CrossTalk

June 2003 The Journal of Defense Software Engineering Vol. 16 No. 6

Commercial and Military Applications Meet

Commercial and Military Applications Meet

4 Upgrading Global Air Traffic Management
In this interview, Program Manager John Schneider discusses how civilian and military air traffic requirements are blending throughout global airspace in a new Global Air Traffic Management system.
by Elizabeth Starrett

7 Airport Simulations Using Distributed Computational Resources
A simulation of Atlanta's Hartsfield International Airport on NASA's Virtual National Airspace Simulation prototype identified air transportation safety improvements by identifying precursors to component failure.
by William J. McDermott, Dr. David A. Maluf, Yuri Gawdiak, and Peter B. Tran

12 SAASM and Direct P(Y) Signal Acquisition
Two key contributors to global positioning system encryption technology describe how the Selective Availability Anti-Spoofing Module enables direct acquisition of the P(Y) code for added military and civilian capability.
by Steve Callaghan and Hugo Fruehauf

17 Improving Information Management Software System Deployment Practices
The study in this article shows that a lack of sharing and replication of best practices across product offices hindered deployment of software-intensive systems.
by Dr. James A. Forbes, Maj. Kurt Bodiford, and Dr. Emanuel R. Baker

21 Pilot Testing Innovative Auto ID Technologies
This article looks at several new technologies to upgrade inventory management and tracking systems in a pilot study at the Jet Propulsion Laboratory in California.
by James E. Bagley

ON THE COVER
Cover Design by Kent Bingham.

Software Engineering Technology

25 Steganography
This author explains the technique of steganography and the art of hiding messages in its inadvertent layer along with its vulnerabilities should the message be discovered.
by 2nd Lt. James Caldwell

28 Trafficability Analysis Engine
This article describes the design and implementation of a new trafficability engine that takes into account previously ignored aspects and degrades gracefully when data are missing.
by Dr. Kevin R. Slocum, Lt. Col. John R. Surdu, 2nd Lt. Jeffrey Sullivan, 2nd Lt. Marek Rudak, 2nd Lt. Nathan Colvin, and Cadet Christopher Gates

Departments

3 From the Publisher

11 Coming Events

20 Web Sites

27 STSC Free Help Desk Services

31 BackTalk

CrossTalk

SPONSOR	*Lt. Col. Glenn A. Palmer*
PUBLISHER	*Tracy Stauder*
ASSOCIATE PUBLISHER	*Elizabeth Starrett*
MANAGING EDITOR	*Pamela Bowers*
ASSOCIATE EDITOR	*Chelene Fortier*
ARTICLE COORDINATOR	*Nicole Kentta*
CREATIVE SERVICES COORDINATOR	*Janna Kay Jensen*
PHONE	(801) 586-0095
FAX	(801) 777-8069
E-MAIL	crosstalk.staff@hill.af.mil
CROSSTALK ONLINE	www.stsc.hill.af.mil/crosstalk
CRSIP ONLINE	www.crsip.hill.af.mil

Subscriptions: Send correspondence concerning subscriptions and changes of address to the following address. You may e-mail or use the form on p. 24.

Ogden ALC/MASE
6022 Fir Ave.
Bldg. 1238
Hill AFB, UT 84056-5820

Article Submissions: We welcome articles of interest to the defense software community. Articles must be approved by the CROSSTALK editorial board prior to publication. Please follow the Author Guidelines, available at <www.stsc.hill.af.mil/crosstalk/xtlkguid.pdf>. CROSSTALK does not pay for submissions. Articles published in CROSSTALK remain the property of the authors and may be submitted to other publications.

Reprints and Permissions: Requests for reprints must be requested from the author or the copyright holder. Please coordinate your request with CROSSTALK.

Trademarks and Endorsements: This DoD journal is an authorized publication for members of the Department of Defense. Contents of CROSSTALK are not necessarily the official views of, or endorsed by, the government, the Department of Defense, or the Software Technology Support Center. All product names referenced in this issue are trademarks of their companies.

Coming Events: We often list conferences, seminars, symposiums, etc. that are of interest to our readers. There is no fee for this service, but we must receive the information at least 90 days before registration. Send an announcement to the CROSSTALK Editorial Department.

STSC Online Services: www.stsc.hill.af.mil
Call (801) 777-7026, e-mail: randy.schreifels@hill.af.mil

Back Issues Available: The STSC sometimes has extra copies of back issues of CROSSTALK available free of charge.

The Software Technology Support Center was established at Ogden Air Logistics Center (AFMC) by Headquarters U.S. Air Force to help Air Force software organizations identify, evaluate, and adopt technologies to improve the quality of their software products, efficiency in producing them, and their ability to accurately predict the cost and schedule of their delivery.

The Knowledge Flows Both Ways

This month's CrossTalk theme, "Commercial and Military Applications Meet," initially evoked thoughts of the 1960s U.S. space program. Numerous everyday items came out of new developments from NASA's program to land a man on the moon. When I read the articles contained in this month's issue, I realized that this knowledge transfer is by no means a one-way transition.

Much of what drives military acquisition today is an interest in integrating hardware and software that are used successfully in commercial enterprises. So, what we see is not only new technology originally developed for military systems being transitioned into commercial use, but significant commercial equipment also being adopted for wide military use. Government and industry partnerships also play a significant role in new technology developments.

Our first article, *Upgrading Global Air Traffic Management*, contains highlights of an interview with John Schneider, program manager at Rockwell Collins. Schneider discusses the testing of a new Global Air Traffic Management system on the KC-135 military aircraft. The requirements for this system derived from a merging of the commercial requirements with the military requirements in order to equip aircraft and make them compliant with civilian requirements to ensure full access to global airspace.

Since 9-11, we are more aware of the complex challenge to control our nation's airspace with increases in air transportation. In *Airport Simulations Using Distributed Computational Resources*, authors William J. McDermott, Dr. David A. Maluf, Yuri Gawdiak, and Peter B. Tran discuss the NASA and Federal Aviation Administration goal to develop technologies that will result in a significant reduction in aviation accidents in the next five to 10 years. While this requires a simulation environment with more computing power than is normally available, the authors offer an alternate solution: using multiple computers distributed throughout the country connected through a common network.

The widespread use of global positioning system (GPS) technology and the proliferation of commercial GPS receivers pose a major dilemma for our military: How do you protect U.S. and allied forces from hostile use of the civil GPS signal during critical military operations? In *SAASM and Direct P(Y) Signal Acquisition*, authors Steve Callaghan and Hugo Fruehauf talk about the advances in cryptography and keying techniques that will alleviate the security risks associated with this proliferation.

In *Improving Information Management Software System Deployment Practices*, authors Dr. James A. Forbes, Maj. Kurt Bodiford, and Dr. Emanuel R. Baker describe a project to improve the deployment of software-intensive information management systems. Surveys of both Army Program Management Offices and commercial organizations showed that deployment problems were due to a lack of sharing and replication of best practices across product offices. The authors believe their findings will be of use to other organizations dealing with similar problems.

Digital identification needs have grown – old-fashioned bar codes that we now take for granted in everything we purchase are no longer sufficient for advanced usage. In *Pilot Testing Innovative Auto ID Technologies*, James E. Bagley describes how the aerospace-government-industry partnership is leading the way in implementation of new automatic identification technology.

The historical tutorial, *Steganography*, by 2nd Lt. James Caldwell provides context for this instrument of security, which is used to hide messages within a physical cover message. Although awareness and progress are unfolding to expose steganographic applications, the advanced computer technology of today holds some interesting network security risks that must be appreciated.

Dr. Kevin R. Slocum of the U.S. Army Engineer Research and Development Center, and Lt. Col. John R. Surdu, 2nd Lt. Jeffrey Sullivan, 2nd Lt. Marek Rudak, 2nd Lt. Nathan Colvin, and Cadet Christopher Gates from the U.S. Military Academy author our final article, *Trafficability Analysis Engine*. They cover their development efforts for a tool to measure how easily vehicles can drive through a particular piece of terrain and discuss some needed future work to enhance the application.

I hope this month's articles provide some insight into the dimension of applications that link our military and commercial worlds, and how current efforts are focused on trying to take advantage of both. We hope that one or more of these articles are useful for your current endeavors.

H. Bruce Allgood
Director, Computer Resources Support Improvement Program

Upgrading Global Air Traffic Management

Elizabeth Starrett
CrossTalk

Traffic management for the airways is moving to a more efficient and effective method to track and control aircraft. While radar could track aircraft over land, verbal communication had to be used to track aircraft over water. This verbal requirement implemented the use of a middleman between the traffic controllers and the aircraft, allowing for communication problems. Now, a new Global Air Traffic Control system is being implemented that will allow traffic controllers to directly track and communicate with aircraft in order to improve navigation and safety.

Rockwell Collins contracted with the Systems Program Office for the U.S. Air Force (USAF) Aeronautical Systems Command to upgrade the Global Air Traffic Management (GATM) avionics in the KC-135 aircraft. On Nov. 20, 2002, the KC-135 GATM program successfully completed its South Pacific integrated systems evaluation mission. The mission was conducted during a span of seven days and covered more than 14,800 miles for the first-ever USAF GATM compliance testing with numerous civilian air traffic controllers. CrossTalk Associate Publisher Elizabeth Starrett interviewed John Schneider, program manager, about how civilian and military air traffic requirements and advancements are coming together throughout global airspace.

Q: How does the current Global Air Traffic Management (GATM) system operate?

Schneider: Traditionally, you use radar to track aircraft over land. You have radar coverage to understand exactly any given aircraft's location. When aircraft go oceanic, you lose that radar coverage because you can't put radar sites in the water. Traditionally air traffic controllers have communicated with the aircraft by voice when they are beyond line of sight.

For instance, Oakland Center oversees the whole Pacific region. They will send the request out for a position report to an intermediary communication company; in this case it is Aeronautical Radio, Inc. (ARINC). Then ARINC will, over high frequency, hopefully get ahold of the aircraft and communicate the [position report] request. The aircraft will report their position back to ARINC, who will then Teletype that information back to the air traffic services.

The need for GATM requirements stems primarily from the growth of air traffic and its burden on worldwide air traffic control services. The increase in air traffic places a greater emphasis on the need for aircraft to operate within closer spacing as well as air traffic services having greater situational awareness of these aircraft within controlled airspace. In support of these objectives, many domestic and international civil aviation agencies continue to phase in functional mandates that ultimately drive requirements into aircraft flight decks. In most cases, such requirements apply to both commercial as well as military aircraft, so it's very important for the USAF to stay in touch with the GATM initiative.

The importance in having these types of capabilities is that it often allows an aircraft access to airspace in which it would otherwise be denied. Denial could come in the form of access to preferred altitude blocks, time slots, airports, or bases. In some cases, access to airspace at all altitudes is possible. Because the USAF has a need to deploy their aircraft wherever and whenever, it's pretty easy to understand the importance of having their aircraft equipped with GATM capabilities.

Q: How will the GATM upgrade operate?

Schneider: The GATM focuses on capabilities in three general functional areas: navigation, communication, and safety/surveillance. Adding related capabilities to the KC-135 aircraft is accomplished by adding several hardware components and software applications. These additions enhance existing navigation accuracy and add capabilities that allow the pilot to communicate with air traffic services via datalink as opposed to more traditional voice communications.

From a navigation standpoint, Rockwell Collins added an improved military global positioning system (GPS) receiver and two commercial GPS receivers to meet Required Navigation Performance (RNP) initiatives, which define the accuracy and reliability of navigation systems. Relatively speaking, navigation performance tends to be more critical when airspace congestion is greater, or the aircraft are departing or arriving. The need for greater levels of navigation performance increases as the aircraft transitions from oceanic and en route phases to terminal and approach phases or flights. We also added two multi-mode receivers to address the GATM requirements associated with FM-immune instrument landing system (ILS) capabilities. Lastly, we've replaced the legacy flight management function (FMF) with a commercial FMF to better align the aircraft's flight management capabilities with the commercial airline industry.

From a communication standpoint, Rockwell Collins has added systems that support datalink communication over VHF, HF, or satellite communications (SATCOM). The addition of the SATCOM system also provides another means of beyond-line-of-sight voice communications. We also added communication management units (CMU) that provide processing capabilities associated with controller/pilot data link communications (CPDLC) and automatic dependent surveillance (ADS). CPDLC replaces traditional voice communications between a pilot and controller with data link-based communications and is intended to address ongoing concerns associated with high controller workload, misinterpretations of air traffic control communications, and overburdened voice communications networks.

The ADS function actually falls under the surveillance portion of GATM and allows for the reporting of aircraft position (latitude, longitude, altitude, etc.) thereby allowing air traffic services to be continually aware of where each aircraft is located within a given airspace sector. Reporting this information typically requires no pilot interaction, and since the aircraft will have long-range data link capabilities via HF and SATCOM radios, these reports can be

downlinked independent of the aircraft's current position. This is especially useful when aircraft are in oceanic airspace beyond the reach of land-based radar. Without the GATM capabilities, pilots were forced to provide manual position reports via long-range voice communications, which typically involved a third party to relay this information to the appropriate air services center, as I mentioned earlier.

There are several other enhancements that while not considered GATM-specific, will aid the pilot from a situational awareness standpoint. For instance, we've added several additional display formats such as heading, tactical, and north-up maps. The system also provides the ability to display navigation background data. We've also included the Airline Operational Command (AOC) function that we believe will provide a great deal of utility. AOC gets its roots from the commercial airline industry and is a means to communicate between an airline's dispatch center and each of its aircraft via a series of data link messages. We've worked with our customer to adapt the standard AOC message set for military command and control purposes. We're really just scratching the surface when it comes to AOC, and we're very excited about its potential in the military arena.

Q: When did the GATM upgrade start?

Schneider: The requirements that bubbled up into GATM have slowly been put into place probably since the late 1990's when you started to see a lot of the civil requirements govern access to airspace. From our perspective, Rockwell Collins received the initial contract award in November 1999. Design, development and verification activities were performed during the next 30 months culminating in the first flight of the GATM system aboard the KC-135 aircraft on April 2, 2002. Delivery of the first production aircraft is scheduled for the summer of 2003.

Q: When is compliance required?

Schneider: It really depends on the specific requirement and the geographical location. There are many functional requirements associated with the GATM initiative and some of them are already being phased in by civil aviation agencies that govern global airspace. Requirements that have already been phased into a large extent, include Required Vertical Separation Minimums (RVSM), Required Navigation Performance-5 (RNP-5) and FM-Immune ILS. We expect to see more stringent navigation requirements (i.e. RNP-4, RNP-1) phased in over the next several years. Additionally, there are several airspace sectors, including many in Europe and the South Pacific that are utilizing both CPDLC and ADS capabilities.

The genesis of the GATM requirements for the KC-135 platforms is from the GATM Operational Requirements Document (ORD) that was published by Air Mobility Command (AMC). The need for the GATM ORD is based upon the recognition that the associated requirements are commonly levied by civil aviation agencies or host nations and they don't typically discriminate between commercial and military aircraft. Since the USAF strives to have unconditional access to global airspace, they recognize the importance of equipping their aircraft with capabilities that can satisfy these requirements.

Q: The future air navigation system (FANS) is just now coming on-line. How many aircraft are able to use this now?

Schneider: Within the U.S. Air Force, there are several GATM upgrade programs underway under the AMC organization, and Rockwell Collins is proud to say that the KC-135 GATM program is the first program to achieve first flight and achieve a follow-on production award. The initial production award for upgrading 50 aircraft has been awarded. Delivery of the first aircraft will take place this summer with the remaining aircraft scheduled for upgrade within a one-year period. The various air traffic control centers are getting the capability for FANS applications. I would say right now, it is predominantly in the South Pacific. You are seeing a lot of CPDLC activity right now in the Pacific oceanic areas and Brisbane, Australia, New Zealand, and Fiji. In addition to that, you are starting to see those types of activities or applications become more prevalent in the European areas.

Q: It is my understanding that the military's KC-135 is the first aircraft to be tested with GATM. Is this correct?

Schneider: This is the first military application within AMC to be tested with GATM. I'll rattle off a couple AMC aircraft: There is KC-135, KC-10 has a GATM program, and C5AMP is adding GATM capabilities. But KC-135 is the first program out of AMC to have GATM capabilities installed, and we have completed flight-testing and are going into production. The first aircraft is scheduled to come out of production in the July 2003 time frame. So there are many firsts, and that is a big one.

Yes, the KC-135 aircraft is the workhorse of the USAF when it comes to in-air refueling operations. It is one of several AMC aircraft platforms that are currently targeted for GATM capabilities.

"Without the GATM capabilities, pilots were forced to provide manual position reports via long-range voice communications, which typically involved a third party to relay this information to the appropriate air services center."

— John Schneider, Program Manager, Rockwell Collins

Q: Do you know of any commercial aircraft that are implementing GATM yet?

Schneider: Certainly. When we talk GATM, it means a lot of things. There is the data link side and the navigation side, but from a FANS standpoint (which is on the data link communications side) there are commercial aircraft that utilize data linking for CPDLC. What you are seeing is the merging of the commercial require-

ments with the military requirements so they can all play in the same airspace together. The FANS requirements came out of the commercial industry, and there are civilian requirements. I think the Department of Defense is looking at this and asking, "How do we equip our aircraft to make them compliant with all of these civilian requirements to ensure access to global airspace?"

Many foreign and domestic air carriers are currently equipped with various GATM-related capabilities such as RNP, RVSM and FM-Immune ILS. Additionally, the air cargo industry is using ADS rather extensively.

Q: Do you envision your software or some of the other earlier versions of this software being reused by different aircraft, or is everybody developing their own software?

Schneider: Our customer has expressed a strong desire for not only software reuse, but technology reuse. This generally can come in two different aspects. The first has to do with the ability of our program to leverage software and technologies previously developed elsewhere. This program has been very successful in leveraging commercial off-the-shelf (COTS) products to fulfill GATM requirements. This includes the reuse of the FMF from Rockwell Collins's Business and Regional Systems division and the SATCOM receiver and MMR developed by our Air Transport division.

