit modulation signal-like chirp or linear frequency modulated signal, Minimum Shift Keying (MSK), etc. Moreover, pulse compression techniques [1] used in pulsed radars to achieve better range resolution and Signal-to-Noise performance, necessitates generation and compression of signals by either analog or digital techniques. Surface Acoustic Wave (SAW) devices were generally employed for both signal generation (pulse expansion) and matched filtering (pulse compression) in traditional pulsed radar systems. However, design and fabrication of SAW devices for large time-bandwidth product chirp signals is very complex and expensive, while the digital approach offers the advantages of programmability, flexibility, signal pre-distortion to compensate for analog errors, better stability, accuracy, and repeatability.

ISRO’s first Airborne Synthetic Aperture Radar (ASAR) employed indigenously-built 25 MHz Surface Acoustic Wave (SAW) devices. ISRO’s subsequent airborne and spaceborne active radar sensors are being built with a standardized Digital Waveform Generator (DWG) module. The initial prototyping of DWG hardware was carried out using high-speed logic, PROM devices, and Actel 54SX32SU Field Programmable Gate Array (FPGA) before arriving at Xilinx Virtex XCV600 FPGA-based generic configuration implementing chirp generation algorithms. This DWG hardware has already been realized and tested with 250 MHz RF clock and DAC strobe rates upto 62.5 MHz. All the clock and timing signals within DWG are derived and synchronized to an external RF clock input.

This DWG is controlled and configured by the radar system controller and interfaces with the RF segment, where the baseband chirp signal is subsequently vector-modulated, multiplied by appropriate factor, and upconverted by RF hardware to meet the transmit chirp bandwidth requirements of 15 MHz to 320 MHz for ISRO’s Radar Imaging Satellite-1 (RISAT-1) SAR, Airborne SAR for Disaster management (DMSAR), Oceansat-2 Scatterometer, and proposed Altimeter sensor at the required transmit frequencies in C- or Ku-band.

DIGITAL WAVEFORM GENERATION ALGORITHMS

The algorithms for digital waveform generation can be either Look-Up table (LUT)-based or Coordinate Rotation
Digital Computer (CORDIC)-based. The LUT-based algorithms include Direct LUT storage technique and Direct Digital Chirp Synthesis (DDCS) techniques. In Direct LUT storage technique, samples of waveforms are stored directly in LUT. While in the case of DDCS technique, periodicity of sine wave is used to reduce the size of memory storage. While the former is suitable for short duration waveforms, the DDCS technique provides more flexibility in programming the parameters of the waveform and also enables the generation of the chirp signal at a suitable intermediate frequency for up-conversion. The advantages offered by LUT-based techniques are better chirp characteristics like flatness, spectral purity, etc. However, both Direct LUT storage and DDCS technique suffer from the disadvantage of large memory requirements. Moreover, the use of memory in on-board hardware increases the probability of single event upsets. CORDIC-based digital chirp generation algorithms overcome these problems as it does not require memory storage. The CORDIC approach, however suffers from disadvantages like slower speed, complex control and timing logic, poorer spectral response, increased logic resource requirements, and complex verification/test benches, etc.

Thus, depending on application requirements like pulse duration, precision, bandwidth, memory storage, systemic error corrections, sin(x)/x pre-distortion, etc., one of these numeric, synthesis, or digital waveform generation algorithms can be easily implemented in FPGA. The design details of these algorithms are discussed in the following sections.

**Fig. 1. Direct LUT Storage Algorithm for Digital Waveform Generation**

**Direct LUT Storage**

In direct LUT storage of the DWG waveforms, the digitally-synthesized chirp signal, which is stored in the Look-Up Table (LUT), is read out at a constant rate. Figure 1 presents internal architecture details for DWG FPGA Logic based on direct LUT storage algorithms. The DWG waveforms (both I & Q Channels) are stored in the internal Block RAMs of FPGA, with N-bit amplitude resolution. The synchronizer and address generator logic module synchronizes the transmit pulse and generates address signals for LUTs. The chirp I/Q data for required pulse width duration are then read every clock cycle from internal RAMs and fed to the external D/A converters.

**Direct Digital Chirp Synthesis (DDCS) Algorithm**

Direct Digital Chirp Synthesis (DDCS) is a method of digitally synthesizing chirp waveforms [2, 3]. Figure 2 presents the internal DWG architecture details for FPGA implementation of DDCS approach. As shown, it consists of control and synchronizer sections, a programmable DDCS, and output latches. A programmable DDCS module is utilized to generate the required chirp signal.

**Fig. 2. DDCS Algorithm for Digital Waveform Generation**

As shown in Figure 3, the DDCS module consists of control logic, register-latches for latching programmable waveform parameters, two cascaded N-bit accumulators, and an output sine/cosine look-up table of programmable size. The first accumulator is the frequency accumulator, which produces a frequency ramp using the start frequency and delta frequency values; the second is the phase accumulator, which integrates the current frequency accumulator output.

**Fig. 3. Block diagram of Direct Digital Chirp Synthesizer Module**

DDCS maintains a running record of frequency in its frequency accumulator register. The frequency accumulator is initially loaded with the start frequency value. At each clock cycle, the delta frequency is added to the frequency accumulator. The value in the frequency accumulator thus represents the current frequency of the synthesized sine function. Similarly, a running record of phase is maintained in the phase accumulator register, which is initially loaded
with a start phase value. At each clock cycle, the frequency accumulator value is added to the value in the phase accumulator. The value in the phase accumulator thus represents the current phase of synthesized sine function. The phase output from phase accumulator is shifted by phase shifter block to enable symmetric and centered chirp generation for \(-T/2 \leq t < T/2\). The phase value is then fed to the quantizer, which is simply a slicer. Due to excessive memory requirements, the full precision of the phase accumulator cannot be used to index the sine/cosine look-up table. A quantized version of phase is used for this purpose. The quantized phase value is presented to the address port of the internal Sine/Cosine LUT to read-out amplitude data for I/Q channels, which are subsequently latched. The LUT stores uniformly-spaced samples of a sine wave, which performs the mapping from phase-space to time.

![Diagram showing the CORDIC-based approach for digital waveform generation.](image)

**Fig. 4. CORDIC-based Approach for Digital Waveform Generation**

The fidelity of a signal formed by recalling samples of a sinusoid from a look-up table is affected by both the phase and amplitude quantization of the process. The length and width of the look-up table affect signal’s phase angle resolution and the signal’s amplitude resolution, respectively. These resolution limits are equivalent to time base fitter and to amplitude quantization of a signal, and add spectral modulation lines and a white broad-band noise floor to the signal’s spectrum. Look-up tables can be allocated to distributed or block memory. Quarter wave symmetry is used in Look-Up tables to construct DDCS with shortened tables so as to use either fewer block RAMs or reduced distributed memory. The control logic generates the control signals required to support reset and loading of the waveform parameters.

The various programmable inputs like start frequency and phase, delta frequency, etc., are initialized in DDCS, which produces the chirp signal for desired duration controlled by the transmit pulse width input signal. The most significant 13-bit or 15-bit output of the DDCS phase accumulator is used to address the internal Sine/Cosine LUT every clock cycle to read-out N-bit amplitude data for I/Q-channels, which are latched and subsequently fed to external DACs.

