Defense Standardization Program
Journal
July/December 2010

Systems Engineering

The Synergies of DoD Systems Engineering and International Standards

Parts Management in Systems Engineering

Technical Excellence

Defense Standardization Program Journal

Contents *July/December 2010*

1 Director's Forum

3 The Synergies of DoD Systems Engineering and International Standards

11 Parts Management in Systems Engineering

16 Mitigating DoD's Acquisition Risks

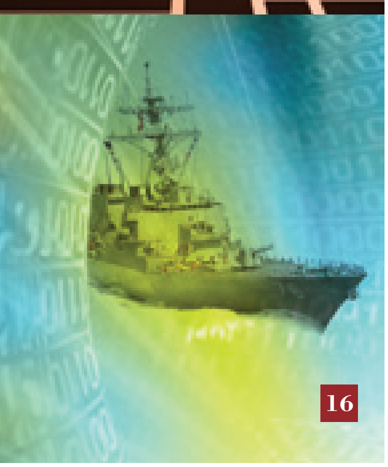
29 The Defense Logistics Agency's Long-Range Plan for Managing Technical Data

34 Technical Excellence
A Requirement for Good Systems Engineering

43 Ensuring Quality through Product Testing

Departments

47 Program News 54 Events 55 People



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

A Message from the Defense Standardization Executive

I was very pleased to recently be appointed as the Defense Standardization Executive. This new role strongly complements my responsibilities as the Director of Systems Engineering for the Department. I believe a robust and productive partnership between the standardization and systems engineering communities will significantly enhance the Department's effectiveness and improve our weapon systems acquisition and sustainment capabilities.

Recent congressional acquisition reform initiatives and Secretary of Defense guidance call for increasing the Department of Defense's emphasis on our engineering capabilities. The 2010 Quadrennial Defense Review executive summary highlights acquisition reform and systems engineering, stating that the Department needs to "improve how it matches requirements with mature technologies, maintains disciplined systems engineering approaches, institutionalizes rapid acquisition capabilities and implements more comprehensive testing." The Weapon Systems Acquisition Reform Act of 2009 (Public Law 111-23) establishes the statutory requirement for a Director, Systems Engineering, who is the "principal systems engineering advisor to the SECDEF and the USD(AT&L)." This emphasis at the most senior level offers the technical community a unique opportunity to positively influence the outcomes of defense acquisition programs. One of those positive opportunities is to make standardization a more effective engineering tool in restoring discipline and consistency to our acquisition and sustainment engineering processes.

The Department of Defense develops and delivers to our soldiers, sailors, airmen, and Marines incredibly effective but increasingly complex weapon systems. As the complexity of our systems has increased, so has the need for effective engineering throughout the life cycle. We face challenges in implementing controlled engineering processes, from re-

Stephen Welby
Director, Systems Engineering and Defense Standardization Executive

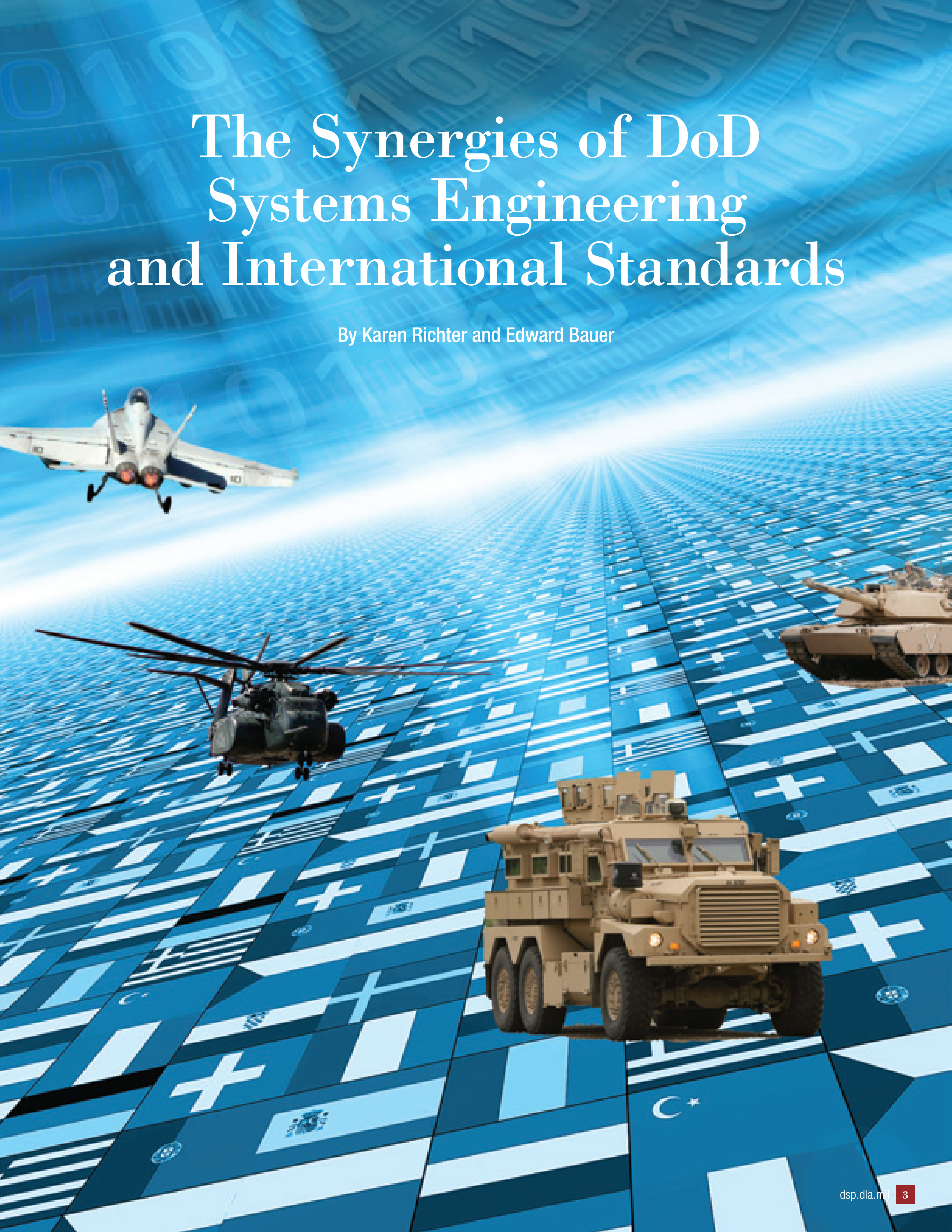
quirements identification and analysis, through technology and architecture selection and assessment, analysis and coordination of complex system design, development, and execution, to delivering rigorously tested production systems with a full complement of sustainable hardware and software capabilities. In the past, the acquisition community has largely focused on the execution of programs at Milestone B and beyond. We are now increasingly focused on addressing early acquisition phases, including requirements definition, development planning, and early acquisition systems engineering support.

To achieve successful program outcomes demands effective acquisition management based on a disciplined approach to systems engineering. Standards help provide that discipline by creating common solutions that reflect our corporate technical process memory and enabling communication of requirements between and across the Department, industry, and our allies.

The Department of Defense is challenged to drive best systems engineering practices back into the way we do business. With the energy, focus, and talent of our engineering and standardization communities, I'm confident that we can meet those challenges.

The Synergies of DoD Systems Engineering and International Standards

By Karen Richter and Edward Bauer



DoD's Office of the Director, Systems Engineering (DSE), is actively involved with international standards organizations working on systems engineering and software engineering processes. That involvement has created synergies for both DoD and the standards organizations over the past 15 years.

Background

In 1994, then–Secretary of Defense, Dr. William Perry, issued a memorandum, known as the "Perry memo," directing the use of performance and commercial specifications and standards in lieu of military specifications and standards, unless no practical alternative existed to meet the user's needs. Shortly after the Perry memo was issued, the Systems Engineering office, under the direction of Mr. Mark Schaeffer, became a member of the U.S. Technical Advisory Group (TAG) to Subcommittee 7 (SC7) of Joint Technical Committee 1 (JTC1), a component of the ISO/International Electrotechnical Commission (IEC). DoD's purpose in joining the TAG was to help ensure that international commercial standards would meet the needs of DoD in the areas of systems and software engineering. DoD also tasked the Institute for Defense Analyses (IDA) with participating in international standards organizations to help achieve DoD's goals for the use of commercial standards.

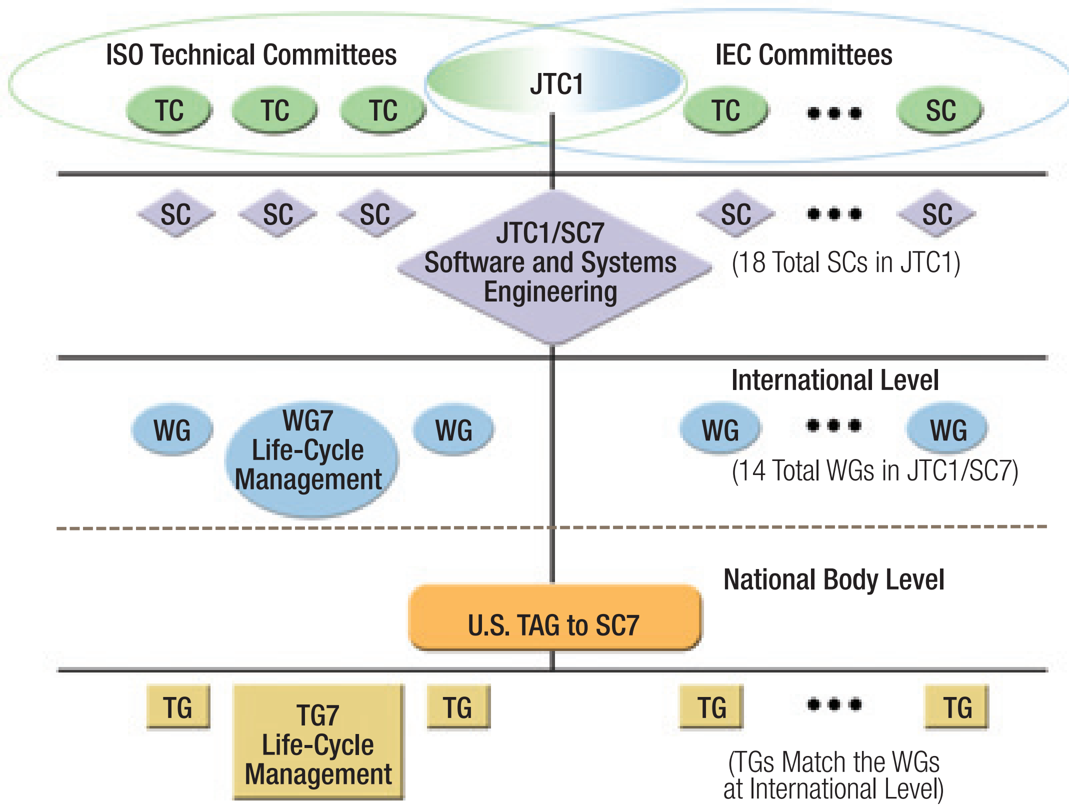
About the Standards Organizations

ISO prepares and publishes international standards across a broad range of technical and functional areas. This work is done through ISO's 209 technical committees (TCs). In addition, ISO participates with the IEC in JTC1, whose focus is information technology. The IEC, which has 219 TCs and subcommittees (SCs), prepares and publishes international standards for all electrical, electronic, and related technologies.

JTC1 has 18 SCs of its own, including SC7. When DoD began its involvement in the mid-1990s, SC7 was named "Software Engineering," but it was the only standards organization for systems engineering process standards. In 2000, thanks in part to DoD's efforts to revitalize systems engineering, SC7 changed its name to "Software and Systems Engineering," with a focus on standardization of processes, supporting tools, and supporting technologies for the engineering of software products and systems. In 2002, SC7 published its first systems engineering life-cycle process standard, ISO/IEC 15288, "Systems and Software Engineering—System Life Cycle Processes."

SC7 now consists of 37 participating national bodies, 20 observer countries, and liaisons with ISO TCs, IEC TCs, and other international organizations. SC7 is divided into 14 working groups (WGs) and additional study groups (SGs) as needed. The United States is a participating national body with full voting privileges. Operationally, the day-to-day work on behalf of the United States is performed by the U.S. Technical Advisory Group; the TAG consists of task groups (TGs) that correspond to SC7's WGs. DoD and IDA mainly participate in TG7 and WG7, whose focus is life-cycle management. Figure 1 shows the structure for JTC1 participation.

Figure 1. The Structure for JTC1 Participation



The other organization of interest is the Institute of Electrical and Electronic Engineers (IEEE), a professional organization dedicated to advancing technology. The IEEE Computer Society is an international organization that develops and disseminates standards related to computer technology and is a liaison organization to SC7. In its role as liaison, it also has a special relationship with SC7 wherein standards are developed and disseminated under both ISO/IEC and IEEE banners. Such a relationship avoids duplication and ensures alignment and harmonization among international standards for software and systems engineering.