The second aspect has to do with ability for other programs to leverage the technologies and software that have been developed for the KC-135 GATM program. The cornerstone of the KC-135 GATM upgrade is Rockwell's Flight 2 architecture and is very much predicated on commercial design standards, thereby ensuring an open architecture that is transferable to other platforms.

Q: Do you know if other contractors are also leveraging off of software that is also being developed for this, or does each contractor have to develop their own software to leverage for themselves?

Schneider: I don't know. I can tell you that Rockwell Collins has certainly achieved a great deal of software reuse across programs where the company is contracted to not only develop software but also the target hardware on which the software resides. Our philosophy is to develop software in accordance with widely adopted, commercially available, and endorsed standards. This helps promote the transfer of the software to other targets and its ability to integrate with third-party software. However, for business reasons, many companies would prefer to develop their own software applications as opposed to purchasing a similar application from a competitor. The bottom line is that Rockwell Collins has been able to reuse technology from the KC-135 GATM program on other programs in which we're involved with, and we'd be happy to sell or license these products to other contractors.

"It is really key that you get out in front of these requirements as far as capabilities are concerned ... It could take months or years to add those capabilities to a fleet like KC-135, which is 540 strong."

Q: What happens now as far as the global system?

Schneider: Well, I believe we will continue to see the evolution of GATM requirements, and they will continue to be phased in over time. This places an emphasis on the need for upgrading aircraft with these capabilities in the near term and having a cockpit architecture that has the growth and flexibility to address future requirements when they become mandated.

It is really key that you get out in front of these requirements as far as capabilities are concerned. You don't want to wait until the requirements are so limiting that it then forces you to add capabilities to the aircraft. It could take months or years to add those capabilities to a fleet like KC-135, which is 540 strong. We positioned the aircraft to meet the requirements (the GATM requirements that we know of at this point in time), and we have also positioned the aircraft because of our Flight 2 growth story to meet the requirements as they do evolve.

Q: Getting more specific to your own project, what makes KC-135 GATM architecture an innovative solution?

Schneider: The cornerstone of the GATM upgrade is Rockwell Collins' Flight 2 architecture. Within this architecture resides the Integrated Processing Cabinet (IPC) which as the name implies, is an integrated, modularized avionics cabinet that hosts many of the GATM software applications. The cabinet itself is highly scalable and flexible and the software applications are partitioned so it can accommodate future program requirements while minimizing design and cost impacts. This is extremely important to the program since GATM requirements continue to evolve, and it's likely that there will be system adaptations to meet these requirements.

The architecture was also designed using widely adopted, commercially available and endorsed standards in order to ensure an open systems architecture. This is important in order to allow third-party development, facilitate insertion of new technology, and safeguard against the development of point solutions.

Lastly, the architecture utilizes several high-speed Ethernet interfaces internal and external to the IPC. One of the chief benefits here is the ability to transfer system information at rates that are significantly higher than traditional interfaces such as ARINC-429 or MIL-STD-1553. The end result is a more capable, responsive system.◆

About the Interviewee

John D. Schneider is a Rockwell Collins program manager for the C/KC-135 Global Air Traffic Management (GATM) program. His responsibilities include execution of GATM design, development, and verification activities. Schneider has more than 15 years of engineering and program management experience associated with U.S. Air Force tanker and transport avionics upgrades, including C-17, KC-10 and KC-135 aircraft. He is a native of Joliet, Ill. Visit Rockwell Collins at <www.rockwell collins.com>.

Airport Simulations Using Distributed Computational Resources

William J. McDermott and Dr. David A. Maluf
NASA Ames Research Center

Yuri Gawdiak
NASA Headquarters

Peter B. Tran
QSS Group, Inc.

To increase air transportation throughput without raising accident rates requires a simulation environment of the highest achievable degree of fidelity. Achieving this national airspace-wide simulation environment demands a revolutionary technology leap in information management. In 2001, using simulation software running over a distributed network of computers, NASA researchers developed a working prototype of a virtual airspace. The Virtual National Airspace Simulation prototype utilized available large-scale resources from a computational grid to attack the problem of improving air transportation safety. It modeled daily flight operations at Atlanta's Hartsfield International Airport by integrating measured operational and simulation data on up to 2,000 flights. By identifying precursors to component failure, this nationwide simulation environment supports the development of strategies for improving aviation safety.

A goal of NASA and the Federal Aviation Administration (FAA) is to develop technologies that contribute to a significant reduction in aviation accidents in the next five to 10 years [1]. The U.S. national airspace is a large and complex system that is defined by the interaction of a large number of entities. In an air transportation system as geographically large as that of the United States, one of the most difficult challenges is transforming massive quantities of highly complex ever-changing data on airport terminal operations into knowledge. The Virtual National Airspace Simulation (VNAS) represented in Figure 1 illustrates this.

The challenge is the 10,000 to 15,000 aircraft in the air at any one time, represented by objects inside the globe in Figure 1. Organizational and aircraft component simulators and a network of computers – represented by models, boxes, and connecting lines in Figure 1 – make up a VNAS. The VNAS application is a suite of components or middleware that expands the scope of airport/air traffic simulation to include whole aircraft modeling [2]. It does this by automating the assignment of large-scale simulation workloads to computers distributed across the Internet, providing researchers in the air transportation community with low-impact access to additional computational resources.

The Simulation Concept

U.S. air carriers account for approximately 50,000 takeoffs and landings each day. To perform an airspace-wide simulation of six sub-assemblies per aircraft on a single day would require 300,000 simulations, generating gigabytes of data in the process. The numbers would be much larger if human and organizational models, such as pilots, air traffic controllers, and airline dispatch were added.

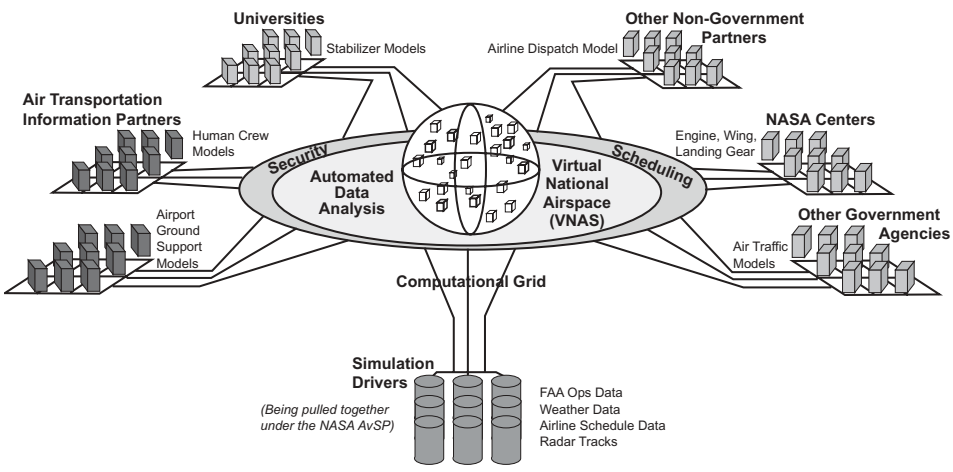
Researchers might want to run simulations with the large amount of air traffic monitoring data that are available. To process this much data they would have to expend significant computational resources. Frequently they do not have sufficient computing power for this level of processing.

> *"Technological progress that enables the creation of large-scale computational grids now makes it possible to transparently assign large-scale scientific workloads to a network of computers distributed across the country."*

Technological progress that enables the creation of large-scale computational grids now makes it possible to transparently assign large-scale scientific workloads to a network of computers distributed across the country. The VNAS is one such concept that mirrors that of SETI@Home, which accomplishes its computational workload by automatically selecting available computer resources connected to the Internet. It then uses these spare central processing unit (CPU) cycles in a search of radio telescope data.

In a similar fashion, the VNAS locates available resources from a network of distributed computers and assigns large-scale scientific workloads to them. Tapping into unused cycles allows researchers who are studying complex operational environments access to significantly more computational power than the resources normally available to the individual effort or group. They can then use these resources to drive multi-discipline simulations with the huge amount of air transportation

Figure 1: *VNAS Structure*



Altitude (ft)	High Speed RPM	Compressor Temp. In (° F)	Compressor Temp. Out (° F)	Thrust (lb)
2,000	8,055	326	855	50,879
2,000	8,057	326	856	51,008
2,100	8,058	326	856	51,082
2,100	8,062	327	857	51,377
2,200	8,063	327	858	51,482
2,300	8,065	327	858	51,571
2,400	8,065	328	858	51,612
2,600	8,063	327	858	51,456
2,700	8,064	327	858	51,468
2,900	8,065	327	858	51,346

Table 1: *Simulation Data Produced by Engine Simulator*

monitoring data that are available.

In 2001, NASA researchers developed a VNAS prototype to demonstrate the concept of complex and computationally intensive integration using distributed computer resources. With this demonstration, NASA researchers also illustrated the technical feasibility of integrating architecture, concepts, and technology covered in this article with a network of computers.

Prototype

The VNAS must provide the underlying infrastructure to support whole aircraft modeling. To achieve this, systems that simulate the operation of key aircraft sub-assemblies such as jet engines are used to provide risk assessments and performance parameters of incoming and outgoing flights from high-density airports.

To produce risk assessment, systems have to process large amounts of input data and return output data to requestors who may be located across the country. A typical request may involve processing flight operations data about a particular airport for multiple days. After simulation and performance parameters have been generated, output data in graphical or tabular form is sent to the user. The operational data, software simulators, and the user interface may be on different computers.

The initial prototype of a national airspace simulation runs on computers making up a VNAS grid. Each night operational data from up to 2,000 flights can be batch processed by three aircraft component simulators running on these machines. When a user makes a request for simulation services, the VNAS system dispatches the work and manages distribution of input and output data. On remote computers, the Numerical Propulsion System Simulation (NPSS), an engine simulation developed by the NASA Glenn Research Center [3]; Wing Sim, a wing simulation application developed by researchers at the NASA Ames Research Center [4]; and a Boeing 737 landing gear simulation process flight data. During this process, they produce parameters reflecting performance of key aircraft sub-assemblies.

System Elements

Traditionally, taking advantage of distributed large-scale computational resources requires detailed, specific information about computers. Researchers have to know the names of hosts and manually submit and track individual jobs. The VNAS changes the user's view from numerous manually intensive steps to a single request.

The VNAS prototype consists of two major parts:

- Intelligent Information Management Node, controlling batch execution of distributed simulations and data integration.
- VNAS grid computers running NPSS, Wing Sim, and 737 landing gear applications at three distributed sites across the United States.

Domain experts plug in models and simulations that are integral parts of the prototype, incorporating them into a model of flight operations at Atlanta's Hartsfield International Airport. In a distributed environment such as the VNAS, however, data, machines, and people are located in different places. Research teams that are developing and maintaining simulators used in the prototype are located in California, Ohio, and Virginia. A whole aircraft simulation comprised of multidisciplinary simulations requires bringing together applications and data that are developed by these different teams. This is achieved by regulating simulations and managing data from a central site, the Intelligent Information Management Node.

Intelligent Information Management Node

The NASA Ames Research Center has expertise in information technology and provides the Intelligent Information Management Node. It is a central executive, providing overall supervision of automated batch processing. It distributes large amounts of data between central and remote sites. It also schedules preprocessing steps on a local host and execution of engine, wing, and landing gear simulations on grid computers.

Simulation Applications and VNAS Grid Computers

Engine Simulation: Engine simulation is provided by the NASA Glenn NPSS. The generic turbofan engine model consists of components of the inlet-compressor-turbine chain and flight characteristics. The input data required by NPSS are altitude, temperature, barometric pressure, and Mach number. Inlet and output temperatures and pressures of compressor and turbine are examples of computed simulation parameters. Component revolution is an example of a category of risk assessment measurement that could be used to improve engine safety.

The Intelligent Information Management Node initiates an engine simulation by calling a client on a grid computer. The client then executes a script, passing parameters to the turbofan simulation program and starting the simulation. A flight's radar tracks are processed individually, producing an output record for each radar track. Sample engine parameters for a departing flight generated by NPSS are provided in Table 1.

Wing Simulation: NASA Ames' Wing Sim provides a simple wing model for one aircraft type that consists of flight conditions and manufacturer's technical specifications. The input data required by Wing Sim are Mach number and altitude. Computed simulation parameters are lift, drag, and side force coefficients, and pitching, rolling, and

yawing moment coefficients. The wing simulator has not been validated.

Clients on grid computers invoke a wing simulation through a shell script that sends several parameters to the Wing Sim executable. A flight's radar tracks are processed individually, producing one output record for each radar track. Data in these records include basic aerodynamic coefficients and forces and moments. Structural stress is an illustration of risk assessment measurement that could improve the safety of wings.

Graphs of sample lift coefficients generated by Wing Sim for arrivals are illustrated in Figure 2. The solid line represents a lift coefficient's baseline curve for simulated arrivals at Hartsfield International Airport. The broken lines represent lift coefficients for two simulated arrivals.

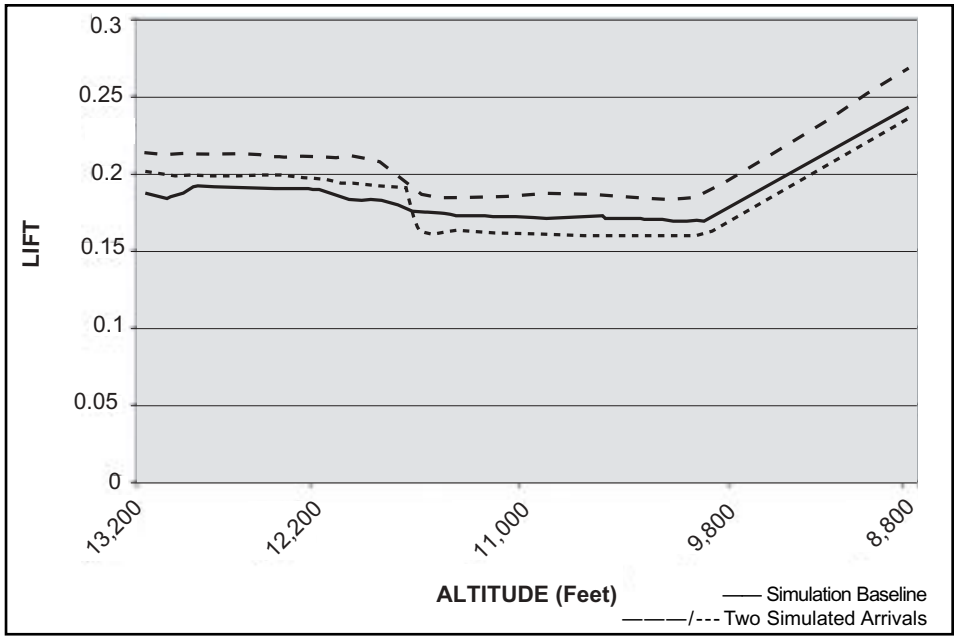


Figure 2: *Simulated Arrival Lift Coefficients Versus Altitude*

Landing Gear Simulation: The NASA Langley Research Center has expertise in airframe systems. A Boeing 737 simulator jointly developed by NASA and Boeing is used to simulate landing gear for arrivals [5]. This simulator contains the capability to auto-land a flight, given runway and aircraft locations and other flight conditions.

This is used as the landing gear model. The input data required by the simulator are aircraft latitude, longitude, speed, weight, and altitude, along with runway threshold altitude, latitude, and longitude. Computed simulation parameters are summed forces and moments for nose and left and right landing-gear subassemblies. Environmental exposure and structural stress on landing-gear components are examples of risk assessment measurements that could improve safety.

VNAS Grid Computers: The VNAS' concept of a computational grid involves interconnecting computers so that they appear to be a single, large virtual computer. To coordinate the various parts of the grid environment, the VNAS grid uses shared authentication, authorization, and auditing systems and directory services provided by Globus [6]. Globus services allow users to submit jobs that run on the spare cycles of computers operating within this network of machines.

For example, in the VNAS prototype each flight simulation may take from one to two minutes to generate engine simulation parameters. On a single grid machine, it will require approximately two days to run engine simulations for 2,000 flights. The same processing can be accomplished overnight by spreading out the workload throughout several grid machines. Grid security services and interconnections between machines support the splitting up of large workloads such as a day's worth of engine simulations onto several grid computers. Grid services are also used to transfer input and output data between the Intelligent Information Management Node and other grid machines.

Lessons Learned

Lessons learned from the VNAS prototype can be divided into two categories:

- Establishing network connections between sites distributed across the country and grid security.
- Transforming measured operational data into a form that is compatible with simulators.

In distributed computing, network connections and grid security are important technical elements. Today, setting up network connections between sites requires person-to-person communication. Direct negotiations with networking officials at each site are required to work out solutions that are consistent with local policies and meet technical requirements.

Other organizations such as NASA's Information Power Grid are working on improving this technical area [7]. As automated means of assigning secure connections are developed, less effort will be required to expand the VNAS prototypes.

Grid security is another area of cutting edge research in which organizations such as the Globus project are making improvements [8]. As mentioned earlier, Globus' security services provide the VNAS prototype with a mechanism for interconnecting remote supercomputers. It eliminates burdensome logons and replaces manually intensive steps with a single transaction.

Another problem is developing an interoperable interface to input data. Radar tracks and weather data are not in units or formats that are compatible with the simulation models. Separate executables are required to calculate and convert values such as latitude, longitude, temperature, and Mach number to satisfy the simulators' requirements.

System Operations

The Intelligent Information Management Node provides overall supervision across automated batch processing of flight data from up to 2,000 daily flights. FAA and other government data collection systems provide measured operational data to the VNAS prototype. The central executive transforms and integrates weather and radar track data. As the next step in the process, the Intelligent Information Management Node disseminates transformed data and invokes remote clients at simulation sites. When driven by this data, subassembly simulators produce simulation parameters that reflect components' operation.

The input data is processed by simulation software running at remote sites. For each flight, the appropriate simulator produces simulation data that reflect the state and performance of a particular aircraft subassembly such as an engine or a wing. When simulations

from multidisciplinary perspectives have finished, the Intelligent Information Management Node manages the retrieval and integration of simulation and monitoring data. When the integration process is complete, the data is stored at the central site for analysis.

