Defense Standardization Program

Journal

October/December 2009

Warfighter Support

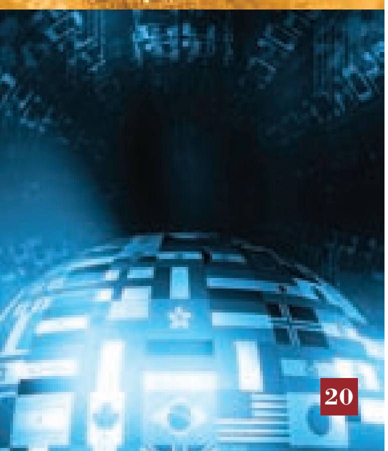
Addressing the Need for Good Data Management

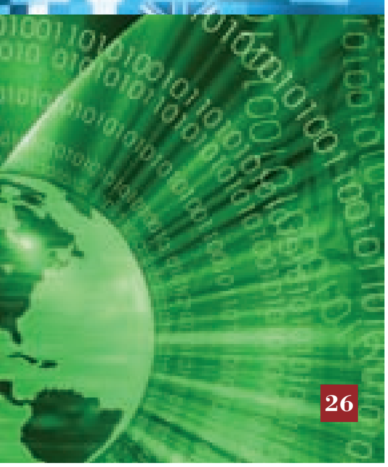
Guarding against Counterfeit Parts

Building a Better Tool to Deliver High-Quality Products to the Warfighter

Defense Standardization Program Journal

Contents *October/December 2009*





The *Defense Standardization Program Journal* (ISSN 0897-0245) is published four times a year by the Defense Standardization Program Office (DSPO). Opinions represented here are those of the authors and may not represent official policy of the U.S. Department of Defense. Letters, articles, news items, photographs, and other submissions for the *DSP Journal* are welcomed and encouraged. Send all materials to Editor, *DSP Journal*, Defense Standardization Program Office, 8725 John J. Kingman Road, STOP 5100, Fort Belvoir, VA 22060-6220. DSPO is not responsible for unsolicited materials. Materials can be submitted digitally by the following means:

e-mail to DSP-Editor@dla.mil
CD or DVD to *DSP Journal* at the above address.

DSPO reserves the right to modify or reject any submission as deemed appropriate.

Gregory E. Saunders
Director, Defense Standardization Program Office

Timothy P. Koczanski
Editor, Defense Standardization Program Journal

Defense Standardization Program Office
8725 John J. Kingman Road, STOP 5100
Fort Belvoir, VA 22060-6220

703-767-6870
Fax 703-767-6876

dsp.dla.mil

For a subscription to the *DSP Journal*, go to **dsp.dla.mil/newsletters/subscribe.asp**

Director's Forum

In many ways, the story of standardization within the United States has its roots with the U.S. military. As far back as the early 19th century, needs, requirements, and resources drove much of the commercial standardization we take for granted today.

Eli Whitney, who is generally considered the founding father of standardization in the United States, received a contract to produce 10,000 muskets for the U.S. military. The reason he received the contract was largely due to his guarantee that the parts of every musket would be interchangeable and that the muskets could be produced quickly because of production standardization. And while his standardization concepts had a strong foundation, in the end, he ended up going over budget and over schedule, and the parts were not as interchangeable as he had promised. Though he fell short of his goals, Mr. Whitney became legendary—not only in the United States, but abroad—for his standardization concepts. In fact, to many throughout the 19th century, standardization was known as the American system of manufacturing.

Although the concept of standardization of materiel in support of the warfighter can be tied to its humble roots in the 19th century with the provision of muskets to the infantry, many standardization lessons were learned the hard way, by witnessing firsthand how the lack of interoperability caused a reduction in capabilities. For instance, during World War II, British tanks and trucks broke down under the strain of desert warfare. The underlying issue was the fact that the nuts, bolts, and screws loosened or wore out due to the harsh desert environment. To assist with the defeat of Rommel, the United States shipped vast quantities of replacement fasteners. Much to everyone's surprise, none of the replacement fasteners worked. As it turned out, the United States used Sellers screw thread standards, while the British used Whitworth screw thread

Gregory E. Saunders
Director
Defense Standardization Program Office

standards. This lack of standardization caused broken-down tanks to remain inoperable.

After World War II, we as a nation were still having interoperability issues with our allies. In an article written more than 40 years ago, Robert Rhodes James commented on the lack of interoperability during a U.S.–British Air Force exercise in which the only standardized items between the two forces were wheel chocks. In the article, Mr. James did not seem very optimistic that NATO would ever achieve any significant standardization success.

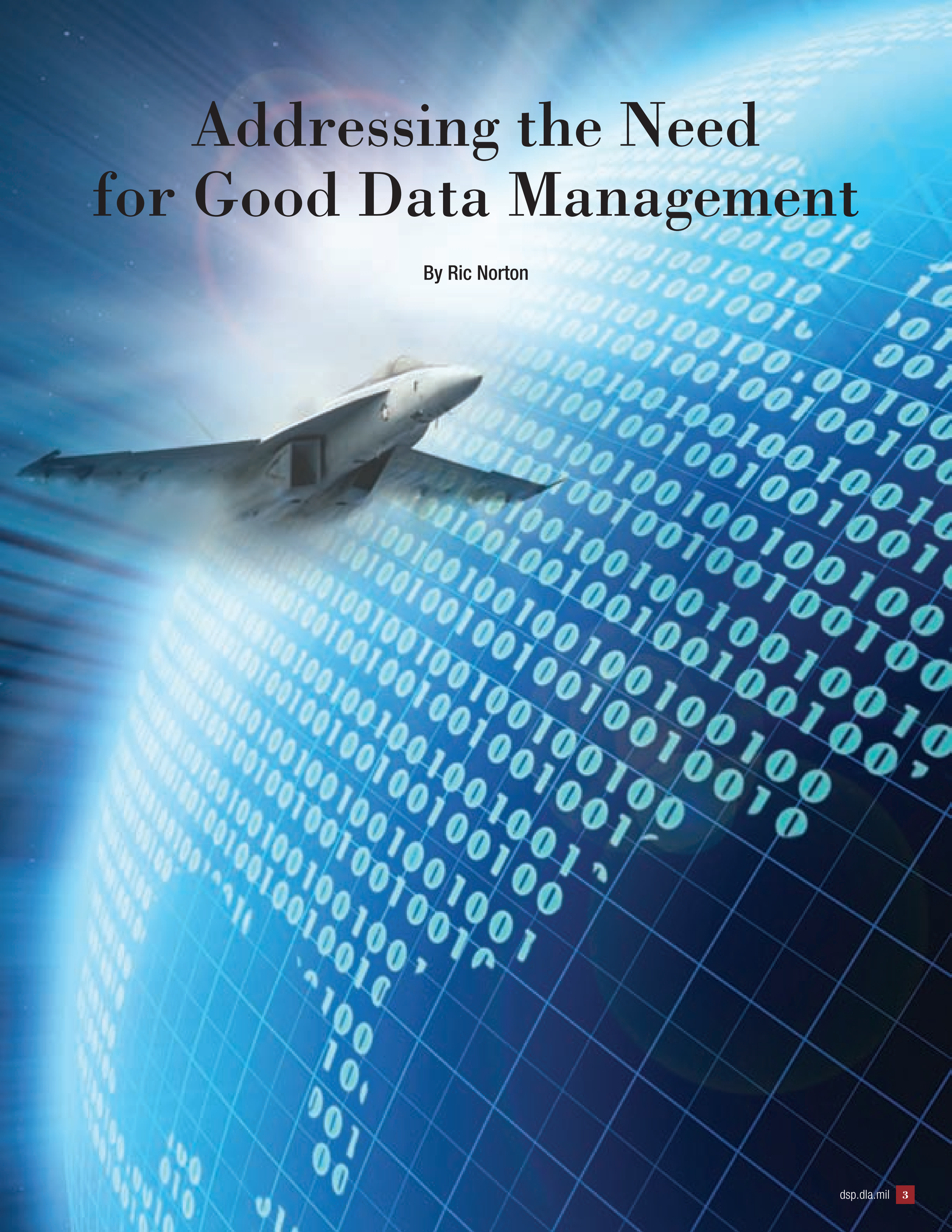
In each of these three cases, standardization was the solution to correcting many shortcomings. Moreover, standardization became the force multiplier of capabilities for both U.S. and allied forces at times of war.

In the case of Eli Whitney's standardization concepts, which drew a lot of praise, it was his cousin, Amos Whitney, who, in the 1860s, perfected those concepts with his business partner Francis Pratt. Together, Pratt and Whitney had great success in mass producing guns for the Union Army during the Civil War. Even after the war, they used those same standardization principles to mass-produce sewing machines, bicycles, automobiles, and, eventually, aircraft engines.

In the case of fasteners used on British tanks, the United States ended up sending hundreds of Sherman tanks to the British, so the allies achieved standardization through common equipment as they faced Rommel. But just think how much simpler and less expensive it would have been to have had a common screw-thread standard.

And finally, in the case of lack of standardization during a joint U.S.–British Air Force exercise in 1967, I believe Mr. James would be quite shocked to find out that during Operation Enduring Freedom, it was not uncommon for U.S. F/A-18 Hornets to receive fuel from British VC-10 tankers. Standardization Agreement 3447, "Aerial Refueling Equipment," is the underlying document that makes that possible.

These historical cases show how standardization was able to support the warfighter. Innumerable other cases of standardization, but without the same visibility, are just as important in supporting the warfighters' mission. This issue of the *Journal* explores some projects of great potential. My hope is that these stories will pique your interest and enable you to apply many of the lessons learned to your own interoperability challenges.



Addressing the Need for Good Data Management

By Ric Norton

Historically, it has been difficult to obtain adequate data to identify, catalog, procure, reprocure, and maintain and dispose of parts and equipment for the warfighter. However, that situation is beginning to change. The December 2008 update of DoD Instruction 5000.02, "Operation of the Defense Acquisition System," includes a requirement for program managers to develop a data management strategy that addresses the long-term need for technical data on their systems, including data required to design, manufacture, and sustain the system. In addition, the Weapon Systems Acquisition Reform Act of 2009 places a renewed emphasis on the importance of systems engineering and directs the Under Secretary of Defense for Acquisition, Technology and Logistics to appoint a senior director of systems engineering to ensure that all weapon systems reviews include systems engineering considerations.

Data management is an essential function that supports systems engineering to help ensure that the as-designed system becomes the as-built system that is fully supportable and sustainable. At the heart of any data management strategy is the technical data package (TDP), which is essential if the system must be remanufactured and can be critical in helping to sustain the system throughout its life cycle. Working together with military services and other government agency provisioning offices, the Defense Logistics Information Service (DLIS) has been integral in helping to define TDPs so that they not only will enhance support in the initial fielding of weapon systems, but also will define and drive technical data requirements in future acquisitions for all military services.

Background

The TDP for a weapon system is intended to provide complete and clear information—overall system design; functional capabilities; performance and design specifications; design constraints; applicable standards; compatibility requirements; and personnel, equipment, and facilities requirements—for system operation and logistical support. Because of the broad range of information, weapon systems TDPs can vary significantly, and the information in them can be interpreted in various ways by different technical data users within the acquisition and sustainment communities. Moreover, the technologies and the way data are furnished have changed.

To determine how to better support the TDP requirement, as well as determine the best way to display TDP information, representatives from the Navy, Army, and National Institute of Standards and Technology formed the DoD Engineering Drawing and Modeling Working Group (DEDMWG).

The initial effort of the working group was to make a data call through the Acquisition Community Connection (sponsored by the Defense Acquisition University) looking for parties in both government and industry that had an interest in attending a DEDMWG meeting to revise MIL-DTL-31000, "Technical Data Packages." With more than 60 subject matter experts representing all branches of the services, the working group determined that the best way to satisfy data requirements, specifically for engineering data, was to develop standards and specifications for fully annotated three-dimensional models, which will replace two-dimensional drawings as the product master. In addition, the group recognized the need to define the levels of data within the Model Based Enterprise (MBE).

About the Model Based Enterprise

The MBE is defined as the linkage, through a common information-based environment, of Model Based Engineering, Model Based Manufacturing, and Model Based Sustainability. The vision of the MBE is to enable the interaction of designers and customers in a fully integrated and collaborative environment to explore and evaluate solution options, based on modeling, simulation, optimization, and visualization techniques.

The basic focus of the MBE is on tools, and the interoperability of tools and processes, that optimize design, effective manufacture, and supportability of a product, for example, a weapon system. Optimization during the iterative steps in the developmental life cycle provides better coverage of the most important requirements, or key characteristics, of the weapon system. In other words, a robust MBE supports an up-front process for making decisions affecting a product's life cycle while designs are still fluid. In addition, it reduces the life-cycle costs borne by the customer and the manufacturer's operational costs.

Problem/Opportunity

Some of the issues that surfaced during DEDMWG discussions appeared to be common across the services, for example, use of inconsistent terminology, data formats, and requirements for complete product definition. Other issues, such as outdated or inaccurate references used to contract for data requirements, related to support. One of the components involved in these high-level discussions, the Defense Logistics Agency (DLA), along with other key members, noted that good support means not only providing the right parts for warfighters, but also trying to anticipate the warfighters' needs while ensuring that all orders arrive at the right place and at the right moment they are needed.

In addition to ensuring that warfighters have the support they need to accomplish their mission effectively, DLA tries to do so without breaking the back of the taxpayer. One can imagine how difficult this would be to accomplish without accurate supporting engineering data and good logistics management information. Therefore, as a key stakeholder, DLA concurs with government intellectual property (IP) legal counsel that TDP requirements must be clearly defined as "deliverables" in any contract creating the information in order to secure government rights to those data.

The DEDMWG also concluded that different users need different levels of data and that different data are needed at different times during the product life cycle. In its discussions, the group discovered that it was not widely known or understood that the government has unlimited rights to the form, fit, and function information used for codification of national stock numbers. At the same time, the group realized that no one knew what defines form, fit, and function information. In short, what was lacking was a clear definition of common terms and standardized contractual language to ensure that the requirements could be understood by all.