International Standards Related to Systems Engineering

SC7 and WG7 have undertaken a concerted effort to produce a harmonized and integrated set of "framework" standards that provide the overall structure of life-cycle processes. In particular, SC7 and WG7 updated two framework standards, aligning them as closely as possible. The two standards, each of which consists of a purpose statement, outcomes, activities, and tasks, are as follows:

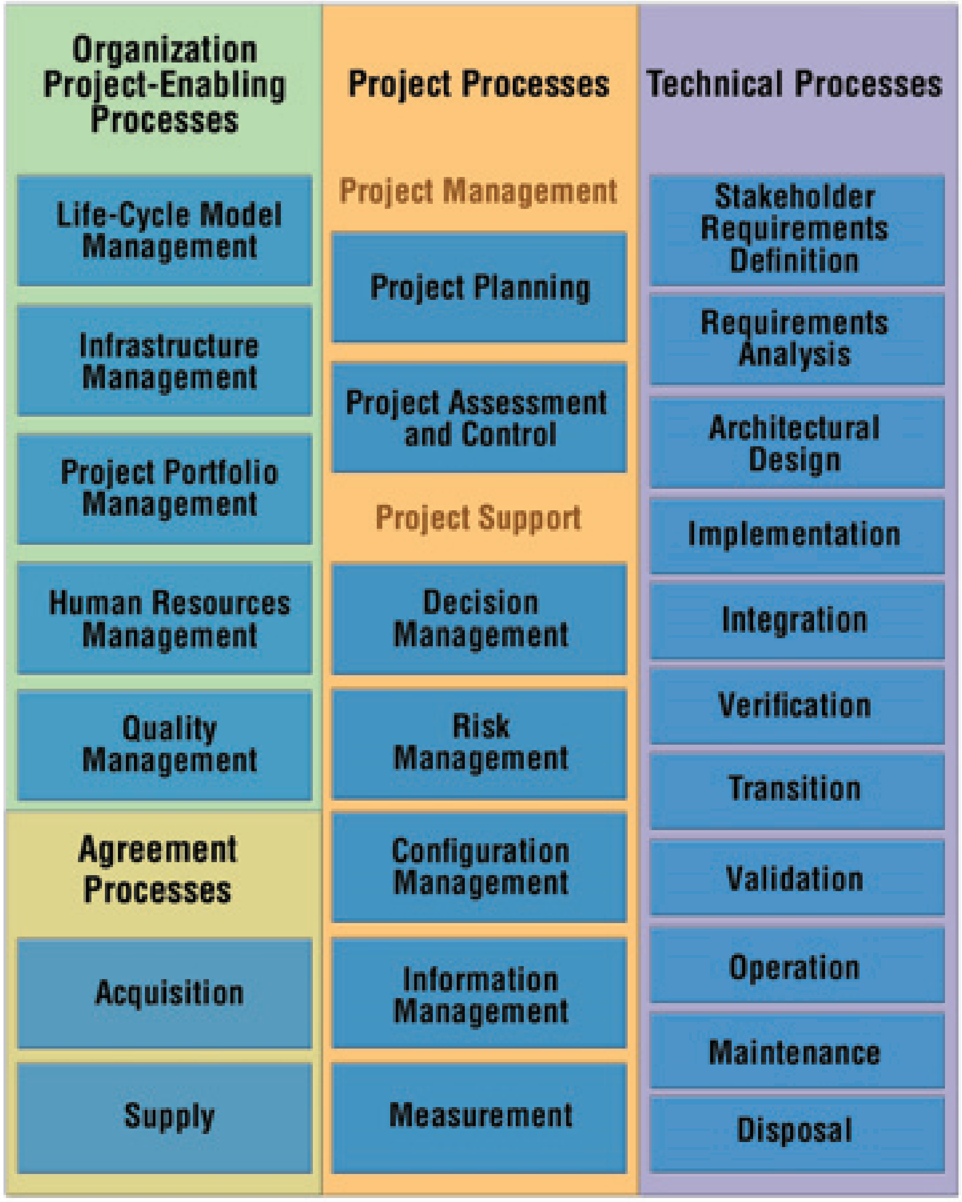
- ISO/IEC 15288:2008, "Systems and Software Engineering—System Life Cycle Processes"
- ISO/IEC 12207:2008, "Systems and Software Engineering—Software Life Cycle Processes."

Recognizing that organizations would need a life-cycle model to implement the processes in the framework standards, SC7 and WG7 are developing a multipart technical report (ISO/IEC 24748, "Systems and Software Engineering—Life Cycle Management") describing the development and use of life-cycle models. Part 1, "Guide for Life Cycle Management," expected to be published in 2010, contains information on life-cycle concepts and descriptions of the purposes and outcomes of representative life-cycle stages. It also illustrates the use of a life-cycle model for systems in the context of ISO/IEC 15288 and provides a corresponding illustration of the use of a life-cycle model for software in the context of ISO/IEC 12207. In addition, Part 1 contains a detailed discussion and advice on adapting a life-cycle model for use in a specific organizational environment, project, domain, discipline, or specialty. Parts 2 and 3 of ISO/IEC 24748, both in the committee stage of the development process, are the guides for 15288 and 12207, respectively. Part 4 will update IEEE 1220-2005, "IEEE Standard for Application and Management of the Systems Engineering Process"; ISO/IEC 24748-4 will address systems engineering planning and the content requirements for a systems engineering management plan. WG7 also has discussed a proposal to develop a Part 5 to address software engineering planning and the content requirements for a software development plan.

The "how to" implementation of the life-cycle processes is left to lower-level standards. Figure 2 lists the system life-cycle processes (from ISO/IEC 15288:2008), grouped into four categories: organization project-enabling, agreement, project, and technical. The software life-cycle processes (ISO/IEC 12207) are essentially the same, but also include processes for software implementation, support, and reuse. Below are some of the published process standards:

- ISO/IEC 15939:2007, "Systems and Software Engineering—Measurement Process"
- ISO/IEC 16085:2006, "Systems and Software Engineering—Life Cycle Processes—Risk Management"

Figure 1. System Life-Cycle Processes in ISO/IEC 15288:2008



- ISO/IEC 15289:2006, "Systems and Software Engineering—Content of Systems and Software Life Cycle Process Information Products (Documentation)."

SC7 is continuing to develop or revise other standards related to one or more of the life-cycle processes, including the following:

- ISO/IEC 29148, "Software and Systems Engineering—Life Cycle Processes—Requirements Engineering" (under development).
- ISO/IEC 15026, "Systems and Software Engineering—Systems and Software Assurance" (being revised). Part 4 of this four-part standard, "Assurance in the Life Cycle,"

will provide systems and software process views (which describe using the activities and tasks of existing processes to achieve a specified purpose and set of outcomes); Part 4 is closely related to DoD guidance on systems assurance and program protection.

Other standards of interest are in the areas of architecture, requirements engineering and configuration management tools, software maintenance, software testing, software quality characteristics, and software quality management. Standards for process definition and assessment also are relevant.

SC7 has published a collection of technical reports that are guides to using these standards, all of which are designed to work together harmoniously with a common vocabulary.

Related DoD Activities

Along with contributing to ISO/IEC standards development, DoD participates in SGs focused specifically on improving harmonization across life-cycle processes and relevant standards. For example, DoD is participating on a WG7 SG tasked with further defining the relationships between the multitude of processes, activities, and tasks in the areas of validation and verification. The scope of the SG is to refine the understanding between the objective of evaluation (verification, validation, test, etc.) and the evaluation techniques used to meet the objective. This SG will conclude its work with a report highlighting recommendations for a consistent and economical terminology related to validation and verification, analysis of documented evaluation techniques, and recommendations for an evolutionary path for users of standards and technical reports that are to be revised or replaced.

Other DoD activities include the alignment of *Defense Acquisition Guidebook* with ISO/IEC 15288, the alignment of NATO's quality management process with 15288, and the coordination of the Body of Knowledge and Curriculum to Advance Systems Engineering (BKCASE) project with ISO/IEC TR 19759:2005, "Software Engineering—Guide to the Software Engineering Body of Knowledge (SWEBOK)."

DEFENSE ACQUISITION GUIDEBOOK

To align with 15288, Chapter 4, "Systems Engineering," of *Defense Acquisition Guidebook* describes 16 processes that DoD considers important to its implementation of systems engineering. The processes are categorized as technical management processes or technical processes, as shown in Table 1. Although these processes do not exactly duplicate those in 15288, they align at the activity and task levels. DSE and IDA maintain that alignment through various versions of both the standards and the guidebook.

Table 1. Processes Important to Implementation of Systems Engineering

Technical management processes	Technical processes
Decision analysis	Stakeholder requirements definition
Technical planning	Requirements analysis
Technical assessment	Architectural design
Requirements management	Implementation
Risk management	Integration
Configuration management	Verification
Technical data management	Validation
Interface management	Transition

NATO QUALITY MANAGEMENT PROCESS

When DoD's Systems Engineering office was helping to prepare the 2002 version of ISO/IEC 15288, it was also active in the quality management activities of NATO. During an international meeting of WG7, DoD ensured that a quality management process was incorporated into ISO/IEC 15288:2002 at the enterprise level.

Subsequently, in 2003, NATO reorganized and created a Life Cycle Management Group, which adopted ISO/IEC 15288:2002 as the standard for life-cycle management. Now, NATO is in the process of adopting the 2008 version of ISO/IEC 15288 and has approved plans to develop a NATO standardization agreement based on 15288 for ratification by NATO nations. Ratification is the commitment that nations will implement the standard. NATO is also developing an implementation guide for ISO/IEC 15288:2008 to add NATO-specific requirements while awaiting the release of ISO/IEC 24748 Part 2.

ISO/IEC 15288 is the basis for the life-cycle processes in the 2000 series of the Allied Quality Assurance Publications. Those publications and the NATO standardization agreements from this series are referenced in Chapter 11, "Program Management Activities," of *Defense Acquisition Guidebook*.

BKCASE PROJECT

The BKCASE project is one of the workforce development initiatives of DSE and its Systems Engineering Research Center. An SC7 working group has a similar effort, maintenance of SWEBOK (ISO/IEC 19759). The Head of Delegation of the U.S. National Body to WG7, Mr. Garry Roedler of Lockheed Martin, is participating in the BKCASE project through his relationship with the International Council on Systems Engineering. In a great coordination effort at the last SC7 plenary meeting in May 2010, SC7 members agreed to serve as reviewers on the project.

Conclusion

Systems engineering standards will continue to be important to DoD and, in particular, to DSE. DoD's commitment to systems engineering standards is evidenced by its recent realignment of DSP to DSE's Mission Assurance team. That team is the gatekeeper for systems engineering standards and specifications to be adopted by DoD and maintained in the ASSIST-Online database for use by the DoD components. Participation in the development of international systems and software engineering standards and inclusion of those standards in the ASSIST database has benefited both DoD and SC7.

About the Authors

Karen Richter is a senior analyst and project leader with the Strategy, Forces, and Resources Division at the Institute for Defense Analyses, a research organization for the Department of Defense. For 25 years, Dr. Richter has conducted projects in the areas of systems engineering, advanced manufacturing, quality management, process improvement, and design methods. She is a representative to the U.S. Technical Advisory Groups for ISO/JTC1/SC7 (Software and Systems Engineering) and ISO/TC176 (Quality Management) to develop international standards that meet DoD's needs.

Edward Bauer is a senior systems engineer for the U.S. Army Armament Research, Development and Engineering Center. He is experienced in applying systems engineering technical processes on defense systems through the technology development and engineering and manufacturing development phases. Mr. Bauer is a representative to the U.S. Technical Advisory Group for ISO/JTC1/SC7 (Software and Systems Engineering) to develop international standards.

Parts Management in Systems Engineering

By Dan McLeod and Jay Mandelbaum

Parts management is a design strategy that seeks to minimize the number of unique or specialized parts used in a system (or across systems) to reduce the logistics footprint and lower total ownership costs. As part of the engineering process, parts management is an integrated effort to streamline the selection of preferred or commonly used parts during the design of weapons systems and equipment within an overarching systems engineering (SE) framework. Typically, preferred parts are those described by non-government standards or military standards, or parts already in use in the DoD supply system. This process determines optimum parts while considering all factors that may affect program outcomes.

Parts Management

Parts management is the practice of considering the application, standardization, technology (new and aging), system reliability, maintainability, supportability, and cost in selecting parts and addressing availability, logistics support, Diminishing Manufacturing Sources and Material Shortages (DMSMS), and legacy issues in supporting them throughout the life of the systems.

It is important to understand what part types are being addressed by the parts management program. The term "part" could denote different hardware levels, depending on how the term is used. In the context of a parts management program, these part types are *one or more pieces joined together, which are normally not subject to disassembly without destruction or impairment of their intended design use*. Microcircuits, connectors, resistors, capacitors, fasteners, bearings, valves, screws, and rivets are some examples of these part types. They are the building blocks from which systems are created and, as such, greatly affect hardware dependability and readiness. Because the reliability and maintainability of the end item is dependent upon these building blocks, the importance of selecting and applying the most effective parts management program cannot be overemphasized.