The Intelligent Information Management Node also handles interactive simulation requests made through a Graphical User Interface (GUI). Monitoring and simulation data can be viewed via a visualization tool provided by the GUI. As an alternative, data can be downloaded to a user's computer where it can be trended and analyzed for risk exposure.

What Can Be Done With Whole Aircraft, Multidisciplinary Simulations?

The VNAS prototypes will support improvements in the design process and reductions in operational costs. Airport-wide aircraft simulations using distributed resources can be applied in three areas: engineering design process, airline operations, and airport/air traffic practices and procedures.

Engineering Design Process

Multidisciplinary airport simulations can be inserted at the front end of the engineering design process. Simulations of interdependent components can provide airframe manufacturers with risk exposure measurements for new designs or modification of existing ones. This early understanding of a new design or change can be fed back into the process, reducing overall design time.

Airline Operations

Whole aircraft simulations can be used by airlines to assess the impact of current or proposed policies and procedures on operations and maintenance. Insight from subassembly simulations of engines can lead to condition-based maintenance and more optimal scheduling of repairs. For example, use of reverse thrusters while landing an aircraft directly influences incidences of foreign object ingestion, a primary cause of engine wear. Feedback from airlines' maintenance staff indicates that they are especially interested in engine simulations that include foreign object ingestion.

Airport/Air Traffic Practices and Procedures

Airport flight simulations that involve whole aircraft models, including noise and emissions provide a more complete picture of operational changes before they are made. Multiple simulations across a range of conditions can provide insight into possible safety and cost issues. This knowledge can then be used in making decisions on changes to airport and air traffic policy and procedures.

Future Research

Two important future research areas are safety and homeland security. A continuous real-time, national airspace, system-risk exposure evaluation is crucial to measuring security risk and evaluating new concepts for improvement of safety and security.

"Simulations of interdependent components can provide airframe manufacturers with risk exposure measurements for new designs or modification of existing ones."

The NASA research team will continue to work with leaders in industry and government who are actively engaged in the process of developing standards for computational grids.

Conclusion

For the national airspace to increase throughput of air transportation while retaining a low accident rate requires a nationwide simulation environment that has the highest achievable degree of fidelity. Technological progress that is enabling creation of large-scale computational grids now makes it possible to bring together data and applications and assign large-scale scientific workloads to a network of computers distributed across the country.

The VNAS is a software platform that is optimized for running computing applications in a distributed manner. It has an infrastructure that consists of a distributed network of computers connected through secure, high-speed links. Collaborative computing allows a suite of tools to direct the workload to the best available network and hardware topology to meet demands. By dynamically distributing the processing load for simulation to computers with spare capacity, it provides access to significantly more computational power than the resources normally available to the individual effort.

With this approach, research teams that do not have enough in-house capacity have access to large-scale computing power for tasks such as airport simulations that include whole aircraft modeling. Large-scale airport simulations can improve the engineering design process, reduce operations costs, and provide a basis for making decisions on airport/air traffic policy and procedural changes.◆

Collaboration

The authors would like to hear from people who are interested in sharing ideas on the concepts, architecture, and technology discussed in this article.

References

1. Goldin, Daniel S. Aeronautics and Space Transportation Technology: Three Pillars for Success. Washington, D.C.: NASA's Aerospace Technology Enterprise, Mar. 1977 <www.aero-space.nasa.gov>.
2. NASA. "Information Technology Base Program, Intelligent System Controls and Operations Project." Data Sharing FY00-FY01 Task Plan, 29 May 2001: 15-20.
3. Follen, G., A. Evans, C. Naiman, I. Lopez. Numerical Propulsion System Simulation. 98-3113. Washington, D.C.: American Institute of Aeronautics and Astronautics, July 1998.
4. Bardina, J., W. McDermott, et al. "Integrated Airplane Health Management System." First Joint Army Navy NASA Air Force Modeling and Simulation Subcommittee, Nov. 2000: 4-6.
5. Wallace, Lane E. Airborne Trailblazer: Two Decades With NASA Langley's 737 Flying Laboratories. Langley Research Center: NASA: Chap. 6:3 <http://oea.larc.nasa.gov/trailblazer/SP-4216/chapter6/ch6-3.html>.
6. Foster, I., and C. Kesselman. "Globus: A Metacomputing Infrastructure Toolkit." International Journal of Supercomputing Applications 11.2 (1997): 115-128.
7. NASA's Information Power Grid <www.ipg.nasa.gov>.
8. The Globus Project "Computational Grids." <www. globus.org>.

About the Authors

William J. McDermott is product manager and a software engineer in the Computational Sciences Division at NASA's Ames Research Center. He is responsible for product management of a software tool that performs information integration. Previously at NASA, McDermott managed a project for three years as project lead on an L1 milestone for the Information Technology Base Level Data Sharing Project. He has also developed software for use in a number of research projects in the aerospace domain. McDermott has a master's degree from California State University, San Francisco.

NASA Ames Research Center
IC, Mail Stop 269-4
Moffett Field, CA 94035-1000
Phone: (650) 604-5650
Fax: (650) 604-4036
E-mail: william.j.mcdermott @nasa.gov

David A. Maluf, Ph.D., is a senior scientist, the Engineering Information Management element manager, and chief information officer for Engineering for Complex Systems at NASA Ames Research Center. Maluf manages from $2 million to $4 million annually and supports national-scale projects for the Federal Aviation Administration. Previously, he taught system engineering and control at McGill University and information management and databases at Stanford University. He has published more than 50 articles in industry journals and conference proceedings. Maluf has a master's degree and a doctorate in electrical engineering from McGill University and postdoctoral work from Stanford University.

NASA Ames Research Center
IC, Mail Stop 269-4
Moffett Field, CA 94035-1000
Phone: (650) 604-0611
Fax: (650) 604-4036
E-mail: maluf@email.arc.nasa. gov

Yuri Gawdiak is program manager of Engineering for Complex Systems Program at NASA headquarters in Washington, D.C. Gawdiak is responsible for strategic planning and implementing NASA's new initiative in Engineering for Complex Systems, and also for briefings to the NASA administrator, the Office of Management and Budget, and other government organizations. Previously he was principal investigator for the personal satellite assistant and principal investigator for the Wireless Network Experiment on STS-76/Mir 21 at NASA's Ames Research Center in Moffett Field, Calif. Gawdiak has a Bachelor of Science in information systems from Carnegie Mellon University.

NASA Headquarters
Code R
Room 6K17
Washington, DC 20546
E-mail: ygawdiaki@hq.nasa.gov

Peter B. Tran is a research and development computer scientist at QSS Group, Inc., and is a member of the Aerospace ExtraNet Intelligent Information Integration Group in the Computational Sciences Division at NASA Ames Research Center in Moffett Field, Calif. Previously he worked as a consultant, architect, and software engineer at several companies, including BEA Systems, XUMA, Computer Sciences Corporation, and Recom Technologies, emphasizing on distributed computing systems, Web-based technologies, and information management. Tran has a degree in electrical engineering from the University of California.

NASA Ames Research Center
IC, Mail Stop 269-4
Moffett Field, CA 94035-1000
Phone: (650) 604-4531
Fax: (650) 604-4036
E-mail: pbtran@mail.arc.nasa.gov

COMING EVENTS

June 29-July 3
INCOSE 2003
Washington, D.C.
www.incose.org/symp2003

July 14-17
JAWS S3 Symposium
Monterey, CA
www.usasymposium.com

July 15-18
Practical Implementation of Software Configuration Management
San Diego, CA
www.stitraining.com

August 18-21
2nd Annual C4ISR Summit
Danvers, MA
www.paulrevereafa.horizons.com

September 8-12
International Conference on Practical Testing Technique
Minneapolis, MN
www.psqtconference.com

September 14-19
International Function Point Users Group Annual Conference
Scottsdale, AZ
www.ifpug,org

September 22-25
AUTOTESTCON 2003
Anaheim, CA
www.autotestcon.com

October 15-18
Diversity in Computing Conference
Houston, TX
www.ncsa.uiuc.edu

April 19-22, 2004
Software Technology Conference 2004

STC

Salt Lake City, UT
www.stc-online.org

SAASM and Direct P(Y) Signal Acquisition©

Steve Callaghan
Spirent Federal Systems

Hugo Fruehauf
Zyfer, Inc.

With the clock running out on a deadline for installing new generation global positioning system (GPS) security components on military platforms, two key contributors to GPS encryption technology describe how the Selective Availability Anti-Spoofing Module enables direct acquisition of the P(Y)-code and the benefits that capability brings to military and civil users alike.

Extensive field experience and technology advances have combined to bring new levels of sophistication to use of the Global Positioning System (GPS) Precise Positioning Service (PPS). The Selective Availability Anti-Spoofing Module (SAASM), a new GPS receiver design currently being incorporated into military and agency user equipment, promises a more robust operational capability as a result of advances in cryptography, *keying* techniques, and direct signal acquisition of the P(Y) code [Precision Code (GPS; encrypted Y code)]. These will alleviate the security risks and logistics faced by military users as well as eliminate the dependence on open coarse-acquisition (C/A) code for obtaining initial access to the P(Y) code itself.

This article will discuss some of the key technology innovations behind SAASM and its implications for operational use of the PPS, particularly in the SAASM's application to time and frequency generation and synchronization for communications systems and command/control terminals.

The Need for SAASM

Civil use of the Standard Positioning Service (SPS), based on the C/A code at the L1 frequency, has produced a huge international market in which millions of low-cost commercial receivers have already been sold for civil navigation and timing applications. This global dispersion of GPS technology, however, means that some of these receivers are also now in the hands of current and potential adversaries of the United States and their allies.

Today, anyone with a C/A-code receiver can navigate with at least 10-meter accuracy most of the time and synchronize to Coordinated Universal Time (UTC) within better than 100 nanoseconds. This proliferation of commercial GPS receivers poses a major dilemma: How to protect U.S. and allied forces from hostile use of the civil signal during critical military operations while sustaining operation of the worldwide infrastructures that have been built on civil GPS such as communication networks, surveying, positioning, and civil aviation. Essentially, the problem revolves around methods for denying use of the open SPS to adversaries while sustaining authorized user access to the encrypted PPS.

Military planners have done a very good job thinking their way through this scenario and have improvised clever ways to solve the problem. Until recently, using GPS called for making the *in-the-clear* civil signal available to all users, but not at full capability. During certain military operations, the C/A-code signal could be degraded even more, a technique called selective availability, or SA.

However, a fundamental change has taken place in the political context in which military leaders and GPS users operate – from global strategic conflict to tactical, localized warfare – and in the accompanying implications for user equipment design.

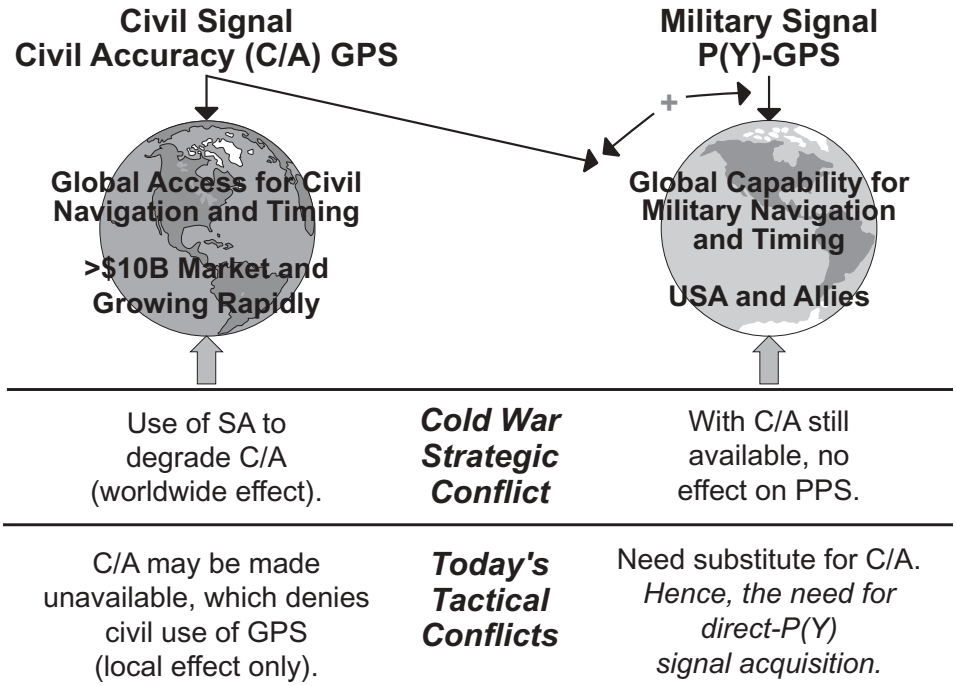
The Elimination of SA

The U.S. Air Force's satellite controllers can set the navigation and timing accuracy of the broadcast GPS signal to any level desired. Beginning in the early 1990s, the controllers intentionally degraded the civil C/A-code signal in GPS satellite transmissions to a horizontal positioning accuracy of about 100 meters, making the related vertical accuracy about 150 meters.

In May 2000, however, SA was turned off. This availability of the full-capability civil signal is the result of the new philosophy from U.S. military planners – to provide full civil accuracy, even with future enhancements and augmentations, while retaining the ability to locally deny the civil C/A signal in times of conflict.

This shift in thinking is actually quite profound. Previously, U.S. military planners relied on SA to make the civil signal unusable in case of a conflict, but the effect of SA cannot be applied regional-

Figure 1: *The New Warfare Realities*



ly and thus is worldwide in scope. Of course, during the Cold War, with its potential for strategic and global conflict, this seemed a reasonable approach. Today, however, with GPS integrated into almost every corner of our lives, the sweeping effects of SA would prove undesirable because they would be felt around the world. Consequently, the new scenario to deny the civil signal locally is very desirable, because it affects only a targeted region. The issues with strategic and tactical warfare scenarios are illustrated in Figure 1.

The Role of SAASM

Local denial of C/A instead of implementing SA has a drawback, however, and this is where one of the SAASM functionalities comes in: direct-P(Y) signal acquisition. The new warfighting environment requires authorized users to be equipped with receivers that allow them to continue using GPS signals while the *bad guys* cannot.

Traditionally, P(Y) code receivers need to initially access the C/A code transmitted by satellites, which repeats its pseudorandom noise (PRN) sequence every millisecond. This is needed to help acquire the encrypted military signal, which has a significantly longer PRN sequence. Use of C/A code enables the PPS receivers to obtain an accurate *time-tick* and with the transmitted hand-over word (HOW), enables alignment with the encrypted P(Y)-code (assuming the receiver has been crypto-keyed).

In the conventional SA signal-degradation scenario the civil signal is still present and, distorted as it may be, the PPS receiver can still use it to initialize. In a theater of operations in which C/A code is denied, however, a SAASM receiver with direct P(Y) code acquisition is the only practical option for continued use of GPS. A less desirable alternative is to have a precise (atomic) cesium clock in the user equipment that provides the ability to synchronize with the P(Y) code, an option not practically available to most users for various reasons, including cost, size, and weight disadvantages. We will discuss the other SAASM receiver functionalities next and return to a more detailed discussion of direct-P(Y) later.

Fielding SAASM

Most observers acknowledge that the military establishment as a whole lags far behind the commercial industry in the availability of state-of-the-art GPS receivers. Of course, many soldiers have commercial receivers, but these do not substitute for PPS receivers. The fielding of military PPS receivers has improved recently, but equipping of U.S. and allied military forces with the new SAASM hardware needs to be expedited for reasons that will become obvious in the course of this article.

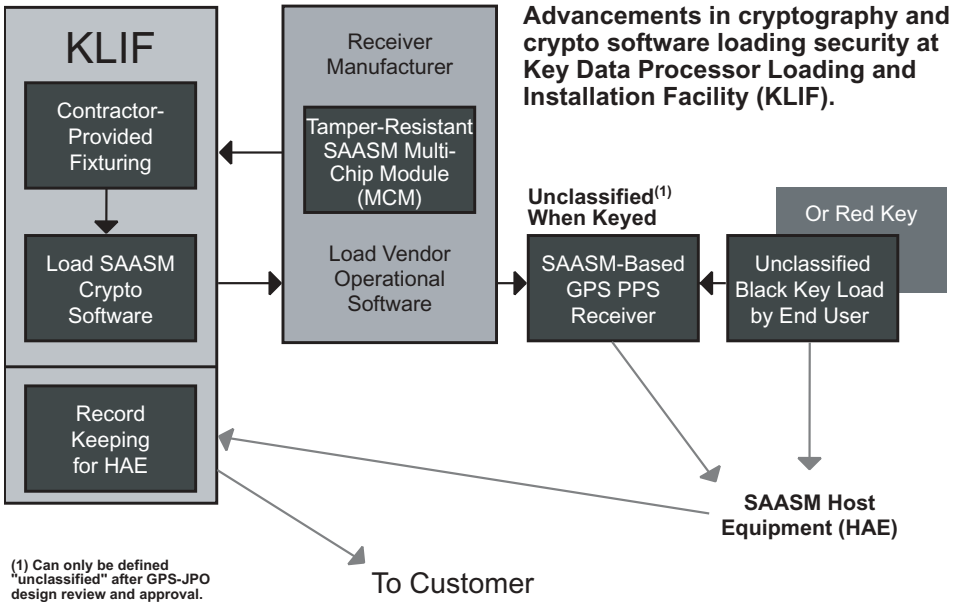


Figure 2: *Black-Key Software Loading Process*

> *"The new warfighting environment requires authorized users to be equipped with receivers that allow them to continue using GPS signals while the bad guys cannot."*

The logistically intensive nature of current-technology PPS hardware has slowed the distribution of equipment. Classification considerations surrounding distribution, use, and disposal of *crypto keys* as well as issues involving hardware, whether keyed or not, have contributed to this situation. If a current-technology PPS receiver falls into the wrong hands, key security may be compromised for a time, and long-range effects will be felt after the hardware is analyzed by a foe. No doubt, this fact has contributed to the phenomenon of PPS hardware reaching higher-ranking military officers first rather than combatants in the field.