CORDIC-based LFM waveform synthesis algorithm: CORDIC-based DWG consists of control logic, a synchronizer, a programmable CORDIC-based block, and the output latches. The internal architecture of the CORDIC-based chirp generator module is similar to that of the DDCS module, except that the sine/cosine Look-Up table PROM in the DDCS module is replaced by the CORDIC block. Thus, phase value output from phase accumulator register is fed to the CORDIC block for computation of sine and cosine values of the input phase angle.

CORDIC is an iterative arithmetic algorithm for the computation of elementary functions, particularly where large amounts of rotation operations are necessary [4]. It is a simple but efficient approach to implement trigonometric functions using only additions/subtractions and shift operations. The algorithm is based on the principle that all trigonometric functions can be computed or derived from functions using vector rotations. Here, all the rotation angles are restricted so that any arbitrary rotation angle can be expressed in the form of \( \tan(2\Phi) \) by performing a series of successively smaller elementary rotations. This enables the coordinate rotation to be implemented with simple shifts and adds, as multiplication with any power of radix can be accomplished by a shift operation, eliminating the need for multipliers in the computation.

Most common architectures available for CORDIC implementation are iterative, serial iterative, and parallel pipelined structures. In iterative structures, the basic CORDIC processor block is reused to evaluate all of the iterations. But because of its iterative nature, the processor has to perform iterations at N times the data rate, this means that the effective data rate at which the sample can be generated is quite low. Hence, parallel pipelined architecture is considered for FPGA implementation.

In parallel pipelined architectures, iterative structures are unfolded as shown in Figure 5. In this architecture, the basic CORDIC block is replicated and connected in cascade. Each block performs computation in parallel and is separated by registers to form the pipelined structure. Since a latch is used after each CORDIC processor block, the effective data rate is only restricted by the propagation delay of a single CORDIC processor.

**HARDWARE CONFIGURATION**

The initial prototyping of DWG hardware was carried out using discrete high-speed TTL and PROM devices. However, the discrete logic implementation has its own associated problems related to high-speed operation. Moreover, it necessitated two such PCB modules, thereby increasing the
also required at current output DAC for both I/Q channels of DWG. If required, the chirp samples can be pre-distorted or pre-compensated to take care of sine / cosine compensation and other systematic errors, as this will allow a simpler filter with linear or no compensation. Since chirps of different

Fig. 6. Block Diagram of Xilinx Virtex XC600 FPGA-based DWG

overall package size. Thus, this approach was not considered further. Subsequently, ASIC-based implementation was also considered and finally discarded in view of the longer developmental cycle, longer delivery schedules, and exorbitant costs. Space qualified FPGA-based programmable and generic Digital Waveform Generator was finalized for hardware implementation. Two different approaches, viz. a viz.; one approach based on Xilinx XCV600 Virtex FPGA and another based on an Actel 54SX32S FPGA were identified for FPGA-based DWG implementation. The XCV600 FPGA-based option offers the advantages like reconfigurability, on-chip memory, etc. Figure 6 presents the block schematic of DWG hardware, based on Xilinx XCV600 Virtex FPGA. Figure 7 shows the photograph of the flight model package of Digital Waveform Generator.

The FPGA-based DWG system consists of a FPGA device from Xilinx (Virtex XCV600), two high-speed D-to-A converters, AD9731 operating up to 100 MHz to synthesize and generate the requisite baseband I/Q complex or real chirp signals of high time bandwidth product (~1000) and associated serial configuration PROM for storing the FPGA configuration data. All of the necessary clock and timing signals within DWG are derived and synchronized to an external IF / RF clock input. The external input clock signal is an ac-coupled to divide-by-8 pre-sealer device, Peregrine PE9313 in DWG unit. The pre-scaler output is fed to FPGA for chirp generation. Digitally-generated chirp from the FPGA is then fed to a 10-bit high-speed DAC. Both I and Q components of the required chirp are generated in the same module. Appropriate current-to-voltage converter Operational Amplifiers, AD8001 and post-DAC filters are

Fig. 7. Photograph of Digital Waveform Generator Flight Model PCB and Package

Fig. 8. Simulated time domain chirp signal for chirp bandwidth of 25 MHz, Pulse width of 20 μsec and 62.5 MHz sampling frequency

Fig. 9. Spectrum for simulated chirp signal for chirp bandwidth of 25 MHz, Pulse width of 20 μsec and 62.5 MHz sampling frequency
Table 1. Test results of Flight Model DWG Hardware

<table>
<thead>
<tr>
<th>DWG Parameters</th>
<th>Measured Results for Scatt. DWG</th>
<th>Measured Results for RISAT-1 DWG for various SAR modes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>HRS</td>
</tr>
<tr>
<td>Simulated chirp 3-dB bandwidth (MHz)</td>
<td>399.86</td>
<td>24.2</td>
</tr>
<tr>
<td>Measured chirp 3-dB bandwidth (MHz)</td>
<td>399.86</td>
<td>24</td>
</tr>
<tr>
<td>Simulated chirp FM rate/slope (KHz/μsec)</td>
<td>296.198</td>
<td>1.25</td>
</tr>
<tr>
<td>Measured chirp FM rate/slope (KHz/μsec)</td>
<td>296.198</td>
<td>1.25</td>
</tr>
<tr>
<td>Amplitude imbalance (dB)</td>
<td>0.04325</td>
<td>-0.06</td>
</tr>
<tr>
<td>Phase imbalance (deg)</td>
<td>1.06185</td>
<td>0.558</td>
</tr>
<tr>
<td>ARMSE (mvols)</td>
<td>17.9896</td>
<td>65.98</td>
</tr>
<tr>
<td>PRMSE (deg)</td>
<td>0.14204</td>
<td>0.012</td>
</tr>
<tr>
<td>ISLR (dB)</td>
<td>-45.4009</td>
<td>-36.5</td>
</tr>
<tr>
<td>PSLR (dB)</td>
<td>-48.7461</td>
<td>-47.4</td>
</tr>
</tbody>
</table>

bandwidths are generated, a loose reconstruction filter is utilized for different chirp waveforms.

PERFORMANCE EVALUATION AND TEST RESULTS

The design algorithms have been simulated using Modelsim software. Figures 8 and 9 present simulation results in time domain and frequency domain, respectively. Hardware tests have been carried out for Digital Waveform Generator flight model boards with maximum RF input frequency of 250 MHz and most of the digital logic operating at a maximum clock speed of 62.5 MHz.

A detailed characterization of captured chirp is also carried out using MATLAB software. Table 1 lists the test results obtained for flight model unit of DWG, for Scatterometer payload requiring chirp bandwidth of 400 KHz at IF 15.625 MHz for 1.35 cosec duration and RISAT-I payload for all four SAR operation modes with bandwidth requirements of 18 MHz to 225 MHz for fixed 20 μsec duration. For RISAT-I SAR payload, only partial bandwidth chirp at baseband is generated, which will be subsequently multiplied by analog multiplication factor 9 to generate signal at desired transmit carrier frequency.