If parts management sounds like an important acquisition engineering design consideration, it is, especially in today's acquisition environment characterized by rapidly changing designs and technologies and by increased risk to DoD weapon systems and equipment due to issues with parts that affect reliability, standardization, and supportability. Parts management takes on even greater importance in the overall defense environment—affordability. In remarks delivered in Abilene, KS, on May 8, 2010, the 65th anniversary of the allied victory in Europe, Secretary of Defense Robert M. Gates highlighted the importance of affordability:

> As a matter of principle and political reality, the Department of Defense cannot go to America's elected representatives and ask for increases each year unless we have done everything possible to make every dollar count—unless there is real reform in the way this department does its business and spends taxpayer dollars.

DEFENSE MANAGEMENT REVIEW AND ACQUISITION REFORM

In the 1980s, parts control was a mandatory requirement for major acquisition programs. (At that time, the program was "parts control" and not "parts management.") Over time, the parts control requirement and its enforcement became overly prescriptive, burdensome, and costly for many programs. In 1991, under the Defense Management Review, the regulatory requirement for parts control was eliminated. Parts control became a discretionary practice for major acquisition programs. In 1996, under Acquisition Reform, the parts control military standard was canceled and superseded by a parts management guidance handbook.

The well-meaning intent of eliminating both the policy mandating parts control and the parts control military standard was not to eliminate the need for effective parts management, but to free the program office and contractor from what was perceived as an overly prescriptive process and allow them to make "smart" decisions. The message that was supposed to be sent was that we want to replace a cumbersome, costly, and time-consuming "parts control" process with an agile "parts management" process that achieves specified performance outcomes to optimize system performance and supportability throughout the life cycle. Unfortunately, the unintended consequence of eliminating the requirement and method for parts management was that many programs stopped addressing any form of effective parts management.

PARTS MANAGEMENT REENGINEERING

In March 2004, DSPO established an ad hoc committee of government and industry representatives to reengineer parts management. This effort revealed that parts management lacks discipline and is decentralized and underfunded. Moreover, responsibility for parts management is widely spread and poorly defined, which limits its value to DoD. The committee recognized that realizing the full potential of parts management would require fundamental changes involving several organizations. The needed changes would improve interoperability, increase operational availability, shorten system development time, and reduce the logistics footprint and total ownership cost.

After studying the situation and identifying problem areas, the ad hoc committee published recommendations to significantly improve defense parts management. Two of the most important recommendations were to

- make parts management a policy and contractual requirement and
- revitalize parts management within the systems engineering discipline.

These recommendations are interconnected, because systems engineering is the area responsible for the parts management contractual requirement.

Systems Engineering

Parts management is an SE design consideration. Selecting the right parts is fundamental to achieving many SE and manufacturing objectives, and it influences cost, schedule, and performance.

To implement the committee's recommendations, DSPO collaborated with the SE community to craft and reintroduce parts management language into SE policy, guidance documents, and training. The response was very positive, because systems engineers are acutely aware of the importance of using optimum parts in design. The Parts Standardization and Management Committee (PSMC) is responsible for implementing strategies for carrying out the recommendations for reengineering parts management. The PSMC is a DSPO-chartered government and industry forum that influences and supports parts management and standardization.

The PSMC, with strong systems engineering participation, has made significant progress concerning the recommendation for parts management in the policy and contractual requirement area. MIL-STD-3018, "Parts Management," and an associated Data Item Description, DI-SDMP-81748, "Parts Management Plan," have been developed for contractual implementation of parts management requirements. DSPO published SD-19, *Parts Management Guide,* to provide government and industry managers a pragmatic approach to parts management that will enhance weapon systems operational and logistics readiness and will reduce the logistics footprint and total ownership cost. When used with MIL-STD-3018, the guidance in SD-19 will help ensure successful parts management to support current acquisition strategy. A directive memorandum that would require weapon systems and equipment acquisition contracts to address parts management is being considered.

Progress also has been made concerning the revitalization of parts management within systems engineering. A recent event that will help ensure success in this regard was the transition of DSPO to the Mission Assurance team of the Office of the Director, Systems Engineering. This is a good fit because the parts management discipline is now in the same specialty engineering group as several related disciplines: reliability, availability, and maintainability (RAM); supportability, quality, and manufacturing and producibility; DMSMS; and value engineering/reduction in total ownership cost. In addition to having a direct positive impact in these areas, parts management will contribute to the overall SE mission in the risk identification and management and the life-cycle focus areas.

Systems engineering's representatives on the PSMC identified four goals for revitalizing parts management within systems engineering:

- *Ensure parts management is adequately reflected in SE policy and guidance.* Recent accomplishments include the addition of parts management language in *Defense Acquisition*

Guidebook, Chapter 4, "Systems Engineering," Section 4.4.12. Other key SE policy, contractual, and guidance documents are under review for potential inclusion of parts management language.

- *Conduct outreach on the importance and benefits of a proactive parts management approach.* Among the accomplishments in this area are presentations at PSMC conferences; development of a Defense Acquisition University course (CLL206, Parts Management Executive Overview) as a continuous learning module; parts management training, SE presentations, and discussion panels at the annual DMSMS and Standardization conference; and journal articles. Opportunities going forward in this area include presentations at conferences hosted by industry associations; the Office of the Director, Systems Engineering; the Office of the Under Secretary of Defense for Acquisition, Technology and Logistics; and service program executive offices and systems commands.
- *Build on the parts management relationship to RAM.* This goal should not be difficult to accomplish, because the relationship between RAM and parts management has always been strong. RAM guidance documents address some form of parts management or part selection, but the verbiage needs to be strengthened and updated.
- *Exploit parts management contributions to manufacturing readiness.* This goal needs further review to determine how best to address parts management considerations.

Although much work remains to be done, the DoD parts management program is now under the optimal organization for accomplishing these SE goals.

Conclusion

One cannot overstate the importance of systems engineering—and the specialty engineering disciplines associated with it—to successful, cost-effective acquisition. Parts management contributes to the overall SE mission in the risk identification and management and the life-cycle focus areas. Today's parts management program is becoming more flexible, more user friendly for contractors, and more comprehensive due to a major reengineering effort that is still underway. The time is right for parts management to be emphasized in the SE area. The PSMC will continue to address SE parts management initiatives with help from the SE and parts management communities. To be involved in this effort, please contact DSPO's Donna McMurry at Donna.McMurry@dla.mil or 703-767-6874.

About the Authors

Dan McLeod, who has 47 years' federal experience, is a consultant for DSPO. He is an expert on parts management and a leader of the Parts Standardization and Management Committee.

Jay Mandelbaum is a staff member at the Institute for Defense Analyses, supporting the Office of the Secretary of Defense. Dr. Mandelbaum leads technology research focusing on readiness assessment, quality assurance, and systems engineering. He spent 30 years in the federal government.

Mitigating DoD's Acquisition Risks

By Brian Mansir

When buying commercial items and nondevelopmental items (NDIs), DoD acquisition teams must be aware of and take steps to mitigate the risks associated with three potential problems: Diminishing Manufacturing Sources and Material Shortages (DMSMS), counterfeit parts and components, and components without leaded solder and finishes. These problems can have large regulatory compliance and life-cycle cost implications, as well as issues with performance.

Diminishing Manufacturing Sources and Material Shortages

THE PROBLEM

DMSMS situations arise when a source for an item stops producing the product, when the manufacturer changes the product enough that it cannot directly replace the original product, or when procurements fail because of product unavailability. Commercial items and NDIs are particularly prone to DMSMS situations. Many of these items, especially those containing electronics, have short life cycles. Such products are continuously being improved or replaced by next-generation products. A typical commercial electronic product may be available for only 2 or 3 years before a new generation of products emerges or before the item is replaced by newer technology. This trend conflicts with DoD's efforts to significantly prolong the life of weapon systems that contain such products. As a result, repair parts disappear long before the end of the weapon system's life cycle.

Obsolescence of nonelectronic and commercial off-the-shelf items also poses a significant problem to weapon systems sustainability. When a commercial item or NDI has been incorporated into a defense system designed to be in service for 30 to 40 years, most of those items will eventually become obsolete and potentially become a DMSMS problem.

RISK FACTORS

The risk of DMSMS is due to several factors:

- *Rapid change.* Commercial markets are driven by competition, profits, and market share. In the electronics technology sector, rapid technological advances drive rapid introduction of newer, more capable products. In this rapidly evolving environment, new product versions may not be interchangeable with earlier versions.
- *Limited product data.* Commercial item data are generally limited to specifications, operating instructions, and maintenance documentation. Buyers of commercial items may obtain interface and performance characteristics but have little or no insight into

the internal composition of a product. This lack of insight may greatly complicate the process of identifying suitable replacement items when a DMSMS situation arises.

- *Configuration and content variation*. While developing and producing commercial items, manufacturers face constantly changing prices and availability of components such as microchips, diodes, resistors, capacitors, disk drives, memory devices, and displays. As a result, different production lots can be functionally equivalent but contain different components and subassemblies. The product manufacturer may or may not identify these configuration changes.
- *Inventory costs.* It is not in a manufacturer's best interest to warehouse quantities of an existing product (or repair parts) when the product will soon be replaced by a next-generation product. To avoid both costly warehousing expenses and unmarketable excess inventory, a manufacturer will minimize his aging stock, thereby limiting product availability.
- *End of production*. When a commercial item will soon go out of production, the effects of the end of production must be examined and understood at both the product and system levels to determine what actions if any are needed.
- *End of support*. As new commercial items are introduced into the market, manufacturers must determine when to stop supporting the older products. To avoid alienating the customer base using the older product, a manufacturer may support the product even if doing so is not profitable. However, at some point, support by the original equipment manufacturer (OEM) will end. (Third-party sources may be available to provide support services.)

Other Information Related to DMSMS

Defense Standardization Program Office, *Diminishing Manufacturing Sources and Material Shortages: A Guidebook of Best Practices and Tools for Implementing a DMSMS Management Program*, SD-22, September 2009.

RISK MITIGATION STRATEGIES

Solving DMSMS problems is complex, data intensive, and expensive. The best way to mitigate the risks of DMSMS is to design systems that enable frequent technology upgrades or refreshments through the insertion of newer items as they become available. For example, systems should be designed with standard interfaces and plug-and-play modules.

Risk mitigation does not stop when the design phase is completed. Rather, it must continue throughout the system's life cycle. The following are among the risk mitigation strategies often used by integrated product teams:

- Involve individuals who understand the interrelationships among commercial market forces, market research, technology trends, commercial standards, commercial product risks, and risk mitigation strategies.
- Involve users early and throughout the program life cycle to identify and resolve constraints related to commercial items. Early end-user involvement helps to ensure that requirements accurately reflect user needs. Users also can help prioritize requirements and identify and resolve potential suitability issues.
- Perform continuous commercial item market research. Market research includes system obsolescence profiling to plan for the continued support or replacement of soon-to-be obsolete products.
- Project the manufacturer's product support period and inventories.
- Integrate market research results with field data, including information technology, obsolescence projections, system supportability, performance requirements, reliability, maintainability, availability, and logistics.
- Ensure that product obsolescence information is part of the overall system life-cycle planning.
- Plan and provide for testing. Commercial products change rapidly and may have undisclosed design changes. In addition, products being considered for system technology refreshment need to be tested within a system context to verify functionality. Testing is necessary to ensure that engineering changes do not have a negative effect on system performance.
- Use product selection factors that include product maturity; manufacturer production and support history, stability, and flexibility; market share; and upward/downward compatibility. These need to be weighted as to their relative importance and influence on DMSMS risks.
- Continually analyze the product to project and prioritize product obsolescence issues; to refine budget estimates; to identify emergent or unplanned commercial item support issues due to changing business or market conditions such as bankruptcies, mergers, and product line changes; and to determine alternatives to avoid obsolescence situations.
- Tailor risk analyses to take into account such factors as market conditions, technology longevity and supportability, optimum technology refresh cycles, numbers of system configurations, and risk mitigation strategies.

The risk mitigation strategies should be identified in the integrated program plan, a "living" document that is continuously updated to address overall strategic planning, including program decisions and changes, and to project the system's evolution. The plan also should address commercial item support options such as end-of-life buys, extended warranties, license extensions, technology refreshment, third-party maintenance, and data rights.

Counterfeit Parts and Components

THE PROBLEM

Counterfeiting of parts and components occurs in nearly every type of commodity, whether electronic or mechanical. A counterfeit part is a part that is a copy or substitute offered without legal right or authority to do so or a part whose material, performance, or characteristics are knowingly, or unknowingly, misrepresented by a supplier in the supply chain. Thus, a counterfeit part could be, for example, a used product sold as new, a commercial product sold as military grade, a product stolen from the manufacturer's production line, a product built without authorization from the intellectual property rights holder, or a product containing pure tin, but sold as containing lead.