The group also identified a host of other concerns regarding TDPs. It soon became apparent that simply redefining TDPs in MIL-DTL-31000 was just one task of many that needed to be accomplished. Therefore, only a portion of the meeting was devoted to a line-by-line review of the specification. A larger percentage of time was devoted to identifying opportunities for the DEDMWG. The experts present realized that they represented a cross-section of key government and industry stakeholders with the knowledge and leverage capable of making major changes in how technical data requirements could be better met in future weapon systems acquisition and sustainment practices.

Approach

To address the opportunities identified in its initial meeting, the DEDMWG decided to hold quarterly meetings to bring the stakeholders together for the purpose of reviewing and implementing changes to MIL-DTL-31000. In these early meetings, the working group developed wire diagrams to illustrate and identify relevant governing documents, manuals, directives, handbooks, letters, and related materials that each service currently uses to define and drive data requirements in their respective acquisition processes.

The DEDMWG also asked government IP legal counsel to help it better understand the contractual allocation of data rights in federal contracts, as defined by Title 10, Section 2320, of the U.S. Code, "Rights in Technical Data." In addition, the group asked systems and software providers to demonstrate their technological availability and three-dimensional imaging capabilities. Finally, DEDMWG members visited military depots to help identify requirements and current TDP utilization and processes, and they extended invitations to the user base to assist with establishing additional requirements. By taking this approach, the working group not only touched all facets of the user community, but also provided the transparency of who was pursuing what actions.

Outcome

After reviewing more than 900 coordinated suggested and essential comments, the DEDMWG began to define model levels (conceptual, developmental, and production) as a first step in the TDP reengineering process. The levels of models are defined in the recently updated MIL-STD-31000D, which revised MIL-DTL-31000C from a specification to a military standard. Subgroups within the DEDMWG have identified 10 major projects, which are in various stages of being funded. Research and development projects are being aggressively pursued to fully engage the MBE and satisfy all technical as well as product data requirements. Membership in the DEDMWG is also growing as more people become aware of the progress made to date. The DEDMWG is also reviewing the knowledge base of program offices to ensure that program managers are enforcing government data rights and that user data requirements are clearly written in contracts to satisfy both the fielding and sustainment of future weapon systems.

Although much work still needs to be completed, the DEDMWG is developing a TDP specification assistant, a web-based program that will create digital templates that program managers can use to write requirements in contracts. Standardization of common terms and abbreviations used to define data requirements throughout DoD is yet another focus of this group.

Despite the many challenges to eliminate many of the stovepipes in place at various activities, the DEDMWG hopes to foster a cooperative culture across the services and other government agencies in regard to defining and using TDPs.

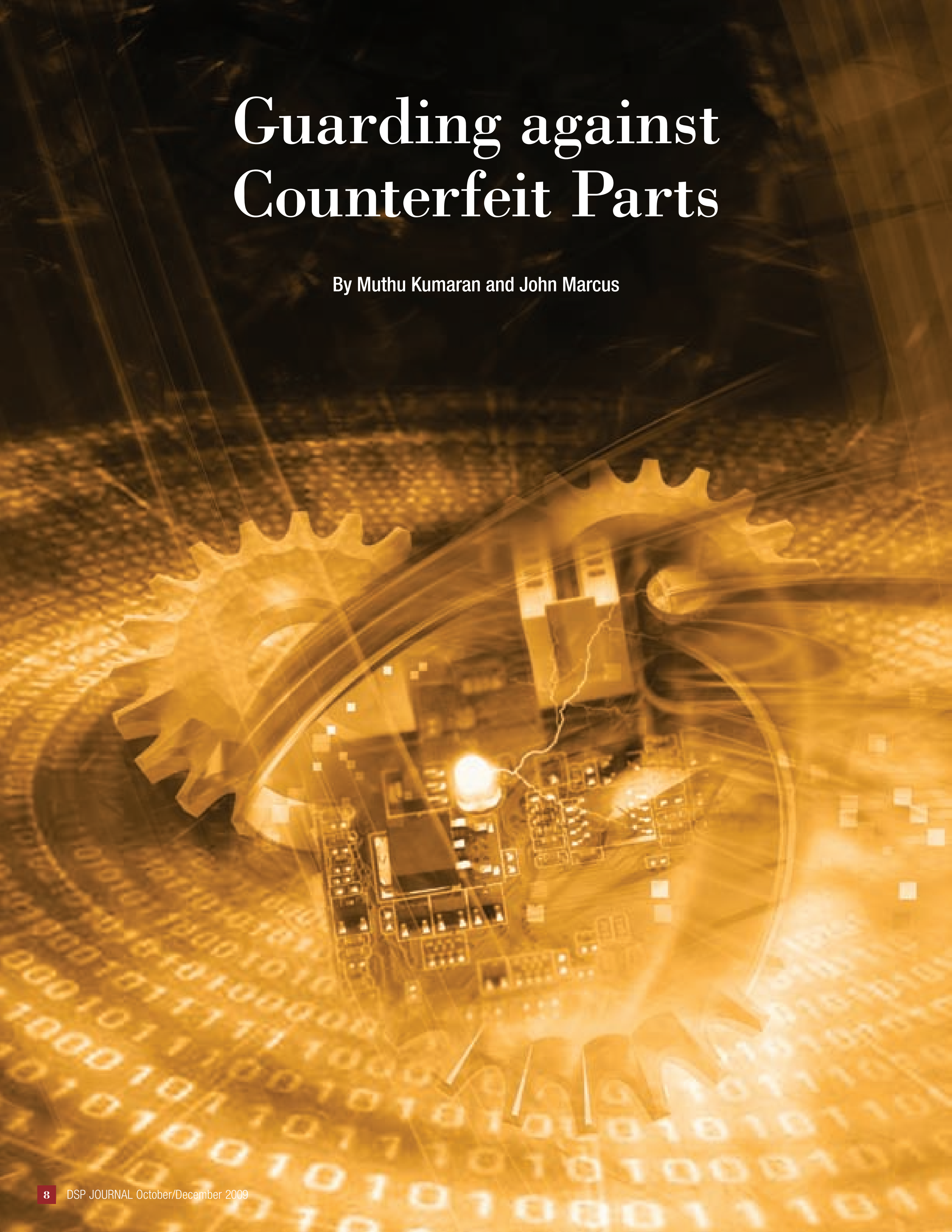
For more information about the DEDMWG and program updates, please contact Paul Huang (paul.huang@us.army.mil) or Ric Norton (richard.norton@dla.mil).

About the Author

Ric Norton, a supply systems analyst, currently leads a DLIS provisioning support team and cochairs the DEDMWG. Previously, he worked for the Air Force Cataloging and Standardization Center. Over the years, Mr. Norton has facilitated or served on numerous integrated product teams, integrated logistics support teams, product improvement groups, and program management reviews.

Guarding against Counterfeit Parts

By Muthu Kumaran and John Marcus



Counterfeit parts can threaten the effective operation of weapon systems and thus the safety of warfighters. And counterfeit parts are not a problem just for DoD. They affect all aspects of U.S. commerce.

The danger of receiving counterfeit parts from unscrupulous suppliers and having those parts find their way into weapon systems is well understood by the military services and the Defense Logistics Agency (DLA). Years ago, DoD began taking steps to keep those parts out of military systems. Today, because of a large body of work by subject matter experts suggesting that the extent of counterfeiting of parts is significant, there is renewed interest in what protections are working and what else should be done about counterfeit parts. By far the biggest area of current concern among government and private organizations involves the counterfeiting of electronics commodities.

Before we address how DoD guards against such nefarious parts, let's understand what we mean by a "counterfeit" part.

What Is a Counterfeit Part?

Each public and private organization seems to have a different definition for counterfeit, but they all have a similar theme, namely, someone along the supply chain intends to deceive the customer buying the part. This does not mean that a supplier is engaged in counterfeiting if it provides a customer a bad part, whether it is the wrong part, a poor quality part, or an incorrectly marked or packaged part. A bad part may be a problem for the customer, but if the manufacturer of the part or the intermediaries (if any) handling the part are not intentionally deceiving the customer, it is simply a bad part—not a counterfeit.

At an April 2009 meeting jointly chaired by the Office of the Assistant Deputy Under Secretary of Defense for Supply Chain Integration (OSD) and DLA, representatives from the military services and defense agencies agreed to define a counterfeit part as "one whose identity or pedigree has been deliberately altered, misrepresented, or offered as an unauthorized product substitution." They further agreed that "identity" refers to the original manufacturer, part number, date code, lot number, testing, inspection, documentation, warranty, and so on. The word "pedigree" in the definition means origin, ownership history, storage, handling, physical condition, previous use, and so on.

Notice the inclusion of the word "deliberately" in the definition. That word protects suppliers that have made a mistake from potential allegations of providing counterfeit parts. Although a good thing, the inclusion of "deliberately" complicates matters in that it can be difficult and time-consuming to prove legally that a supplier intended to cheat the customer. Of course, that too is a good thing, because, although it may be inconvenient to the government, it forces the government to proceed thoughtfully and thoroughly. The consequences to a supplier of any implication of counterfeiting are significant. Such implications cannot be made lightly.

How Does DoD Track Counterfeit Parts?

DoD has two main sources of commonly available data about counterfeit parts:

- *Government-Industry Data Exchange Program (GIDEP).* Both commercial and government entities can file a report on the GIDEP website when they encounter counterfeit parts.
- *Product Quality Deficiency Reports (PQDRs).* Military end users can submit a PQDR when they return an item to the supply system and seek a refund. The PQDR includes sections on manufacturer information, contract information, item quantity and cost, and description of defect, to name a few.

Both GIDEP and PQDRs are voluntary, which may result in underreporting of counterfeits, but for different reasons. For example, anecdotal evidence suggests that industry participants are hesitant to submit GIDEP reports because they are not anonymous. Companies are reluctant to submit reports, fearing lawsuits from suppliers. (Only about 90 incidents of counterfeit parts were reported to GIDEP between 2003 and 2007.) The PQDR has no section reserved specifically for counterfeits. If someone suspects a part is a counterfeit, the section seemingly most applicable is the "description of the defect," but we cannot be sure it will be interpreted that way by everyone, every time. (Between December 2005 and April 2009, only three reports specifically citing counterfeit parts were added to the PQDR database: one for a disk brake parts kit, one for a stepladder, and one for a rope and wire item.)

GIDEP and PQDRs may be the common sources of data, but they are not the only sources. Each DLA inventory control point has a counterfeit materiel/unapproved product substitution (CM/UPS) team. These teams are charged with investigating and taking appropriate action whenever a suspect part is encountered. The teams have subject matter experts from procurement, engineering, and other fields as necessary, and because the appropriate action sometimes involves legal recourse, CM/UPS teams are led by legal counsel. Such information, understandably, must be carefully guarded and shared only with those with a need to know. Thus, data associated with the work of these teams are not routinely accessible.

It is difficult to determine, due to the reporting issues cited above, the extent to which counterfeits have infected DoD's supply chains. (In any case, even a single failure can have a catastrophic effect.) The picture may improve once the OSD/DLA working group definition of a counterfeit part is officially approved. In particular, the existence of an official definition, which would be objective as opposed to subjective, would give legitimacy in accessing counterfeit parts and would offer more consistent reporting of counterfeits (versus defects) on PQDRs.

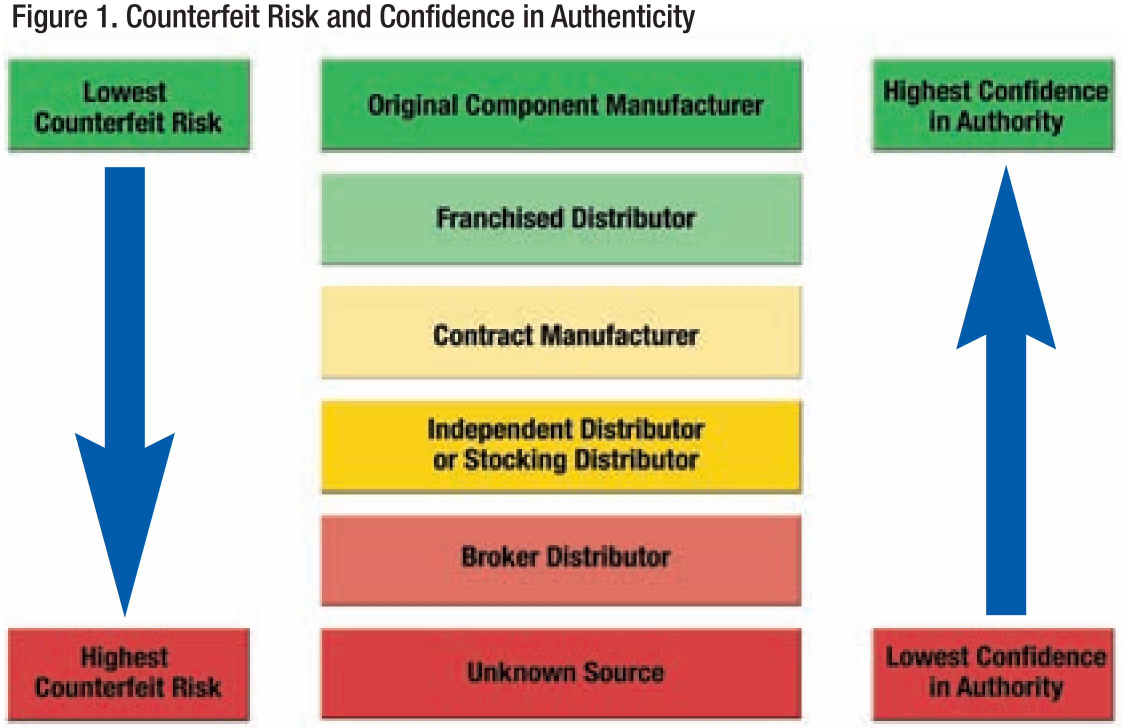
Another area offering opportunities to improve on determining the extent of the counterfeit problem concerns GIDEP. GIDEP managers are looking for ways to increase reporting, but there appear to be no easy solutions. One possibility under consideration is to make reporting of counterfeits mandatory in GIDEP, which would be logical because GIDEP is the federal government's central database for receiving and disseminating information about counterfeit and other nonconforming products and materials.