Although SAASM is mostly understood as the new military GPS navigation receiver technology, it also will provide less well-known benefits for communications, time/frequency synchronization, and command/control terminals. Before exploring these benefits, it will serve us well to first understand the overall SAASM infrastructure.

The Security Boundary

SAASM inventors have come a long way toward making PPS receiver hardware more user-friendly and securely deployable. Having created a tamper-resistant security module for the most sensitive signal processing and cryptography functions of the receiver provides two important security improvements.

First, the software is very carefully controlled. As a matter of fact, the Key Data Processor (KDP) Loading and Installation Facility (KLIF) is the only place where the crypto software can be loaded. All SAASM receiver manufacturers must cycle their hardware through the KLIF. This so-called black-key software loading process is shown in Figure 2. Second, the tamper-resistant module provides physical security, significantly reducing the risk of compromise should the receiver fall into enemy hands. Figure 3 (see page 14) shows a typical SAASM receiver architecture with its tamper-resistant security module and the direct-P(Y)-code parallel correlator.

When a receiver is built into Host Application Equipment (HAE), the KLIF again enters the picture to reregister the final destination of the SAASM receiver hardware. Although the build-flow of the receiver is more complicated

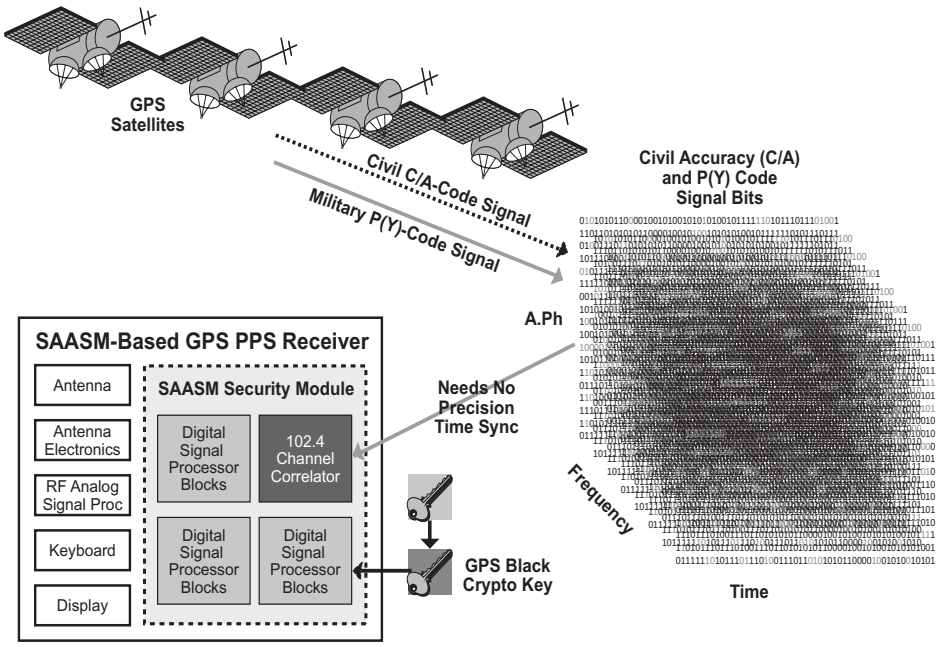


Figure 3: *Typical SAASM Receiver Architecture*

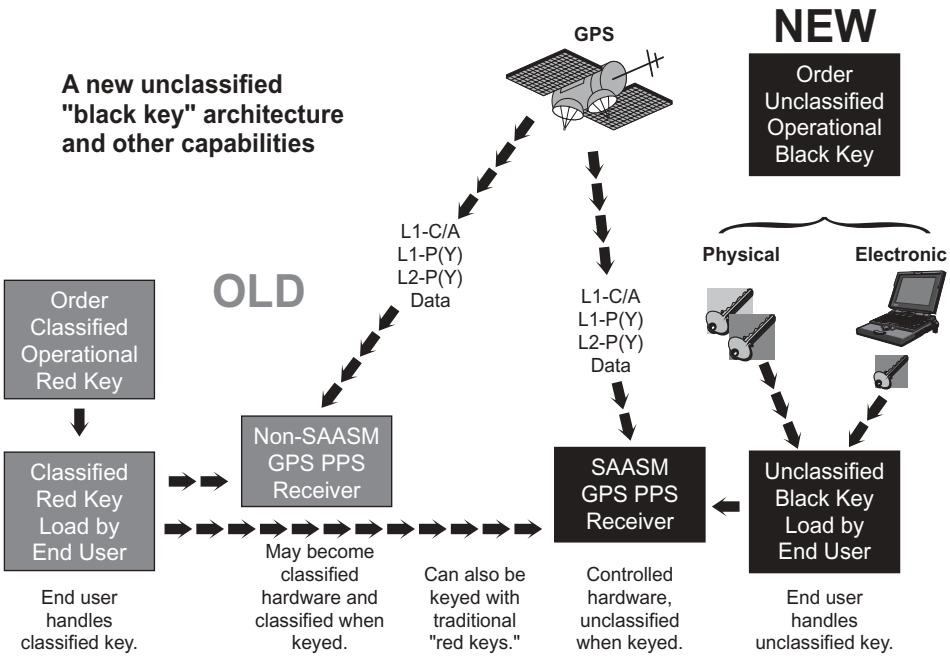
for the manufacturer as a result of the KLIF, the keying is simpler for the user and the hardware is unclassified, assuming that the HAE has been certified by the GPS Joint Program Office. The increased manufacturing complexity of the SAASM receiver comes from the fact that the receiver must be built in two sections, one being the security module and the other the motherboard to which the security module is attached after the KLIF software loading cycle.

The Black-Key Infrastructure

In addition to the security module and the secure software loading process, the keying architecture is being changed from a classified *red-key* infrastructure to an unclassified black-key approach. The current red keys require physical transfer of certain key and key elements to the user by secure means. This is generally called a *symmetric* or secret key architecture.

The symmetric approach creates a host of logistic issues, not the least of which are distribution, control, storage, and disposal of keys and key material. The SAASM black-key architecture on the other hand combines two cryptography methods – the symmetric key structure and what is called an *asymmetric key*.

Figure 4: *Old Versus New Black-Key Keying Process*



The asymmetric key technique has long been the basis for the public key infrastructure (PKI). The public key of a person or agency in the public key database is combined with a private key known only by its holder. The combined, mathematically related keys encrypt and decrypt information transferred cryptographically from point A to point B without keys being transferred in the process.

To obtain a maximum level of security and infrastructure synergism, SAASM combines the best of both techniques: It uses asymmetric key cryptography to securely transfer the symmetric key to the PPS user in an electronic fashion.

Most importantly, however, and contrary to the current PPS structure, the black key physically transferred is unclassified because the key itself is encrypted. This old versus new keying process is shown in Figure 4.

In addition to the black-key keying process, the SAASM receiver has been outfitted with other sophisticated capabilities to further enhance its operational usefulness for the PPS user.

Direct P(Y)-Code Signal Acquisition

As mentioned earlier, P(Y)-code receivers have needed to initially access the C/A code in order to obtain an accurate time-tick enabling them to access the much longer P-code.

Until recently, direct acquisition of the military P(Y)-code signal without a very accurate clock was not practical or even possible. However, advances in signal processing speed and micro-miniaturization now allow for massive parallel data processing and bit correlation to compensate for the lack of accurate time. A comparison of the traditional PPS receiver with the SAASM direct P(Y) acquisition receiver is functionally demonstrated in Figure 5.

A key element in direct P(Y) code acquisition is the number of signal correlator channels and processing *bins* available in a receiver to match up locally generated PRN codes with the codes transmitted by the satellites. Figure 6 compares the C/A-code search process, which may employ only a few correlator channels, with the direct P(Y) acquisition process, using massive parallel signal processing with 1,024 or even 2,048 correlator channels searching for a code match. Depending on the number of correlators and the receiver design, the external time reference used to initialize the direct P(Y) SAASM receiver can now be a factor of 10,000 to 10 million less accurate than

before.

This means its UTC time reference can be off as much as ±1 second or so instead of the previous 100 nanoseconds. (Throughout this article, the reference to UTC is done for convenience. There is actually a time difference between UTC and GPS system time. This is due to the fact that UTC is maintained using *Leap-Second* updates, whereas GPS time is pure atomic time. The GPS system tracks leap seconds separately so that users can choose GPS time or UTC. The differences in these time scales are not germane to the discussions here.)

The receiver's P(Y)-code signal-acquisition time, generally referred to as the *time to first fix* (TTFF), is mainly a function of how well the initialization time reference is known and the severity of the jamming environment.

SAASM and Time/Frequency Users

In addition to a host of advantages for military applications in terms of navigation, positioning, and weapons targeting, SAASM brings benefits to the time and frequency synchronization community as well. Civil and P-code-equipped GPS time and frequency systems play a major role in both ground and space-based communications and command/control operations.

Three main categories of GPS-equipped communication terminals exist today.

- **The conventional C/A-only SPS terminal.** When the civil C/A signal is unavailable, this category of GPS-aided terminal goes into so-called *holdover* mode, using its internal oscillators. It eventually goes out of spec or down altogether if the C/A signal is not restored. Unfortunately, this category is by far the most widely deployed terminal for commercial and military applications.
- **The conventional military C/A-P(Y) PPS terminal.** Here, the situation is improved somewhat. If the terminal is operating on the P(Y) signal at the time that a C/A-code signal becomes unavailable, the receiver will stay online. However, if the P(Y)-code signal is interrupted or a power failure occurs, the system cannot reacquire the military P(Y) signal in the absence of C/A.
- **The new SAASM Direct P(Y) PPS terminal.** Not only will this category of terminal stay online without a C/A signal, but it can also start *cold* without it. SAASM goes a long way towards protecting the terminals against hostile jamming and spoofing. In a world facing terrorism threats, military and agency infrastructures should not only adopt SAASM technology, but high-value commercial assets should also become authorized users of SAASM. (*Authorized* refers to users who have government-approved security infrastructures in place and are authorized to receive crypto keys.)

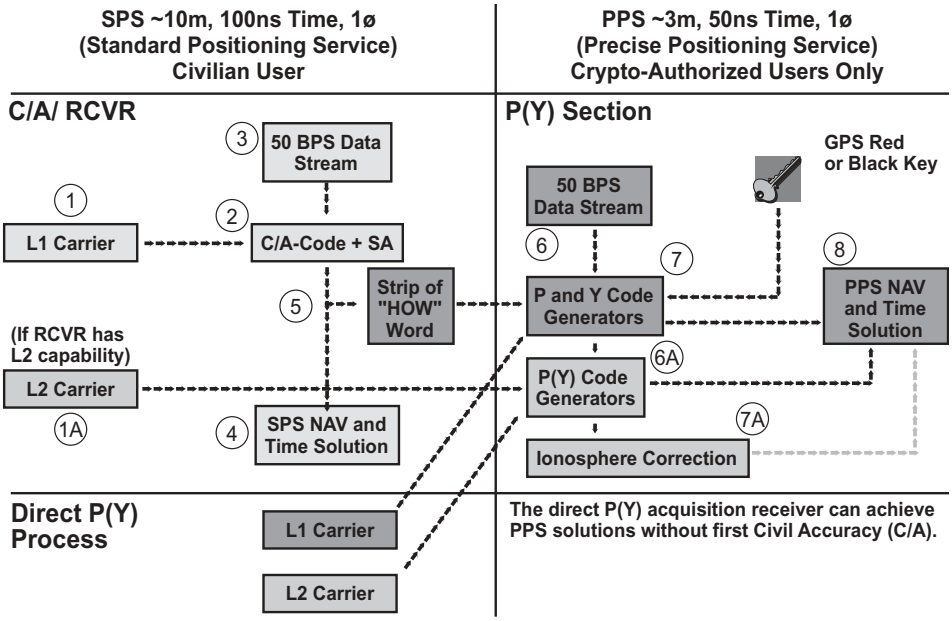


Figure 5: *Traditional PPS Versus SAASM Direct P(Y) Functionality*

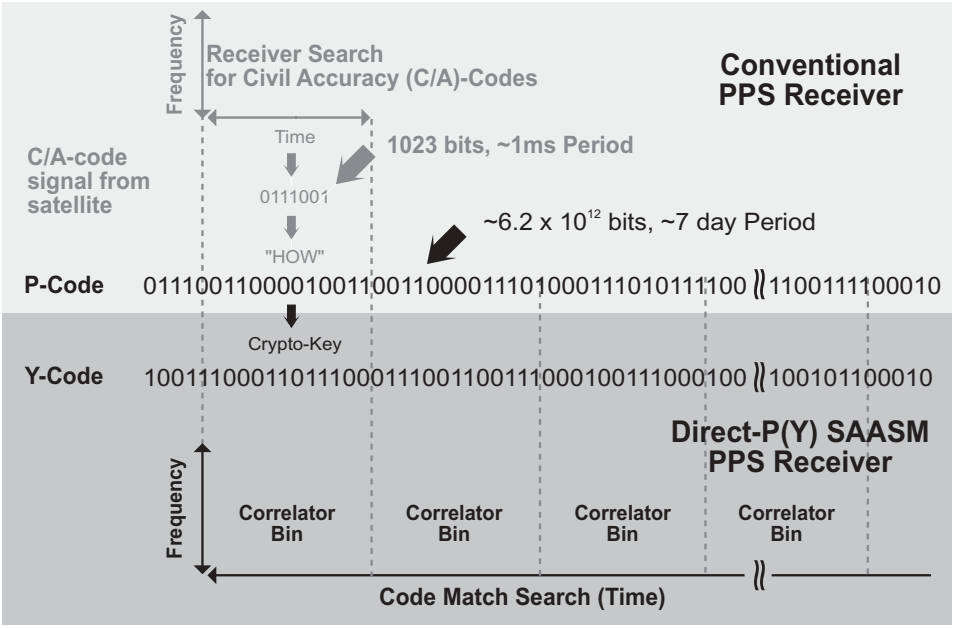
Types of Direct P(Y) SAASM Receivers

Two primary categories of direct P(Y) SAASM receivers exist, each with different operational requirements and values of initialization parameters – the weapons navigation/targeting receiver, such as might be incorporated onto a rocket or artillery projectile, and the communications time/frequency receiver.

The weapons navigation/targeting receiver must have the capability to acquire the P(Y) signal very rapidly in the absence of C/A, because the weapon's flight time may only be a minute or so. To facilitate rapid acquisition, the GPS host platform provides the weapon's receiver with very accurate initialization parameters, such as projectile position as it exits the launch tube, and GPS time.

Although the GPS host platform can provide the weapon to be launched with a time accurate to better than 100 nanoseconds, the accuracy is subsequently degraded by the effects of the launch environment on the weapon's GPS

Figure 6: *Conventional Search Versus Massive Parallel Signal Processing*



receiver oscillator. As a result of the requirements and the support available from the GPS host platform, the weapons receiver can deal with a time uncertainty of milliseconds and a position inaccuracy within a few meters. Only several hundred parallel correlator channels are needed to satisfy rapid P(Y)-code acquisition.

In comparison, the communications time/frequency receiver generally does not need to acquire satellite signals as rapidly as its weapons system counterpart, mainly because it is assumed to be stationary or moving not faster than a truck. More importantly, however, it does not have the benefit of a GPS host platform system – in other words, it has to operate on its own. Since acquisition time is generally not a driver, the initialization parameters can be significantly less precise, for example, time uncertainty in the seconds. As a result, this category of receiver is correlator-intensive, requiring at least 1,000 or more correlation channels to handle the relatively large position and time uncertainty.

As discussed earlier, the TTFF is mainly a function of how accurately the initialization parameters can be specified, especially time, which in turn determines the size of the P(Y) signal bit-field to be searched. Initialization data can either be provided automatically, as in the case of the GPS host platform and weapons receiver, or by keypad entry or use of a portable clock as in the case of communications time/frequency receiver.

One additional element is the GPS almanac broadcast in the GPS satellites' navigation message, which plays an important role in the acquisition initialization process. The almanac is a library of satellite information, including estimates of satellite ephemerides (orbital positions) and a host of other parameters needed for the receiver to determine its own position.

The almanac that a receiver has loaded in its memory since the last time it received GPS signals should not be older than a week. Without access to the C/A-code signal, a receiver making a cold start cannot obtain the broadcast ephemerides of the satellites it is attempting to acquire. As a result, the receiver uses a stored almanac or *library* to estimate satellite positions. Because the GPS constellation is relatively stable, a week-old almanac should do the job, but a younger data set will speed up the TTFF process.

For the wristwatch initialization, the receiver will use the latest almanac in its memory – the one loaded during the last time the receiver was on-line. Using a portable clock for initialization brings the added advantage of the latest almanac stored in its memory. Its dataset will likely be only a day or so old, again, as recent as the last time the portable clock was in the standby mode receiving the C/A signal.

The SAASM Mandate

In 1998 the chairman of the Joint Chiefs of Staff issued a SAASM deployment mandate. It requires PPS users to procure SAASM only, use black keys only, and cease fielding non-SAASM GPS equipment after Oct. 1, 2002. This mandate has not changed since then, and waivers must be requested for non-compliance.

Also, The Department of Defense has revised security regulations for builders of host applications equipment. Makers of such equipment must first have a government security structure in place and, additionally, must go through rigorous design reviews of their HAE architecture. A list of authorized SAASM receiver and SAASM HAE developers may be accessed through the GPS Joint Program Office Web site at <http://gps.losangeles.af.mil>.

Conclusion

The SAASM receiver and its direct P(Y)-code acquisition capability will prove to be a powerful tool in the hands of our military and authorized users. What C/A has done for the GPS boom in civil community, SAASM will do for the military user and authorized community. SAASM provides solutions for some very critical operational complexities:

- Depending on the design of the HAE, the equipment fielded will be unclassified, even after keying.
- It makes for a more secure receiver were it to fall into the hands of adversaries determined to compromise our crypto technology secrets and crypto keys.
- The crypto black keys are unclassified and can be distributed in an unclassified manner.
- The receiver can acquire the military crypto signal directly without the aid of the civil C/A-code signal.