The counterfeiting problem is huge. Research from *Businessweek* indicates that counterfeit products probably make up at least 7 percent of world merchandise trade. The total for counterfeit merchandise may have been as much as $512 billion during 2004.

A 2009 Department of Commerce survey, focused on discrete electronic components, microcircuits, and circuit board products, found that 45 percent of participating organizations had encountered counterfeit parts. The participating organizations represented the entire supply chain from manufacturer to end user. The high percentage of organizations with counterfeit incidents indicates the pervasiveness of the counterfeit threat, which is of particular concern to DoD and the aerospace industry because of the potential threat to safety and security.

That same survey also found that incidents of suspected or confirmed counterfeit parts rose by more than 240 percent from 2005 to 2008. The survey showed that item resale value is not a major factor in determining what products are counterfeited; of the reported counterfeit incidents, most parts had a selling price between $10 and $100. Parts need not be expensive to be lucrative in the counterfeit marketplace. The counterfeiters do not have the costly research, development costs, or marketing expenses. In addition, counterfeit goods are typically manufactured with deficient raw materials and substandard manufacturing processes.

RISK FACTORS

The risk of counterfeit parts and components entering the supply chain is due, in large part, to DMSMS and electronic waste (e-waste). The link between DMSMS and counterfeit parts is strong. Counterfeiters find markets with serious shortages and seize the opportunity to fill the shortages with counterfeit parts. At the same time, the counterfeit market is lucrative, because customers seeking to fill a critical need will often buy from risky sources, either in spite of the danger or because they are unaware of the danger. To put it another way, DMSMS creates a demand for hard-to-find components. In many instances, these components are essential to keep older weapon systems or equipment operating. Parts obsolescence often forces buyers to seek out unfamiliar sources when known and trusted sources can no longer supply the needed items. The vast majority of counterfeit parts enter the supply chain through unauthorized distributors, or those most removed from the original component manufacturer (OCM). Although unauthorized distributors make up the largest part of this problem, sometimes counterfeits are passed along, unknowingly, from trusted sources.

The link between e-waste and counterfeit products also is strong. Many electronic components contain hazardous materials such as lead, barium, beryllium, mercury, cadmium, or arsenic. The danger associated with environmental contamination from equipment containing those substances has led to legislation or directives in Europe and other places governing and restricting the disposal of e-waste. Two of the most important of these directives—Reduction of Hazardous Substances (RoHS) and Waste Electrical and Electronic Equipment (WEEE)—were issued by the European Union and apply to such electronic items as computers, cell phones, televisions, appliances, tools, toys, and sports equipment.

Key Standards and Other Information Related to Counterfeits

SAE Aerospace Standard AS5553, "Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition."

IDEA-STD-1010-A, "Acceptability of Electronic Components Distributed in the Open Market."

U.S. Department of Commerce, *Defense Industrial Base Assessment: Counterfeit Electronics*, January 2010.

Compliance with the legal requirements greatly increases the cost of recycling e-waste. Consequently, tons of scrapped electronic products are shipped from around the world to nations where these requirements do not exist or are not enforced. (The National Safety Council estimates that 75 percent of all personal computers ever sold are now part of the e-waste stream.) The majority of this e-waste is shipped to China and a handful of other Asian nations. Those nations, in turn, strip components from the e-waste; re-mark them with new part numbers and recent date codes, update the packaging, and so on; and return the items—now counterfeits—to the global supply chain. Counterfeit parts and components originate in many different countries, but according to some estimates, approximately 80 percent of all counterfeit items come from China. The top 10 countries are China, Taiwan, India, Malaysia, Philippines, Indonesia, Singapore, Thailand, Russia, and South Korea. Eastern Europe, South America, and the Middle East are also known sources of counterfeit parts.

RISK MITIGATION STRATEGIES

The risk of counterfeits can be mitigated in one of two ways:

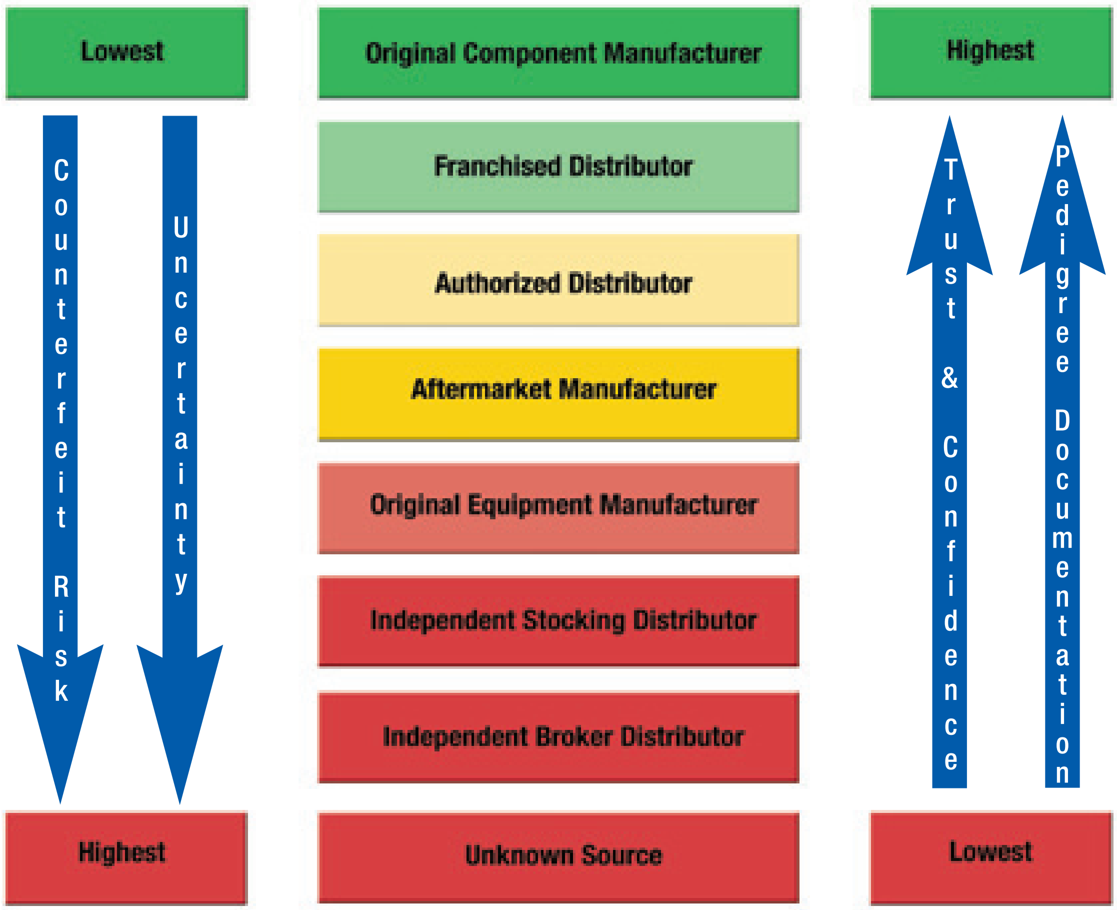
- Avoid buying parts and components from unknown sources; instead, purchase such products only from trusted suppliers
- If no known, trusted supplier is available, subject the purchased products to rigorous inspection and testing.

The degree of trust, and the risk of counterfeits, varies with the type of supplier, as shown in Figure 1:

- The OCM designs and engineers the part, owns the intellectual property rights, and can easily provide a pedigree or proof of a part's authenticity.
- A franchised distributor has a contractual agreement with the OCM to buy, stock, repackage, sell, and distribute its parts.
- An authorized distributor is officially authorized by the OCM to sell its parts.
- An aftermarket manufacturer has permission from the OCM to manufacture and sell the OCM's intellectual property as replacement parts.
- An OEM produces or builds equipment or systems containing OCM parts.
- An independent distributor purchases parts with the intention to sell and redistribute them, generally with no contract, authorization, or direct relationship with the OCM.
    - A stocking distributor is an independent distributor that stocks large inventories of parts. These parts may be purchased from any number of sources.
    - A broker distributor is an independent distributor that searches the market and locates parts that meet the customer's requirements and target price. Brokers locate parts but do not necessarily stock parts. A broker distributor may, in some instances, be a single individual operating out of a private home, warehouse, or storefront.

According to organizations that have investigated the counterfeiting problem, the best mitigation strategy is to procure items only from OCMs and their franchised or authorized distributors. When the original manufacturer no longer makes the required item, or the item is in short supply, users must obtain these products on the open market, which increases the risk of purchasing counterfeits. Therefore, purchasing on the open market warrants special precautions.

Figure 1. Relationship between Type of Supplier and Level of Risk and Trust



The most effective precaution is to purchase from suppliers that maintain full traceability. The most important document for traceability is the certificate of conformance, a formal declaration by the supplier that all requirements have been met. Responsible suppliers must provide traceability certificates that trace parts back to the OCM. Lacking a certificate, the next best trail is an unbroken chain of documentation (certifications, packaging slips, etc.) tracing the movement of the parts back to the OCM. Although traceability provides some level of assurance, be aware that, just as parts can be counterfeited, certificates can be faked as well.

Products backed by the original manufacturer's warranty offer the greatest assurance of integrity and traceability. Each step further away from the OCM adds a new layer of uncertainty about the pedigree, decreasing buyer confidence in the product's authenticity and increasing the risk that the part may be a counterfeit. Another precaution is to know what the item should cost. If a supplier's prices are significantly lower than expected, or significantly lower than the competition's prices, the supplier may be offering counterfeits.

If it is impossible to avoid buying products from an unknown or less trusted source, the purchased products should be subjected to rigorous inspection and testing to determine

Checklist of Key Best Practices for Mitigating the Risk of Counterfeits

- ❑ Determine if distributor has membership in GIDEP.
- ❑ Determine if distributor has history of suspected counterfeits in GIDEP.
- ❑ Provide institutionalized policies and procedures on how to avoid and handle counterfeit components.
- ❑ Provide clear written guidance on how to test, handle, and track incoming and outgoing parts and how to manage and dispose of suspected counterfeits.
- ❑ Purchase electronic components through reputable distributors with stringent quality-control procedures.
- ❑ Determine if a distributor is certified by ISO (ISO 9001:2000), SAE International (AS9120), and Electrostatic Discharge Association (ESD S-2020-2007).
- ❑ Determine if a distributor follows IDEA-STD-1010-A inspection techniques for counterfeit detection.
- ❑ Determine if a distributor has CTI CCAP-101 certification for counterfeit avoidance and detection.
- ❑ Determine if a distributor has memberships in leading trade organizations such as IDEA and ERAI.
- ❑ Check with the Better Business Bureau or similar organizations to assess whether a distributor uses ethical business practices.
- ❑ Maintain a register of approved suppliers.
- ❑ Review the distributor's past business practices, request letters of recommendation, and schedule on-site visits.
- ❑ Determine if a distributor offers potential buyers enough time to carefully inspect or test component lots prior to final payment.
- ❑ Before trading with an unknown supplier, check trade references.
- ❑ Build strong relationships with suppliers you trust.
- ❑ Specify a preference to procure directly from OCMs or authorized distributors.
- ❑ When possible, buy parts directly from OCMs and their authorized distributors.
- ❑ Require supply chain traceability to the OCM or aftermarket manufacturer.
- ❑ Require suppliers to trace parts back to OCMs in order to prove part authenticity.
- ❑ Require suppliers to provide proof of a valid OCM warranty.
- ❑ Specify quality requirements in contracts and purchase orders intended to minimize the risk of being provided counterfeit parts.
- ❑ Avoid buying batches of components with different colors, dates, or batch codes.
- ❑ Determine if a distributor uses escrow accounts and offers product warranties.
- ❑ Visit or audit potential suppliers to verify their quality practices, including their ability to perform authenticity testing, ensure compliant parts, and identify and block counterfeit parts.
- ❑ Periodically test components to confirm that they meet or exceed OEM specifications.
- ❑ Verify how the components were handled, stored, and shipped.
- ❑ Confirm that suppliers use effective counterfeit avoidance policies and practices.
- ❑ Ensure that suppliers maintain effective processes for mitigating the risks of buying and selling counterfeit parts
- ❑ Assess potential sources to determine the risk of receiving counterfeit parts.
- ❑ Communicate with suppliers, monitor supplier performance, and provide feedback to suppliers.
- ❑ Require independent third-party inspection and testing.
- ❑ Use contractual clauses that help protect the buyer from counterfeit parts.
- ❑ Train all employees who handle electronic parts (including purchasing, quality assurance, and receiving personnel) on how to inspect parts and identify possible counterfeits.
- ❑ Conduct training and increase awareness about counterfeit risks and risk mitigation.

Notes: CCAP = Counterfeit Components Avoidance Program, CTI = Components Technology Institute, ERAI = Electronic Resellers Association, Inc., GIDEP = Government-Industry Data Exchange Program, and IDEA = Independent Distributors of Electronics Association.