CONCLUSION

Considering the increasing demand of wide bandwidth, longer duration chirp signals in imaging and non-imaging radar systems, the design and development of a
programmable and generic Digital Waveform Generator is taken up. The flight model hardware of this Digital Waveform Generator for Scatterometer and RISAT-1 sensor missions is completed and tested. This DWG meets the application requirements of 8-10 bits amplitude resolution, 12-13 bits phase / frequency resolution, 0.5 dB I/Q imbalance and 6° rms phase imbalance for the above ISRO radar missions. Various radiation protection and SEU mitigation features are also being implemented in DWG in order to meet the stringent requirements of ISRO's space programmes. The space-qualified DWG unit weighs around 2 Kgs and consumes 7 Watts of satellite raw bus power. The DWG design configuration is also being upgraded using Xilinx Virtex-II FPGA and 4:1 MUXDAC to meet futuristic ultra-large bandwidth (100 - 800 MHz) and long duration (10-2000 μsec.) chirp requirements for ISRO's future radar sensors.

ACKNOWLEDGEMENT

The authors thank Dr. R.R. Navalgund (Director, SAC) and Shri S.S. Rana (Deputy Director, MRSA) for their guidance and encouragement to microwave sensors-related developmental activities. The authors also acknowledge the contributions of their colleagues in MSDPD/MSDG, Scientists / Engineers, and other staff members of SAC / ISRO and other ISRO centres involved in the activities related to Oceansat-2 Scatterometer.

REFERENCES

[1] S.A. Hovanessian, 
Introduction to Synthetic Array and Imaging Radars, 
Artech House, 1980.

[2] 0-400 MHz GaAs High-speed direct digital chirp synthesizer 
hybrid stel-2375; 
Stanford telecom.

[3] Bar-Giora Goldberg, 
Digital Frequency Synthesis Demystified, 
Technology publishing, 1999.

[4] Andraiek, R., 
A survey of CORDIC Algorithms for FPGA Based Computers, 
Monitoring Ball Grid Array
Solder Joints 24 × 7

James P. Hofmeister, Justin B. Judkins, Douglas Goodman
Ridgetop Group, Inc.
Terry A. Tracy
Raytheon Missile Systems
&
Norman N. Roth
DaimlerChrysler AG

ABSTRACT

As FPGA density and overall usage increases, there is a corresponding and growing need to monitor these solder joint networks. Prior to the introduction of a first sensor, SJ BIST™ (SJ Built-in-Self-Test™), there were no known methods for detecting faults in the solder joint networks of fully-programmed, operational Field Programmable Gate Arrays (FPGAs). Because SJ BIST™ requires over 100 mW at 3.3 V to test 8 FPGA pins, we introduce SJ Monitor™, a lower-power design (less than 5.0 mW) to provide 24×7 health monitoring of selected I/O pins; the complementary form SJ Monitor™, can be used to monitor the pins of unpowered FPGAs. SJ Monitor is able to detect all solder joint network faults that last at least as long as 15 msec and which are at least as low as 100 Ω with no false alarms. This capability allows for detection of faults before they begin to exhibit intermittent failures, which, in turn, facilitates condition-based maintenance to reduce failures during critical missions.

INTRODUCTION

FPGAs are widely used as controllers in aerospace applications, and modern FPGAs, such as a XILINX® FG1156, have over one thousand pins, each of which is part of a solder joint network and each of which is prone to damage and intermittent faults. As FPGA package density increases and as the use of FPGAs increases, there is a corresponding increase in the need to monitor those solder joint networks. Being able to detect solder joint faults increases both fault coverage and health management capabilities and provides support for comprehensive condition-based and reliability-centered maintenance. Prior to the introduction of the first sensor, SJ BIST™ (SJ Built-in-Self-Test™), there were no known methods available for detecting faults in the solder joint networks belonging to fully-programmed, operational Field Programmable Gate Arrays (FPGAs) especially FPGAs in Ball Grid Array (BGA) packages such as a XILINX® FG1156 [1-6].

Herein, we introduce a low-power sensor design, SJ Monitor™, which uses innovative circuit design on an Integrated Circuit (IC) chip in-situ on an FPGA’s board to provide a method to monitor 8 I/O pins 24 × 7 for solder joint faults and which uses less than 5.0 mW. SJ Monitor is able to detect all solder joint faults of at least 100 Ω (sensitivity) that last at least as long as 15 ns (resolution) with no false alarms. The complementary form of SJ Monitor™ can be used to monitor the pins of powered-off FPGAs.

Mechanics of Failure

Solder joint fatigue damage caused by thermo-mechanical and shock stresses is cumulative and manifests as voids and cracks, which propagate in number and size. Eventually, the solder ball (or bump) of the joint fractures [7-10] and FPGA operational failures occur.
Fig. 1. Cracked Solder Ball (Bump), 15mm BGA [8]

Fig. 2. Crack at BLM – Solder Ball Junction

An illustration of a damaged solder bump on the verge of fracturing is shown in Figure 1. Figure 2 and Figure 3 depict a cracked solder ball of a BGA package attached to an electronic printed circuit board (PCB); Figure 4 depicts a fractured solder ball, which is what happens to a crack as an end result of accumulated fatigue damage. A fracture is the complete separation of a solder ball that can result in a break in the electrical connection between the BGA and the electronic board.

Over time, contamination and/or oxidation films form on the fractured surfaces and a failure progression occurs: from degraded joints to intermittent opens of short duration (nanoseconds or less) to longer durations (microseconds) to very long durations (milliseconds or longer). The latter case, with intermittent faults lasting milliseconds or longer, are very likely to cause faults in the correct FPGA operation.

Test results confirm this physics of failure behavior. As seen in Figure 5, during periods of high stress, fractured bumps tend to momentarily open and cause hard-to-detect intermittent faults of high resistance of 100s of Ohms [10-12]. Such faults typically last for periods of hundreds of nanoseconds, or less, to more than 1 μs [7, 11, 13-16]. The intermittent faults are caused by the opening and closing of the fractured faces of the solder balls (see Figure 6).

These intermittent faults increase in frequency as evidenced by a practice of logging BGA package failures only after multiple events occur of high-resistance. An initial event followed by some number (for example, 2 to 10) of additional events within a specified period of time, such as ten percent of the number of cycles of the initial event [14-16]. Even then, an intermittent fault in a solder joint network might not result in an operational fault. For example, the fault might be in a redundant ground or power connection; or it might occur during a period when the network is not being written. It might be too short in duration to cause a signal error. In Figure 5, the duration of the fault in the 5th cycle of stress is over 3 milliseconds.

Damage accumulates and eventually there is a catastrophic failure of the FPGA, such as might happen when a solder ball becomes displaced as depicted in Figure 7. Figure 8 represents Highly Accelerated Life Test (HALT) results performed on XILINX FG1156 Daisy Chain packages in which 30 out of 32 tested packages failed in a test period.
Fig. 7. Displaced (Missing) Solder Ball

30 OF 32 FAILED - 3108 CYCLES, MTTF = 2386 CYCLES

Fig. 8. XILINX FPGA HALT Test Results [15]

consisting of 3108 HALT cycles. Each temperature cycle of the HALT was a thermal transition from \(-55^\circ\text{C}\) to \(+125^\circ\text{C}\) in 30 minutes; 3-minute ramps and 12-minute dwells. What is not immediately apparent is that each of the logged FPGA failures (diamond symbols) represents at least 30 events of high resistance, a FAIL was defined as being at least 2 OPENS within the same temperature cycle. A single OPEN in any temperature cycle was not counted as a FAIL event and the package was deemed as failed only after 15 FAILS [15] had been logged.