Beyond DoD, the Department of Commerce and the Federal Bureau of Investigation are significant players in anticounterfeit activities and have data that would be useful for guarding against counterfeit parts.

What Best Practices Can Lessen the Exposure to Counterfeits?

According to organizations that have investigated the problem, the best way to guard against counterfeits is to procure items only from original component manufacturers or their authorized suppliers. Figure 1 shows how the risk of counterfeits increases as confidence in authenticity decreases.

Figure 1. Counterfeit Risk and Confidence in Authenticity



Private companies have few restrictions on their selection of suppliers, but DoD does not have the same flexibility. The acquisition regulations to which DoD is subject generally require full and open competition, meaning any original component manufacturer, franchised distributor, or unaffiliated parts broker that can meet DoD's needs can compete for a contract. (Brokers can range from a single individual working out of his or her home to a formal, incorporated business with many employees.) DLA has taken steps to comply with the intent and spirit of the acquisition regulations, while still improving the likelihood that its suppliers are qualified to provide legitimate parts. The Defense Supply Center Philadelphia (DSCP) and Defense Supply Center Columbus (DSCC) have implemented the Qualified Suppliers List of Distributors. The current list covers specific counterfeit-susceptible commodities, such as fasteners and electronics parts. Distributors on the list must follow quality control procedures that are subject to DSCP and DSCC inspection.

Other best practices for keeping counterfeit parts out of the supply chain include developing counterfeit parts control plans, increasing the sharing of information, creating incentives to improve the reporting of counterfeits, and ensuring the proper disposition of counterfeits.

Another way to guard against counterfeits involves traceability, that is, the paper or electronically certified trail of a part from the manufacturer through all intermediate parties. DLA recently updated its instructions on how procurement personnel should ensure traceability.

Laboratory testing of parts can also ensure the detection of counterfeits. DLA has three specialized product test centers (in Pennsylvania, Ohio, and California) staffed and equipped to do the technical evaluation of parts and determine if they are genuine or not. In addition, the Navy has a laboratory testing center in Indiana that provides a similar service for customers who want assurance about the quality of their parts.

Training is another counter-counterfeit practice. The military services and DLA provide their employees with job-specific training, but there has been no overarching anti-counterfeit course. In response to this deficiency, the Naval Air Systems Command contracted with a private-sector company to develop an online course to be hosted on the Defense Acquisition University's website. It will be available to both private-sector and government personnel.

Other best practices for keeping counterfeit parts out of the supply chain include developing counterfeit parts control plans, increasing the sharing of information, creating incentives to improve the reporting of counterfeits, and ensuring the proper disposition of counterfeits. DoD is addressing each of these practices to determine how to reduce any vulnerability it may still have to counterfeits.

Conclusion

Recognizing that counterfeit parts can threaten the effective operation of weapon systems and the safety of warfighters, DoD is examining the extent of its exposure to counterfeits and the effectiveness of its current processes for reducing that exposure. As a result of that effort, DoD has identified ways it can improve the processes to detect, prevent, report, and dispose of counterfeit parts.

About the Authors

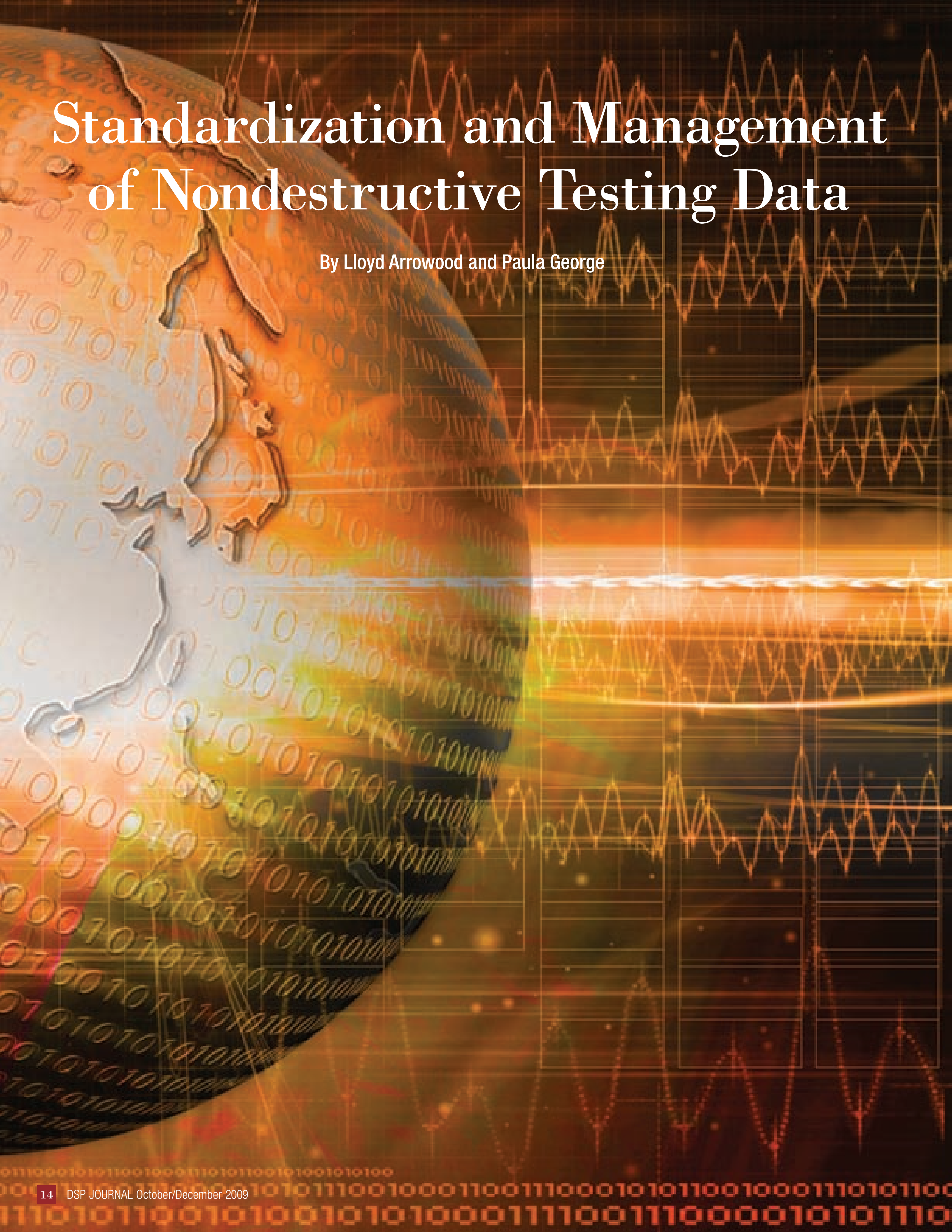
Muthu Kumaran and John Marcus are research fellows with LMI.

Mr. Kumaran has many years of experience as an information technology consultant, providing services in custom software development and data warehousing to a number of public-sector and Fortune 500 clients.

Mr. Marcus has extensive experience with the Office of the Deputy Under Secretary of Defense (Logistics and Materiel Readiness), where he was the deputy director for supply management policy. At LMI, he has worked on projects involving performance-based logistics, DoD executive agents, and Defense Acquisition University course development.

Standardization and Management of Nondestructive Testing Data

By Lloyd Arrowood and Paula George



Nondestructive testing (NDT) encompasses a wide variety of analytical techniques used in science and industry to evaluate the properties of materials, components, or systems without damaging or permanently altering them. NDT can save both money and time in evaluation, troubleshooting, and research, and it is invaluable for inspecting systems such as nuclear power plants, bridges, and military hardware.

A number of commonly used NDT methods generate large amounts of data. Among those methods are digital radiography, phased-array ultrasound and phased-array eddy current, shearography, and thermography. The data generated, along with inspection records, must be maintained for the entire system life span. Because the life spans of some systems are long (20 to 100 years or more), and because NDT data need to be accessed periodically throughout the system life cycle, efficient and effective data management solutions for long-term data retention and access are crucial.

One problem that must be addressed is data standardization. Data standardization is an issue because, over long time periods, inspection equipment will be replaced, while the need to access the data acquired with that equipment will remain. An added problem is the development of new technology. Not only will obsolete technology no longer be supported, but to keep up with technological changes, the NDT community will need to make the transition from analog to digital. In short, to ensure that NDT data are readily accessible throughout system life spans, the data must be standardized and managed in a way that promotes interoperability as inspection equipment is modernized and data are transferred to the newer systems.

The Federal Working Group on Industrial Digital Radiography (FWG-IDR)—organized by representatives of several federal agencies, including DoD, the National Aeronautics and Space Administra-

Examples of Systems with Long Life Spans

Nuclear power plants—40 to 60 years
Reference: James G. Hewlett, "The Operating Costs and Longevity of Nuclear Power Plants," *Energy Policy*, Vol. 20, No. 7 (1992), pp. 608–622.

Bridges—50 to 100 years or more
References: Fred Moses, "Bridge Reliability Concepts and Methods," *Bridge Safety and Reliability*, Dan M. Frangopol, ed. (Reston, VA: American Society of Civil Engineers Publications, 1999), p. 9.
Public Information Office, Oakland, CA, "Bay Bridge East Span Project," http://www.dot.ca.gov/dist4/eastspans/index.html, August 15, 2008.

Military and commercial aircraft—20 to 90 years
Reference: Sydney J. Greenberg Jr., "Wear and Tear Adds Up on Military Aircraft," *National Journal*, March 21, 2008.

Naval ships—30 years or more
Reference: Stan Zimmermann, *Submarine Technology for the 21st Century*, 2nd ed. (Bloomington, IN: Trafford Publishing, 2000).

tion, and the Department of Energy—has begun addressing some of these issues as they relate to digital radiography. The FWG-IDR has identified several transitional hurdles facing the industrial NDT community as it transfers from analog and physical methods of data capture to digital methods. One example is the long-term retention of digital radiographic data and the associated metadata as the production of radiographic film is discontinued by suppliers. Although the FWG-IDR is focused on digital radiography, its work on data standardization and management will benefit all methods of NDT data management.

Background

In the 1980s, the medical field faced problems similar to those found in the NDT inspection equipment industry today, in that manufacturers of medical imaging devices supported only proprietary communication and data exchange mechanisms.[1] At the time, data captured on one manufacturer's equipment could not be transferred or used on equipment built by another manufacturer, and the data were not standardized (files in a certain modality were not necessarily the same for all manufacturers). To address this problem, manufacturers and users of radiological imaging equipment started the Digital Imaging and Communications in Medicine (DICOM) Committee to develop a standard. The committee issued DICOM 1.0, the first version of the standard, in 1985 and DICOM 2.0 in 1988. The standard continued evolving and was issued as DICOM 3.0 in 1993. (DICOM 3.0 was subsequently published by the National Electrical Manufacturers Association.) Patterned after ISO's Open System Interconnection, DICOM enables digital communication between diagnostic and therapeutic equipment and systems from various manufacturers.

In the late 1990s, a group of experts in nondestructive evaluation examined the similarities between medical and industrial NDT inspection systems. Using DICOM 3.0 as a foundation, ASTM International Committee E07.11 developed the Digital Imaging and Communications in Nondestructive Evaluation (DICONDE) standard, ASTM E 2339.[2] The DICONDE standard still faces many challenges due to the differences in medical evaluations and industrial inspections. Some modalities such as computed radiography, direct digital radiography, and computed tomography have analogous data requirements in the medical domain. Other modalities such as ultrasonic inspection, some phased-array methods, and neutron radiography can adapt existing medical data areas to create an NDT representation. Inspection modalities such as eddy current and shearography have no medical analogy and require novel approaches. The ASTM subcommittee is working on some of these modalities, but others such as neutron radiography, shearography, and thermography are not being developed at this time.

The FWG-IDR is supporting the continued maturation of the ASTM DICONDE standard and is promoting the adoption of DICONDE by DoD, as well as by other government agencies and by government contractors. Currently, the Defense Logistics Agency is working toward DoD adoption of ASTM E 2339.

The FWG-IDR is also promoting the active involvement of its members and all federal government NDT professionals in ASTM subcommittees to extend ASTM standards related both to new NDT imaging modalities and to NDT data management. In addition, the FWG-IDR is addressing NDT data standardization and management issues. For example, the group formed a team to develop recommendations for long-term retention of digital NDT inspection data. That team authored a paper describing the need for retaining inspection data for extended periods of time and defining the need for standardized data exchange mechanisms to preserve legacy data.

Although considerable progress has been made, much remains to be done. Currently, the focus is on the use of conformance statements and on media management and technology migration.

Use of Conformance Statements

Currently, when new equipment is used for industrial inspections, it is unlikely that any data captured by an older legacy system will be compatible with the new equipment; data may be lost, may not be transferrable, or may not be openable. To address this problem, the DICONDE standard has specific requirements for interoperability among equipment vendors. Vendors demonstrate their products' DICOM/DICONDE compliance using conformance statements. A typical conformance statement identifies the storage classes that can be transmitted and indicates any vendor extensions, specializations, or privatizations to modules (e.g., the use of any private tags). It also specifies configurations, documents, supported modules, and tags. The availability of conformance statements enables detailed comparisons of vendor products.

Both ASTM and the FWG-IDR are working to develop ways to further address compatibility and standardization among manufacturers' inspection systems. ASTM is considering the development of DICONDE interoperability CDs or test suites as companions to the conformance statements. The availability of such suites would accelerate the adoption of DICONDE-compliant solutions, because federal government NDT procurement personnel could objectively evaluate the interoperability of each vendor's product to make an informed purchase decision.