Other sources of information: Aerospace Industries Association's Counterfeit Integrated Project Team, Coalition Against Counterfeiting and Piracy, Government Electronics and Information Technology Association, and National Electronics Distributors Association.

their authenticity. The inspectors should look for signs of counterfeiting in two places: the products themselves, and the documentation and packaging accompanying the products. Table 1 identifies some visual cues or indications of possible counterfeit parts.

Table 1. Indications of Possible Counterfeiting

Component	Documentation and packaging
Blacktopping	Misspellings
Indents	Poor use of English
Body molds	Missing manufacturer's logo or label
Part markings	Mismatch between the logo or label on the product and that on the manufacturer's website or on previous shipments
Locations where the parts were made	
Part texture	Impossible date codes (e.g., in the future)
Leads	Mismatch between date codes or lot codes on the certificate of conformance and the codes on the parts
Evidence of prior use	
Variations in size or shape	
Improper fit	
Packaging variations	
Variations in graphics and colors	

Products that pass the initial inspection should then be subjected to various types of testing:

- Thermal-cycle testing
- Electrical testing (continuity, functional, parametric, and radio-/high-frequency testing for parasitics)
- Burn-in
- Curve-tracer testing
- RoHS compliance testing
- Microscopic inspection using advanced microscopes and cameras with charge-coupled devices
- X-ray and x-ray fluorescence
- Destructive physical analysis
- Internal visual verification using decapsulation.

Some counterfeit detection approaches may not be cost-effective for all parts and components. The best application is on larger units such as avionics, computers, instruments, and actuators or on anything that is deemed a safety- or mission-critical component.

In sum, the procurement process is the main entry point for counterfeits due to the use of unapproved suppliers, lack of part authentication procedures, lack of communication and cooperation between suppliers and customers, insufficient inventory control procedures, and limited counterfeit-avoidance procurement policies and practices.

The strategies for mitigating the risk of counterfeiting should be documented in a counterfeit parts control plan. The plan should, among other things, address the detection, verification, and control of in-process and in-service suspect counterfeit parts; detection of counterfeit parts before formal product acceptance; supply chain traceability to the OCM or aftermarket manufacturer; procedures for assessing potential sources of supply and maintaining a register of approved suppliers; flow down of applicable requirements; and methods for physical identification, segregation, quarantine, and control of suspect or confirmed counterfeit parts to preclude their use or installation. The plan also should require reporting of all occurrences of counterfeit parts to internal organizations, customers, Government-Industry Data Exchange Program, industry-supported reporting programs (e.g., the Electronic Resellers Association, Inc.), and criminal investigative authorities (Federal Bureau of Investigation or Department of Commerce). Finally, it should discuss requirements for certificates of conformance and testing certifications.

Components without Leaded Solder and Finishes

THE PROBLEM

DoD and the U.S. aerospace industry want electronic components, particularly those used in applications requiring high-reliability performance, that are made with leaded solder and finishes. However, finding such components is difficult because of various bans on the use of lead. Without lead, solder is more brittle and, therefore, may not be able to handle mechanical stresses such as the g-force created when spacecraft lift off.

Lead-free finishes can be problematic because of the risk of tin whiskers. Tin whiskers are elongated, electrically conductive crystalline structures that grow spontaneously from pure-tin surfaces. Tin whiskers have caused failures in electronics by short-circuiting to adjacent conductors. Aircraft, satellites, and missiles also have failed due to tin-whisker short circuits. In 1998, a $250 million Galaxy IV communications satellite was lost after two processors failed; the backup satellite could not be used because tin whiskers had shorted it out a year before. At least 10 other satellite failures have been blamed on tin whiskers. Most tin whisker-related failures occur after 1 to 3 years of service, early in the life cycle of defense weapon systems.

RISK FACTORS

The risks related to leaded versus lead-free components are twofold: the difficulty of finding manufacturers that will produce electronic components using lead solder and finishes, and the difficulty of distinguishing between parts that appear to be identical but are, in fact, different in terms of their lead content—some are lead free while others are not.

Lead has long been known as hazardous to humans and the environment, and its use has, for many years, been banned in plumbing, coatings, gasoline, paint, and other products. In an effort to further reduce the risks, the European Union nations sought to reduce the amount of lead in the manufacturing process by issuing the RoHS and WEEE directives, which became European law in 2003. Beginning on July 1, 2006, the European Union began banning the import of electronic components that include lead and other heavy metals. The United States, Japan, China, South Korea, Argentina, and Australia have taken similar measures.

To be able to sell parts to countries in Europe and beyond, and to remain competitive, manufacturers must comply with the RoHS and WEEE directives. The RoHS and WEEE directives do not apply to defense and aerospace products. However, the defense and aerospace industries depend on commercial manufacturers as their sources for electronic components. Manufacturers design and produce electronic components primarily for the commercial market, and those products are lead free. Producing the same product, but using lead, for the defense and aerospace industries would not be economical, because the defense and aerospace requirement for electronic components accounts for less than 1 percent of the electronic components market. Few, if any, can afford to operate two independent manufacturing lines for the same product, one without lead and one containing lead. The end result is that many key components and assemblies used in aerospace systems are now available only in their lead-free forms.

Even when the defense and aerospace industries can obtain electronic components with lead solder and finishes, they risk mistakenly using lead-free parts in applications requiring high-reliability performance unless they implement practices that will mitigate the risk.

Key Standards Related to Leaded Solder and Finishes

GEIA-STD-0005-1, "Performance Standard for Aerospace and High Performance Electronic Systems Containing Lead-free Solder."

GEIA-STD-0005-2, "Standard for Mitigating the Effects of Tin Whiskers in Aerospace in High Performance Electronic Systems."

GEIA-STD-0005-3, "Performance Testing for Aerospace and High Performance Electronic Interconnects Containing PB-free Solder and Finishes."

GEIA-HB-0005-1, "Program Management/Systems Engineering Guidelines for Managing the Transition to Lead-Free Electronics."

GEIA-HB-0005-2, "Technical Guidelines for Aerospace and High Performance Electronic Systems Containing Lead-Free Solder and Finishes."

GEIA-HB-0005-3, "Rework and Repair Handbook for Aerospace and High Performance Electronic Systems Containing Heritage SnPb and Lead-Free Solder and Finishes."

GEIA-HB-0005-4, "Impact of Lead Free Solder on Aerospace Electronic System Reliability and Safety Analysis."

ASTM F2725–08, "Standard Guide for European Union's Registration, Evaluation, and Authorization of Chemicals (REACH) Supply Chain Information Exchange."

RISK MITIGATION STRATEGIES

It is essential to understand from the outset whether an application needs RoHS-compliant (lead-free) components or whether it needs components containing lead. RoHS-compliant components should be used in all applications except those requiring high reliability; this practice will preclude penalties associated with noncompliance. On the other hand, if a military or aerospace application requires high reliability, then only components with traditional tin-lead solder (63 percent tin and 37 percent lead) and lead finishes should be used. Below are a few best practices that may help to avoid potential issues related to leaded versus lead-free components:

- Ensure that suppliers fully understand the issues of using leaded versus lead-free components.
- Verify that suppliers use different part numbers for leaded and lead-free components that are otherwise identical. If different part numbers are not issued, it is difficult to distinguish lead-free parts from leaded parts. This is also an issue when components are returned or when they are recycled.
- Whenever possible, buy from trusted sources. Avoid unknown sources offering questionable products at a low price.
- Seek components that have a clear pedigree to verify whether components are lead free or not.
- Upon receipt of the components, verify that they are truly RoHS compliant or contain lead, whichever is needed to meet the requirements. Sample and test parts whenever a pedigree for the part is not available. An x-ray process can tell if there is lead in the part, without destroying the part, but it cannot detect all of the hazardous materials listed in the RoHS directive. The most certain way of testing a part involves destroying it to get a complete chemical breakdown.
- Never comingle leaded and lead-free components in inventory or applications. Although maintaining dual inventories and manufacturing lines can be costly, the costs of failures can be far greater.
- Stay informed about research on solder alloys being tested to replace tin-lead. Although none yet is a proven replacement for tin-lead, research may soon yield an acceptable substitute that will meet high-reliability requirements.

About the Author

Brian Mansir has worked at LMI, a not-for-profit government consulting company, for the past 30 years. He leads research and analysis projects and provides counsel to senior leaders of the nation's national security and other public-sector organizations.

The Defense Logistics Agency's Long-Range Plan for Managing Technical Data

By Denise Duncan

Technical data are "invisible assets" that enable DoD to build and repair its weapon and other systems and to keep our nation's warfighters supplied with the material they need in-theater. In other words, DoD is dependent on technical data to ensure that planes, vehicles, and other systems are repaired and returned to the warfighters as quickly as needed. And, like any other organization, DoD wants to do this effectively and at the lowest possible cost.

The technical data required to build and repair DoD systems are developed as part of the systems engineering processes in the acquisition life cycle. Decisions made throughout that life cycle determine what data will be available for system support. Below are examples of data-related decisions made in the different life-cycle phases:

- *Material solution analysis phase.* This phase includes establishment of a program management office and development of a technology development strategy. The technology development strategy addresses, among other things, plans for data management and technical data rights.
- *Technology development phase.* This phase includes initial definition of the product support strategy and initial development of an evolutionary acquisition strategy. Among the topics addressed in the acquisition strategy is the data management strategy.
- *Low-rate initial production phase.* During this phase, the acquisition strategy, including the data management strategy, is refined.
- *Deployment phase.* In this phase, product support and performance-based logistics rely on technical data acquired in the preceding phases. This phase also includes management of new technical data developed as part of continuous technical refreshment.

The complexity of major defense systems and the length of time their technical data must be usable—it is not unusual for a DoD system to remain in use for decades—pose a challenge to the organizations that support those systems once they are fielded. To successfully meet the challenge, support organizations must depend on many processes that occur in the development and production phases of the system life cycle to obtain the technical data and correct rights to the technical data needed to support the systems. Without good technical data, the rights to use those data, and the effective management of the data over decades, system support can suffer.[1]

The Defense Logistics Agency (DLA), DoD's largest logistics combat support agency, is facing that data management challenge. Another challenge for DLA is that the organization responsible for managing the technical data for a particular system changes over the system acquisition life cycle. During the development phase of the life cycle, a program management office in the military service that "owns" the system is responsible for acquiring and managing the technical data about the system. After the system has been deployed, the service's engineering support activity (ESA) controls the technical data. Consequently, DLA must work with many organizations across DoD to ensure that it will have the rights to use the best technical data to procure the correct parts for DoD systems.

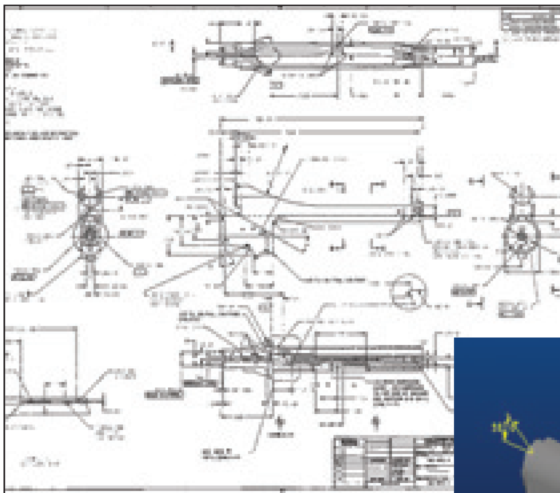
DLA recently articulated a long-term vision for the use of technical product data: "DLA will have access to a continuous flow of authoritative product data sufficient for economical reprocurement." This vision encapsulates DLA's need to locate, for a particular product part, the best source of technical data that can be used in procurement and that will result in the best pricing for the part.