**State-of-the-Art**

The use of leading indicators of failure for prognostic indication of impending failure of electronics has been previously demonstrated [17-20]. One important reason for using an in-situ solder joint fault sensor is that stress magnitudes are hard to derive, much less keep track of [21]; another reason is that even though a particular damaged solder joint might not result in immediate FPGA operational faults, the fault indicates the FPGA is likely to have, or will soon have, other damaged I/O ports – in short, the FPGA is no longer reliable.

FPGAs are not amenable to the measurement techniques typically used in manufacturing reliability tests such as Highly Accelerated Life Tests (HALTs) [10]. This is because, for example, a 4-point probe measurement requires devices to be powered-off; and because FPGA I/O ports are digital, rather than analog, circuits (see Figure 9).

Modern BGA FPGAs have more than one thousand pins and very small pitch and ball sizes, for example, the left side of Figure 10 shows the position of the XILINX FG 1156 FPGA die with respect to the FPGA mount, and the right side shows the bottom of the package a footprint of 35 \(\times\) 35 mm\(^2\), and a 34 \(\times\) 34 array of solder balls. The dense array of fine-pitch and ultra-fine-pitch BGA packages with very small pitch and solder ball tends to make physical-, optical-, X-ray, and sonic-based inspection techniques impractical for detecting the onset of damage.

One of the Ridgetop test boards was physically ground to create the cut view shown in Figure 11. The cut view shows the FPGA die is connected by either flip-chip collapsed connections or by bonding to a die-mounting base. Wire
interconnects connect the die to ball limiting metallurgy (BLM), to which solder balls are attached. The FPGA package is then placed over connection lands on the printed circuit board (PCB) and soldered. Note the presence of voids in the two solder balls on the right-hand side of Figure 11, such voids lead to early onset of solder ball failure.

SJ MONITOR

During the design and development of SJ BIST, Raytheon Missile Systems, Tucson, Arizona, asked if Ridgetop would provide a solder joint fault solution that met the following requirements: 1) battery powered, and 2) used to monitor FPGAs that were in a powered-off state. Accordingly, Ridgetop designed and developed SJ Monitor to meet those requirements.

Analog Block Diagram

SJ Monitor, as shown in the block diagram in Figure 12, is designed and is being developed as an Integrated Circuit (IC) chip, which is mounted adjacent and connected to the FPGA on the board. SJ Monitor is a low-power, continuous monitoring sensor.

A solder joint fault of at least 100 Ω is detected and amplified by an amplifying detector, which also produces a self-biasing reference voltage. The circuit design is such that SJ Monitor: 1) rejects all noise of 3.0 mV or less; 2) accepts all fault signals of 5.0 mV or higher; and 3) is insensitive to the exact steady-state DC voltage on an FPGA pin. The amplified analog signal from a high-gain comparator is conditioned to produce a digital pulse whenever a fault is detected. Each digital pulse is processed for Prognostic Health Management (PHM) purposes: counts, flags, and health level.

SJ Monitor is fully designed and simulated at 3.3 V for a TSMC® 0.25-µm process; and at 1.2 V and 2.5 V supply voltages for the IBM® 130-nm 8RF bulk CMOS process node. At 1.2 V, SJ Monitor uses less than 5.0 mW of power, which means SJ Monitor can be used in a battery-powered, 24 × 7 monitoring application. There is flexibility on the number of test cells included on a single IC chip. Board wiring constraints might require 4 cells on each IC chip; in turn, this requirement might then require the placing of two SJ Monitor chips on the board.

A complementary version of SJ Monitor using negative 1.2 V power was also designed and simulated using a circuit design simulator. The complementary version provides a monitoring capability for FPGAs that are powered-off. The simulation results for the complementary version are similar to those shown in Figure 12 through Figure 16, separate figures are not provided.

---

**Fig. 11. View Showing FPGA Die to PCB Connection**

---

**Fig. 12. SJ Monitor, Analog Block Diagram**

**Pull-Down Level of FPGA I/O Ports**

Measurements and evaluations of various FPGAs from more than one manufacturer indicate that for I/O ports pulldown low and sourced with external currents of less than 0.5 mA, the noise on an output I/O port is less than 1.0 mV. This allowed us to design SJ Monitor to source less than 200 µA to each monitored I/O pin of an FPGA.

SJ Monitor is insensitive to the exact level of the pull-down voltage on an I/O port, and this was verified by simulations of pull-down levels from 0 to over 300 mV. The simulations included noise perturbations of 2.0 to 3.0 mV, which is about 3 times larger than the maximum level of measured noise, none of the noise perturbations caused a false alarm and all signal perturbations of 5.0 mV or larger were detected and reported as faults. The design is easily changed to produce larger sourcing currents to overcome a greater-than-expected noise margin.

**Simulation Results:**

**Noise Rejection and Fault Detection**

Referring to Figure 13A shows an I/O pin with a pull-down voltage level of 10 mV and (B) shows an I/O pin with a pull-down voltage level of 100 mV. Superimposed on each of the pull-down voltage levels are 3.0 mV noise pulses and 9.5 mV fault perturbations caused by injecting a 100 Ω
levels were used – 1.08 V, 1.20 V, and 1.32 V; 3) three different temperatures were used – -25°C, 27°C, and 100°C; and 4) the complementary version of SJ Monitor was simulated using negative power voltages of -1.08V, -1.20 V and -1.32 V. For all variations, SJ Monitor produced correct results, all faults detected and no false alarms.

Fig. 15. Temperature, Fault Resistance, and Fault Duration Curves

SJ Monitor Sensitivity and Resolution
The value of the minimum detectable fault resistance is primarily dependent on the duration of the fault and the operating temperature as shown in Figure 15. The results indicate that SJ Monitor is able to detect a fault resistance of at least 100 Ω when the fault duration is at least 20 ns.

SJ Monitor Power
Test simulations showed SJ Monitor has a power requirement of between 0.9 mW and 2.4 mW (Figure 16) to monitor 8 I/O pins, depending on temperature and voltage. This low power requirement makes SJ Monitor suitable for continuous monitoring and for short test applications.

SJ Monitor Signals
SJ Monitor has the following signals for each monitored pin: 1) currently active fault; 2) at least one fault detected; and 3) 1:255 count of the number of faults detected. Common control input control signals are: 1) enable monitoring, and 2) reset counts and flags.

INTERMITTENCY MITIGATION
SJ Monitor is a very useful sensor for mitigating intermittencies. Early detection of failure of an unused I/O
stress occur; a hard open longer than a millisecond did not occur until the fifth shockwave. SJ Monitor would have recorded at least eight instances of faults: two in each of the first three waves and one each in the fourth and fifth waves.

Intermittent Confirmation and Prognostic Warning
Detection of intermittent faults can be used to confirm that the electronic board with that FPGA is a likely candidate for replacement to address reported operational anomalies. In the absence of any reported operational anomalies, detected faults can be used as a prognostic warning that the board is likely to experience future operational anomalies.

PIN SELECTION

A deployed FPGA should not use the 8 I/O ports nearest the 4 corners of the FPGA package (the pink-shaded pins in Figure 17); instead those ports should be pulled low and should be attached via wiring to a monitoring pin on the chip package for SJ Monitor—we might change the recommendation to “near each corner of FPGA die shadow.” Research, such as the strain diagram in Figure 18 [24], indicates the solder balls nearest the corner of the package or the FPGA die are most likely to fail first. In Figure 18, the areas of high strain are yellow-red in color, and the areas of low strain are blue in color.