As a result, civil and military users can enjoy a symbiotic relationship, allowing full-accuracy civil GPS SPS operations while protecting our military from adversaries using civil GPS in an area of military conflict. The military is on a fast track according to the latest Joint Chiefs of Staff mandate – no non-SAASM-based GPS hardware can be fielded after the year 2002 without a waiver.◆

Original Article

This article was originally published in *GPS World* and is available at <www.gpsworld.com/gpsworld/article/articleDetail.jsp?id=25974&pageID=1>. GPS World is a monthly business-to-business publication focusing on innovations and best practices that provide a competitive edge for the user/developer community employing global positioning and timing technologies.

About the Authors

Steve Callaghan is director of engineering for Spirent Federal Systems. Previously, he served as chief systems engineer and architect for the NAVSTAR GPS selective availability antispoofing module (SAASM) and key data processor program and was responsible for the design of related security algorithms and approval processes. In February 2002, he received a Joint Staff certificate of appreciation for his support of the GPS precise positioning service SAASM security architecture. He has a Bachelor of Science in biomedical and electrical engineering from the University of Southern California.

Hugo Fruehauf is president, chief executive officer, and chief technology officer of Zyfer, Inc., a wholly owned subsidiary of Odetics, Inc. He was the chief engineer for the design and development of the initial Block I GPS satellite system for Rockwell International (now Boeing). Since then, he has focused on GPS applications for communications, time and frequency synchronization, network data security, and tactical weapon systems targeting. While group vice president at Alliant Techsystems, he influenced the development of the first SAASM receiver and the direct-P(Y) code acquisition functionality. He is a graduate of DeVry Institute of Technology in electronic engineering.

Improving Information Management Software System Deployment Practices

Dr. James A. Forbes
Logistics Management Institute

Maj. Kurt Bodiford
U.S. Army

Dr. Emanuel R. Baker
Process Strategies, Inc.

In response to a request by the Program Executive Office for Standard Army Management Information Systems (PEO STAMIS), the Logistics Management Institute assisted in a study to improve the deployment of software-intensive systems. We conducted structured interviews internal to PEO STAMIS and with PEO STAMIS customers to survey current practices. We also surveyed several commercial organizations and identified a number of best practices, 16 of which were applicable to PEO STAMIS. Eight of these practices already existed within the PEO; PEO STAMIS product managers had also created internal best practices well tailored to their environment. The problem was not lack of best practices inside or outside the PEO, but the lack of sharing and replication of best practices across product offices. The methodology developed as part of the study should be of use to other organizations dealing with similar problems.

Responding to a request by the United States Army Program Executive Office for Standard Army Management Information Systems (PEO STAMIS), the Logistics Management Institute (LMI) assisted in a study to improve the deployment of software-intensive information management systems[1]. At the time of the research, PEO STAMIS was responsible for nearly 40 retail information system products for the U.S. Army and other services.

The products spanned a wide range of functionality and geographical distribution both inside and outside the continental United States. Examples of the kinds of systems for which PEO STAMIS was responsible included the Standard Installation/Division Personnel System, Unit Level Logistics System, and the Joint Computer-Aided Acquisition and Logistics System.

The following are two major research outcomes of interest to the general software community:

- Development of a deployment process model applicable to both government and commercial practice.
- Identification of a set of at least very good (if not *best*) deployment practices applicable to both military information systems and the commercial realm.

This article describes the deployment process model and provides the best practices. The full model is available at the CrossTalk Web site <www.stsc.hill.af.mil/crosstalk/2003/06/forbes.html>. We obtained the basic data primarily via structured interviews of PEO STAMIS Program Management Offices, PEO STAMIS customers, and a number of commercial organizations outside of the defense industry. The interview questions that led to the validation of the model constructs and the definition of the best practices are also available at the STSC Web site.

Background

The PEO STAMIS vision was to be the warfighter's choice for leading edge, integrated, global information solutions across the operational spectrum. The perception of the PEO and its customers was that processes within PEO STAMIS for deploying hardware, software, and training – and sustaining them once deployed – were interfering with the realization of the PEO STAMIS vision. Each product manager used product-specific processes for hardware and software fielding, system training, and sustainment. The end result was often customer dissatisfaction – much of which was attributable to inconsistent and sometimes ineffective deployment practices.

"The end result was often customer dissatisfaction – much of which was attributable to inconsistent and sometimes ineffective deployment practices."

The objective of the LMI study was to give the PEO STAMIS several potential strategies that would improve fielding and training, sustainment, customer satisfaction, and reduce life-cycle costs. The LMI was asked to perform five tasks to fulfill its part in the study:

- Survey selected projects to assess current deployment practices.
- Selectively survey user communities to determine their satisfaction with the current practices for transitioning systems to operational use.
- Selectively survey commercial organizations to determine their approach to deploying systems.
- Determine commercial practices that improve usability and reduce time and resources during deployment.
- Determine a set of best practices for deployment and improving usability.

The survey of commercial practices in use by successful companies was considered to be an important element, since customer satisfaction is recognized as essential to their continuing success.

Methodology

To provide a consistent framework against which to compare the various PEO STAMIS offices' and commercial firms' practices, we created a three-stage (initial, intermediate, and advanced) deployment process model. It comprised 16 general areas (such as computer hardware, software, architecture, and training), nine of which are further broken down into sub-areas, comprising a total of 32 categories. Many, but not all, areas have sub-areas. Three levels of ability (initial, intermediate, and advanced) further characterized each area and sub-area. A listing of areas and sub-areas is provided in Table 1 (see page 18). We obtained information using interview questionnaires keyed to the deployment process model.

In our deployment process model, the initial level is characterized by ad hoc practices. Very little planning is done, and situations are addressed as they arise. Also, little or no consideration is given to identifying potential risks and implementing practices to avoid them. The intermediate level is characterized by some degree of planning, although a number of activities are still addressed informally. Organizations functioning at this level in a specific area are getting by, but their

Area	Sub-Area
Computer Hardware	• Hardware Upgrades • Hardware and Software Compatibility • Failed Hardware Component Replacement
Hardware and Software Architecture	• Hardware • Commercial Off-the-Shelf (COTS) Software • Application Software • Architecture Standardization • Form of Architecture
Application Software	• Update Planning • User/Maintainer Impacts
COTS Software	• Evaluation of COTS Software • Assessment of Impact of Changes • User/Maintainer Knowledge
Training	• Planning for Training • Training Delivery • Training Records Database
Installation Policy	• User Installation of Personal Software • Control of Software Used
Interfaces with Other Systems	
Security	
Metrics	
Costs	
Configuration Management	
Quality Assurance	
Deployment/Support Organization	• Experience • Use of Service Level Agreements • Involvement in Development Process
Help Desk	• Initial Deployment and Changes • Integration
Test Bed	• Use of Test Beds • Regression Testing
Documentation Updates	

Table 1: *Process Model Areas and Sub-Areas*

actions are not as effective as they probably could or should be. Detailed planning and risk avoidance characterize the advanced level. An advanced-level organization is focused on functioning as effectively as it can.

We initially populated the deployment process model based on our understanding of what the functional levels would be for each of the areas or sub-areas. We set forth our perception of what practices would exist for each level of the model. We then used the interviews with commercial participants to validate this model. The complete process model, together with the typical practices at each level, is too large to include in this article; however, Table 2 illustrates what a sub-area looks like. The complete model can be viewed at the CrossTalk Web site <www.stsc.hill.af.mil/crosstalk/2003/06/forbes.html>.

Participating companies included a biotech firm, a systems integrator, an oil company, and a major producer of commercial software products. For commercial firms, our interview technique was to ask the respondent one question for each area or sub-area. For each area and each level within the process model, we asked the respondent to describe practices followed by a typical organization within their industry. Our intent was not to make the questions specific to the company, but to have the respondents characterize what they believe the model would look like based on common practices within their segment of the industry. This was done for two reasons:

"One result of this study was the determination of a set of good deployment practices that have been applied not only to military information systems, but also to the commercial world."

- We wanted to validate our model constructs.
- We wanted to ensure the respondent would answer all the questions and not opt out because a response could or would reveal proprietary practices.

Table 2: *Example of the Practices at Each Level*

Area	Sub-Area	Initial	Intermediate	Advanced
Computer Hardware	Hardware and Software Compatibility	Executable software/hardware configuration compatibility is considered only for initial system definition. Little or no planning for hardware upgrades exists. Effects on compatibility usually not assessed when upgrades are installed. Little thought is given to compatibility across a wide area network (WAN).	Executable software/hardware configuration compatibility is considered for initial system definition. Planning is cursory. Effect on compatibility is assessed at installation. Certifies each component separately and individually, but not the entire environment (whole system). Testing is performed at a higher level. There is some understanding that compatibility across a WAN is required, but thorough testing does not occur. Some ad hoc testing would be performed in addition to planned testing. Some incomplete documentation (e.g., test scripts for the new hardware).	Hardware upgrades evaluated for performance impact: • Proposed hardware upgrades are planned in advance and analyzed for impact on performance prior to installation. Components to be installed at a site are tested beforehand for compatibility. Scalability and load tests are performed. Total system is certified: • Proven certification that hardware component and software work together. The whole environment is certified, not just the hardware or the software provided by the vendor. Certification team puts in the time up front to ensure connectivity and compatibility across all parts of a WAN.

Results

The results indicated that the deployment model the LMI constructed reasonably represented the various levels of *maturity* – or capability – indicated by our model. Some changes were made to the model during the interview process. The bulk of these changes resulted from additional characterizations of the levels proposed by the interviewees.

The interview process identified 16 commercial best practices, all of which were applicable to PEO STAMIS. However their relative merit was not clear. As an aid in implementation, and in conjunction with the PEO STAMIS staff, we evaluated the best practices against the factors contained in each of the seven major areas of the deployment model and then integrated the results to create a prioritized list of best practices. (Evaluation was based on the multi-attribute utility method, i.e., we assigned scores to indicate the importance of each practice to each factor.) We also confirmed that eight of these practices already existed within the PEO. However they were not widely shared or replicated from one product to another.

It should also be noted that although all best practices are in use by commercial firms no one firm used them all. In some cases, a given best practice was identified as being used by some of the respondent companies, while others indicated a desire that their organizations use a similar practice. Consequently, one of the results of the study was to develop a list of best deployment practices useful in industry. Table 3 lists these best practices.

Interviews of PEO STAMIS product offices demonstrated that no product was totally situated in the initial, intermediate, or advanced stage – all had a mixture of characteristics from more than one phase. Although there may have been some unintended inflation in our results, intermediate and advanced stages dominated. Of particular note, product managers had created internal best practices well tailored to the PEO STAMIS environment. The problem was not lack of best practices inside or outside the PEO, but the lack of sharing and replication of best practices across product offices.

Recommendations

The LMI recommended that PEO STAMIS implement a process improve-

ment effort that emphasized replication of best practices. We identified and evaluated five potential strategies. We also recommended implementation of a collaborative process improvement strategy that had at its foundation the best practices identified by this study and the deployment process model created by this study. The deployment process model can provide a uniform groundwork for product manager self assessment, an essential element of improvement

A *collaborative* strategy meant its execution included product managers, PEO STAMIS headquarters staff, developers, and users. The product managers were closest to the customers and in the best position to understand real-world problems that needed to be solved. The headquarters, on the other hand, was in the best position to see across products and facilitate replication of best practices. Developers had the best information on functionality embedded in applications. Involvement of user representatives was essential so users could understand what was being attempted, how it was being approached, and how it was expected to effectively address their needs.

We recognized that the PEO could not attempt to fix everything at once; organizations can absorb only so much change at one time, and not all changes are equally beneficial. The working group the LMI supported identified four initiatives that appeared to lend themselves to early implementation and momentum building. These recommendations included best practices that were very comparable to some of the best practices used by commercial organizations:

- Use of one particular product as a pilot vehicle to develop a template for replication of best practices. This product was early in its life cycle and was controlled by one of the PEO STAMIS directorates, minimizing the lateral coordination that would be needed.
- Replication of the Systems Extension and Acceptance Team (SEAT) fielding practice for other products. This was a PEO STAMIS best practice. The SEAT concept is essentially a team that is responsible for planning and implementing the deployment of systems, but was only used for a limited number of systems. Users specifically recommended expanding the use of the SEAT methodology.
- Expanded use of an existing test laboratory for retail-level systems. This is a practice consistent with the use of test beds by commercial organizations to ensure the compatibility of system interfaces. Broader use of this laboratory would facilitate a common approach to testing.
- Replication of the three-tier help-desk architecture vision of the Global Combat Support System-Army across additional products. This architecture had the preferred modern features of an excellent help-desk capability.

Best Practice	General Area	Sub-Area	No. of Companies
An asset management system exists, documenting in detail what hardware and software are deployed, who is using it, and what problems exist in order to know whose hardware to replace. A change control system is utilized with the capability to back out of previous changes, if need be. Testing, staging, and burning in of parts are performed. They collect and use system utilization statistics, do performance monitoring, document process flows, and do capacity planning. A set of tools is utilized (for example, Tivoli or SMS) to keep track of installed base, and to use that information for planning for upgrades, replacements, updates, and revisions.	Computer Hardware	All	3
	Application Software	All	3
	COTS Software	Assessment of Impact of Changes	3
	Installation Policy	All	3
Have a centralized organization with a manager charged with the responsibility for ensuring that architecture is defined in a common way, establishing policies and procedures, and filtering all acquisitions and installation of upgrades, replacements, updates, and revisions, to ensure that the integrity of the standard architecture(s) is maintained. This organization is also responsible for deployment and maintenance.	Hardware and Software Architecture	Architecture Standardization	1
Promulgation of a mission statement concerning architecture: "commonality as possible, and unique as necessary."	Hardware and Software Architecture	Application Software	1
Rotate people from development into maintenance and back again to ensure that developers properly incorporate the needs and concerns of maintenance into the development effort.	Application Software	User/Maintainer Impacts	1
A specialized product usability lab exists comprised of super users to test out changes. Lab emulates or includes all system interfaces (at minimum, 85% - 90% of the interfaces for very complex systems where replication of the total system environment for all applications would be extremely costly).	Interfaces with Other System	N/A	1
Utilize test beds to prove that hardware and software components work together.	Computer Hardware	Hardware and Software Compatibility	2
Support, development, and information technology organizations fall under the same executive management. When organizations are closely aligned, you can have successful customer alliances.	General Recommendation		1
Make the developers of the system be the first user community. This has two effects: (1) it makes the development organization more careful in the development process, since they know they will have to suffer through the initial rollout themselves, and (2) it makes the turnaround time faster for correction of any initial deficiencies.	Deployment/ Support Organization	Involvement in the Development Process	1
Security testing is planned. A developer's identification is never used as part of system testing to log on to the system when testing the security provisions. Full security testing is performed using production identifications. A security group exists and is brought in as part of the test planning process. Planning and results are reviewed and approved.	Security	N/A	1
Automation is used to determine if unauthorized software has been installed on a workstation. Involves census taking at logon, automatic deletion of unauthorized software, and messages to the user that the software has been deleted.	Installation Policy	Control of Software Used	2
A portal exists that everyone on-line has to go through several times per day. Informs people of changes, scheduled outages, bug patches, etc.	General Topic of Communicating Changes	N/A	1
Creation of career paths for help-desk personnel.	Help Desk	Integration	2
Use of standard architectures provides capability to establish better pricing arrangements with vendors.	Hardware and Software Architecture	Architecture Standardization	1
Use of a central organization to evaluate new technology. New technology cannot be introduced into the architecture without their approval.	Hardware and Software Architecture	Architecture Standardization	3
Use of a three-tier help desk. Third tier is organized by line of business (latter aspect was cited by only one organization).	Help Desk	Integration	4
Use of technology to facilitate help-desk functions. Use standard tools for self-help; implement self-help tools and computer recovery tools that provide front-end help to the help desk. Web-based, integrated with call center, interactive Web site to report problems. Integrate asset management tool with help-desk problem reporting.	Help Desk	Integration	2

Table 3: *Commercial Organization Best Practices*

Deployment of operational or production information systems is a process that many organizations do not always perform well, whether or not we are talking about governmental or commercial organizations. Hopefully, such organizations can benefit from the results of this study. We believe the deployment process model and the interview guides – because they were intentionally constructed to span government and commercial practices rather than those specifically within the sphere of PEO STAMIS – can be valuable to enterprises other than PEO STAMIS. The same is true of the best practices we identified: One result of this study was the determination of a set of good deployment practices that have been applied not only to military information systems, but also to the commercial world.◆

Note

1. PEO STAMIS has since been re-designated as the United States Army Program Executive Office for Enterprise Information Systems. In this article, we retain the designation in use at the time of the study.

On-Line Article

The on-line version of this article also contains a table of the complete Deployment Process Maturity Model and an Interview Questions/Response Form.

About the Authors

James A. Forbes, Ph.D., is a senior research fellow at the Logistics Management Institute. He is a certified professional logistician with more than 25 years of experience analyzing policy, technology, acquisition programs, and total ownership costs; researching operations; and supervising operational logistics. He has extensive experience assessing the effects of technology on organizations and managing technology-driven change. Forbes has been a principal researcher in a number of studies of functional strategies for logistics-related information systems. He is also leading projects for managing data and knowledge.

Logistics Management Institute
2000 Corporate Ridge
McLean, VA 22102-7805
Phone: (703) 917-7572
Fax: (703) 917-7518
E-mail: jforbes@lmi.org

Maj. Kurt Bodiford is a career Army officer. He is a graduate of the United States Military Academy and is concluding graduate studies at Johns-Hopkins University. Bodiford's experience as an operations research/systems analyst was of significant value during his one-year fellowship at the Logistics Management Institute where he was a major contributor to the study described in this article. He is currently serving on the Department of the Army Staff in the Joint Requirements and Assessments Division.