To achieve its vision, DLA has set the following specific goals:

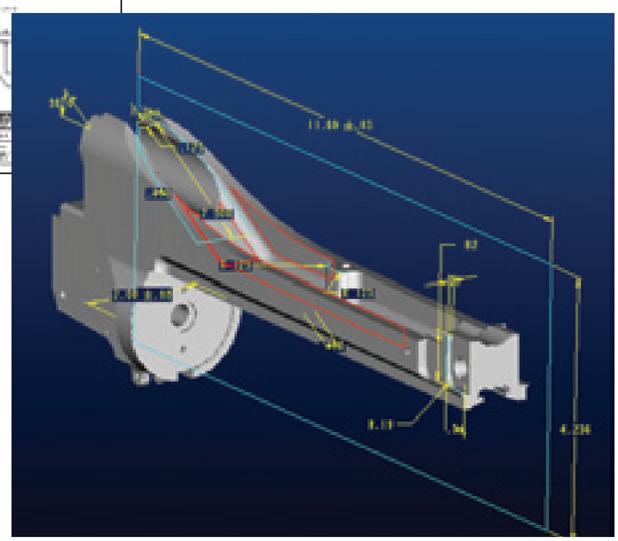
- *Ensure that DLA employees can easily locate and access the authoritative source of product data for the procurement of a specific part.* This goal implies that the authoritative source of data for a part can be easily identified and that the information systems used by the military services to store technical data have complete metadata to allow DLA to identify the authoritative source of the data. This goal also implies that DLA acquisition support personnel will have online access to those product data systems. To achieve this goal, DLA must liaise with the military services to understand their enterprise resource planning (ERP) systems and their product data management (PDM) systems. DLA must also work with the Office of the Secretary of Defense (OSD) and the military services to establish standard metadata for product data files.
- *Use complete, accurate, authoritative, and up-to-date product data.* This goal focuses on the content of the product data files, regardless of the PDM systems in which they are maintained. For example, the three-dimensional model of a part may be in one database, and the associated manufacturing process, finish, and other information may be in another. In other words, to procure a part with the correct form, fit, and function for a particular system, DLA needs a wide variety of technical information, such as geometry, dimensioning and tolerancing, numeric control machine code, text instructions, and material. Finally, all components of the product data must be easily found, linked, and accessed. To achieve this goal, DLA must collaborate with the military services, sharing information on DLA's and the services' ERP and PDM systems and identifying technical data packages that merit investment to improve their utility in parts procurement.
- *Ensure that DoD product data enable efficient, economical reprocurement.* This goal implies that the preferred form of product data is one that is complete and is easily used by the manufacturing base. In today's environment that means a three-dimensional model with associated material and process data that have been approved by the service's ESA for use in procurement. This goal also implies the use of standardized product data

formats. Establishing a limited set of standardized product data formats will require collaboration between DLA and the services. For example, they may jointly agree upon a set of native, neutral, and viewable formats. DLA has already started this process through its membership in the DoD Engineering Drawing Modeling Working Group, which is working on common practices and formats for three-dimensional models for engineering weapon systems. Figure 1 shows a two-dimensional drawing and a three-dimensional model of the same item.

Figure 1. Comparison of a Two-Dimensional Drawing and Three-Dimensional Model



Two-dimensional drawing



Three-dimensional model

- *Obtain product data and data rights for all new noncommercial parts entering the logistics system.* To achieve this goal, DLA must depend on other DoD organizations; in other words, this goal is executed entirely through collaboration with those organizations. DLA will work with OSD to establish policy, procedures, and practices that will ensure the acquisition of complete product data for new parts. DLA can also review all new parts presented for cataloging to ensure that product data are complete and usable for procurement.[2]

- *Strategically modernize legacy technical data packages.* Achieving this goal requires DLA to assess the legacy data packages it uses to identify those meriting an investment to improve their content. In other words, DLA needs to analyze the costs and benefits of improving select data packages. In some cases (for example, a data package for an infrequently used part), DLA may find that it cannot justify the cost, while in other cases (for example, a data package for a high-volume part that could be produced by multiple manufacturers), DLA may find that although costly, the benefits of improving the content of a particular data package will be significant. DLA will work with the services' ESAs to obtain their approval of the improved data for procurement.
- *Provide the DLA workforce with the training and tools it needs to use modern product data effectively.* If DLA succeeds in all the activities described above, the technical data available to the parts procurement workforce will be very different than now; the tools and business processes also will be different. To gain maximum value from these improvements, workflows may be adjusted, and the staff must be trained.

By actively pursuing its vision for improving the technical data needed to keep DoD's systems operational, DLA will be positioned to supply needed parts quickly and at the best cost.

[1]Lloyd Arrowood and Paula George, "Standardization and Management of Nondestructive Testing Data," *Defense Standardization Program Journal*, October/December 2009.

[2]Ric Norton, "Addressing the Need for Good Data Management," *Defense Standardization Program Journal*, October/December 2009.

About the Author

Denise Duncan is an LMI consultant with some 30 years of experience in information systems management. She co-chaired the panel that developed ANSI/GEIA-859, "Data Management," a standard published by the American National Standards Institute/Government Electronics and Information Association in 2004, and the ANSI/GEIA-859 handbook, *Implementation Guide for Data Management*. She advises government organizations as the industry expert on scientific and technical data management and maintains close relationships with government and industry data managers.

Technical Excellence
A Requirement for Good Systems Engineering

By William Vaughan

Technical excellence is a requirement for good systems engineering. Initiatives that address the enhancement of an organization's technical excellence are key to the organization's maintaining a high level of performance on current programs and projects as well as preparing for new programs and projects. This article addresses the interrelationships of technical excellence and systems engineering, as well as some key initiatives, of which technical standards are a part, associated with technical excellence and thus with good systems engineering.

Technical Excellence

Technical excellence is the goal of all engineering organizations and individuals, whether in government or private industry, national or international. What do we mean by technical excellence? Most people have their own ideas and interpretation as to what constitutes technical excellence. Entering "technical excellence" into the search page of Google produced over 28 million results, evidence that technical excellence is important to a large number of organizations and people, whether in the systems engineering discipline or other disciplines.

According to "Mr. Webster," excellence is defined as the state, quality, or condition of excelling; superiority. To excel is to be better than, or to surpass, others. We believe most, if not all, people would be comfortable with this definition. However, because the intent of this article is to demonstrate the importance of technical excellence relative to systems engineering, it may be good to explore some statements that have been made concerning technical excellence. One author, Teresa Vanhooser, defined technical excellence as an effort to ensure that well-considered and sufficient technical thoroughness and rigor are applied to programs and projects under an uncompromising commitment to safety and mission success.[1] Another author, Chris Scolese, identified four guiding principles to achieving technical excellence:[2]

- Clearly documented policies and procedures
- Effective training and development
- Engineering excellence
- Continuous communications.

According to Scolese, two fundamental attributes must be considered when pursuing technical excellence: (1) personal accountability, whereby each individual must understand and believe that he or she is responsible for the success of the organization's mission, and (2) organizational responsibility, whereby the organization provides the proper training, tools, and environment.[3]

NASA's Aeronautics Research Mission Directorate is an example of one organization that stresses technical excellence. On the NASA website, the directorate has noted its commitment to technical excellence, to technical accomplishments that benefit the public, and to its role as steward of the scientific and technical workforce and facilities responsible for civil aeronautics research. In addition, each year, the directorate highlights the technical accomplishments of its scientists and engineers.[4]

It has also been noted that due to the rapidly expanding technology and science, engineers and technologists in the 21st century must have a strong technical background in their fields and understand technology at the interface between traditional fields. They must be creative, skilled problem solvers who can think critically using sound principles and concepts.[5]

Louis Armstrong is understood to have remarked that "if you have to ask what jazz is, you will never know." This remark could also apply to technical excellence. This becomes clear when one tries to quantify the meaning of technical excellence by producing metrics to establish whether a particular objective or goal has been achieved. For example, what provides a measure of the technical excellence achieved by an organization: number of patents received? number of professional journal publications? number of individuals with advanced degrees? number of engineers versus nonengineers at work? positive versus negative feedbacks on products? equipment or system successes versus failures? profit a company makes?

In the aerospace and defense engineering arena, one can certainly equate organizational technical excellence and thus good systems engineering to mission success, at least in the eyes of the public and in the eyes of Congress. In the final analysis, technical excellence may be the most important systems engineering goal of any engineering organization. How one achieves and maintains it is another question for which there is no simple answer. Unquestionably, an organization with recognized technical leaders who have vision, superior technical competence, and the desire to excel will achieve technical excellence. Thus, technical leadership is key for an organization's success and the ability of the managers assigned to carry out the organization's mission.

Technical excellence is also related to the strategic management of an organization's human capital. The technical excellence of its workforce is an organization's most critical asset in accomplishing its mission. Therefore, ensuring the continued development of scientific and technical expertise is necessary to preserve an organization's, and the nation's, role as a leader in technology. It is also significant to achieving technical excellence and, accordingly, good systems engineering.

In an attempt to identify a few outstanding characteristics of managers or management approaches that would ensure a program's success, NASA, after completing the very successful Saturn-Apollo program, undertook a research study in 1974. The study identified three "tall poles" important to program management:[6]

- "Pay attention to detail." (George M. Low)
- "Leave no stone unturned." (Werner von Braun)
- "Be aggressive—not passive." (Lee B. James).

These philosophies create policies and management methods that are highly conducive to program success or, in other words, technical excellence.

Systems Engineering

Like the term "technical excellence," the term "systems engineering," when entered into the Google search page, produced a significant number of results, evidence that systems engineering is recognized as being important for the success of essentially all products. Because most readers of this article will be rather well versed in DoD documents concerning systems engineering, as well as many of those by other agencies and nongovernment organizations, I have elected to share some of the points made on this subject in a document developed by the European Cooperation for Space Standardization (ECSS), a component of the European Space Agency.[7]

The systems engineering process is intrinsically iterative across the whole life cycle of the project and is produced under the leadership of engineering talents with technical excellence attributes.

The ECSS document defines systems engineering as "an interdisciplinary approach governing the total technical effort to transform requirements into a system solution." Here, "system" is defined as an integrated set of elements to accomplish a defined objective. These elements include hardware, software, firmware, human resources, information, techniques, facilities, services, and other support elements. The systems engineering process is intrinsically iterative across the whole life cycle of the project and is produced under the leadership of engineering talents with technical excellence attributes. Systems engineering is not an administered, focused, or led function. Technical excellence is the key to successful systems engineering and, thus, a successful project.

A recent article that addressed the synergies between systems engineering and Diminishing Manufacturing Sources and Material Shortages made two important points:[8]

- Systems engineering principles and best practices should be applied to enhance reliability, availability, maintainability, and sustainability through the entire life of a program.

- Managing major programs effectively requires sound systems engineering.

Accordingly, technical excellence and the associated "tall poles" noted above are integral to ensuring that the application of the principles and best practices of systems engineering to DoD programs, as well as to other programs, achieve the intended goals.

Technical Authority and Technical Excellence

In August 2003, the Columbia Accident Investigation Board issued a report documenting its investigation of the February 1, 2003, loss of the Space Shuttle Columbia during reentry.[9] One of the board's recommendations was to "establish an independent Technical Engineering Authority that is responsible for technical requirements and all waivers to them, and will build a disciplined, systematic approach to identifying, analyzing, and controlling hazards throughout the life cycle of the Shuttle System." With this introduction of independent technical authorities, the board placed further emphasis on the development and identification of technical excellence within NASA's workforce.

Technical authority is about ensuring that decisions on technical excellence balance program pressures with technical needs. According to Vanhooser, technical excellence involves thoroughness and rigor of the work performed, along with a commitment to safety and mission success. Obviously, one endeavors to ensure that those people identified as the technical authority for a discipline also reflect the organization's people with recognized and respected technical excellence in the discipline. Thus, technical excellence is recognized by the individual's accomplishments and by the products of the organization.

Following the Columbia Accident Investigation Board's recommendation, NASA implemented an independent technical authority to set and approve technical requirements for all flight programs and projects. The intent was to ensure safe and reliable operations. Technical authority, with the responsibility to execute, was delegated by the NASA chief engineer to specific individuals.

What are some of the attributes of an organization's culture that reflect a commitment to technical excellence and, therefore, to good systems engineering? Vanhooser suggests the following:

- Highest value integrated engineering products
- Continual growth, learning, and diversity of experience
- Technical conscience

- Responsive and technically engaged leaders at all levels
- Shared accountability for successes and failures
- Proactive, engaged, and predictive approach to technical content
- Teams whose members complement and complete each other
- Recognition that engineering requires versatility and mobility to meet the needs of the organization
- Placement of "the right person at the right place at the right time."

Some Examples of Technical Excellence Initiatives

In 2007, NASA undertook a technical excellence initiative to identify and resolve engineering challenges.[10] The initiative was designed to provide quality solutions and work that will translate into an agency investment strategy for application to present and future missions. Among the attributes of this initiative are improvement to overall technical capability; development of analysis and testing beneficial to multiple missions, programs, and projects; and advancement to tool/technique capability.

In 2006, the aerospace industry released a position paper that argues for standards based on technical excellence rather than the source of a standard.[11] Experts from the Aerospace Industries Association's Strategic Standardization Forum for Aerospace prepared a position paper on the use of aerospace standards in response to growing concern that certain policies and legislation may be putting the industry—and consumers—at risk.[12] The paper argues that the aerospace industry must select standards based on safety, quality, and technical merit, rather than based on which organization developed them. Thus, the paper recognized technical excellence relative to ensuring that the products of good engineering can be achieved.

The philosophy relative to enhancing technical excellence through the interplay of standards and their use on international missions is reflected in the following remarks by Michael Griffin, NASA Administrator from 2005 to 2009:

> One aspect of this discussion is the need to set certain engineering technical standards to ensure compatibility and interoperability in our exploration architecture. Analogous to my previous comments about spoken languages for future space explorers, it is important that the engineering standard for NASA's architecture be specified with the international metric, or SI, standards as the base unit of measure, with English units only by exception when it makes sense for NASA to do so. Thus, we hope for a high degree of compatibility of interfaces and standards, as space-faring nations explore the Moon, Mars, and near-Earth asteroids together.[13]

Thus, technically excellent standards, especially engineering technical standards, are crucial to ensuring the compatibility and interoperability of a system's architecture. Good systems engineering is important to achieving this goal.