The FWG-IDR is developing a suite of DICONDE interoperability tests to validate metadata, CDs, and DICONDE messaging between workstations and NDT imaging devices. This suite of tests will complement a vendor's conformance statement by exercising the features of a vendor's products to verify compliance with the DICONDE standard.

Media Management and Technology Migration

The impermanence of digital media has been recognized for several years. Researchers have suggested the use of standards, among other approaches, to solve problems associated with obsolete storage media and proprietary formats. Part 10 of the DICOM standard discusses the use of CDs and DVDs to store data. With the advent of Blu-ray storage media, portable storage is increased dramatically. Although this increase in capacity permits multiple studies or emerging multiframe studies to be stored on a single Blu-ray disk, care must be taken to ensure that disks are duplicated regularly so that media failure will not result in the loss of data. It has been found that some CD and DVD media degrade after only 6 to 8 years, so a robust backup schedule must be followed unless high-quality storage media are used.

Centrally managed digital archives should follow backup schedules with disaster recovery procedures. DICONDE-compliant software systems could store studies on centralized storage systems and migrate data to newer media on a prescribed schedule. This approach, however, requires adequate funding to procure new media as technology changes and to support data migration. It remains a constant challenge to obtain funding to gain long-term benefits in periods of constrained funding.

The most important task in technology migration is the identification of the most valuable data and the establishment of a schedule to migrate the data to newer media. Most of the failures have involved the loss of data or a large expense in recovering data from media that had been ignored for long periods of time. Another goal of the FWG-IDR is to raise awareness of the issues involved in technology migration.

Future Work

The FWG-IDR is exploring data transmission and image-sharing techniques to ensure data integrity and security across wide area networks. It also is devising approaches to analyzing network performance for determining the impact of multiframe Information Object Definitions (IODs). One of the tasks facing government NDT operations is the establishment of secure communication channels using virtual private networks or hardware encryption/decryption devices. It needs to analyze wide area and local area network performance to determine the need for compression when transmitting large data streams such as multiframe IODs consisting of computed tomography or radioscopy data.

Another area being investigated by the FWG-IDR is data mining of metadata. The group's focus is on identifying possible performance degradation of NDT imaging equipment over time through usage statistics or the analysis of calibration data. Equipment usage statistics (such as plate exposures) could be used to identify subtle, yet meaningful, changes in the inspection process. Component aging studies could be supported by metadata analysis.

Finally, the FWG-IDR is attempting to conduct quantitative studies of legacy data management costs. Its goal is to demonstrate the efficacy of data standardization and management techniques to minimize the costs. The possibility of significant cost savings by the federal government and its contractors is a motivating factor in devising a unified approach to standardization and management of NDT data.

Conclusions

Adoption of new inspection techniques within the federal government will require NDT professionals to be cognizant of the differences between, and the limitations and benefits of, data management of analog and physical inspection records versus digital inspection records. In addition, as the DICOM and DICONDE standards evolve, their proponents will face other challenges. For example, they will need to develop modules for capturing and storing NDT inspection data for modalities with no medical analog (such as eddy current).

A new effort of the ASTM Committee E07.11 will be to update the DICONDE standard to address the new media being used to store digital radiographic and tomographic data. Specifically, although DICOM Part 10 specifies data archival mechanisms, the standard's descriptions of the appropriate storage requirements for archival media must be updated to eliminate the obsolete term "radioscopy" and to address CDs and DVDs.

[1] Herman Oosterwijk, *DICOM Basics*, 3rd ed. (Aubrey, TX: OTech, Inc., 2005).

[2] See NEMA Standard PS3, "Digital Imaging and Communications in Medicine (DICOM)" (Rosslyn, VA: National Electrical Manufacturers Association, 2008), and ASTM Standard E 2339, "Standard Practice for Digital Imaging and Communication in Nondestructive Evaluation (DICONDE)" (West Conshohocken, PA: ASTM International, 2008).

About the Authors

Lloyd Arrowood and Paula George co-lead the FWG-IDR's Data Standardization and Management Task Team.

Mr. Arrowood is a senior technical staff member for Babcock & Wilcox Technical Services, which manages the Y-12 National Security Complex in Oak Ridge, TN, for the Department of Energy. He has 30 years of experience in advanced information technologies, including 10 years of experience in deploying information systems for nondestructive testing operations.

Ms. George is a quality/technical analyst at the Defense Logistics Agency, Logistics Operations and Readiness. She has more than 30 years of experience in materials engineering, including 20 years with nondestructive testing.

The Transformation of NATO Standardization and Interoperability

Challenges and Opportunities for DoD

By George Sinks

The end of the Cold War two decades ago precipitated a fundamental, if uneven, transformation of NATO capabilities, strategy, and membership. The United States and other allies dramatically reduced the number of heavy forward-deployed forces in Central Europe, agreed on a new strategic concept, and restructured NATO's military command structure. Most important, NATO nearly doubled in size as it admitted the new democracies of Central and Eastern Europe. As significant as these changes were, NATO transformation remained incomplete. However, the events of September 11 and the alliance's subsequent involvement in Afghanistan injected new urgency in this effort. In particular, they underscored the need to improve NATO capabilities and structures to operate in complex crisis response operations in austere locations far from NATO territory.

The operational challenges of Afghanistan and the admission of new members has focused new attention on the state of interoperability within NATO and on its key enabling process: standardization. There is a growing consensus that significant alteration, if not transformation, of the alliance's approach to interoperability and standardization will be required if NATO is to remain relevant in the current and future security environment. Enhancing interoperability improves the effectiveness of NATO operations and saves allied lives and resources.

The United States has been a leading advocate within NATO for these changes, and their ultimate success will depend in large measure on how well they are accepted and implemented by the United States. In light of this fact, it is important for a U.S. audience to understand NATO's ongoing efforts to enhance interoperability and refashion its standardization policy and process, as well as to understand the implications for DoD.

NATO Action Plan for Enhancing Interoperability

At the April 2008 Bucharest Summit, the heads of state and government directed the North Atlantic Council to review and recommend ways of improving the state of interoperability within the alliance. In the first phase of this effort, known formally as the Action Plan for Enhancing Interoperability (APEI), key NATO defense planning committees and the NATO military authorities (NMAs) completed a questionnaire on the current and projected state of interoperability within their areas of responsibility. Nations were invited to provide input as well.

The results of Phase I, reported in spring 2009, were not surprising. Widespread shortfalls in interoperability exist across many capability areas within nations, between national forces, and among national and NATO forces and their systems and equipment. The most critical shortfall identified by the NMAs was the inability to communicate at all levels of command, caused by a combination of human factors, such as lack of language skills, and the lack of interoperable equipment. The NMAs also identified shortfalls in equipment, logistics, education, training, and doctrine.

Respondents from NATO and its allies agreed that the mechanisms for achieving interoperability are poorly understood and that one of the causes of insufficient interoperability was the nations' failure to implement agreed-on NATO standardization agreements (STANAGs). At the same time, the Phase I report concluded that the need for real and effective interoperability among nations is increasing as NATO operations become more expeditionary, ad hoc, and dynamic and as nations and NATO migrate to a network-enabled operational environment. Though its initial conclusions echoed prior interoperability assessments, the APEI is the first to involve all key stakeholders and NATO processes. Moreover, it has a mandate to provide regular progress reports to the defense ministers of NATO nations.

> A critical element of such a long-term approach is the identification of interoperability requirements and the validation of interoperability solutions.

Phase II of the APEI, which began early in 2009, is focusing on identifying solutions and developing implementation plans. As part of this work, the NMAs and lead committees are reviewing and prioritizing NATO interoperability shortfalls, with a focus on short-term solutions. At the same time, the Phase I report noted that interoperability is inherently a long-term challenge that must be addressed as part of a new or adapted NATO defense planning process, not a standalone process. A critical element of such a long-term approach is the identification of interoperability requirements and the validation of interoperability solutions. Tellingly, the Phase I report also highlighted the long-term need to facilitate national implementation of NATO STANAGs and allied publications.

As of this writing, work on Phase II continues. In support of this effort, allies, including the United States, may be requested to update the implementation status of selected NATO STANAGs. Additional Phase II work will include the development of a long-term plan to resolve remaining interoperability shortfalls and a revision of the NATO policy for interoperability.

Changes to NATO Standardization Policy and Process

Paralleling NATO's high-level work to enhance interoperability is a less-publicized, but equally important, effort to revise policies and procedures for NATO standardization. In December 2005, the NATO Committee for Standardization Representatives agreed to establish an ad hoc working group, known as the Standardization Document Management Working Group (SDMWG). The purpose of the group was to examine a proposal made by France to restructure the management of NATO standardization documents. The SDMWG was eventually tasked with recommending a new architecture for the development, ratification, management, and promulgation of standardization documents and to revise the relevant portion of AAP-3, the capstone document for the development of NATO standardization agreements. One of the primary strategic drivers of this work was to better focus NATO standardization activities and agreements on achievement of alliance interoperability requirements.

The ambitious mandate for the SDMWG's work inevitably raised concerns among some allies as to the purpose and feasibility of the original tasking. However, thanks to the consistent support of a core group of allies, including the United States, the SDMWG agreed to a revised version of AAP-3, designated as AAP-03(J), early last summer. The revised version, "Directive for the Production, Maintenance, and Management of NATO Standardization Documents," is in the final stages of national review at NATO, and final approval is expected soon.

The revised AAP-3 contains the following major changes:

- Establishes linkages between NATO standardization documents and the initial requirements
- Improves the scope of NATO STANAGs to support allied interoperability requirements
- Introduces a new type of NATO standardization document, the standardization recommendation (STANREC), for standards or procedures that do not relate to interoperability
- Expands procedures for using civil standards within NATO.

An important aspect of these changes is that existing STANAGs and allied publications will be assessed against existing interoperability requirements as part of the current review cycle of NATO standardization documents. Documents that cannot be linked to an interoperability requirement may be converted to STANRECs; remaining STANAGs will focus on interoperability-related standards.

Though not yet published, AAP-03(J) has the potential to improve the integration of NATO standardization processes and products with interoperability and to accelerate the release of nonbinding best practices to allies for early use. It implicitly addresses the concerns of new, smaller allies (and perhaps larger ones as well) that have pointed to the difficulty of knowing which NATO standardization documents are truly vital for enhancing interoperability in alliance operations. These same allies have also expressed a desire to quickly identify and share best practices across all capability domains to enhance their participation in ongoing NATO operations.

Implications for DoD

As the largest member of the NATO alliance, and as a strong supporter of the APEI and the new AAP-03(J), the United States has a strong interest in and responsibility for the success of both efforts. For over a decade, we have pushed NATO and allies to develop and focus alliance capabilities on expeditionary crisis response operations. NATO's 2006 *Comprehensive Political Guidance* articulates a need for "forces that are fully deployable, sustainable and *interoperable* and the means to deploy them" (emphasis added). Notwithstanding recent substantial progress in improving allied deployability and sustainability, interoperability has been ignored or given lip service until now. The APEI is bringing badly needed high-level attention and an operational perspective to the management of NATO interoperability, and it has the potential to formalize and nest interoperability planning within NATO's core defense planning processes. The ongoing and prospective efforts to prioritize interoperability shortfalls and identify long-term interoperability requirements are crucial to the ultimate success of the APEI, and these will need strong U.S. political and technical support.

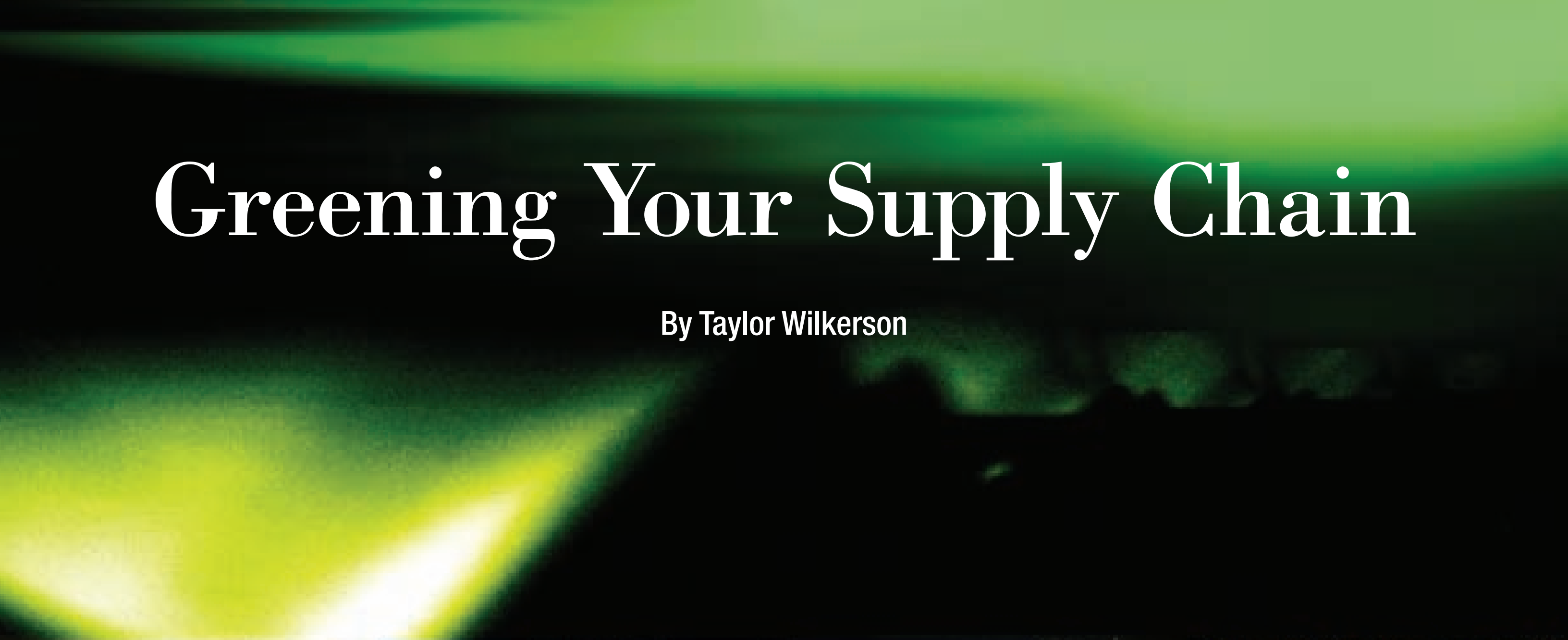
In that same vein, the revised new AAP-03(J) promises to focus one of NATO's longstanding core processes, standardization, on interoperability and, through the STANREC, make NATO standardization more timely and operationally relevant. Allies will be looking to the United States, as the largest and most important contributor to NATO standardization, to make these changes work. Within DoD, there are legitimate concerns about increased workload due to the need to review STANAGs and allied publications and to manage a new type of standardization document, the STANREC. Changes to internal DoD policies, procedures, and automated tools may be necessary. In the long run, however, the new AAP-03(J) promises to simplify and reduce the burden of managing NATO standardization within DoD by enabling it to focus its efforts on operationally important interoperability-related standardization requirements, while eliminating the need for time-consuming ratification and implementation of NATO standardization documents that do not meet this standard. Today, it is difficult for a U.S. operator, or anyone else, to identify those STANAGs or allied publications that are vital to our ability to operate effectively with NATO allies. If properly implemented, the new standardization procedures will make it easier to distinguish the operationally essential from the merely desirable in NATO standardization. At the same time, they will provide a vehicle for sharing doctrinal or technical best practices in response to a current operational need.