US Army G-8
Deputy Chief of Staff for Programs
JROC Management Office
ATTN: MAJ Kurt Bodiford
DAPR-RMI-SJ
700 Army Pentagon
Washington, DC 20310
Phone: (703) 692-4490
Fax: (703) 692-5478
E-mail: kurt.bodiford@hqda.army.mil

Emanuel R. Baker, Ph.D., is a principal and co-founder of Process Strategies, Inc., a Los Angeles- and Maine-based software process management consulting firm. He has 30 years of software development, management, and consulting experience. His areas of expertise include software process assessments, software systems engineering, software configuration management, software quality assurance, software test, and requirements management, as well as training in these disciplines. Baker is a SEI-authorized lead assessor for both CBA-IPI and SCAMPI℠ assessment methodologies. He is co-author of "Software Process Quality: Management and Control."

Process Strategies, Inc.
10219 Briarwood Drive
Los Angeles, CA 90077
Phone: (310) 278-0856
Fax: (310) 550-1992
E-mail: erbaker@process-strategies.com

WEB SITES

GPS World

www.gpsworld.com

GPS World is an international, business-to-business monthly journal that features news and applications of the global positioning system (GPS), the developing Galileo system, Glonass, and related technologies. GPS World provides news reporting and analysis of business and technology developments, marketing trends, and policy issues affecting the GPS community. Its articles are targeted to design engineers, systems integrators, original equipment manufacturers, and those experienced in high-precision GPS applications. The site features current and past issues, descriptions of new products and services, and connections to other GPS-related Web sites.

ISO

www.iso.org

The International Organization for Standardization (ISO) is a worldwide federation of national standards bodies from more than 140 countries, one from each country. The ISO promotes the development of standardization and related activities in the world with a view to facilitating the international exchange of goods and services, and develops cooperation in the spheres of intellectual, scientific, technological and economic activity. It is the source of ISO 9000 and more than 13,700 international standards.

Defense Modeling and Simulation Office

www.dmso.mil/public

The Defense Modeling and Simulation Office (DMSO) is the catalyst organization for Department of Defense (DoD) modeling and simulation and ensures that modeling and simulation technology development is consistent with other related initiatives. The DMSO encourages cooperation, synergism, and cost-effectiveness among the modeling and simulation activities of the DoD components. The DMSO supports the warfighter by leading a defense-wide team in fostering the interoperability, reuse, and affordability of modeling and simulation and the responsive application of these tools to provide revolutionary warfighting capabilities and improve aspects of DoD operations.

autoid.org

www.autoid.org

The goal of autoid.org is to keep end users, organizations, and companies in the automatic identification and data collection industry up to date with essential standards activities and technical information that can effect business decisions. The site features new documents and news sections with information from and links to the American National Standards Institute, ISO, International Electrotechnical Commission, International Committee for Information Technology Standards, industry links, presentations, standards, and more.

Pilot Testing Innovative Auto ID Technologies

James E. Bagley
Code Corporation

The Flight Hardware Logistics Group at the Jet Propulsion Laboratory in Pasadena, Calif., has implemented a variety of innovative automatic identification technologies. By incorporating small high-density codes, local data routers, and cordless readers, the group aims to drastically improve inventory management and tracking.

It's all about keeping track of things. Driven by the need to keep track of a myriad of items ranging from chairs and desks to spacecraft payloads, the government-industry partnership in the aerospace field has led the way in implementing new automatic identification (Auto ID) technologies.

The Flight Hardware Logistics Program (FHLP) at the Jet Propulsion Laboratory in Pasadena, Calif., is currently developing and piloting several new technologies to upgrade their inventory management and tracking systems. The goal of this pilot program is to improve the configuration management process. The scope of the pilot program includes the following:

- Identify parts through labeling and permanent marking.
- Upgrade to smaller, two-dimensional symbol.
- Upgrade reader hardware – wireless.
- Improve database connectivity internally and with vendors, and subcontractors.

Fortunately, the aerospace industry, the Auto ID industry (makers of bar code equipment and the like, including radio frequency data transmission and identification equipment), and vendors from all product-related areas have been working on standards and technologies that make this daunting task feasible. The Internet provides a highly efficient transport medium for the data, and Internet-related standards for high-level program and computer independent programming languages to facilitate the process.

The following technology components are being researched or implemented within the FHLP system:

- Bar codes and two-dimensional codes.
- Data collection hardware.
- Data management software.
- Radios and radio frequency identification device (RFID).

The system can be implemented in a stepwise manner, which is a new concept. Historically, major system upgrades have required all-or-nothing leaps with substantial hardware and software integration that is essential before the plug can be pulled on an old system and a new method put into operation.

Old-Fashioned Bar Codes

Also known as *one-dimensional* or *linear* code, old-fashioned bar codes carry data using a method called bar *width modulation* – an easy way for machines to determine binary information using the analog input methods that were prevalent 30 years ago.

These simple wide and narrow striped symbols (see Figure 1), which carry between 10 and 20 bytes of data, exist on many items ranging from consumer products to fixed assets such as chairs and PCs, to doorways (location codes), to automotive vehicles (vehicle identification numbers). Here is the rub though: the method of encoding data varies and, depending on where and when the code originated, it may or may not be unique or even fall into a recognizable category.

> *"Bar codes have a capacity to carry a license plate or key to a database, but need additional information from another source to fully identify the item, and often, the appropriate database to find the information."*

Fortunately, standards have been in place for nearly three decades that describe the method of encoding the information, and modern bar-code readers can quickly decide which method of encoding was used and the content of the data encoded. The bar code crowd refers to this as *automatic discrimination*. Bar codes have a capacity to carry a *license plate* or key to a database, but need additional information from another source to fully identify the item, and often, the appropriate database to find the information.

Advanced Two-Dimensional Bar Codes

Also known as *matrix symbols*, advanced two-dimensional (2D) bar codes are a relatively new addition to the machine-readable arsenal that uses the vertical, as well as horizontal dimension, to encode information. The result is a symbol that looks like a miniature checkerboard (see Figure 2), and can encode an order of magnitude more information in the same area as a linear bar code. As a result, more information can be carried with an item, including data identifiers specifying each field of encoded data.

Designed to be read by more modern digital imaging technology, the 2D marks are rapidly showing up on everything from

Figure 1: *UPC Code*

Figure 2: *Advanced Two-Dimensional Bar Code*

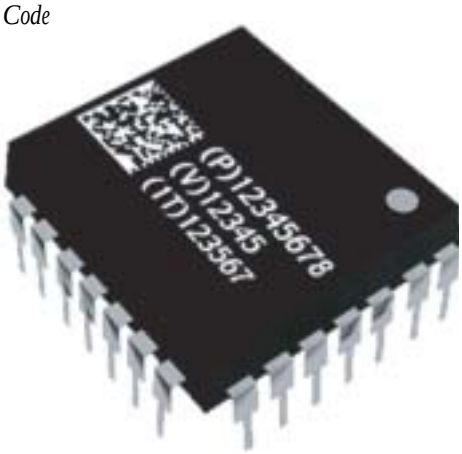


Figure 3: *Code Corporation's Code Reader 2.0*

postage machine stamps to computer chip packages. Standards have been developed during the past decade that include data identifiers encoded along with data content, making these symbols, literally, miniature databases that travel along with an item, with from 60 to several hundred bytes of data typically encoded.

Along with the advantages of this plethora of information, however, come some major integration issues with computer systems that need to access this information. The standards for encoding this information have been driven by the industries that need better ways to interchange data. These have included the electronics industry represented by the Electronics Industry Alliance, the automotive industry represented by the Automotive Industry Action Group, the telecommunications industry represented by the Telecommunications Industry Forum, the transportation industry that has coordinated activities through the American National Standards Institute (ANSI), and which represents all of the above, and others, to the ISO.

Critical to these activities has been the creation of the aforementioned data identifiers, which are collected, numbered, and identified by the ANSI Materials Handling (MH) 10.8.2 standard [1]. While this creates a reference point for data identifiers, it also is continually being updated. For example, if two trading partners wish to send each other information on shipping cartons, they can do so using ANSI MH10.8.2 standard matrix codes. Within the matrix codes, part numbers carry a data identifier, followed by the actual part number. Additional data elements such as production date or purchase order carry their own unique data identifiers. Each label on a shipping carton becomes its own database providing the receiver with all or much of the information needed to receive the shipment and keep track of it. The creation of new data identifiers is an ongoing process, and synchronizing systems with new data is a daunting, ongoing maintenance activity.

These matrix codes use field separation sentinels to handle variable length data encoding and have built-in forward error correction using Reed-Solomon principles[1] for forward error correction that have since been deployed in everything from disc drives to deep space probe radio transmissions.

In basic terms, in addition to the data, additional information is sent with the data to detect any errors and correct them by mathematically reconstructing the information. This is an important feature due to the high probability of partial damage to labels and permanently marked symbols during the shipping, constructing, mission, and recovery processes.

"Each label on a shipping carton becomes its own database, providing the receiver with all or much of the information needed to receive the shipment and keep track of it."

Bar-Code Readers Become Mini Digital Cameras

There are many types of bar-code readers deployed in millions of locations around the world. The technologies used for reading bar codes always involve the use of light, since bar codes are an optical technology. Machines must be able to see the codes in order to derive the data from them. The sensing equipment always involves a light source, a method of interrogating the light reflected from the object with the bar code on it, and an electrical circuit that translates the light-and-dark patterns into digital information for a receiving computer.

As bar codes have become more diverse and complex, the automatic identification industry has responded with more complex systems, which have deployed moving laser beams, charged-coupled devices, microprocessor chips, and most recently, complimentary metal oxide semiconductor camera sensors controlled by powerful micro computers with tremendous calculation processing capacity (see Figure 3). The industry has benefited from the consumer products that have driven the costs of these components downward, including compact disc players, digital cameras, and Internet-capable home computers. Cellular phones have added cheap and reliable miniature rechargeable batteries and low-cost digital radios. The overall electronics industry supplies memories, keyboards, switches, displays, and connectors.

The latest generation of bar-code readers includes palm-sized devices that can read and decode any matrix or linear symbol and transmit the information over a local radio connection to a host computer, which is typically a client operating within a broader LAN or WAN. The host uses the Internet to communicate transactions over the World Wide Web to other trading partners, and high-level, open platform programs written in XML can control all.

The latest generation of bar-code readers are small handheld devices that use digital photography and cordless data transmission.

Data Routers Send the Right Stuff to the Right Place

The routing of data between host computers has been a core element in the rapid deployment of the Internet into every aspect of modern business communications. A similar component is used in the software of client systems that accepts input from the bar code reader and then determines the proper recipient of the data elements. This is fairly simple in a rigid, linear bar-code system such as the type that exists in every modern grocery store.

At checkout, the bar-code reader sees the code on the item as it is moved over the reader in the checkout lane. The reader in the checkout lane sends the information to a computer that uses it as a key to look up the price of the item in a database, and totals the price of all items being purchased. When the buyer swipes a credit or ATM card to pay for the goods, the point-of-sale computer is smart enough to route that information to a different network that does the money transaction.

Now, imagine a palmtop computer that receives a 100-character record from a matrix bar code, including 12 different data elements followed by a six-digit location number that the bar code reader

derives from a linear code on a storage bin. The palmtop computer routes the information from the matrix code to a receiving system that generates inventory update transactions, to another computer that generates an electronic data interchange closure transaction to the supplier that shipped the system, and to the local warehouse computer that keeps track of the location of the item just received. Now multiply these transactions by the activities involved in the logistics support of a space payload, and the original problem – keeping track of things – is solved.

Ongoing Maintenance Is Mission Critical

Most systems involving commerce require a substantial, continuing maintenance effort. This maintenance effort has certainly been improved with a variety of Internet tools and the establishment of eXtensible Markup Language as an open standard for applications development. This allows Auto ID system developers the ability to pool resources to define data identifier lexicon standards.

Furthermore, tools are being developed that will analyze a matrix code, determine the data identifiers used, and then analyze a Web interface program to automatically match the data elements, requiring only the exceptions to involve further programming. What this means is that new applications can be quickly implemented in parallel to legacy operations, which can exist without being disturbed, thanks to the intelligence contained in the data router nodes.

Among the early adopters of the matrix codes and data identifiers is the Aerospace Industries Spec2000, which contains a system road map for applying intelligent data identifiers to information exchange between trading partners. In Figure 4, a developer selects Spec2000 elements for encoding and intelligent routing from a matrix bar code.

As new data elements get incorporated into Spec2000 and ANSI MH10.8.2, the requirement for periodic updates to the systems becomes evident. This is another important feature of the intelligent data routing capability. As new data elements enter the system, a simple update of the rules from a subscription service, similar to those deployed to prevent the spread of new computer viruses, keeps the new data flowing.

Radios: From Sputnik to Bluetooth

Data always needs a method for movement. Many components involved in the aerospace technology are not conveniently brought to a bar-code reader. So the reader must be taken to the bar code. It was this application characteristic that created the need for small, portable data radios. While we currently take the digital radios in our pocket cell phones for granted, it was not too many years ago that this was merely a dream for applications developers.

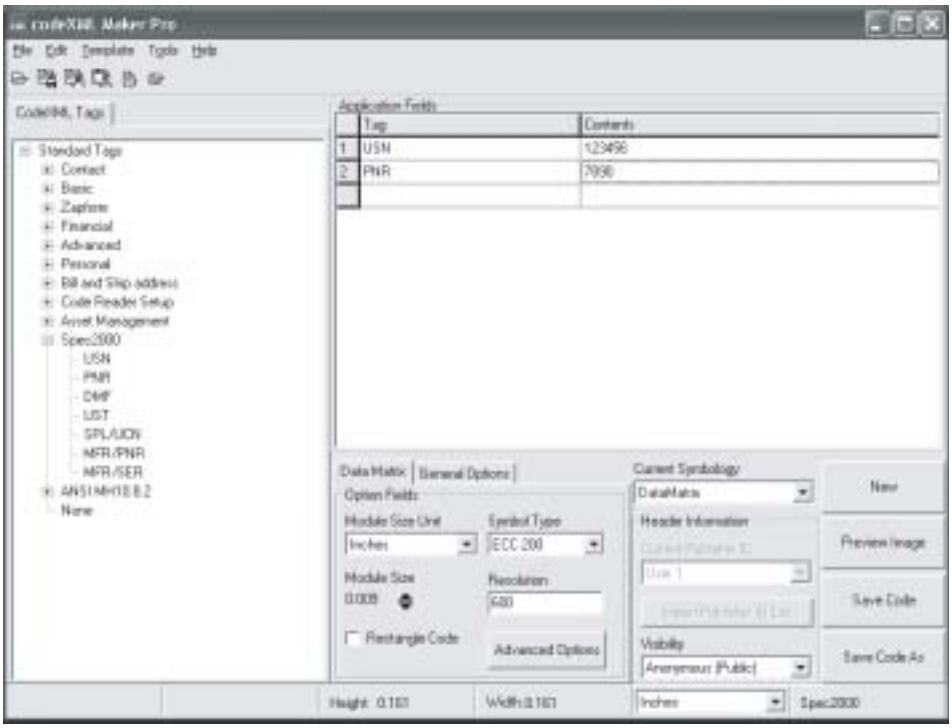


Figure 4: *Spec2000 Computer Display*

Ten years ago, the majority of data radios used a part of the radio band that required a Federal Communication Commission (FCC) site license for each location. Data rates averaged about a hundred characters per second, and the batteries necessary to operate these radios were the size and weight of a brick. The first step toward modern cordless data transmissions was when the FCC declared several radio bands free of the need for site licensing. Deemed *ISM* – Industry, Science, Medical – these radio bands created an instant area of development for the Auto ID industry. They also attracted a number of other gadgets, ranging from cordless phones to cordless speaker systems.

With many gadgets deploying into these bands, the need for standards became paramount. The first standard, Institute of Electrical and Electronics Engineers (IEEE) 802.11 [2], was developed as a relatively high-speed (millions of bytes per second) communications scheme for use in wireless local area networks. Now deployed worldwide in millions of locations, the IEEE 802.11standards-based products represent an excellent example of industrial competitors achieving a consensus standard for complex equipment interoperability. While 10 years ago it was discussed as a remote possibility, today, people go to the local electronics mega-store and buy IEEE 802.11 components from multiple vendors, then go home and plug-and-play wireless, nearly as simply as plugging a DVD player into a new TV set.

While the IEEE 802.11 standard works well for full-time local area networks, its requirement of session maintenance creates a tremendous drain on the batteries of portable devices. Recognizing the need for a cable replacement strategy, a new standard – designed to operate within the same radio band and coexistent with the 802.11 networks – began about six years ago. Dubbed *Bluetooth*, the new standard promised lower cordless device costs due to a number of factors, including smaller batteries. For example, the Compaq iPAQ H5450 in Figure 5 includes a 400 MHz CPU, 64

Figure 5: *The Compaq iPAQ H5450.*

MB RAM and supports both IEEE 802.11 and Bluetooth wireless communications.

Bluetooth is now becoming the de facto standard for cordless digital products with literally thousands of devices available, ranging from cellular telephone headsets to industrial computer links. United Parcel Service recently announced that, beginning June 2003, more than 50,000 Bluetooth-equipped bar code reading devices will be deployed throughout its worldwide network of computerized parcel handling systems [3]. Bar-code readers without Bluetooth as an option will soon be relegated to the has-been pile.

Direct Identification Through Radio Frequency Identification

As useful as the bar code technologies are, they are still an optical technology, meaning, simply, that the item must be seen by the reader in order to be decoded. Another relatively new technology offers an alternative, albeit far more expensive, method for cases where an item that is embedded in another item, or covered with a coat of paint or encased in rubber inside a tire, can still identify itself to the outside world. This RFID method involves a miniature radio transmitter attached to, or embedded into the item being identified.

While still very early in its evolution – there is no standard in place for interoperability of RFID systems – the technology is promising and will be deployed in future systems. While far from achieving interoperability, and therefore far from mass deployment, the ANSI committees involved with the MH10.8.2 standard are already planning for RFID within the world of data interchange. This means that existing systems with intelligent data routers will easily be adapted to these components when they begin to overcome the manufacturing standards and cost problems currently confounding the promise of this technology.