High stress/strain caused by physical mounting coupled with thermal-mechanical stresses and strain are the most likely cause of the observed failure distribution of solder balls in BGA packages. Further evidence of the validity of these observations is the reserving of the four I/O pins at each corner for ground and all of the pins under the die for power and ground (the orange-shaded pins) in Figure 17.

PRESENT ACTIVITIES

The detailed design and simulation of the analog circuits used in SJ Monitor were accomplished using internal...
research and development (IR&D) funding. We are using the same digital circuit building blocks in multiple projects to leverage our work. The tape out for the test circuitry blocks occurred in late September 2007.

FUTURE ACTIVITIES

The steps necessary to reach Technology Readiness Level (TRL) 6 are the following: 1) complete the IC layout and masks for both the analog and digital circuits; 2) fabricate and package SJ Monitor; 3) perform extended evaluation tests, make any required and desired circuit changes and fabricate and package in a final form factor; 4) perform all tests required for a Silicon Validation Report (SVR); and 5) write the SVR and an initial data sheet specification.

SUMMARY AND CONCLUSION

Herein, we introduced a new solder-joint fault sensor, SJ Monitor. A brief overview of the mechanics-of-failure was included, the primary contributor to fatigue damage is thermo-mechanical stresses related to coefficient of thermal expansion (CTE) mismatches, shock and vibration, and power on-off sequencing. Solder joint fatigue damage can result in fractures that cause intermittent instances of high-resistance spikes that are hard-to-diagnostics. In reliability testing, OPENS (faults) are often characterized by spikes of 200 Ω or more lasting for 200 ns to 1 μs or longer.

Prior to SJ BIST, also presented in this conference, and SJ Monitor, there were no known methods for detecting high-resistance faults in solder joint networks belonging to the I/O ports of operational, fully-programmed FPGAs. SJ Monitor is designed to be a low-power monitor for 24 × 7 applications, it can be battery-powered and the complementary version of SJ Monitor monitors the pins of powered-off FPGAs.

SJ Monitor to test or monitor selected I/O pins is useful because stress magnitudes are hard to derive, which leads to inaccurate life expectancy predictions; and even though a particular damaged solder joint port might not result in immediate FPGA operational failure, the damage indicates the FPGA is no longer reliable.

ACKNOWLEDGEMENT

The work presented herein was partially funded by Small Business Innovation Research contract awards from the Department of Defense, Naval Air, Joint Strike Fighter program, Contract No. N68335-06-C-0356 P00002. Final patent applications have been filed: one for SJ Monitor technology; one for a related SJ BIST technology. US Patent 7,196,294, March 27, 2007, has been issued for a third related technology.

REFERENCES


[24] Sraia diagram produced by Norman Roth, Daimler, as part of the HALT of Ridgetop test boards, September 2007.

[25] IBM is a registered trade mark of IBM Corp.

[26] TSMC is a registered trade mark of Taiwan Semiconductor Manufacturing Corporation.

[27] XILINX is a registered trade mark of Xilinx, Inc.
Security Threats in Wireless Sensor Networks

Hiren Kumar Deva Sarma
Sikkim Manipal Institute of Technology
&
Avijit Kar
Jadavpur University

ABSTRACT

Wireless Sensor Network (WSN) is an emerging field. These are normally designed to perform a set of high level information processing tasks; for example, detection, tracking, or classification. Different application areas of WSNs are Environmental Monitoring, Industrial Sensing and Diagnostics, Infrastructure Protection, Battlefield Awareness, Context Aware Computing, etc. From application areas of WSN, it has been observed that ensuring security and privacy is one of the highest priorities for Wireless Sensor Network Systems. Information in the network must be protected from attackers. Attackers may devise different types of security threats to make the WSN system unstable. Herein, we have identified different security threats possible for a Sensor Net Setting. Effort has been made to model the threats mathematically. Future scope of the work has also been outlined.

INTRODUCTION

Wireless Sensor Networks have emerged as a dominant technology in the current decade. Diversified application areas of Wireless Sensor Networks indicate the bright future of this new paradigm. WSNs are becoming popular day by day. Already many companies have started developing commercial applications. At the same time they have posed numerous unique challenges to researchers. Wireless sensor networks are generally composed of hundreds or even thousands of tiny sensor nodes, which are constrained in many aspects like memory capacity, processing power, and most importantly, energy or battery power. Most of the time sensor nodes do not have access to renewable energy resources. The overall cost of a WSN is also required to be relatively lower.

Moreover when we look at the applications of WSNs, there are many applications areas, e.g., battlefield awareness, traffic monitoring system, etc., in which security of information remains as an important issue. Providing security to a WSN is a nontrivial problem. Security mechanisms which are applicable of being wired or other ad-hoc networks are not suitable for WSN. There are many reasons behind it and we discuss those in subsequent sections.

Though there are varieties of challenges in sensor networks, herein we focus on different security issues and possible remedies.

To make WSN feasible for all kinds of applications at lower cost we need simple protocols for communication, security, topology management, medium access control which are supposed to be energy efficient. Though security is a very important issue in WSN, very little work is available for securing a WSN. To understand the limitations of current security mechanisms, it is necessary to realize the features of a wireless sensor network. Different features of WSN such as low memory, low energy, low bandwidth for communication, and large scale nodes make most of the current security solutions available for other ad hoc and wired networks impractical for WSNs.

We have identified different challenges in providing security to a WSN deployment.

The First Challenge:
There is a conflicting interest between minimization of resource consumption and maximization of security level. A better solution actually gives a good compromise between these two. During the design of any security solution we need to take care of following resource constraints [1]:

- limited energy,
- limited memory.
• limited computing power;
• limited communication bandwidth; and
• limited communication range.

The Second Challenge:
The type of security mechanism that can be hosted on a sensor node platform is dependent on the capabilities and constraints of sensor node hardware.

The Third Challenge:
Ad-hoc networking topology of WSN facilitates attackers for different types of link attacks ranging from passive eavesdropping to active interfering. Attacks on a WSN can come from all directions and target any node leading to leaking of secret information, interfering message, impersonating nodes, etc.

The Fourth Challenge:
The communication in WSN is through wireless media, mainly radio. This characteristic of WSN makes wire-based security schemes impractical for WSNs.

The Fifth Challenge:
The topology of WSN is always dynamic. The sensor nodes can come and go in an arbitrary fashion. Node failures may be permanent or intermittent and this gives a higher level of system dynamics. Again very often large numbers of nodes are expected in sensor network deployments and the nature of this deployment is unpredictable.

The Sixth Challenge:
The overall cost of the WSN should be as low as possible.

KEY ISSUES FOR ACHIEVING THE SECURITY IN WIRELESS SENSOR NETWORKS

Based on the analysis on security challenges and potential attacks on Wireless Sensor Networks, four key issues have been identified for providing security to the WSNs:

1) Key Management in WSN:
Confidentiality, integrity, and authentication services are critical factors for maintaining the security of a WSN. Key management is a highly important issue for this kind of protection in WSN. However, providing key management service in WSN is extremely difficult due to various constraints in the WSN environment, e.g., ad-hoc nature of the network, intermittent connectivity, resource limitation, limited communication bandwidth, etc.