Summary

Financial constraints and the complex challenges of Afghanistan mandate a more operationally focused, yet affordable, approach to NATO interoperability and standardization. Though not yet complete, the APEI and the new AAP-03(J) represent major steps in this direction. Their ultimate success and the prospect of further transformation of NATO interoperability and standardization capabilities depend on a shared vision of the importance of these capabilities to NATO's future. The responsibility for defining and communicating that vision rests with the United States.

About the Author

George Sinks is an LMI research fellow with extensive experience at many levels of DoD in strategic planning, training development, organizational and process improvement, policy analysis, and procedures development for international defense programs and activities. He recently completed an Intergovernmental Personnel Act assignment in the Office of the Deputy Assistant Secretary of Defense for Europe/NATO Policy, with responsibility for NATO standardization and interoperability.



Greening Your Supply Chain

By Taylor Wilkerson

Can you estimate the effect your overall supply chain has on the environment? If you could, would you strive to make it more environmentally friendly? Today, many managers aspire to reduce the effect their organizations have on the environment. They know sustainable operations spare critical environmental resources, but they also recognize that sustainability can save money.

Supply chain sustainability integrates environmental thinking with traditional supply chain management. The scope of a sustainability program can incorporate the entire product life cycle. This cradle-to-grave approach checks environmental effects through product design, material sourcing and selection, manufacturing, product delivery, and end-of-life management of a product after its use (recycling or disposal).

In the private sector, many organizations may pursue sustainability for the cost savings from a reduction in waste and energy use. Others may want to market themselves as environmentally friendly. In the public sector, government agencies and departments must respond to regulations and executive orders to limit consumption and emissions. As the single largest buyer and distributor of supplies and services throughout the world, DoD must strive to ensure that the supply chain uses all resources efficiently, including energy, natural, and financial resources.

Whatever the motivation, significant benefits are to be had from greening the supply chain. Achieving those benefits requires careful coordination with each participant in the supply chain working toward a common goal. To help organizations understand how they can operate a sustainable supply chain, LMI developed the GAIA model. The model's value is in its application: it allows managers to implement and mature programs that will best support their goals of financial solvency and customer service excellence while reducing the impact of their operations on the environment.

Sustainability in DoD

On October 5, 2009, Executive Order 13514 directed federal government agencies to operate with energy and environmental efficiency. Among other requirements of the executive order, federal agencies must do the following:

- Measure and reduce greenhouse gas emissions from operations
- Measure and reduce emissions from the supply chain and other indirect sources
- Reduce fossil fuel consumption at least 2 percent per year through 2020
- Reduce water consumption by 2 percent per year through 2020
- Reduce waste generation and increase recycling
- Procure energy-efficient products and equipment.

In implementing these requirements, agencies must "prioritize actions based on a full accounting of both economic and social benefits and costs and shall drive continuous improvement by annually evaluating performance, extending or expanding projects that have net benefits, and reassessing or discontinuing underperforming projects."

From Executive Order 13514, *Federal Leadership in Environmental, Energy, and Economic Performance*, October 5, 2009.

GAIA Model Structure

The GAIA model is a process maturity model. Managers use maturity models to determine their organizations' current capabilities and plan for a desired maturity state. Such models must be detailed enough to identify areas in which process improvement will benefit the organization and the supply chain as a whole.

LMI's model evaluates sustainability initiatives by examining project cost savings, social value, and customer service enhancement. The model defines the maturity of current supply chain sustainability efforts and assesses the value created as those efforts mature. With the GAIA model, managers can make more informed decisions about which sustainability projects to implement, and in what order.

The GAIA model measures an organization's maturity against six fundamental components of sustainable supply chain management: strategy and vision, organization and culture, process and policy, information and communications, workforce and skills, and management systems. The model helps map the steps organizations must take for each component to move their supply chain toward sustainability and the next stage of maturity. The stages of maturity give the GAIA model its name: Genesis, Advancing, Innovating, and Accelerating:

- *Stage 1: Genesis.* A stage 1 organization is reactionary. It is compliance focused and fulfills only the bare minimum needed to be considered "green." Its processes are not aligned with corporate environmental goals, and the organization's supply chain is highly disjointed. The organization does not follow written standards, and sustainability efforts depend on individual personnel.
- *Stage 2: Advancing.* At stage 2, an organization anticipates the future of its sustainability initiatives. It establishes a slightly longer strategic timeline. Processes and policies are developed to comply with set corporate goals and objectives. An organization at stage 2 begins to use standards to collect, retrieve, and store data about the supply chain. Internal departments may be integrated, but supply chain partners are not. Sustainable supply chain decision making and development are still isolated to a few key people.
- *Stage 3: Innovating.* Once an organization's environmental and supply chain strategies are coordinated, it has reached stage 3. The workforce is working across units to coordinate strategies, and related training is available. An organization in stage 3 has developed formal standards for collecting, retrieving, and storing supply chain information and coordinating activities. It has some success in communicating with supply chain partners and engaging its stakeholders.
- *Stage 4: Accelerating.* An organization that has achieved stage 4 has fully integrated sustainability initiatives into its supply chain. It operates on a long-term strategic time-

line with an outcome-driven, visionary approach. The organization's processes are coordinated to achieve a corporate mission and fulfill well-defined goals and objectives. A stage 4 organization stays on the cutting edge of environmental discoveries by training its workforce and strategically outsourcing. The organization uses formal standards for collecting, retrieving, and storing supply chain data, and supply chain partners work together to plan new initiatives.

The six management components and four maturity stages of the GAIA model work together to define an organization's maturity. Table 1 illustrates this overall structure.

TABLE 1. Simplified GAIA Maturity Model

Management component	Stage 1: Genesis	Stage 2: Advancing	Stage 3: Innovating	Stage 4: Accelerating
Strategy and vision	Near term and tactical, with focus on compliance	Short term (1–3 years), with incremental improvements and focus on proactive compliance	Mid term (3–5 years), with delivery of outcomes, coordinated supply chain and environmental strategy, and focus on pollution prevention	Long term (5+ years), with transformation and sustainability as key driver and focus on standards that deliver value
Organization and culture	Unofficial advocacy and not by a manager; functional organization with little to no coordination	Advocacy as a collateral duty for a mid-level manager; informal coordination based on social networks	Advocacy as a designated management-level duty; cross-functional coordination of efforts; use of standardized processes	Sustainability manager reporting to chief executive officer; efforts coordinated through executive council and tied to corporate strategy
Process and policy	Designed for minimal compliance; locally developed, with scope covering specific activities	Designed for proactive compliance; locally developed but coordinated across functions, with scope covering multiple activities	Based on responsibility tenets; corporately developed and standardized, with scope covering functional requirements	Based on processes that implement corporate missions and minimize risk; corporately developed with full supply chain input, with scope covering supply chain operations
Information and communications	Segregated and limited; communication at local level	Visible but not shared; communication at local level; separate supply chain and environmental information	Visible among key partners; communication internal and external	Shared across the supply chain in real time; communication targeted to specific audiences; extensive use of information-sharing standards
Workforce and skills	Functionally focused, with few cross-functional requirements; training is ad hoc, with no structured requirements	Primarily functional, with some cross-functional awareness; training is anticipatory and recommended, but not mandatory	Cross-functional for a limited set of employees; training is organized and structured, but not mandatory	Fully cross-functional; mandatory training is organized, structured, standards based, and focused on specific skills
Management systems	Task-level oversight; task-level metrics used intermittently; focus on short-term return	Task-level oversight, but considers overall process; task-level metrics applied inconsistently; sustainability is part of budget overhead	Program-level oversight, with focus on performance improvements; standardized metrics applied consistently; sustainability is distinct part of overhead budget	Formal program-level oversight, with focus on outcomes; tailored metrics used on all tasks; costs tracked across the product life cycle; sustainability is dedicated budget line item

Applying the GAIA Model

Application of the GAIA model involves an assessment of maturity, an evaluation of that maturity in the context of organizational objectives, and the identification of actions necessary to improve to a desired level of maturity. Table 2 illustrates this phased progression toward the ultimate goal: achieving an optimal maturity level and a sustainable supply chain that cuts costs and reduces environmental impacts, among other benefits.

TABLE 2. Example Maturity Evaluation

Management component	Stage 1: Genesis	Stage 2: Advancing	Stage 3: Innovating	Stage 4: Accelerating
Strategy and vision		1	2	
Organization and culture			2	
Process and policy		1	2	
Information and communications				
Workforce and skills		1	2	
Management systems			2	

Note: = current state; = desired state; 1 = Phase 1 improvements; 2 = Phase 2 improvements.

MATURITY ASSESSMENT

The first step is to assess the supply chain's current maturity. An organization can implement a plan to improve sustainability only after determining which areas lack maturity. The initial assessment involves one of two questionnaires (quick or detailed). Both questionnaires gauge the degree to which an organization satisfies sustainable supply chain requirements. The assessment does not require an organization to perform each process to the same degree of satisfaction. The lowest maturity stage achieved for any one component will be the overall maturity of the organization. For example, if an organization has reached stage 4 in information and communications but is only at stage 2 for all other components, that organization is classified as having reached stage 2 overall.

EVALUATION AGAINST OBJECTIVES

After assessing the current state of maturity, managers can review the results and analyze the gaps between the current and the desired maturity (the corporate objective). Because all components in the maturity model must be performed satisfactorily before moving to the next stage, an organization can improve only by addressing the components with the lowest scores. This reduces uncertainty and immediately helps an organization prioritize its efforts. Managers can then implement new policies and procedures to move all components to the same stage in the maturity model.

Gaining a maturity stage must be systematic. For example, if an organization has achieved stage 3 for the organization and culture component, but it lags in several others, it makes no sense to advance the higher level component until the others reach a comparable level of maturity.

ACTIONS NEEDED FOR IMPROVEMENT

The third step to achieving an optimal maturity level and a sustainable supply chain is to enact changes that will improve maturity. After identifying its initial maturity, managers can set goals and create a plan to move from the current stage to an improved stage. Managers incorporate proven sustainability practices to improve the lowest stages of maturity. Once all components reach an equivalent stage of maturity, the organization can focus on improving all components to reach the next stage of maturity. After implementing new initiatives, the organization should reassess its maturity position to track progress. Because improving process maturity in the supply chain invariably involves coordinating improvements with supply chain partners, developing process, data, and communication standards with partners is a key element of success. Standards form the foundation of relationships with supply chain partners. The better the standards, the better the relationship, and the more efficient and sustainable operation will be.

Conclusion

Moving from one stage of maturity to the next will generate noticeable benefits: cost savings, environmental impact reduction, and various other benefits. The values created are not always specific to the component that has been improved, but the overall result is a supply chain that operates more efficiently with a renewed focus on effective resource use. Achieving these results relies heavily on applying standard reporting and execution processes across supply chain partners to gain visibility and to improve coordination.