Role of Technical Standards

Various endeavors are undertaken to ensure technical excellence and thus good systems engineering. Determining how to measure and ascertain the degree to which technical excellence has been achieved is another matter. Technical standards are an integral part of technical excellence. In this regard, those responsible for the development of technical standards must collaborate closely with the engineering elements within an organization.

Perhaps we should again consult "Mr. Webster" for what we mean by a "standard." The term means, among other things, a degree or level of requirement, excellence, or attainment. It is this meaning that we associate technical standards and their role in technical excellence.

Technical standards are an integral part of all systems engineering and related engineering development efforts, especially those in the aerospace and defense industry. Designers and engineers should be among the most aggressive supporters of strong technical standards. Standardization activities establish engineering and technical applications for processes and practices and, in doing so, enhance all engineering capabilities and promote technical excellence. Thus, they enable designers to not dissipate their energies on the costly exercise of "reinventing the wheel."

The motivations for technical excellence and the associated development of technical standards vary considerably. One most often sees economic issues as the principal motivation. Applications to regulatory matters are another strong motivation. Among the principal motivations for technical standards are international competitiveness; commodity confidence; safeguards for health, safety, and environment; risk reduction; facilitation of commercial communications; and technology transfer. However, enhancing systems engineering capabilities and technical excellence, although readily recognized as a key motivation, is not often seen in the list of motivations for the development and promotion of technical standards. The American National Standards Institute noted the following:

> Within the U.S. standardization system, stakeholders—companies, government agencies, public interest organizations, and individuals—follow the method of standards development and the conformity assessment scheme most appropriate for their particular needs. Rapidly evolving fields have requirements that are far different from those of traditional manufacturers or highly regulated technologies.[14]

Enhancing technical excellence is the key to the nation's future in the rapidly growing globalization of industry. For the United States to remain competitive and maintain its technical leadership in the world, enhancing the nation's engineering capabilities will be critical. These capabilities can be realized only by achieving technical excellence. This is necessary for the education of future engineers and the improvement of current engineers. Technical standards provide a major opportunity to achieve the goal of enhancing engineering capabilities and providing a means whereby technical excellence can be infused into the process, whether by DoD, other government agencies, or industry in general.

Enhancing an organization's systems and other associated engineering capabilities and technical excellence is an important value of technical standards, especially when coupled with allied information such as engineering lessons learned and experiences with the use of the standard. Such must be the thrust of any viable organization's technical standards activity. This thrust is reinforced and expanded based on feedbacks from the engineering staff of the organization, its contractors, and users of its products. This integration is one step toward the goal of significantly enhancing the systems engineering capabilities and technical excellence of the aerospace and defense industry to meet demands for timely, productive, and reliable systems, plus contribute to improved costs.

Concluding Remarks

This article has endeavored to focus on the subject of technical excellence and its importance to good systems engineering and to provide readers with some information and motivations that will enhance the quest for technical excellence. Not only is the need for technical excellence a significant matter for the aerospace and defense industry, both for government and nongovernment organizations, but it is equally important for all industries. Technical standards are an important element of technical excellence. The role standards play in achieving technical excellence includes the transfer of systems and other associated engineering experiences, lessons learned, best practices, and infusion of new technology for the further enhancement of technical excellence within all organizations. Thus, not only do technical standards support the achievement of technical excellence, and thus good systems engineering, they also enable technical excellence to be passed on to others. Although technical excellence is not easy to quantify, there is no doubt it is readily recognized, both by those involved in engineering activities and by those who are the "customers," be they public, congressional, or otherwise.

This article is based on "Technical Excellence: A Requirement for Good Engineering" (AIAA-2008-1120), prepared and presented by the author at the 47th American Institute of Aeronautics and Astronautics Aerospace Sciences Meeting, January 7–11, 2008, Reno, NV.

[1]Teresa Vanhooser, "MSFC Technical Excellence/Technical Authority," NASA Marshall Space Flight Center, Huntsville, AL, May 2007.
[2]Chris Scolese, "Four Guiding Principles of Technical Excellence," *ASK OCE*, Vol. 1, Issue 4, NASA Headquarters, Washington, DC, February 8, 2006.

[3]Chris Scolese, "Technical Excellence: Roles and Responsibilities," *ASK OCE*, Vol. 1, Issue 5, NASA Headquarters, Washington, DC, February 24, 2006.

[4]See http://www.aeronautics.nasa.gov/te_2006.htm.

[5]"Engineering and Technology for the 21st Century: Technical Excellence," Brigham Young University, Provo, UT, March 16, 2007.

[6]Konrad K. Dannenberg, *Management Philosophies as Applied to Major NASA Programs*, NASA-CR-141258, 1974.

[7]European Cooperation for Space Standardization, "System Engineering General Requirements," ECSS-E-ST-10C, http://www.ecss.nl, March 6, 2009.

[8]Chet Bracuto, Alex Melnikow, and Ed Zelinski, "New Synergies between Systems Engineering and DMSMS," *Defense Standardization Program Journal*, January/March 2010.

[9]NASA, *Columbia Accident Investigation Board Report*, Volume I, August 2003.

[10]NASA, "RFP for Technical Excellence Initiative Cross-Cutting Issues," November 5, 2007.

[11]American National Standards Institute, "Aerospace Industry Argues for Standards Based on Technical Excellence Rather Than Source," March 7, 2006.

[12]Strategic Standardization Forum for Aerospace, Aerospace Industries Association, "Safety of Aerospace Products Demands Freedom to Select Most Appropriate Standards," http://www.ssf-aerospace.org/, March 2006.

[13]Michael D. Griffin, "Partnership in Space Activities" (remarks, 56th International Astronautical Congress, October 20, 2006).

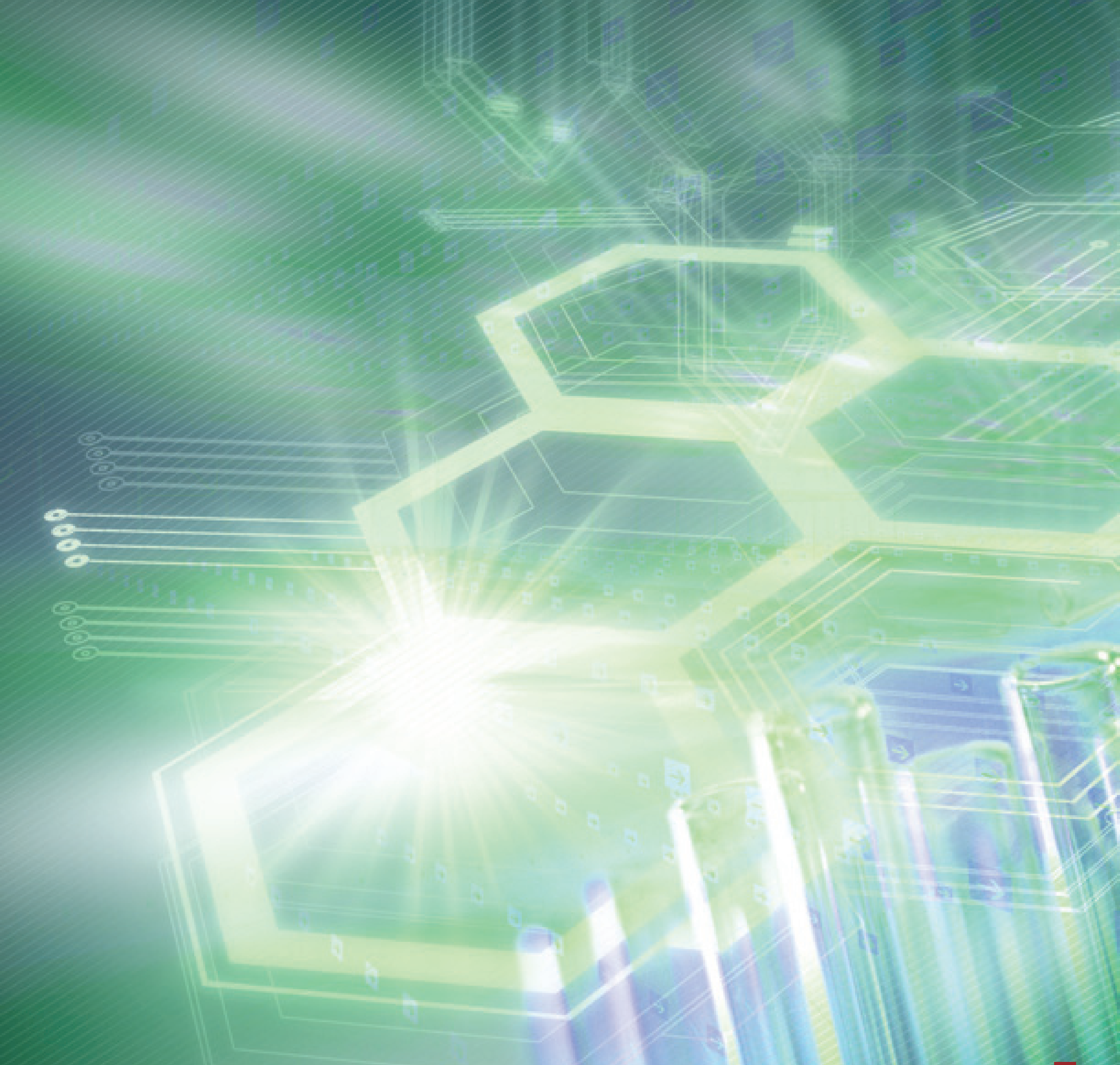
[14]American National Standards Institute, *Overview of the U.S. Standardization System: Voluntary Consensus Standards and Conformity Assessment Activities*, Third Edition, 2010.

About the Author

William Vaughan is a research professor at the University of Alabama in Huntsville, AL.

Ensuring Quality through Product Testing

By Joe Doyle and Yasmin Virani



High-quality products are the aim of systems engineering. The International Council on Systems Engineering defines systems engineering as

> an engineering discipline whose responsibility is creating and executing an interdisciplinary process to ensure that the customer and stakeholder's needs are satisfied in a high quality, trustworthy, cost efficient and schedule compliant manner throughout a system's entire life cycle.[1]

The Defense Acquisition University further defines systems engineering as

> a technical management and problem-solving process applied through all stages of development to transform needs and requirements into a set of system product and process descriptions (adding value and detail with each level of development).[2]

Ensuring that the products procured by DoD are of the requisite quality requires continual monitoring, an important mission of the Defense Logistics Agency (DLA). DLA monitors quality through its Product Verification Program (PVP), which encompasses comprehensive product testing and quality assurance for DLA-managed commodities. This article addresses DLA's efforts to improve the product testing processes.

Background

DLA administers four modern laboratory facilities, called product testing centers (PTCs), that are critical contributors to the agency's ability to monitor products destined for our nation's warfighters. The PTCs conduct professional scientific evaluations and related services across a wide range of DLA-managed commodities, and they provide product testing services along with engineering analysis and technical assistance in support of DLA's acquisition of spare parts for its customers. In short, these PTCs ensure that DLA purchases, stores, and delivers products that fully meet warfighter requirements.

The four PTCs are as follows:

- Analytical/Chemical PTC, which is located at DLA Troop Support, Philadelphia, PA. The Analytical/Chemical PTC conducts ballistic, electrostatic decay, optical, textile, and other testing to ensure the quality of articles that are critical to the personal safety and comfort of our nation's warfighters. For example, this PTC tests Marine Corps hot-weather and temperate-weather boots to ensure that they retain an adequate moisture vapor transmission rate and do not leak.
- Electronics PTC, which is collocated with PTC headquarters at DLA Land and Maritime, Columbus, OH. The Electronics PTC performs electrical, environmental, performance, and similar testing to ensure the conformance of electronic components—for example, microcircuits and connectors—to functional and safety specifications. Electronic components play a critical role in the performance of DoD's major weapon systems.

- Two Mechanical PTCs—Mechanical Central, which is located at DLA Land and Maritime, and Mechanical West, which is located at Sharpe Army Depot in French Camp, CA. The Mechanical PTCs conduct dimensional, finish, metallurgical, and tensile testing of components for weapon systems such as Mine Resistant Ambush Protected vehicles to ensure that their composition, durability, and strength are within specifications to provide the requisite protection to vehicle occupants.

DLA's PVP and its PTCs use the DLA Enterprise Business System (EBS) to manage their product testing processes and record transactional data. EBS, DLA's enterprise resource planning platform for supply chain management, provides visibility across the entire supply chain, from order placement to item delivery.

Each PTC is ISO 9001 compliant.