2) Encryption and Decryption Mechanism:
Since the WSN environment is resource-constrained this encryption procedure as well as the decryption mechanism has to be very simple and energy efficient. Due to memory and energy constraints in a WSN environment we can not go for traditional asymmetric cryptography.

3) Secure Routing of WSN:
The major two types of threats in routing protocols of Wireless Sensor Networks are:
A) external attackers – external attackers may become successful in partitioning a network or in introducing excessive traffic load into the network. Various attacks include: injection of erroneous routing information, replaying old routing information, distorting routing information, etc. Use of cryptographic schemes can defend against external attacks.
B) Internal compromised nodes – it is difficult to put defense against such attacks. These nodes may send malicious information to other nodes in the network.

4) Prevention of Denial-of-Service:
A denial of service attack is any event that diminishes or eliminates a network’s capacity to perform its expected function. Hardware failures, software bugs, resource exhaustion, environmental conditions, or any complicated interaction between these factors can cause a Denial-of-Service.

THREATS AT DIFFERENT LAYERS IN WIRELESS SENSOR NETWORK PROTOCOL STACK

We discuss different types of security threats present in different layers in the protocol stack of a Wireless Sensor Network. There are some types of security threats which span over more than one layer.

1) Physical Layer:
The communication media among the sensors is normally radio. Since the media is open there is a high risk present. Some of these threats are:

JAMMING
In this type of attack, adversaries interfere with the communication frequencies (radio frequencies) of the sensor nodes present in the network. For this purpose the adversary may select a few jamming nodes from within the network and then may apply jamming simultaneously from these selected nodes. In this case, the number of nodes the adversary...
needs is a small fraction of the total number of nodes present in the network. Jamming is a popular Denial-of-Service (DoS) attack.

**TAMPERING**
In most of the applications, the number of sensor nodes deployed is very high and the geographic area over which those nodes are distributed is also very large. Therefore, it becomes impossible to control the access to all nodes from others. Again, the fabrication of the sensor nodes is simple and this is done mainly to reduce the cost. Normally tamper-resistant hardwares are not provided as it adds more cost to the sensor nodes. Due to these factors anybody can get access to the sensor nodes physically and even adversaries may introduce some identical sensor nodes into the sensor network field from their own side. Again, adversaries may become successful in compromising some of the legitimate nodes in the network. After compromising a node, adversaries may carry out lots of misleading activities inside the network.

**SYBIL ATTACK**
The base of Sybil Attack is actually at the physical layer but it becomes more prompt in the higher layers like link layer and network layer. In this class of attack, the adversary introduces a malicious node into the network. This can be done by compromising any legitimate sensor node or by fabricating a new node. This malicious node acquires identity through one of two ways: by fabricating new identities, or by stealing other identities. The malicious node behaves as if it were of different identities from different places in the network. It is a famous Classical Attack.

2) **Data Link Layer:**
Following are some of the security threats in link layer:

**COLLISION**
In this type of Denial-of-Service attack, adversary can induce collision in only one small portion of the entire packet transmitted by a node. A small change in the data portion of the packet leads to an error in the checksum of the whole packet and asks for retransmission of the same packet.

**EXHAUSTION**
Some link layer protocols attempt retransmission repeatedly, in the event of the transmission getting triggered by a collision. Adversaries may exploit it for doing exhaustive Denial-of-Service attack in which they continuously disturb the communication between two nodes and force the source node to retransmit continuously. This leads to quick decay in the energy level of the sensor nodes.

**INTERROGATION ATTACK**
Some Medium Access Control layer implementations use Request To Send (RTS) and Control To Send (CTS) packets to reserve channel access to transmit data. A malicious node can send RTS packets continuously to a targeted node by ignoring CTS reply packets. Then this can flood the network link of the targeted node. Normally, this type of attack is done by either a malicious node or by a self-sacrificing node.

**SYBIL ATTACK**
This type of attack is very much prominent in the Link Layer. Different variations of Sybil Attacks are as follows:

**Data Aggregation:**
Data aggregation is an important part in Wireless Sensor Networks as it reduces the power consumption as well as the bandwidth requirements for individual message transmission. In this situation, a Sybil Attack can be used to induce negative reinforcements. A single malicious node is sufficient to act as different Sybil Nodes and then this may give many negative reinforcements to make the aggregate message a false one.

**Voting:**
Voting may be a choice for a number of tasks in a Wireless Sensor Network. Many MAC protocols may go for voting for finding the better link for transmission from a pool of available links. Here, the Sybil Attack could be used to stuff the ballot box. An attacker may be able to determine the outcome of any voting and, of course, it depends on the number of identities the attacker owns.

3) **Network Layer:**
Major security goals of Network Layer are:

A. Every eligible receiver should receive all messages intended for it. Every receiving node should also be able to verify the integrity of every message as well as the identity of the sensor.
B. Routing protocol should also be responsible for preventing eavesdropping caused by misuse or abuse of the protocol itself.

In a Wireless Sensor Network, every node behaves as a router and routing issue is complicated from security point of view also. Designers of routing protocols did not consider security aspects during the design of the routing protocols and that is why Wireless Sensor Networks routing protocols are vulnerable to different types of attacks.

Here is a list of different types of attacks on the network layer:

**NEGLIGENCE AND GREED**
In this type of attack a node that is present in the routing path can drop the message by participating in the lower level protocols. What the node does is send the “ACK” message of the link layer and drop the network layer message. The node can also give arbitrary priorities to the messages that pass through it.

**MISDIRECTION**
This is a more active attack in which a malicious node present in the routing path can send the packets in the wrong direction through which the destination is unreachable. In place of sending the packets in the correct direction, the attacker misdirects those and that too toward one node and thus this node may be victimized.

**INTERNET SMURF ATTACK**
In this type of attack, the adversary can flood the victim node’s network link. The attacker forges the victim’s address and broadcasts echoes in the network and also routes all the replies to the victim node. This way the attacker can flood the network link of the victim.

**BLACK HOLE ATTACK**
In this type of attack, some of the malicious nodes in the WSN intentionally advertise zero cost routes through them. Then some routing protocols (e.g., distance vector routing) establish a route to a destination by selecting this malicious node as an intermediate node into the routing path; (as they look for low cost link). Also the neighbors of this malicious node select this route and compete for the bandwidth. In this process the neighbors of this malicious node waste their energy and create a hole or partition in the network called a black hole.

**SYBIL ATTACK**
All multi-path routing protocols are vulnerable to Sybil attacks. The malicious node present in the network may advertise different identities. Then all paths in the multipath protocol may pass through the malicious node. And the protocol may have a picture of existence of different paths. But actually it is the same path through the malicious node. Sybil attack can actually fool the protocol giving a picture of existence of different routing paths to the destination but it is the same path through the Sybil node. On top of that even Geographic Routing Protocols are vulnerable to Sybil attack. It is because of the fact that the same Sybil Identity or different Sybil Nodes may give an illusion of their presence at different geographic locations.

**SPOOFING AND ALTERING THE ROUTING INFORMATION**
This is the most direct attack on a routing protocol because it targets the routing information which is exchanged between the nodes. By spoofing, altering, or replaying routing information, adversaries may be successful to create routing loops, attract or repel network traffic, extend or shorten source routes, generate false error messages, partition the network, and increase end-to-end latency.