Putting It All Together

The benefits of these technologies will be available for scientists and aerospace designers for many years to come. The Jet Propulsion Laboratory, managed by the California Institute of Technology, is NASA's lead center for robotic exploration of the solar system. To support continued exploration, the laboratory is making advances in technology with new instruments and computer programs to help spaceships travel farther and telescopes see further than ever before.◆

References

1. The American National Standards Institute, Inc. The ANSI MH10.8.2 Standard. New York: ANSI.
2. Institute of Electrical and Electronics Engineers. The IEEE 802.11 Standard <www.computerworld.com/services/research/linkspage/0,4848,LNK886,00.html>.
3. Brewin, Bob. "UPS to Deploy Bluetooth, Wireless LAN Network." Computerworld. 23 July 2001 <www.computerworld.com/mobiletopics/mobile/story/0,10801,62459,00.html>.

Notes

1. Named after the Massachusetts Institute of Technology (MIT) scientists who developed them about 40 years ago, and first published in a five-page paper that appeared in 1960 in the *Journal of the Society for Industrial and Applied Mathematics*, "Polynomial Codes over Certain Finite Fields," by Irving S. Reed and Gustave Solomon, then staff members at MIT's Lincoln Laboratory. Reed, later a professor at the University of Southern California, consulted for the Jet Propulsion Laboratory on projects to ensure the receipt of correct data in transmissions involving space exploration, as related in the *Society for Industrial and Applied Mathematics Newsletter* in January 1993.

About the Author

James E. Bagley is vice president of Sales and Marketing for Code Corporation. He has held senior management positions with Metanetics Corporation, Symbol Technologies, Norand, and Radix Corporation. Code Corporation designs, develops, and manufactures automatic identification implementation and data collection platforms. Its worldwide headquarters are located in the Salt Lake City, Utah metropolitan area.

Code Corporation
11814 S. Election Road
Draper, UT 84020-6814
Phone: (801) 495-2200
Fax: (801) 495-2202
E-mail: jbagley@codecorp.com

Steganography

2nd Lt. James Caldwell
U.S. Air Force

Steganography is the ancient art of embedding a secret message into a seemingly harmless message. This art, in contrast to cryptography, does not use ciphers or codes to scramble a message, and therefore is not obvious. U.S. and foreign officials suspect that Osama bin Laden is using steganography to pass embedded maps and photographs of terrorist targets through chat rooms and pornographic Web sites.

The text below contains a message sent by a German spy in World War II.

> Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects for pretext embargo on by-products, ejecting suets and vegetable oils.

Decoding the message by extracting the second character of every word reveals the following text: "Pershing sails for NY June 1."

This type of ciphering is known as steganography, the ancient art of hiding messages so that they are not detectable [1]. No substitution or permutation was used. The hidden message is plain, but unsuspecting to the reader. Although a cousin to cryptography, steganography is not inherently obvious. Whereas cryptography is easily detectable as secret code, steganography, as its Greek root implies, is *covered writing*. It uses a physical cover message to camouflage its secrecy.

History

Steganography is widely employed today, but its origins trace back millenniums ago. Before the computers and e-mail of today, messengers had two options for delivering messages: memorize the message or hide it on the messenger.

Several techniques of steganography are etched in history. One account speaks of the Greek ruler Histaeus who shaved the head of one of his slaves, tattooed the message onto his scalp, and sent him along to deliver the message *after his hair had grown back*. The recipient would shave the slave's head to uncover the message and find an untainted scalp on which to reply.

Other accounts in Greek history tell of Demeratus who wrote a message to the Spartans warning of an eminent invasion from Xerxes. The message was carved on a wood backing of a wax tablet, and then covered in a fresh layer of wax. The *seemingly* blank tablet was then delivered successfully.

Invisible ink was also used commonly throughout history, but not through stamps or specially equipped markers. Instead, onion juice, alum, ammonia salts and several other materials were used and would glow dark when held over a flame.

Wartime especially involved steganography. During the American Revolution, the British and Americans used invisible inks extensively. During World War II, for instance, the Germans used microdots. The microdot was essentially a secret message photographed and reduced to the size of a period. When the Americans realized the volume of microdots contained within communications and transactions intercepted, they quickly realized as FBI director J. Edgar Hoover did, "the enemy's masterpiece of espionage" [2].

The advent of computers further advanced disguising messages. For instance, laser printers could be used to offset lines and character spaces by as little as 1/300th of an inch. A binary message could be sent easily using a normal space to represent 0s, and by offsetting characters 1/300th of an inch to represent 1s.

These early approaches were based on the principle that secret messages were hidden inside the physical object containing them. Ostensibly, the cover message holds the intrinsic meaning of the communication, but in reality, nothing could be further from the truth. However, despite the myriad of approaches to steganography aforementioned, this approach is unquestionably powerless in digital communications. Only pure information can be sent. There is no hot wax or hair regeneration to camouflage the secret transmission. Even so, a technique was found.

This article will address uses of steganography today and discuss several approaches to steganography. This knowledge will then be applied to understanding how the network has proliferated the accessibility and employability of steganography, and the benefits and perils associated with it.

Secret Channels

Digital technology offers new ways to apply steganography techniques, including the ability to hide information inside digital images[1]. A digital image is "an array of numbers that represent light intensities at various points" [3]. Combined, these light intensities or pixels form the image's raster data. Images with 640 x 480 pixels and 256 colors can contain up to 300 kilobits of data. But it is more typical to see digital images in sizes of eight-bit or 24-bit files. This provides an excellent opportunity for hiding information, especially in image sizes of 24-bits.

Each pixel on a computer monitor selects from three primary color variations: red, blue, and green. Each color is represented by a single storage byte. With 24-bit images, three bytes are allocated for each primary color (hence eight bits per byte multiplied by three bytes).

Represented in binary values, for instance, a white background is 11111111, 11111111, 11111111. Pixel representation makes up a file's size. Thus a 24-bit image displayed in high resolution (1,024 x 768) has more than 2 million pixels, producing a file over 2MB in size. The larger the file, the greater opportunity there is to apply steganography techniques. The downside to this of course is that large file sizes might induce unwanted suspicions.

To deal with this, file compression is used. There are two kinds available today: lossy and lossless. Both methods compress files to save storage space, but do so differently. This is important because certain compression applications can interfere with hidden messages. Lossy compression is the most efficient space saver, but does not retain the original image's exactness. JPEG (Joint Photographic Experts Group) is an example of such compression. A lossless approach, in contrast, retains the integrity of the original

image. Images saved as GIF (Graphic Interchange Format) or BMP (bitmap file) apply lossless compression.

Inserting Hidden Data

Two files are required for steganography to work. The first file is an innocuous cover image that will host the second file containing hidden information. The hidden message can be anything that is embeddable into a *bit stream* such as plain text or cipher text. There are several methods to hide information in digital images, from taking advantage of *noisy* areas that draw less attention in an image, to scattering the message randomly throughout the image. A brief discussion on each of these approaches is in order before continuing.

Least Significant Bit

In her book "Information Warfare and Security" [4], Dorothy Denning addresses the least significant bit and its vulnerability to modifications without careful detection. A color byte contains eight bits, each of which varies in terms of impact on the resulting color. The least significant bit (or the final bit in a stream) affects the smallest change of the eight bits. On the other hand, the first bit of the stream has the largest influence on color selection. For instance, as Denning illustrates, the least and most significant bit are similar to the hour and second hand on a clock. While a change in the second hand alters time very slightly, a change in the hour hand is extreme.

If the least significant bit of every bit stream were to be allocated for a hidden message, the resulting image file would appear unaltered. Moreover, the larger the bit size, the more subtle the change. For example, using the least significant bit in a 24-bit image size, the original raster data for three pixels is:

00101100 10101100 10101000
00101011 01101000 00101011
00101010 00111001 00101010

Inserting the binary value for A (**10000001**) would result in[2]:

00101101 10101100 10101000
00101010 01101000 00101010
00101010 00111001 00101011

Several software tools for implementing least-significant bit insertion are available and easy to use. S-Tools, for example, executes by dragging the document you wish to hide over the cover image. The user is asked for a password to recover the message.

The least significant bit approach is simple to understand and use, but it is largely vulnerable to changes in data due to file compression. Since JPEG compression is so efficient in reducing file sizes, most image traffic over the Internet utilizes it. However, as stated previously, the lossy compression technique JPEG employs may alter the least significant bit.

Steganography Uses

The use of steganography undeniably connotes dishonest activity, but there is a peaceful aspect to consider. Steganography is used in map making, where cartographers add a nonexistent street or lake in order to detect copyright offenders. Or similarly, fictional names are added to mailing lists to catch unauthorized resellers. Modern techniques use steganography as a watermark to inject encrypted copyright marks and serial numbers into electronic mediums such as books, audio, and video. For instance, DVD recorders detect copy protection on DVDs that contain embedded authorizations.

Potential uses of steganography are undoubtedly vast. Companies could advertise public Web pages containing private, hidden text that only internal members could intercept. An attempt to decipher the hidden text would be unwarranted since no encryption (or code) was used. Steganography could also be used to hide the existence of sensitive files on storage media. This would entail a cover folder and an embedded hidden folder.

Protection Against Steganography

The proliferation of networks has added intensity to both noble and ignoble purposes of steganography. Network security analysts face an insidious foe for sure. But how is steganography detected, and why should network security analysts be alarmed and cautious?

Nearly all steganography programs in use leave behind traces or fingerprints that indicate something is not right. Based on research conducted over the years, organized crime, terrorists, and various other groups operating worldwide commonly use steganography to operate via public forums, Web sites, etc.

Software programs that detect steganography do exist, and enhanced iterations are under development. Neil Johnson, a graduate student at George Mason University, is developing a *stego detector*. The program, he describes, is designed to search hard drives for electronic fingerprints that typically result from steganography applications. Similar to a virus scanner, this stego detector identifies signatures. As Johnson explains:

> Different authors have different ways to hide information to make it less perceptible. The author may come up with ideas that nobody else is using. That tool may have a special signature. Once that signature is detected, it can be tied to a tool. [3]

Johnson and other law enforcement agencies use software to locate signatures by studying the native structure of files including image, voice, text, and video files, and known software tools that implement steganography.

The Pentagon is also interested in uncovering ignoble practices of steganography and annually funds the Naval Research Laboratory. Their interest spawns, in part, from news reports that link terrorist Osama bin Laden to steganography communications. The concern is that data messages are being embedded in chat room messaging or bulletins unnoticed, while intelligence agencies are *off in another world* monitoring communications traffic (e.g., e-mail).

Cyber forensics at WetStone Technologies have successfully developed several tools to detect steganography. The ultimate device will uncover steganography regardless of its implementation methods. So far, steganography has turned up primarily on hacker Web sites. But steganography was also found on frequently visited sites such as Amazon.com and eBay. The forms of steganography vary, but unsurprisingly, *innocuous* spam messages are turning up more often containing embedded text.

WetStone Technologies considered steganography a technological threat worthy enough to caution the U.S. Air Force, beginning in 1998, to guard against it. But the National Security Agency took it a step further and cautioned all government agencies and private employers, warning that internal employees could send embedded, sensitive information via e-mail that would pass through firewalls and security unsuspected. Without a doubt, the ubiquity of steganography merits closer observation by network security analysts.

Conclusion

Steganography is an instrument of security, but not exclusively secure. There are tradeoffs with steganography of which

the security community is becoming aware: There is a tradeoff between reliability and message size and there is a tradeoff between message size and detectability. The approach steganography offers reduces the chance of a message being detected by its *inadvertent* layer of cover. However, if the hidden message is discovered, it is easily readable. For this reason, combining encryption algorithms with steganography offers a much stronger encryption routine.

Although this article discusses some applications of steganography, there are many more uses in voice, media applications (such as communication channels), audio, and text, to name a few.

This article unveils potential exploits of steganography regarding network security. Although awareness of steganography applications today is limited, progress is unfolding to expose the hidden art. Unfortunately, in the information age, the old adage "what you don't know can't hurt you" is not always accurate.◆

References

1. Clair, Bryan. "Steganography: How to Send a Secret Message." 8 Nov. 2001 <www.strangehorizons.com/2001/20011008/steganography.shtml>.
2. Kahn, D. The Codebreakers. New York: MacMillan, 1967.
3. Johnson, Neil F., and Sushil Jajodia. "Exploring Steganography: Seeing the Unseen." IEEE Computer Feb. 1998: 26-34.
4. Denning, Dorothy E. Information Warfare and Security. Boston, MA: ACM Press, 1999: 310-313.

Notes

1. Note that steganography can be used to embed hidden files into text documents, audio, video, or images. The scope of this will include an image-based approach primarily, with some mention of other media applications.
2. Least significant bit insertion in this example is possible only by discarding the 9th byte in the data stream.

About the Author

2nd Lt. James Caldwell was commissioned into the United States. Air Force through the Air Force Reserve Officer Training Corps and was assigned to Tinker Air Force Base, Okla. Caldwell has a bachelor's degree in management information systems and is pursuing a master's degree in computer resources and information systems at Webster University. He is currently assigned to the 552 Computer Systems Squadron as a Project Manager in the Software Services Flight.

552 Computer Systems Squadron
Bldg. 284 Rm. 209
Tinker AFB, OK 73145
Phone: (405) 734-3394
E-mail: james.caldwell@tinker.af.mil

Trafficability Analysis Engine

Dr. Kevin R. Slocum
Engineer Research and Development Center

Lt. Col. John R. Surdu, 2nd Lt. Jeffrey Sullivan, 2nd Lt. Marek Rudak,
2nd Lt. Nathan Colvin, and Cadet Christopher Gates
U.S. Military Academy

Trafficability is a measure of how easily vehicles can drive through a particular piece of terrain. Manual processing of trafficability analysis is time consuming and coarse. A new trafficability engine has been developed that takes into account previously ignored aspects of trafficability and degrades gracefully when data are missing. This article describes the design and implementation of this trafficability engine, as well as needed future work.

Trafficability is a measure of how easily vehicles can drive through a particular piece of terrain. Military terrain analysts have a requirement for an automated tool to conduct trafficability analysis as part of a larger decision-support framework. The proof-of-concept system described in this article uses an expert system to combine the outputs of various geography modules into an estimate of trafficability.

The unique aspects of this system are its rating of trafficability as a floating-point number between zero and one; the use of a confidence measure to assess the accuracy of the trafficability prediction; and its consideration of the capabilities of individual vehicles with respect to slope, vegetation, and soil conditions. In addition, the system degrades gracefully as terrain data are missing and reflects the confidence in the predicted outcome; if data are missing, the system does not break but instead provides the best estimate possible. Finally, this system reflects the effects of weather on trafficability.

This article describes the design and implementation of this trafficability engine, as well as needed future work.

Background and Motivation

Trafficability is important to the U.S. Army. Detailed, thorough trafficability analysis helps tactical decision makers determine likely enemy avenues of approach and possible friendly avenues of approach. Manual processing of trafficability analyses is time-consuming and coarse. The output of the manual terrain analysis process often takes days and results in a product known as the Modified Combined Obstacles Overlay (MCOO).

The MCOO classifies terrain into one of three coarse categories: *go*, *slow-go*, and *no-go*. The names are self-explanatory, but they do not provide a sufficient amount of information to the intelligence officer who must plan for such routes as enemy avenues of approach, friendly attack routes, and supply routes.

Many factors that affect trafficability are not considered in the manual process. First, as a manual process, its efficacy is dependent on the experience and skill of the intelligence officer who usually prepares the MCOO. Trafficability analysis often is concerned with tracked vehicles, wheeled vehicles, and dismounted soldiers. This process assumes that all wheeled vehicles, for instance, are created equal. Recent effects – and projected effects throughout the operation – of weather are often ignored. The load-bearing capacity of soil is dependent on its moisture content. Roads often become *slow-go* or *no-go* after heavy rains.

The purpose of this research was to build a trafficability analysis engine that had the following attributes:

- Predicts trafficability as a floating-point number between zero (a cliff) and one (the salt flats of Utah).
- Considers the capabilities of individual vehicle types (e.g., the M113A3 armored personnel carrier) rather than generalizations (e.g., a generic tracked vehicle), with respect to slope, vegetation, and soil conditions.
- Degrades gracefully as terrain data are missing.
- Reflects the confidence in the predicted outcome.
- Performs most of the difficult computation at a server and sends just the results of the analysis to the user.
- Allows a skilled user to modify the rules by which trafficability is determined.
- Reflects the effects of weather on trafficability.

The prototype described in this article takes into account geographic factors, including location, vehicle type, off-limits terrain, water, weather, soil, land use, topography, vegetation, and roads. In addition, the system was designed to be user-friendly. The goal of this work has been to build an architecture in which various trafficability modules can be inserted. If a developer has a better soil-moisture evaporation module, it could easily replace the one used in this prototype.

Design and Implementation

The design of this system is modular as shown in Figure 1. The overall architecture involves a terrain server (or hierarchy of servers) above the Army division level. The user (at lower echelon units) selects an area of interest and sends that information to the trafficability engine's server. The trafficability engine's server fetches terrain data (in the form of ASCII files in the case of this proof-of-concept system) from the terrain server(s). If terrain products are unavailable for the area of interest, the engine's server may ask the user for general information about the area. For instance, the engine may query the server for recent precipitation information such as dry, wet, or very wet. Once the trafficability analysis engine has all available information, the geography modules begin processing the data.

As the clients are meant to be thin, in this proof-of-concept, the user interface is a Web browser. In the target application, a Web browser might be sufficient; however, the interface might be connected directly to systems within the Army Battle Command System such as the All-Source Analysis Station (ASAS) [1]. The trafficability engine is implemented as a Java servlet (running on a Jakarta Tomcat server). Each of the geography modules is a Java object called by the servlet.

Geography Modules

The geography modules each look at different aspects of trafficability such as weather, topology, vegetation, land use, and soil. Some modules' output serves as input to other modules. For instance, the results of the weather module are inputs to the soil and road modules. While the actual implementation is a two-dimensional array of Java objects, one can think of each of these geography modules as filling in an *overlay*, as shown in Figure 2. Each cell of an overlay includes two elements: an estimate of the trafficability of that point on the ground, and a confidence in that estimate. This confidence is not strictly a standard *deviation* because it is computed in an *ad hoc* manner

by the expert system; however, for purposes of this research it serves much the same purpose.