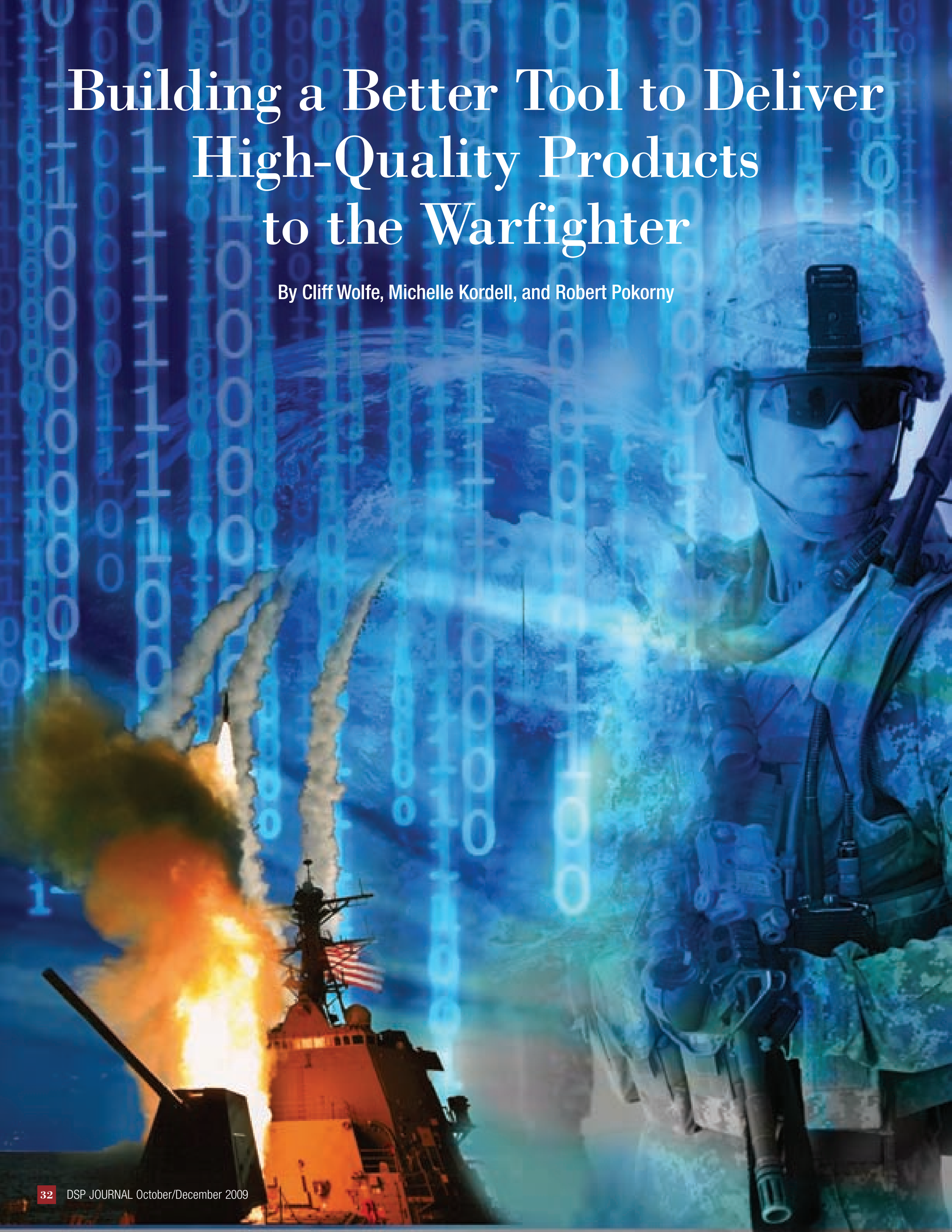
As supply chains are extended across organizations and geographies, it is increasingly important that managers understand the interactions between supply chain partners. Viewing the supply chain through a lens of sustainability highlights process efficiencies, engineering concerns, and operational results. As organizations mature, they look for more standardization across the supply chain, driving better coordination, better results, and a greener organization.

About the Author

Taylor Wilkerson, a research fellow at LMI, advises private- and public-sector clients about supply-chain and process management techniques and practices. He developed the GAIA model and has used it to assess the current state of environmental and operations management in a supply chain and to identify methods to improve sustainable operations performance.

Building a Better Tool to Deliver High-Quality Products to the Warfighter

By Cliff Wolfe, Michelle Kordell, and Robert Pokorny



Providing high-quality parts to military customers is the highest priority of the Defense Logistics Agency (DLA). When suppliers deliver defective or wrong parts, customers experience long wait-times and decreased weapon system availability. Typically, defective and wrong parts are reported through the Product Quality Deficiency Report (PQDR) system. DLA then uses the system to analyze PQDR issues individually.

Until now, the agency has been unable to routinely identify, analyze, or take action on systemic problems—problems common to a part, weapon system, supplier, or Federal Supply Class (FSC)—because of the time-consuming, labor-intensive, manual effort involved. For example, in an FY08 research and development (R&D) effort, analysts had to manually comb through more than 4,000 PQDRs looking for a suspected root cause of a quality problem for a single part. After a 400-hour, 6-month effort, the suspected cause was proven unfounded. However, the research uncovered a systemic quality issue involving not just a single part, but multiple stock numbers, multiple contracts, and multiple suppliers. The root cause was traced to an incomplete technical data package lacking sufficient specifications for defect-free manufacturing. This discovery highlighted the need for an efficient and standardized means to extract and consolidate PQDR information at the part level and higher.

To address that need, DLA's Weapon System Sustainment Program developed a web-based tool, called the PQDR Analysis Tool.[1] Introduced in 2009, the prototype tool automatically identifies and categorizes quality deficiencies based on text descriptions contained in PQDRs. Users can query across multiple item attributes (for example, national stock number, supplier, material, weapon system, profit center, and quality problem) to identify, analyze, report, and resolve systemic quality problems, as well as individual PQDR issues.

Using the PQDR Analysis Tool, analysts replicated the manual analysis mentioned above. The outcome? What took a team of analysts 6 months, took the new tool just minutes.

The Technology Behind the Tool

The PQDR form contains a discrepancy code field in which the recipient of a defective part can enter a code describing the quality issue. Often, the quality problem associated with the discrepancy code does not match the quality problem described in the form's narrative section. For various reasons, the selected discrepancy code may be inaccurate. Moreover, the narrative descriptions contain a more detailed explanation of the quality problem.

To capitalize on the narrative information, researchers developed a way to extract key words from the form and group them into problem "buckets." First, they established a list of potential problem types and built a taxonomy that organizes these types in a hierarchical structure. The researchers then used automated data extraction and classification processes, developed by XSB, Inc.,[2] to extract problem types from sample PQDR data, and they trained the classifier to automatically classify additional PQDR data to the appropriate problem types on an ongoing basis. (A classifier is a software-based tool that reads the PQDR text and assigns it to the appropriate problem category.) Problem types then are related to other higher level data, such as national stock numbers, weapon systems, suppliers, and specifications to identify potential systemic issues.

Excerpt from the Standardized Problem Taxonomy

1. Wrong item for application
   . . .
2. Quality deficiency
   - 2.1 Item manufactured incorrectly
     - 2.1.1 Does not meet specification
       - 2.1.1.1. Wrong size
         - 2.1.1.1.1 Nonconforming dimension
         - 2.1.1.1.2 Does not fit
         - 2.1.1.1.3 Incorrect threading
       - 2.1.1.2. Holes/pins do not align
       - 2.1.1.3. Manufacturing defect
         - 2.1.1.3.1 Improperly welded
         - 2.1.1.3.2 Improperly soldered
         - 2.1.1.3.3 Out of tolerance
         - 2.1.1.3.4 Improperly assembled
           - 2.1.1.3.4.1. Parts/fasteners/subassemblies installed incorrectly
           - 2.1.1.3.4.2. Missing parts in assembly
           - 2.1.1.3.4.3. Other assembly problem
     - 2.1.2 Functional defect

       . . .

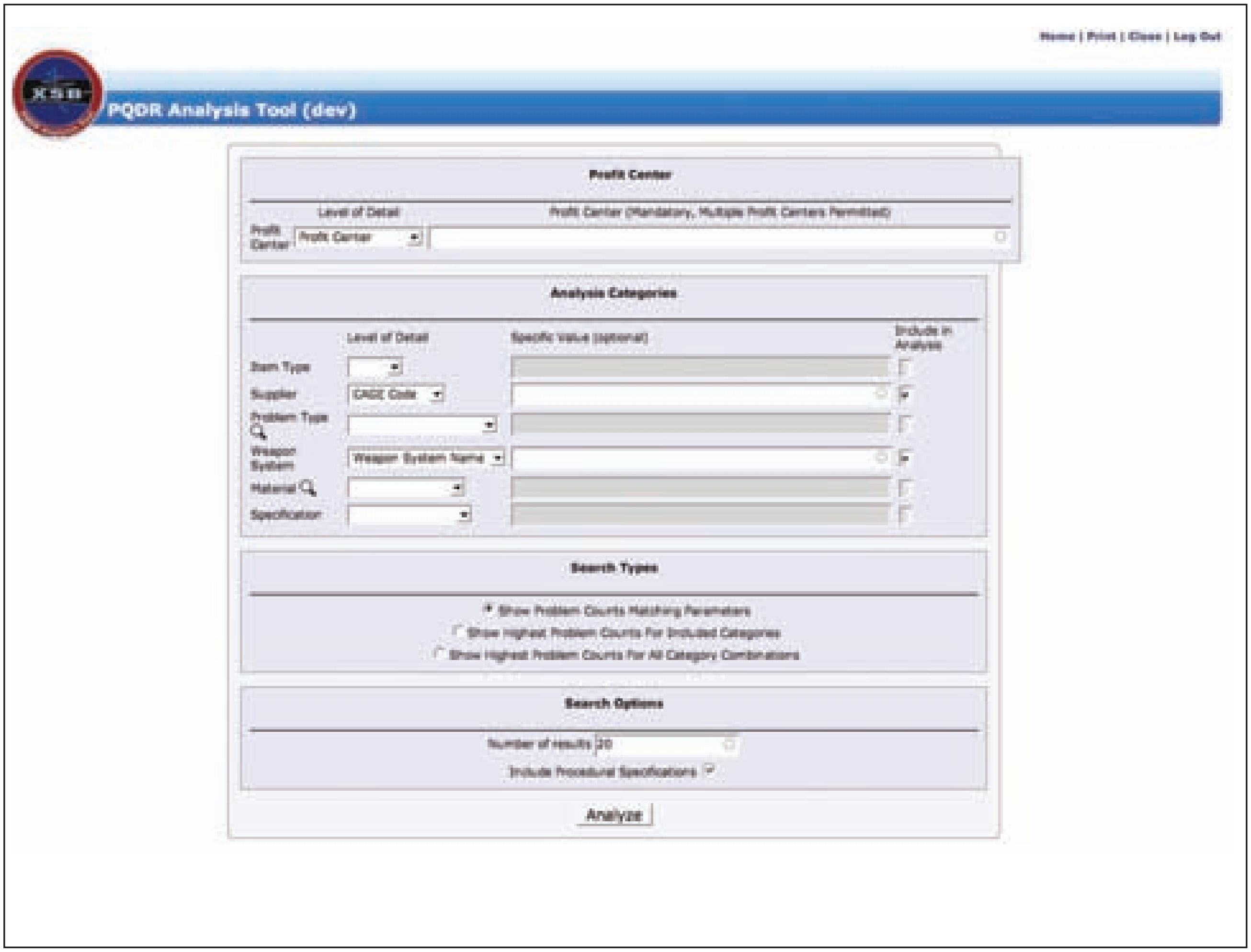
To facilitate analysis, the PQDR Analysis Tool has a roll-up capability that allows the user to manipulate the processed PQDR data such that potential systemic issues can be identified by National Item Identification Number (NIIN), part number, weapon system, supplier, contract number, FSC, or other identified part property. This enables the user to take an individual PQDR and quickly determine if there are other similar PQDRs that may help resolve the problem. The tool also allows the user to download the actual PQDR forms, aggregated based on criteria selected by the user, so that the user can quickly review all applicable PQDRs and resolve the problem.

A Case in Point

Let's look at a typical quality problem analysis to explore some of the features in the PQDR Analysis Tool.

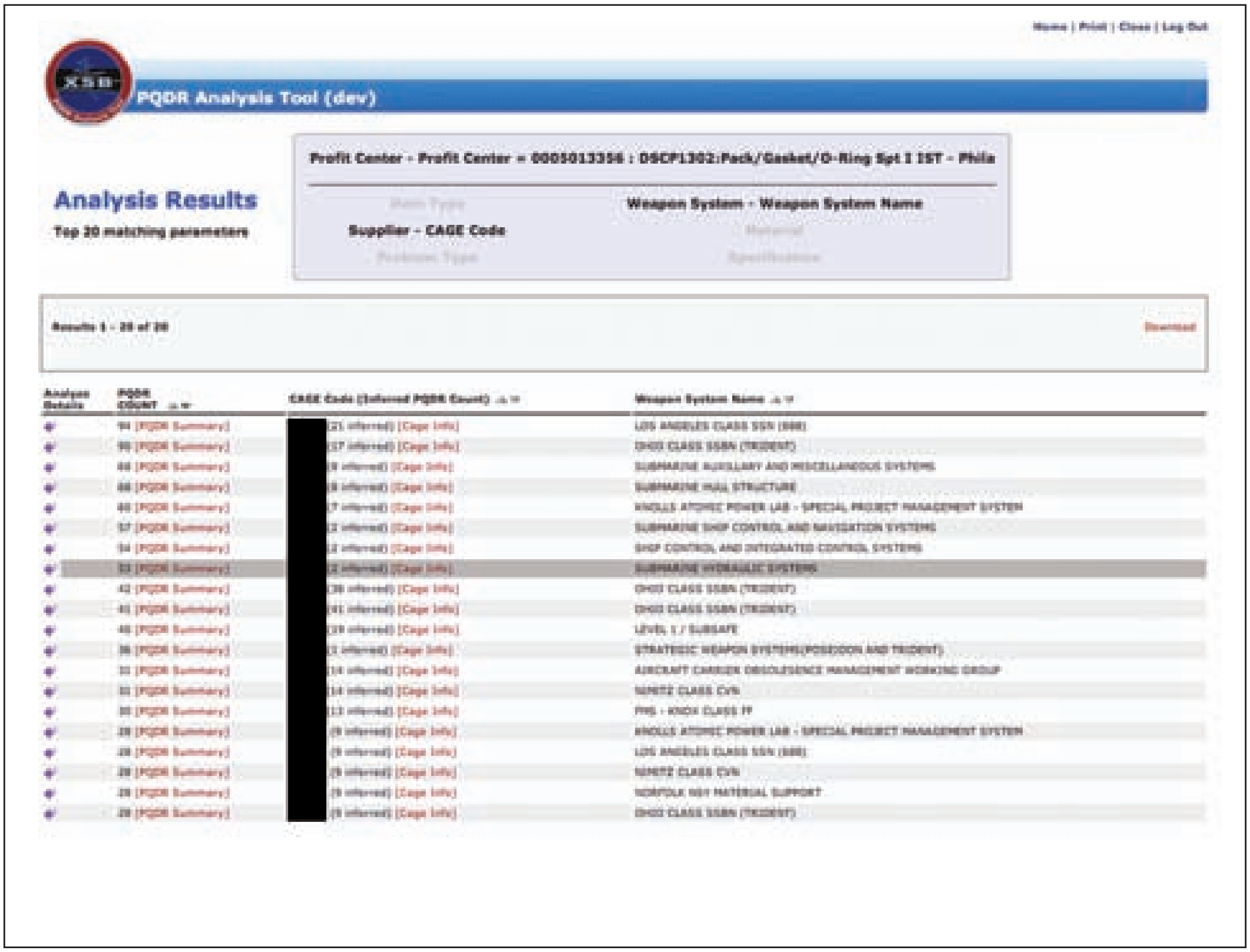
On the tool's website, the user begins by choosing categories for analysis, including level of detail. In the example shown in Figure 1, the user is interested only in items managed by a particular profit center. (The analyst may also search by supply chain.) The user directs the tool to retrieve the highest problem counts by supplier and weapon system for the specific profit center. The user has the option to select other search criteria, such as item type (FSC, NIIN, Federal Supply Group) or material (linked to a material taxonomy), as well as the option to define the values for the search criteria and to limit the number of results displayed.