**WORM HOLE ATTACK**
An adversary situated close to the base station may completely disrupt routing by creating a well-placed wormhole. An adversary could also convince nodes who would normally be multiple hops from a base station that they are only one or two hops away via the wormhole. All existing routing protocols are vulnerable to this type of attack and there is no solid defense existing against the wormhole attack.

**SELECTIVE FORWARDING ATTACK**
Normally it is believed that in a multihop network, participating nodes will faithfully forward the received messages. But sometimes this does not happen. This is what exactly happens in a selective forwarding attack – malicious nodes may refuse to forward certain messages and they drop these messages to ensure that the messages do not get propagated further. A simple form of this attack is a malicious node behaves like a black hole and does not forward every packet it receives. But
such an attacker may fail because the neighboring nodes may conclude that it has failed and decide to seek another route.

Another form of this attack is: an adversary may selectively forward packets. Here the adversary may be interested in suppressing or modifying packets originating from a few selected nodes. In this situation, the adversary reliably forwards the remaining traffic to limit the suspicion of wrong-doing.

HELLO FLOOD ATTACK
Many protocols require nodes to broadcast HELLO packets to announce themselves to their neighbors. A node receiving such a packet may assume that it is within radio range of the sender. And this assumption may be false.

4) Transport Layer:

Different types of threats present in the Transport Layer are as follows:

FLOODING ATTACK
Protocols that maintain state information at either end of the communication are vulnerable to flooding attack. One well-known attack is TCP SYN flood attack in which the adversary continuously sends the connection requests and floods the network link at the targeted node.

DE-SYNCHRONIZATION
By disrupting some of the packets transmitting in between the nodes and by maintaining proper timings, an adversary can make a pair of nodes stuck in synchronization recovery protocol. This compels the nodes to waste their energy.

SOLUTIONS AT DIFFERENT LAYERS IN WIRELESS SENSOR NETWORKS

1. Physical Layer:

JAMMING
Various forms of spread-spectrum communication are used as defense against Jamming. Frequency hopping is one form of spread-spectrum approach and this has been widely used as a defense against Jamming. In this approach, all communication nodes maintain a hopping sequence. Here the tricky point is, a jammer can get the hopping sequence if he observes the transmission and therefore hopping should be done very fast. In that case the jammer cannot interfere with the communication. The cost involved against frequency hopping is higher as the sensor nodes are power constrained as well as have low computational capability.

TAMPERING
The defense mechanism designed against tampering should prevent the attackers (adversaries) from getting any information about cryptographic keys or about the network, even though it is successful in compromising some of the nodes. Here is a list of few defenses:

1) Self Destruction— whenever somebody accesses the sensor nodes physically, the nodes vaporize their memory contents and this prevents any leakage of information.

2) Fault Tolerant Protocols— the protocols designed for a WSN should be resilient to this type of attack. This means even if some nodes are removed from the network setting or they are compromised, still the network should function properly.

SYBIL ATTACK
Normally this class of attack is tackled efficiently in the higher layers of the protocol stack in a WSN, though they originate in the physical layer only. Some preventive measures like fixing of the number of nodes in a WSN (which may depend on the type of application the WSN is intended for) can be taken which will prevent the adversary from fabricating new identities.

2. Link Layer:

Good encryption mechanism, authentication mechanism, and error correcting techniques are required to put defense against most of the link layer threats. Since the sensor nodes are resource constrained, the above-mentioned techniques should not be computation intensive and they should not put much overhead to the sensor nodes and also communication overhead should be minimum.

COLLISION
Providing error correcting codes – error correcting codes can be incorporated in the data packets to defend against collision. But this solution comes at a higher cost in terms of computational complexity and energy consumption.
EXHAUSTION
The defense against exhaustive Denial-of-Service attack is very simple and still effective. If a node retransmits a message for more than a threshold number of times, then the node identifies itself as under attack and goes to sleep mode. Later it may be awakened and resume its normal operation.

INTERROGATION ATTACK
To put a defense against such type of attacks, a node can limit itself in accepting connections from same identity. During implementation, it may be decided that a particular node will not accept more than a fixed number of connections from the same identity. A careful selection has to be made in fixing this threshold value.

SYBIL ATTACKS
Radio Resource Testing – It is a popular defense against Sybil Attack. If one node is interested in verifying whether its neighbors are valid or Sybil identities, then this node can assign each of its “n” neighbors a different channel to broadcast some test messages. After this, the node can listen to any channel and find out whether the neighbor that was assigned that channel is legitimate. Apart from this, some secret information may be shared by a node with its neighbors and Sybil identities may be detected. But this may put some extra communication overhead.

3. Network Layer:
The problem of securing the network layer reduces to the problem of securing route discovery of a routing protocol.

NEGLECT AND GREED AND
SELECTIVE FORWARDING ATTACK
One simple defense against this type of attack is: use multiple routing paths or send redundant messages (which is, of course, not a power efficient scheme), through which the probability of selecting a vulnerable route can be reduced. This can also force the adversary to compromise more nodes to succeed.

MISDIRECTION AND
INTERNET SMURF ATTACK
This kind of attack can be handled easily as follows: If it gets observed that a node’s network link is flooded without any useful information, then the victim node can be scheduled into sleep mode for sometime.

BLACKHOLE ATTACK
This type of attack can be defended by accepting routing replies only from authorized nodes. Unauthorized nodes can easily be identified by just checking if some node is behaving abnormally.

SYBIL ATTACK
There is no effective defensive mechanism available against Sybil attack in Network Layer. But it is important to note that this attack cannot survive only in routing layer. First, the attacker interested in Sybil attack must attack the link layer and also get Sybil identities. And very good defensive mechanisms for Sybil attack in link layer are available through which this type of attack can be defended in the link layer itself.

RUSHING ATTACK
One defense against rushing attack is by detecting a secure neighbor. And this may be done by bi-directional checking of the link while electing the route.

WORMHOLE ATTACK AND
HELLO FLOOD ATTACK
One defense against these types of attacks are by checking the bi-directional link whenever selecting a path.

Again location-based routing protocols can avoid wormhole attacks since, in these protocols, each node knows approximately how many hops it is from sink. Here, wormholes cannot fool the nodes since they know their location.

SPOOFING, ALTERING MESSAGES
Efficient encryption and authentication techniques can defend against spoofing attacks. Encryption may be applied to some required fields in the header of the message. This may save some energy from computing and communicating some extra bits. TESLA can be adopted for authentication.

4. Transport Layer:
The security issues in the transport layer are mainly due to the existence of the flaws in the transport layer protocols. Efficient design of
transport layer protocols can avoid transport layer threats.

FLOODING ATTACKS
As a defense against this class of attack, a limit can be put on the number of connections from a particular node. Again, a careful selection has to be made in determining this upper limit on the number of connections. A study of the topology of the network may be helpful in this regard.

DESYNCHRONIZATION
A solid authentication mechanism can be deployed to authenticate all packets exchanged, including all control fields in the transport packet header. It is assumed that the authentication mechanism is robust and adversaries also cannot forge this mechanism. In this situation, the end nodes can detect malicious packets and ignore same.