An advantage of the modular design is that each module can use the most appropriate mechanism to compute trafficability. The Topography Module takes the floating-point slope value at each point and compares it to the known maximum slope capability of each specific vehicle, using a formula found in Field Manual (FM) 5-33 [2]. The result of this calculation is an estimate of trafficability as a floating-point number between zero and one.

The Soil and Vegetation Modules query a lookup table and determine the characteristic of each different type of soil or vegetation at that specific point. That value is then used in further computations to determine trafficability based on soil or vegetation, respectively.

Each module fills in values on its respective overlay, which in turn are used to perform the final trafficability computation.

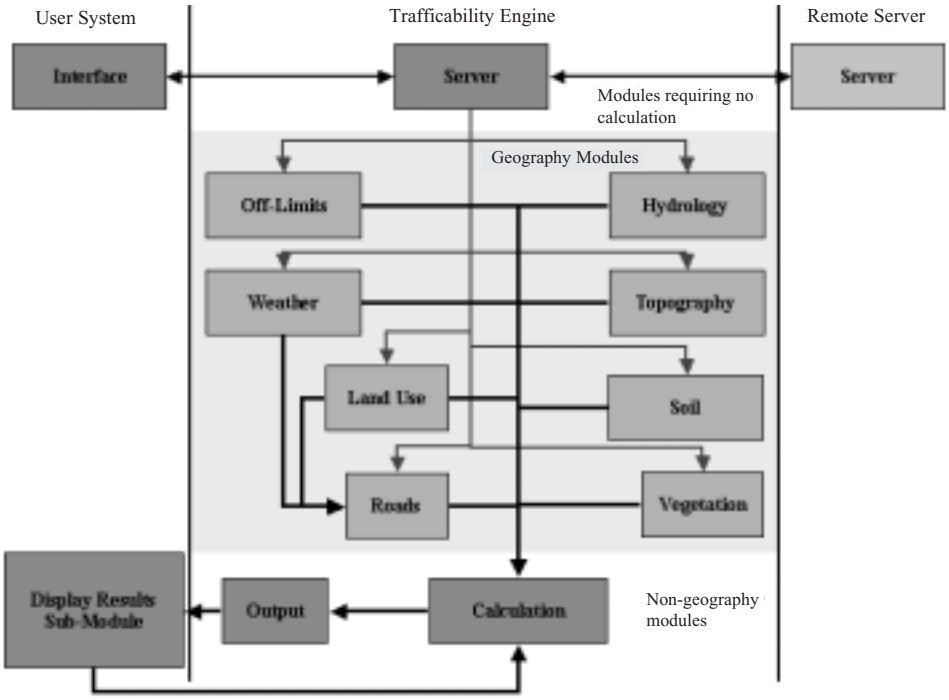


Figure 1: *Architecture of the Trafficability Engine*

Trafficability Computation

Once each module has performed its analysis, the calculation module uses an expert system to give each node an overall trafficability rating. Though often slower than compiled code, an expert system was chosen for the final analysis for two reasons:

- Expert systems provide a means of explaining to the human user how a decision was reached.
- Human experts could modify the expert system without modifying or recompiling the base program.

The expert system shell used is the Java Expert System Shell (JESS), developed at Sandia National Laboratory [3]. While the JESS project began as a port of C Language Integrated Production System (CLIPS) [4] to Java, JESS is now richer than CLIPS in many ways. The current expert system uses only crisp rules; however, support for fuzzy logic, using Matlab.fis files [5], has been implanted in Java and linked to the program.

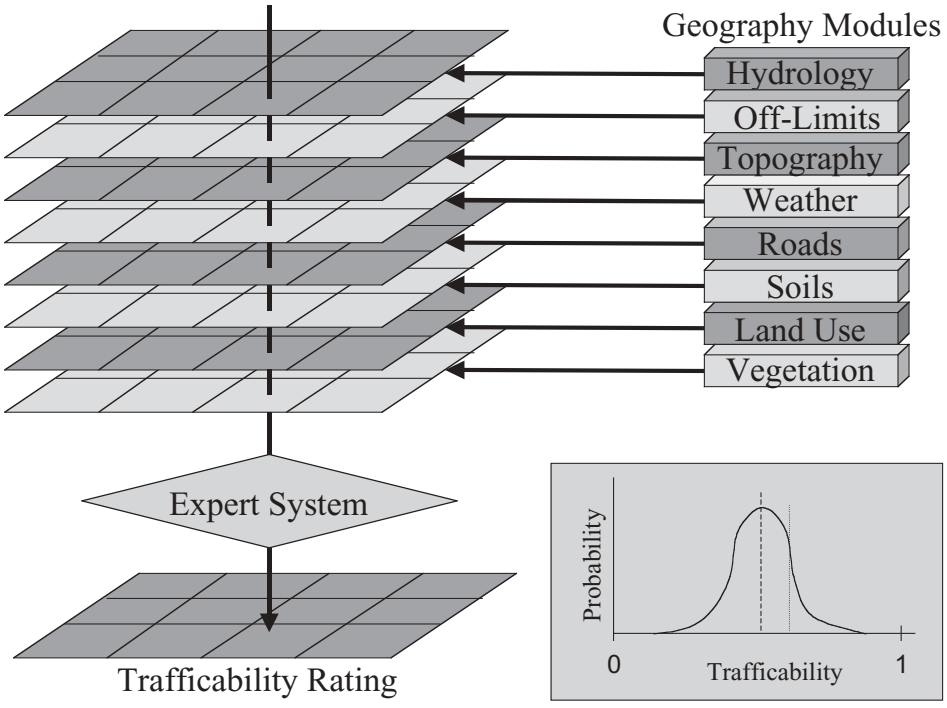
The manner in which the expert system combines the various ratings of confidence is purely arithmetic at this point. A weighted average of the eight *overlay* means is used. If an overlay is missing data (or the overlay is missing entirely), this has a large, negative impact on confidence. In the proof-of-concept system, all overlays are weighted equally. For future work, experiments will be conducted to determine which overlays have the greatest impact on trafficability in various geographic regions. For instance in Kansas, most of which is very flat, missing the topography overlay might have less effect on trafficability than missing the soils overlay. This *sensitivity analysis* will help determine the weights' uses in the weight-average computation.

The use of a *mean* (i.e., the estimate of trafficability) and *standard deviation* (i.e., measure of confidence) allows the system to degrade gracefully when data are missing. When data are missing, the system still provides an estimate of trafficability; however, the system indicates (through its confidence rating) that it is less certain of the estimate. The Engineer Research and Development Center's Topographic Engineering Center for who this work is being done, has indicated that in the future, terrain products will come tagged with confidence in the data, and that confidence might not be uniform across the product. This technique also allows the system to adapt easily to non-homogenous input (i.e., input files in which the level of fidelity is not uniform across the whole file). As a result, the system provides the user with useful information even when some data are missing or it is a *best guess*.

Results

In the proof-of-concept system, the out-

Figure 2: *The Output From the Various Geography Modules Is Combined in an Expert System*



come of the analysis is a matrix that rates the trafficability of each point in the area of interest. The highest resolution input file determines the size of this matrix. If the area is 10km x 10km with 10m resolution, the final matrix would be 1,000 x 1,000 cells.

Clearly the speed of computing trafficability is based on the size of each of the overlays and is an order of magnitude of *n*, where *n* is the number of cells in the final matrix. (Since the area does not have to be square, complexity cannot be based on just height or just width of the area.) The slowest execution of the computation is the use of the expert system for each cell in the final matrix.

Even though the computations in each of the geographic modules need to be more fully developed and refined, the output of this system is very close to the results gained through detailed, manual analysis. Since the manual computation takes days, the fact that this system takes less than three minutes is a major improvement.

Future Work

Improving the Fidelity of the Geography Modules

The algorithms used in many of the geography modules came from existing field manuals [2]. In the process of implementing the geography modules, it became obvious that some badly needed models are missing. For instance, there seem to be no readily available models for the moisture content of soil. Such a model would need to take into account recent precipitation, soil texture, air temperature and humidity, topography, etc.

Parallelize the Computation

The ability of the system to automatically make use of multiple processors must be incorporated. Ideally, the system could first assign each geography module to different processors then assign portions of the final trafficability computation (since it is the slowest) to different processors. As there is no interaction (at this point) between the computation of trafficability in one cell of the final matrix and that of its neighbors, this process is easily made parallel.

Displaying the Results

While the output of the trafficability analysis engine is a matrix, that matrix is not what is displayed to the user. The proof-of-concept system converts that matrix into a GIF file that is displayed over the top of a map. This system is really intended to interface with other command-and-control systems such as the Maneuver Control System and ASAS [1]. The matrix would then be converted into an overlay for those systems and displayed to the user.

The trafficability analysis engine computes a trafficability estimate and a confidence for each point. Research must be conducted to determine how best to convey to the user the confidence in the estimate. Options include right-click functionality; however, the goal is a means by which the user can see the trafficability estimate *and* the confidence without any active querying.

Trafficability is computed as a floating-point value between zero and one. In the proof-of-concept system, arbitrary thresholds are set for *no-go*, *slow-go*, and *go* terrain, and the categories are assigned colors of red, yellow, and green, respectively. The intent is to display a gray-scale view of trafficability in which colors close to white (255, 255, 255) would represent go terrain and colors close to black (0, 0, 0) would represent no-go terrain. When this overlay was made transparent, the areas of terrain that were most clearly visible through the trafficability overlay would be most easily traversed.◆

References

1. Bessler, J. E. Army Battle Command System (ABCS) Capstone Requirements Document (CRD). Rev. 1.0. TPIO-ABCS. Ft. Leavenworth, KS: U.S. Army, 10 Feb. 1998.
2. U.S. Army. Field Manual 5-33: Terrain Analysis. Washington, D.C.: Headquarters, Department of the Army, 1990.
3. Friedman, E. "JESS: The Rule Engine for the Java Platform." 20 May 2002 <http://herzberg.ca.sandia.gov/jess>.
4. Giarratano, J., and G. Riley. Expert Systems: Principles and Programming. Boston, MA: PWS-Kent Publishing Co., 1989.
5. MathWorks. "MATLAB." 2 May 2002 <www.mathworks.com/products>.

About the Authors

Kevin R. Slocum, Ph.D., is a research scientist team leader at the U.S. Army Engineer Research and Development Center, Topographic Engineering Center, where he is active in the development of innovative methods of geographic data generation and analysis. Slocum's background also includes efforts in addressing environmental science issues and a long tenure in international nautical charting. He is a recent graduate of the marine science program at the College of William and Mary's Virginia Institute of Marine Science, and retains prior graduate and undergraduate degrees in the field of applied geography.

Engineer Research and Development Center
Topographic Engineering Center
7701 Telegraph Road
Alexandria, VA 22315-3864

Lt. Col. John R. "Buck" Surdu is an Army Acquisition Corps automator at the U.S. Military Academy. He has had infantry assignments in Vicenza, Italy; Ft. Benning, Ga.; and the Republic of Korea; and has worked at the Army Research Laboratory and the Department of Electrical Engineering and Computer Science. His research interests involve the use of simulations and artificial intelligence in decision support. Surdu has a Bachelor of Science in computer science from West Point, a Master of Business Administration from Columbus State University, a Master of Science in computer science from Florida State University, and a doctorate in computer science from Texas A&M University.

2nd Lt. Jeffrey Sullivan graduated in June 2002 from the U.S. Military Academy with a Bachelor of Science in computer science. He will attend the Signal Officer's Basic Course at Ft. Gordon, Ga., before reporting to his first assignment at Ft. Lewis, Wash.

2nd Lt. Marek Rudak graduated in June 2002 from the U.S. Military Academy with a Bachelor of Science in computer science. He will attend the Infantry Officer's Basic Course at Ft. Benning, Ga.

2nd Lt. Nathan Colvin graduated in June 2002 from the U.S. Military Academy with a Bachelor of Science in environmental science with a concentration in computer engineering. He has branched Aviation and plans on posting to Korea to fly attack or scout helicopters.

Cadet Christopher Gates is a senior at the U.S. Military Academy earning a Bachelor of Science in geospatial information science and computer science. Upon graduation, he will be commissioned as a second lieutenant in the Signal Corps.

Shock and Awe

In my first published BackTalk article [1], I proposed that software engineers should, like other professionals, have one ultimate goal or measure that directs, motivates, and defines their success. I referred to this as the "measure that eclipses all others" or "the acid test." All other measures and tests are fruitless if you don't pass the acid test. I proposed, and still propose, that the acid test for software engineers is customer satisfaction.

While many struggle to define customer satisfaction, in the defense industry it's clear that our customers are warriors, and they are satisfied when we enhance their ability to accomplish a mission. At the time of that article, our mission was in the Balkans; yet while successful, there was definitely room for improvement.

Four years later a new acid test is being applied between the Euphrates and Tigris rivers. As I write, the liberation of Iraq is two weeks old and far from complete, but the early test scores are looking very promising. The use of technology and the ability of our troops to accomplish their missions with lightning speed and pinpoint accuracy are truly impressive.

The strategy in the current campaign has been coined as *shock and awe*. The term has left many from the drive-thru generation in disappointment. Like a spoiled child on the 4th of July, members of the media and their armchair generals have complained because the fireworks are not big enough to shock or awe.

Those of us that work in the defense industry have a different view of shock and awe. The shock for me is how far we have come from Desert Storm in terms of accuracy, communication, and flexibility. While we all have seen certain systems in test and training, this is the first time we have seen all those components come together in the fog of war. The awe is in the execution and results.

The complexity of the conflict increased as the oppressors scattered like cockroaches among the innocent. Stop and think of the complexity and challenge of removing them with minimal harm to civilians and infrastructure. One would not even contemplate such a mission without the technologies engineers have nurtured to maturity.

But, before we dislocate our shoulders patting ourselves on the back, we should assess how we can do better in the future. The following are suggested follow-up engineering campaigns.

Gawk and Jaw

This is a campaign to look closely (gawk) at your system's performance and thrash out (jaw) with colleagues and customers what worked and what didn't work.

Knock and Flaw

This is a campaign to kick around (knock) your systems and wheedle out their shortcomings (flaws). This is an effort to avert overconfidence and remove impediments to future customer satisfaction.

Rock and Moi

This is a campaign to disrupt (rock) your mental equilibrium (moi). Look within yourself for new thoughts, ideas, and inspiration.

Stock and Draw

This is a campaign to explore your current supply (stock) of technologies and extract (draw), the most promising for new applications.

Flock and Yaw

This is a campaign to work together (flock), focus on our customer's course of action, and work to minimize deviation (yaw) from that course.

Wok and Gnaw

This is a campaign to collect and simmer (wok) assorted technologies, integrate them, and let customers chew (gnaw) on them to make sure they satisfy their appetite.

Walk and Ohm's Law

This meta-campaign is for engineers to stride (walk), towards the maximum flow of technology (Ohm's Law) to customers. George Simonga Ohm postulated that an electrical current is directly proportional to the potential difference and indirectly proportional to resistance [2]; to maximize the flow of current, increase potential, and decrease resistance. Applying Ohm's Law to technology transfer in this campaign is to maximize the steady flow of technology by increasing mental potential and decreasing emotional resistance.

Before we get caught up in the technology, let us not forget our customer: young soldiers, marines, seamen, and pilots executing their missions with courage, resolve, fidelity, and compassion. Whether you are for or against this action, appreciation for the troops and their sacrifice is well earned. I worked with and for them, and I'm greatly indebted to and proud of these heroes. I hope and pray that they quickly return from harm's way. The only shock and awe these young men and women should have to deliver in the future is on their ma and pa.

Filling the role of enforcer is never easy or popular but necessary. As Lee Harris puts it:

> ... if any social order is to achieve stability there must be, at the heart of it, a double standard governing the use of violence and force. There must be one agent who is permitted to use force against other agents who are not permitted to use force. [3]

I sense the fashionable stance that peace can be achieved without violence is fading. Governing in an age of chemical, biological, and nuclear weapons differs greatly from the age of guns, knives, and clubs. Therefore, I hope most of all that we are always prepared for the next acid test.

– Gary Petersen
Shim Enterprise, Inc.

References

1. Petersen, G. "The Acid Test: Measuring Your Success." CrossTalk June 1999: 31.
2. Merriam-Webster Online Dictionary. Copyright 2003 by Merriam-Webster, Incorporated <www.m-w.com>.
3. Harris, Lee. "Our World Historical Gamble." Tech Central Station. Online posting. 11 Mar. 2003 <www.techcentralstation.com/1051/defensewrapper.jsp?PID=1051-350&CID=1051-031103A>.

An Independent Expert Program Review provides an in-depth analysis of your project by a team of software acquisition and development professionals. Let the Software Technology Support Center in partnership with the Tri-Service Assessment Initiative help you to improve your organization's project management, product quality, production efficiency, and predictability by identifying areas of strength as well as areas needing improvement and providing actionable recommendations.

We can help with any of the following:

- Reducing cost overruns and schedule slippages
- Identifying and managing program risk
- Outlining acquisition strategy and program milestones
- Pinpointing reccurring problems and finding solutions for avoiding them

Whether your organization is big or small, just starting a project or embattled in difficulties, we can help. Just give us a call.

TAI
Tri-Service Assessment Initiative
Scott Lucero, Assessment Manager
1931 Jefferson Davis Hwy. #104, Arlington, VA 22202-3517
Phone (703) 602-0851 ext. 114 • Fax (703) 614-9884 • http://tai.pica.army.mil

Software Technology Support Center
Dave Berg, Program Manager
6022 Fir Avenue, Building 1238 • Hill A.F.B., UT 84056-5820
Phone (801) 777-4396 • Fax (801) 777-8069 • www.stsc.hill.af.mil

Sponsored by the Computer Resources Support Improvement Program (CRSIP)

Published by the Software Technology Support Center (STSC)

CrossTalk / MASE
6022 Fir Ave.
Bldg. 1238
Hill AFB, UT 84056-5820

PRSRT STD
U.S. POSTAGE PAID
Albuquerque, NM
Permit 737