FIGURE 1. Analysis Categories



The tool returns the supplier/weapon system combinations with the highest PQDR counts, as shown in Figure 2. (Note that most items returned in this example are related to submarine systems.)

FIGURE 2. Results of Simple Search by Profit Center



The user now has the option of examining any single item or continuing to look for systemic issues. Specifically, from this screen, the user may

- click the arrow at the left of a line to return to the previous screen and refine the search criteria or drill down to a finer level of detail,
- click PQDR Summary (in the PQDR COUNT column) to obtain high-level information about each PQDR and a link to the full PQDR, and
- click CAGE Info (in the CAGE Code column) to access a complementary capability called Pin Point. The Commercial And Government Entity codes have been blacked out to preserve supplier confidentiality.

In this example, the user wants to look at the issue related to submarine hydraulic systems (the highlighted line in Figure 2). In particular, the user is interested in the suppliers or manufacturers associated with the PQDRs for that issue. Therefore, the user clicks CAGE Info, which opens Pin Point in a separate window (Figure 3). The Pin Point

FIGURE 3. Pin Point Window

screen contains a wide range of attribute information on DoD parts, including supplier information.[3] This type of detailed information can be particularly useful in resolving a single issue and identifying systemic issues.

For additional insight into the problems associated with a particular CAGE code and weapon system combination, the user returns to the PQDR Analysis Tool screen, which has remained open. (The PQDR Analysis Tool enables users to quickly and seamlessly move from screen to screen within multiple applications without having to leave any application. This significantly reduces the analyst's time and effort when gathering and evaluating data.) In this example, the user wants to run a query on problem type, which has six levels. Figure 4 shows a query setup for a Level 3 problem type.

FIGURE 4. Query Setup Using Level 3

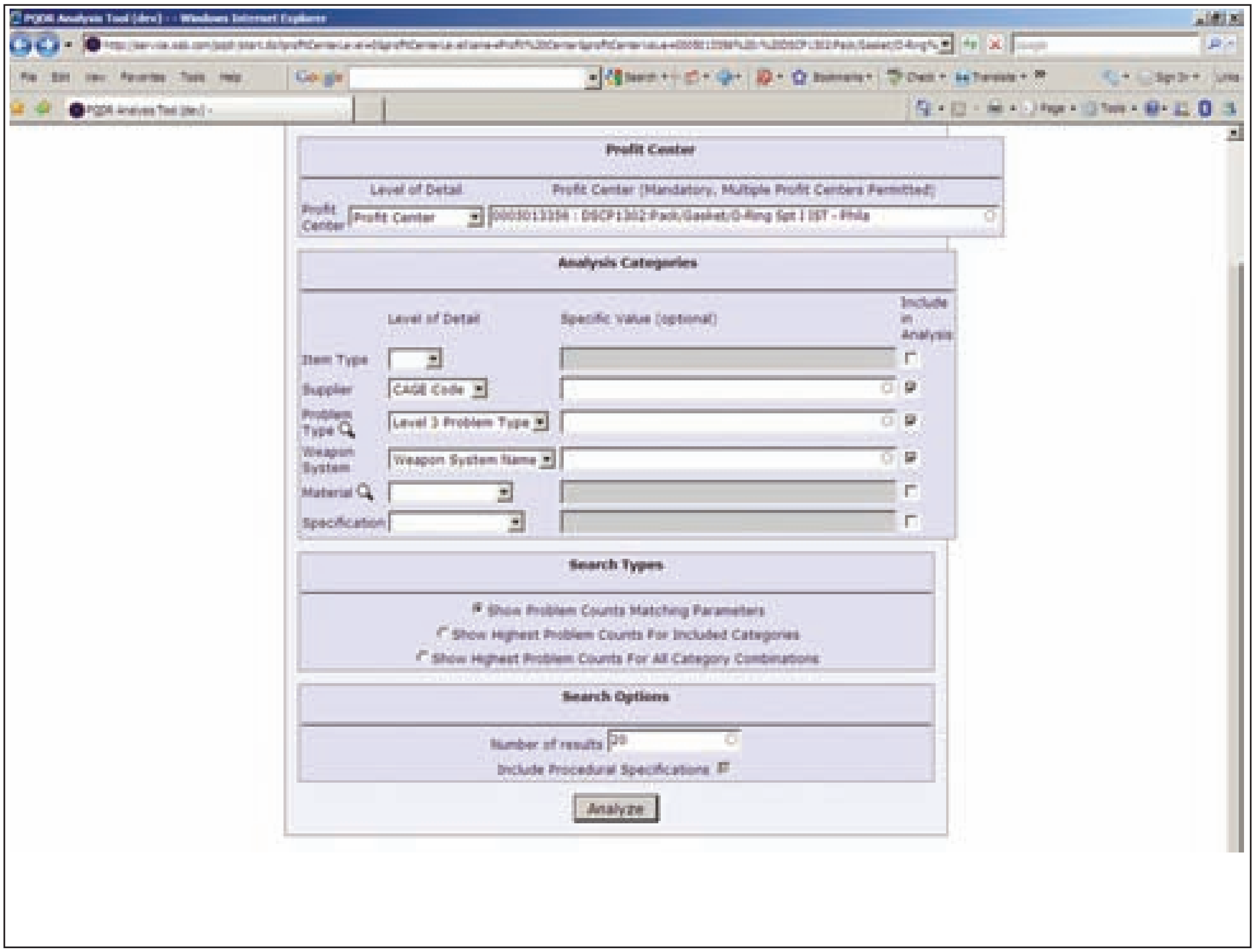
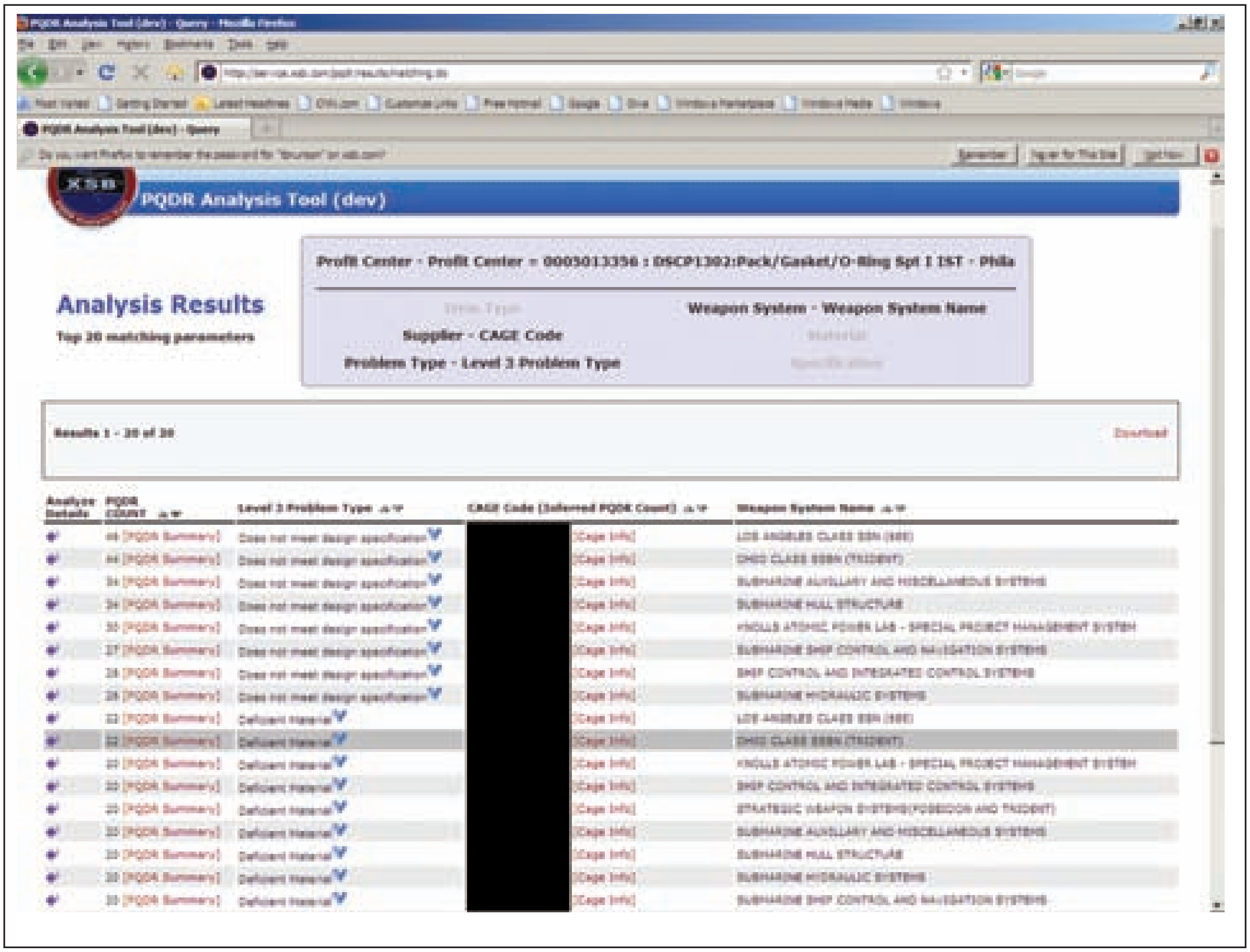


Figure 5 shows the results of the query setup of Figure 4. At this point, the user discovers a possible systemic quality problem affecting submarine systems in particular. Specifically, the products for submarine systems from a particular supplier have a significant number of material defects or do not meet specifications. The user can then use the tool for further detailed analysis of the problem, supplier, and items.

Multiple Benefits

R&D efforts to date have clearly demonstrated the feasibility and promising benefits of the PQDR Analysis Tool. During beta testing, the Defense Supply Center Philadelphia (DSCP) received several PQDRs on an internal part for a personal weapon system. Part failure in this application could lead to loss of life. A DSCP specialist had anecdotal information on this item and its supplier, but insufficient time and technical expertise to investigate and identify a systemic issue. Using the tool, the specialist quickly located all quality notifications and contracts associated with the item, as well as all contracts associated with the supplier for which quality notices for other items had been submitted. The

FIGURE 5. Results of Query on Level 3 Problem Type



specialist identified a suspicious pattern regarding solicitation bidding and contract execution leading to a formal investigation. DSCP would not have identified this issue without the PQDR Analysis Tool.

By solving systemic problems, DLA can reduce the quantity of PQDR submissions and associated processing requirements, reduce inventory levels held as not-ready-for-issue due to quality and legal problems, and reduce back orders while procurements to replace defective parts are processed and the parts are manufactured. And, it can contribute to improved quality performance by industry through better supplier selection and improved quality at existing suppliers. The tool enables DLA to recognize and subsequently resolve or mitigate systemic quality problems and provide better products to the warfighter.

What's Next

In FY10, the Weapon System Sustainment Program will perform a full operational test of the tool at three of DLA's inventory control points (Richmond, VA, Philadelphia, PA, and Columbus, OH). Test results will support a business case analysis describing the costs and benefits of the new capability. In addition, the program will focus on establishing a permanent host. Specifically, it will recommend options for transitioning, hosting, maintaining, and accessing the PQDR Analysis Tool and for institutionalizing the complementary business processes.

Interested users should contact Cliff Wolfe at 804-279-4675 or clifford.wolfe@dla.mil to request access to the test site.

[1]The Weapon System Sustainment Program's mission is to provide tools and methods to improve the delivery of parts and services to DLA customers. Each year, the program solicits the DLA community for R&D project ideas focused on providing such tools and methods. If you have suggestions for R&D projects, please contact the program manager, Cliff Wolfe, at 804-279-4675 or clifford.wolfe@dla.mil.

[2]For more information on XSB and its data mining processes, see http://www.xsb.com/.

[3]Pin Point uses advanced data mining technology to extract attributes from disparate public and military data sources (legacy databases and documents, websites and product data sheets of original equipment manufacturers, military and nongovernment specifications and standards) to support decisions about substitution, item reduction, and standardization. To request a Pin Point account, please see https://pinpoint.xsb.com/.

About the Authors

Cliff Wolfe manages DLA's Weapon System Sustainment Program. He also is chairman of the Aircraft Airworthiness and Sustainment Conference 2010.

Michelle Kordell is a program manager at LMI. She manages the R&D for a DLA Supply Support contract, which supports the Weapon System Sustainment Program. Ms. Kordell has authored several standardization case studies for the Defense Standardization Program Office.

Dr. Robert Pokorny has worked with XSB, Inc., over the last 12 years developing artificial intelligence and data mining techniques for supply chain sourcing and management, drawing on his extensive background in computer science and mechanical engineering.