CONCLUSION AND FUTURE SCOPE
Providing security in Wireless Sensor Network is a non-trivial task. Herein, we have studied different key issues in achieving security in WSN. We have also studied different threats existing in different layers of the protocol stack of WSN. Possible solutions against different threats have also been outlined. This work was undertaken by the authors and is in progress regarding the design of a security framework for wireless sensor networks. The mathematical modeling of different threats present in the WSN is another aspect of this work.

ACKNOWLEDGEMENT
The authors are grateful to Prof. Rajib Mall, Department of CSE IITKGP, India, for his constant support and guidance.

REFERENCES
IEEE-NANO 2008
8th IEEE Conference on Nanotechnology
August 18-21, 2008
Sheraton Hotel and Arlington Convention Center
Arlington, TX, USA
Sponsored by the IEEE Nanotechnology Council
Register at
http://www.ieee.org/NANO2008

IEEE Nano 2008 is sponsored by the IEEE Nanotechnology Council, Region 5, and Fort Worth and Dallas Sections.

The 8th IEEE International Nanotechnology Conference is the premier IEEE conference in the field of nanotechnology. Expect exhibits and demonstrations that present the latest innovations, products, experiences, and practices in nanotechnology. Over 500 university, science, and engineering professionals are expected to attend. The technical program includes: plenary presentations by world leaders in the field; case studies; talks from industry, universities, and government agencies; tutorials; research and commercial application demonstrations in the exhibit hall.
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 on the impact of security-related technology on society. Participation in the conference also provides a basis for long-range support and assistance to authorities and agencies in the use of technology for security, safety, law enforcement, and emergency response purposes.

TOPICS
1. Sensor and detection technology, including principles of operation and signal analysis
2. Alarm devices, searching aids, and systems
3. Monitoring, command, control, and communication systems
4. Computer systems security and privacy
5. Information security
6. Communication security and privacy, including modulation techniques, spectrum management, and encryption
7. Biometric identification systems, utilizing voice, handwriting, fingerprints, hand geometry, facial recognition, etc.
8. Entry control systems, access delay technology, and surveillance
9. Counter-terrorism techniques and technology
10. Impact on society of security systems and technology
11. User experiences of operating security systems including their introduction and testing
12. Police and forensic technology
13. Cryptology
14. Less-than-lethal weapons technology
15. Counter proliferation of weapons of mass destruction
16. Port and airport security
17. Emergency management
18. Network intrusion detection technology and virus protection
19. Border security

CONFERENCE SITE:
Diplomat Hotel
Prague
Evrupska 15
Prague 6
Czech Republic
http://www.hoteddiplomat.cz

http://www.action-m.com/carnahan2008
# IEEE 2008 AEROSPACE AND ELECTRONIC SYSTEMS SOCIETY MEMBERSHIP APPLICATION

(Counting and reinstating IEEE members joining AESS complete areas 1, 2, 7, 8)

Mail to: IEEE, Admission & Advancement Dept., 445 Hoes Line, P.O. Box 8804, Piscataway, New Jersey 08855-8804 USA

For info call (732) 981-0060 or 1 (800) 678-IEEE. E-mail: newmembership@ieee.org or www.ieee.org/join

1. NAME AS IT SHOULD APPEAR ON IEEE MAILINGS: SEND MAIL TO:  Home Address OR  Business/School Address

If not indicated, mail will be sent to home address. NOTE: Enter your name as you wish it to appear on membership card and all correspondence. PLEASE PRINT: Do not exceed 40 characters or spaces per line. Abbreviate as needed. Please circle your last name/first name as a key identifier for the IEEE database.

<table>
<thead>
<tr>
<th>TITLE</th>
<th>FIRST OR GIVEN NAME</th>
<th>MIDDLE NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SURNAME/LAST NAME</th>
<th>CITY</th>
<th>STATE / PROVINCE</th>
<th>POSTAL CODE</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2. Are you now or were you ever a member of IEEE?  Yes  No

If yes, please provide: Known:

<table>
<thead>
<tr>
<th>MEMBERSHIP NUMBER</th>
<th>GRADE</th>
<th>Year Membership Expired</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

DEMOGRAPHIC INFORMATION – ALL APPLICANTS –

Date of Birth:  Day  Month  Year  Male  Female

3. BUSINESS / PROFESSIONAL INFORMATION

Company Name:

Department / Division:

Title / Position:  Years in Current Position

Years in the Profession Since Graduation:  PE  State / Province

Street Address:

<table>
<thead>
<tr>
<th>CITY</th>
<th>State / Province</th>
<th>POSTAL CODE</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4. EDUCATION A bachelor’s degree from an IEEE reference list of programs assures assignment of “Member” grade. For others, additional information and references may be necessary for grade assignment.

<table>
<thead>
<tr>
<th>Baccalaureate Degree Received</th>
<th>Program / Course of Study</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>College / University</th>
<th>Campus</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>State / Province</th>
<th>Country</th>
<th>Mo / Yr. Degree Received</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Highest Technical Degree Received</th>
<th>Program / Course of Study</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>College / University</th>
<th>Campus</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>State / Province</th>
<th>Country</th>
<th>Mo / Yr. Degree Received</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5. SIGNATURE OF APPLICANT

I hereby make application for IEEE membership and agree to be governed by IEEE’s Constitution, Bylaws, Statements of Policies and Procedures, and Code of Ethics.

Full signature of applicant  Date

6. CONTACT INFORMATION

<table>
<thead>
<tr>
<th>Office Phone</th>
<th>Home Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Office Fax</th>
<th>Home Fax</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Office E-mail</th>
<th>Home E-mail</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

7. 2008 IEEE MEMBER RATES

Check (✓) a box

<table>
<thead>
<tr>
<th>IEEE DUES</th>
<th>Residential</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payment</td>
<td>Pay Full Year</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

United States  $165.00  $105.00  $82.50
Canada (includes GST)  $152.50  $92.00  $76.25
Canada (includes HST)  $162.64  $101.70  $81.32
Africa, Europe, Middle East  $137.00  $85.25  $68.50
Latin America  $130.00  $80.00  $65.00
Asia, Pacific  $131.00  $80.00  $65.50

2008 AESS MEMBER RATES

Aerospace and Electronic Systems Society Membership Fee

<table>
<thead>
<tr>
<th>Full</th>
<th>Half</th>
</tr>
</thead>
<tbody>
<tr>
<td>$25.00</td>
<td>$13.00</td>
</tr>
</tbody>
</table>

METHODS OF PAYMENT: Prices stated are in US dollars.

- Credit Card – American Express, VISA, MasterCard, Diners Club
- Check - Bank Drafts - Money Orders Payable on a US bank

8. IEEE Membership Dues

<table>
<thead>
<tr>
<th>Aerospace and Electronic Systems Society Fees Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>$</td>
</tr>
</tbody>
</table>

Canadian residents only pay 7% GST or 15% HST on Society fees only. Reg. No. 125634188

TAX $ $_

AMOUNT PAID WITH APPLICATION TOTAL $ 

Prices stated are in US dollars; subject to change without notice.

☐ Check or money order enclosed (Payable to IEEE)
☐ American Express  ☐ VISA  ☐ MasterCard
☐ Diners Club

Exp. Date  Mo./Yr.

Charge Card Number

Cardholder 5 Digit Zip Code

Billing Statement Address  USA Only

Full signature of applicant using credit card  Date