A New Standard for Transportation Loads

By Roy Smith

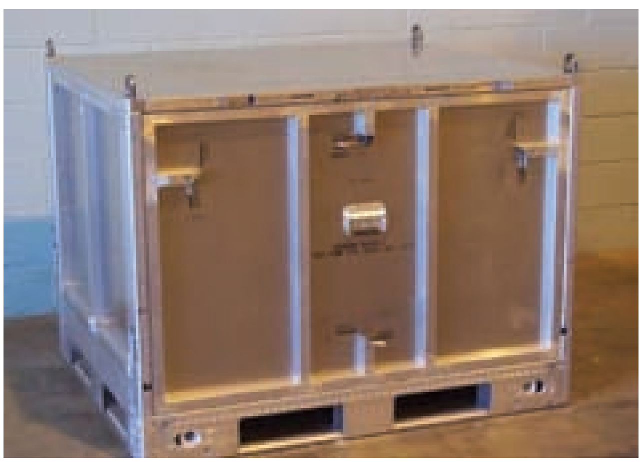
The Joint Standardization Board (JSB) for Intermodal Equipment recently completed a new interface standard, MIL-STD-3028, for the Joint Modular Intermodal Container (JMIC) system. Approval and publication of this new standard culminated a nearly 3-year effort initiated under the guidance of the United States Transportation Command (USTRANSCOM). An all-volunteer group, the JSB consists of 12 packaging and transportation subject matter experts representing various Army, Navy, Air Force, Marine Corps, and Defense Logistics Agency (DLA) commands.

What Is JMIC?

According to MIL-STD-3028,

> JMIC is a standardized intermodal shipping configuration used by the DoD. JMIC refers to any container, configuration, or platform meeting the requirements of this standard and is compatible with common transportation platforms. JMICs are used to effectively build and break down loads within 20-foot equivalent unit (TEU) containers or other commonly used platforms. JMICs can be transported as single units or as multiple units on platforms that can be rapidly transitioned between modes.

Originally developed for the Navy under the Operational Logistics Program in OPNAV N42, the JMIC technology was selected as the basis for the hardware used in the Joint Modular Intermodal Distribution System (JMIDS) Joint Capability Technology Demonstration (JCTD) program. (The following photos show a JCTD JMIC and JCTD JMICs during demonstrations.)



The JMIDS program was a Focused Logistics JCTD that ran several large-scale demonstrations with the new JMIC hardware in various transportation and use scenarios. As a result of the success of the demonstrations, USTRANSCOM recommended—to the Deputy Under Secretary of Defense (Advanced Systems and Concepts)—that the JMIC technology be transitioned to the field. More than 1,000 JMIC units produced during the JMIDS JCTD remained with troops in the field at the conclusion of the program. The JMIC design demonstrated in the JCTD was assigned national stock numbers (Unpainted NSN 8145-01-551-5311, Green NSN 8145-01-564-5802, Tan NSN 8145-01-564-5795) and has been made available for purchase by DLA. Currently, about 2,000 JMICs are deployed to troops in all services around the globe, and nearly 2,500 additional JMICs have been ordered. Many of these JMICs are being delivered to units deployed in Afghanistan and Iraq. These photos show ISO container loads before and after JMIC:

What Did the JSB Do?

As a result of the initial efforts of the JMIDS JCTD program, the JSB looked at the JMIC system as a potential standardization effort. This decision was later substantiated by the successful JCTD program demonstrations and the USTRANSCOM recommendation to transition JMIC to the field. Realizing that the JMIC technology needed standardization to grow and succeed, the JSB worked with the Naval Surface Warfare Center, Indian Head Division engineers, who developed the JMIC technology, as well as with representatives from the JMIDS program, to select requirements that were critical for the interface standard. Through a series of working group meetings and draft documents, the requirements were reviewed and refined to define the minimum dimensional and performance parameters for a shipping configuration within the JMIC system.

To formalize and prepare the interface standard, the JSB enlisted the services of the Army Logistics Support Activity, Packaging, Storage and Containerization Center (LOGSA, PSCC) under Project PACK-2007-011. LOGSA, PSCC functioned as the lead standardization activity, because the JSB did not formally have this authority. The draft standard underwent a full joint service and industry coordination review to finalize and prepare it for submittal to DSPO for approval.

Why Develop a Military Standard?

The requirements defined in MIL-STD-3028 ensure that all current and future hardware developed within the JMIC system will interface and function correctly with other JMICs and with other hardware or platforms. As the JMIC system grows in use, the standard will allow technology developers from all services to take advantage of the JMIC shipping configuration for new or modified transportation conveyances or material-handling equipment. (The following photo shows JMICs on a potential transportation platform.)

The JMIC system has the potential to immediately generate efficiencies in joint operations and during sustainment operations of forward-deployed troops. And similar to the process refinements and modifications that followed the introduction of standard pallets and ISO shipping containers, the JMIC interface standard ensures that vehicles, ships, and aircraft used for cargo transportation have defined requirements for the shipping configurations that will be moved. This load standardization could then be leveraged to generate more efficiency and savings in the future through new, fully integrated vehicle, ship, and aircraft designs. Automated cargo-handling systems could also be developed based on the JMIC standard.

What's Next?

As the JMIC system gains acceptance in both the military and commercial cargo transportation fields, the JSB may possibly engage ISO Technical Committee 104 for freight containers to document the JMIC interface requirements as an ISO standard.

For more information about the JMIC technology, e-mail ihdivjmic@navy.mil. More information about the JSB for Intermodal Equipment can be obtained from the current chair, Robbin Miller, at Robbin.Miller@wpafb.af.mil, or the former chair, Roy Smith, at roy.a.smith@navy.mil. More information about the JMIDS JCTD can be obtained by contacting the transition manager, Doug Chesnulovitch, at douglas.m.chesnulovitch@us.army.mil.

About the Author

Roy Smith, a Navy mechanical engineer with 28 years of experience, is the manager of the Engineering Development Branch of the Naval Surface Warfare Center, Indian Head Division, Detachment Earle, located in New Jersey. In addition, he is the vice-chair of the Navy Packaging Board and a member of the ASTM International Committee D10 on packaging and Subcommittee D10.12 on shipping containers, crates, pallets, skids, and related structures. Mr. Smith chaired the JSB for Intermodal Equipment in 2007 and 2008.

Defense Parts Management Portal–DPMP

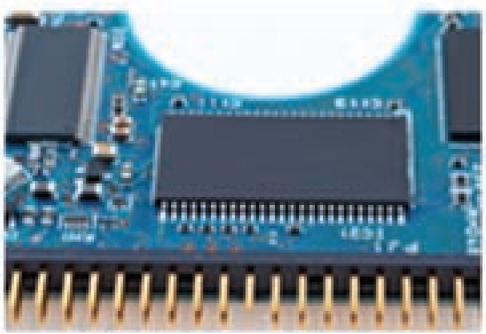
The DPMP is a new public website brought to you by the Parts Standardization and Management Committee (PSMC) to serve the defense parts management community.

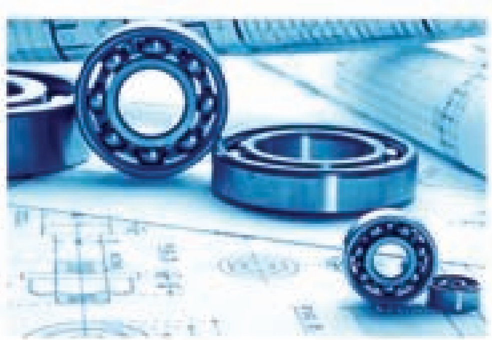
The DPMP is a new resource, a new marketplace, and a "one-stop shop" for parts management resources. It is a navigation tool, a communication and collaboration resource, and an information exchange. It gives you quick and easy access to the resources you need, saves you time and money, connects you to new customers or suppliers, and assists you with finding the answers you need.

This dynamic website will grow and be shaped by its member organizations. A new and innovative feature of the DPMP is its use of "bridge pages." Organizations with interests in parts and components are invited to become DPMP members by taking control of a bridge page. Chances are good that your organization is already listed in the DPMP.

There is no cost.

Explore the DPMP at https://dpmp.lmi.org. For more information, look at the documents under "Learn more about the DPMP." Click "Contact Us" to send us your questions or comments.





Program News

Topical Information on Standardization Programs

NIST Begins Developing "Smart Grid" Interoperability Standards

Under the Energy Independence and Security Act of 2007, the National Institute of Standards and Technology (NIST) has "primary responsibility to coordinate development of a framework that includes protocols and model standards for information management to achieve interoperability of smart grid devices and systems." What is a "smart grid"? The term has different meanings to different economic sectors. To many sectors, the term means making the physical grid (transmission and power lines) operate and communicate more effectively and efficiently via technology, computers, and software. To other sectors, it means making the entire process—from generating electricity through transmission and distribution to the actual consumers choosing to turn on an appliance—more efficient.

NIST's role is to consider all sectors' understanding of a smart grid and to develop a comprehensive framework for a nationwide, interoperable smart grid for the U.S. electric power system. Working with industry, government, and consumer stakeholders, NIST is identifying and developing standards critical to achieving a reliable and robust smart grid.

Interoperability is key to a smart grid's success, because it enables the integration and two-way communication among many interconnected elements of the electric power grid. Effective interoperability is built on a framework of interfaces, protocols, and other consensus standards. These standards will enable such interactions as "smart" appliances and meters communicating to consumers regarding how much power they are using and at what cost, and they will provide them with more control over their power consumption and energy bills. Widely adopted standards also will help utilities mix and manage varying supplies of solar, wind, and other renewable energy sources and better respond to changing demand.

Developing interoperability standards for the smart grid project is similar to developing standards for the next-generation telecommunications network. This evolving effort involves dozens of standards developing organizations and is almost entirely owned and operated by industry.

NIST has imparted expertise in such areas as cybersecurity and advanced networking, as well as provided leadership and coordination for many years. NIST plans on continuing to play a vital role in the smart grid project for the foreseeable future.

Conversion to the Qualified Products Database Is Progressing

DoD qualifying activities continue to make good progress in converting their paper-based qualified products lists (QPLs) and qualified manufacturers lists (QMLs) into electronic QPLs/QMLs in the qualified products database (QPD). Currently, 83 percent of the 746 QPLs have been published in the QPD. An additional 11 percent have been partially loaded but not yet published in the QPD. Work has not yet begun on the remaining 6 percent of the QPLs. As qualifying activities update their QPLs and enter them into the QPD, the number of outdated QPLs continues to decrease. For more information on the DoD qualification program or the QPD, please contact Ms. Donna McMurray, DSPO's manager for the qualification program, at Donna.McMurry@dla.mil or 703-767-6874.

Events

Upcoming Events and Information

March 8–11, 2010, Huntsville, AL

2010 Life Cycle Logistics Tools Workshop and User Group

The Council of Logistics Engineering Professionals is sponsoring the 2010 Life Cycle Logistics Tools Workshop and User Group, a working group for professional logisticians, with educational support provided by the U.S. Army Materiel Command Logistics Support Activity. This year's workshop will highlight five logistics life cycle tools—POWERLOG-J, SYSPARS, CASA, COMPASS, and PFSA—as well as the new GEIA 0007 logistics data standard and GEIA 927 condition-based maintenance. For more information, please visit www.logisticsengineers.org/mar10.htm or contact Ms. Kaydee Waterbury at 256-955-9774/DSN 645-9774 or at kaydee.waterbury@us.army.mil.

April 20–22, 2010, McLean, VA

PSMC Spring Conference

The Parts Standardization and Management Committee (PSMC), chartered by DSPO, will hold its spring conference at LMI in McLean, VA (Washington, DC, metropolitan area). Please note that attendance is open only to PSMC participants. If you are involved in some aspect of parts management and are interested in being a first-time participant, please contact Donna McMurry at Donna.McMurry@dla.mil or call 703-767-6874.

May 15, 2010, Washington, DC

QPD Users Group

DSPO will be hosting a 1-day Qualified Products Database (QPD) Users Group in the Washington, DC, area. DoD and General Services Administration personnel who enter data into the QPD are encouraged to attend. Even if you have already had QPD training, you may want to attend the May gathering, because we will be reviewing the latest QPD enhancements, such as validation, stop ship function, and PDF capability. This session will also provide a forum for database users from different organizations to discuss QPD issues and lessons learned, as well as to suggest ideas for possible enhancements.

October 25–28, 2010, Las Vegas, NV

DMSMS 2010 Conference

Mark your calendars now and plan to attend the 2010 Diminishing Manufacturing Sources and Material Shortages (DMSMS) Conference at the Rio All-Suite Hotel and Casino in Las Vegas, NV. Once again, the conference will include multiple tracks of topics, including one featuring topics relating to the Defense Standardization Program and another on the Government-Industry Data Exchange Program. As the conference planning develops, key information will be posted on the DMSMS 2010 website. For more information, please contact Alex Melnikow at Alex.Melnikow@DLA.mil or 703-767-1415.

Upcoming Issues
Call for Contributors

We are always seeking articles that relate to our themes or other standardization topics. We invite anyone involved in standardization—government employees, military personnel, industry leaders, members of academia, and others—to submit proposed articles for use in the *DSP Journal*. Please let us know if you would like to contribute.

Following are our themes for upcoming issues:

Issue	Theme
January/March 2010	Diminishing Manufacturing Sources and Material Shortages
April/June 2010	2009 Standardization Stars
July/September 2010	Systems Engineering

If you have ideas for articles or want more information, contact Tim Koczanski, Editor, *DSP Journal*, Defense Standardization Program Office, 8725 John J. Kingman Road, STP 5100, Fort Belvoir, VA 22060-6220 or e-mail DSP-Editor@dla.mil.

Our office reserves the right to modify or reject any submission as deemed appropriate. We will be glad to send out our editorial guidelines and work with any author to get his or her material shaped into an article.


DEFENSE STANDARDIZATION PROGRAM
MAKING SYSTEMS WORK TOGETHER