Opportunities for Process Improvement

DLA recognizes the challenges it faces in maintaining a strategic view of the monitoring mission across the expansive DLA testing environment. As part of its ongoing efforts to ensure product quality, DLA is embarking on a series of studies to evaluate aspects of the testing processes that could be improved, for example, by making moderate administrative changes or enhancing user guidance. Such changes could materially improve the decision-making ability of DLA quality assurance personnel and deliver numerous benefits to DoD. Some early candidates for investigation are increased standardization of testing terminology, prioritization of testing types, and procedures for selecting the proper sampling method and sample size.

Implications for DLA Product Testing

DLA takes its monitoring mission seriously. The agency is continually exploring ways to improve decision making for a broad range of DLA testing personnel. The nation's warfighters will ultimately reap the rewards. Other benefactors of enhanced product testing could include DLA headquarters personnel, PVP and supply chain personnel, and PTC lab managers and technicians. Used in concert, increased standardization and other improvements in the testing processes assist DLA with meeting its monitoring mission—perform product verification that ensures that the items procured are of the requisite quality—by

- helping DLA understand the total cost of product testing;
- assisting PVP and supply chain personnel with making wise choices of lab assignment for targeted and high-risk populations;
- providing testing methods that consider failure rates, item criticality, and counterfeit potential; and

- allowing PVP, supply chain, and lab personnel to choose scientifically suitable sampling methods and select the most appropriate sample size.

Potential Benefits across DoD

We owe it to our warfighters to provide them high-quality commodities while making the best possible use of DoD's resources. The entire Department could benefit from enhanced product testing of DLA-procured or -managed items. Below are examples of advantages that could accrue at different levels of the Department:

- For the warfighter
  - Greater confidence in DLA commodities
  - Increased availability of commodities
  - Improved product quality
- For DLA headquarters
  - Informed decision making
  - Enhanced data integrity
  - Reduced cycle time
- For DoD
  - Higher likelihood of detecting counterfeit material and unauthorized product substitutions
  - Less waste
  - Lower total cost of ownership.

[1]See http://www.incose.org/practice/fellowsconsensus.aspx.
[2]See https://acc.dau.mil/CommunityBrowser.aspx?id=250180#definition.

About the Authors

Joe Doyle, a senior consultant at LMI, manages a variety of advice and assistance initiatives supporting research and development programs for DLA and the Defense Threat Reduction Agency. Dr. Doyle also teaches master's-level courses as an adjunct professor of business management.

Yasmin Virani is a consultant at LMI. She served on site at DLA assisting with the implementation of the Base Realignment and Closure Commission's supply and storage recommendations. Ms. Virani advises public-sector clients on supply chain management and on processes for ensuring product technical quality.

Program News

Topical Information on Standardization Programs

NATO Standardization Agency Plans Policy Update

The NATO Standardization Agency is slated to promulgate changes to the NATO policy for standardization and the directive for the production, maintenance, and management of NATO standardization documents (AAP-03J). The most notable changes in these policy and procedure documents are the updates to the principles, the integration of civil standards and intellectual property rights, the close linking of standardization agreements to interoperability requirements, the implementation of traceability between standardization documents and the initial requirements, and the introduction of a new standardization document type, the standardization recommendation. These policy documents will be available in ASSIST. For more information about the updates, please contact Latasha Beckman at 703-767-6872 or latasha.beckman@dla.mil.

Qualified Products Database Users Group Meets at Wright-Patterson Air Force Base, OH

The Air Force hosted a DSPO-sponsored qualified products database (QPD) users group session at Wright-Patterson Air Force Base, OH, on June 16, 2010. The event, attended by Air Force and Army qualification personnel employed in the region, focused on the QPD software updates that have been released over the past year. The event provided participants with a forum to ask questions and recommend potential enhancements. The database, which went live in 2006, is the official repository of qualified products and suppliers that meet technical requirements stipulated in specifications. To date, 90 percent of the 743 qualified products lists and qualified manufacturers lists have been converted from static paper documents to electronic files and published in the QPD. The use of qualified products or suppliers eliminates the need for first-article testing and thus can shorten acquisition lead-times and reduce costs. Attendees provided positive feedback and offered helpful suggestions.

GIDEP Announces an Interim Policy Change on Suspect Counterfeit Reporting

On September 15, 2010, the program manager of the Government-Industry Data Exchange Program (GIDEP) announced an interim policy change concerning reporting of suspect counterfeit parts and materials through GIDEP. Specifically, the interim policy change removes the requirement to name the supply source of suspected counterfeit parts or materials. The change is based on feedback from a number of government-industry committees and supported by data from recent Government Accountability Office and Department of Commerce reports indicating that far more companies and agencies have encountered counterfeits than were reported through GIDEP. When this information is withheld, the whole defense and industrial base community suffers.

For the next 3 months, GIDEP members will be able to report their suspected counterfeits through GIDEP without having to name their source of supply. If the change results in an increase in the number of organizations willing to report instances of suspected counterfeit parts or materials, the interim policy will be renewed on December 15, 2010. If the number does not increase, the interim policy will expire. The 3-month test will help the federal government develop sound and comprehensive federal policy concerning suspect counterfeit parts and materials reporting requirements. Follow this link to see the interim policy: http://www.gidep.org/mgmt/opmanual/gidep_interim_counterfeit_policy_change_15sep2010.pdf.

DSP Recognizes Achievements in Standardization

Annually, the DSP recognizes individuals and teams from the military departments and defense agencies who have achieved significant improvements in interoperability, cost reduction, quality, reliability, and readiness through standardization. Since 1987, DSP has recognized these outstanding performers in a formal ceremony. The ceremony recognizing the 2009 award winners was held on July 7 at the Pentagon's Hall of Heroes. Mr. Greg Saunders, Director, DSPO, officiated the ceremony with help from Mr. Stephen Welby, Director, Systems Engineering.

This year, for the first time, DSPO identified two individuals as being equally deserving of the Distinguished Achievement Award:

- Martin Snyder, for developing the world's first 24-volt military vehicle headlamp using only light-emitting diodes, significantly reducing the danger to our warfighters
- David Leight, for developing a specification for fiber optic connectors that can be used in hundreds of shipboard, submarine, and avionic military applications, greatly reducing the logistics footprint.

Mr. Snyder and Mr. Leight each received an engraved crystal Pentagon and a check for $5,000.

The remaining awards were presented to four teams:

- Army team from the Weapons and Materials Research Directorate, U.S. Army Research Laboratory, for overhauling three major armor steel specifications and developing two new specifications, ensuring that the Army is getting an adequate supply of high-quality armor steel produced by the most effective processing available
- Navy team from the NATO SEASPARROW Project Office, for creating a common set of test equipment that can be used by all missile testing facilities, resulting in a doubling of final test yields, a doubling of maximum surge capacity, and a 50 percent increase in steady-state throughput
- A team from the Navy Automatic Information Technology Program Office, Naval Supply Systems Command, for designing and implementing a passive radio frequency identification system to support receipt-and-issue transactions for the entire Navy Department
- A Navy team led by individuals from the Naval Surface Warfare Center, Carderock Division, and the Naval Sea Systems Command, for the simultaneous revision of five specifications affecting critical end-use submarine components—specifically, rubber gaskets, seals, and other rubber parts—identified by the Navy as being used in "SUBSAFE" applications.

2009 Distinguished Achievement Award Winners

Pictured above are, left to right, Mr. Martin Snyder and Mr. David Leight.

2009 Distinguished Achievement Award Winner

Light-Emitting Diodes Brighten the Warfighter's World

Pictured above are, left to right, Mr. Stephen Welby, Mr. Martin Snyder, Ms. Marta Tomkiw, Mr. Fred Krestik, Mr. Thomas Mathes, LTG James Pillsbury, and Mr. Ron Davis.

2009 Distinguished Achievement Award Winner

Standardized Fiber Optic Connectors Save Millions

Pictured above are, left to right, Mr. Stephen Welby, Mr. David Leight, Mr. Michael Radecki, Mr. Samuel Merritt, Mr. James Jobe, Mr. Bill Lee, and Ms. Christine Metz.

Achievement Award Winners

Warfighters Now Have More—and Better—Steel

Pictured above are, left to right, Mr. Stephen Welby, Mr. Richard Squillacioti, Mr. Kirk Stoffel, Mr. Matthew Burkins, Mr. William Gooch, Mr. Jonathan Montgomery, Mr. Ernest Chin, Mr. Jeffrey Zabinski, LTG James Pillsbury, and Mr. Ron Davis.

"Flex" Factory Improves Missile Production

Pictured above are, left to right, Mr. Stephen Welby, Mr. Donald Hoffman, Mr. John Pieti, Mr. Bruce Tuskey, CAPT Michael Anderson, CAPT Jerry Reid, and Mr. Scott White (Navy Departmental Standardization Officer).

Achievement Award Winners

Revolutionary pRFID System Improves Asset Visibility

Pictured above are, left to right, Mr. Stephen Welby, Mr. Robert Bacon, Mr. Douglas Verhagen; CAPT Jerry Reid, and Mr. Scott White (Navy Departmental Standardization Officer).

Improved Rubber Keeps Our Submarines Safer

Pictured above are, left to right, Mr. Stephen Welby, Mr. Mark Lattner, Mr. Forrest Pilgrim, Mr. Steve Lutgen, Mr. Roland Lemieux, Mr. Richard Dempsey, Mr. Edward Godfrey, Mr. Beau Brinckerhoff, Mr. John Lee, Mr. Robert DeNale, CAPT Jerry Reid, and Mr. Scott White (Navy Departmental Standardization Officer).

Mr. Greg Saunders officiated at the Defense Standardization Program Awards ceremony.

Mr. Stephen Welby, Director, Systems Engineering, also officiated at the ceremony.

Events

Upcoming Events and Information

August 14–18, 2011, Las Vegas, NV

60th Annual SES Conference

The 60th Annual SES Conference will be held at the Encore at Wynn, Las Vegas, NV. The conference theme will be "The Evolving World of Standards: What's on the Horizon?" The conference includes a welcome reception, keynote address, and 2 days of technical sessions. Two professional development courses will be offered for an additional cost. The keynote address and technical sessions will be broadcast live from the Encore on August 15 and 16, 2011, as a virtual conference. If you are not able to make it in person, plan to attend virtually. For more information, please go to the SES website at http://www.ses-standards.org.

August 29–September 1, 2011, Fort Lauderdale, FL

DMSMS and Standardization Conference

Mark your calendars now and plan to attend the 2011 Diminishing Manufacturing Sources and Material Shortages (DMSMS) and Standardization Conference at the Westin Diplomat Hotel in Hollywood, FL. 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 2011 website. For more information, please go to the DMSMS website at http://www.dmsms2011.com.

October 24–27, 2011, San Diego, CA

14th Annual Systems Engineering Conference

Mark your calendars now and plan to attend the 14th Annual Systems Engineering Conference, which will be held at the Hyatt Regency Mission Bay in San Diego, CA. Though details are still being worked out, prospective attendees are encouraged to check the conference website at http://www.ndia.org/meetings/2870/Pages/default.aspx for information as it becomes available.

People

People in the Standardization Community

Welcome

Chris Paquette, of the Naval Sea Systems Command (NAVSEA), was recently named Navy Departmental Standardization Officer (DepSO). Mr. Paquette has been with the Navy for more than 27 years. Currently, he is the deputy director for Technical Policy and Standards, where he leads the related value streams of technical authority, technical standards, systems engineering, and system safety for NAVSEA. Mr. Paquette has been serving as the Command Standardization Officer for NAVSEA since 2007.

James Dwyer, of the U.S. Army Materiel Command (AMC), is serving as Acting Army Standardization Executive. Mr. Dwyer is a retired Army Colonel with more than 27 years of military experience, specifically in combat logistics. He is now serving as the Deputy G-4 for Support Operations, Headquarters AMC.

Ramon Campos, of AMC, was recently named Army DepSO. Mr. Campos assumed the duties of chief of the Industrial Base Capabilities Division, Headquarters AMC, Deputy Chief of Staff G/4/7/9. Mr. Campos started his career with the government when he joined the Army in 1985. He comes to Headquarters AMC from the Theatre High Altitude Area Defense Launcher Product Office, where he served as the deputy product manager.

Farewell

Ron Davis has transferred to a new position with the U.S. Marine Corps. Previously, he served as Deputy G3 for Industrial Operations as well as the Army Standardization Executive.

Scott White, formerly with the Naval Air Systems Command, left for a job with industry. In his most recent position, Mr. White served as the Navy DepSO.

Defense Parts Management Portal–DPMP

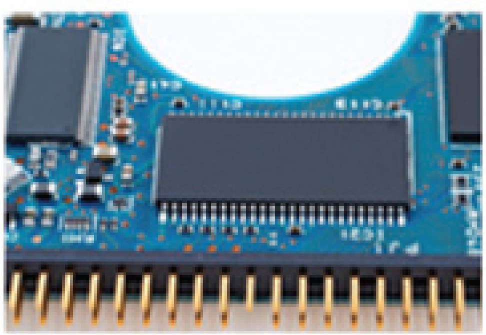
The DPMP is a new public website brought to you by the Parts Standardization and Management Committee (PSMC) to serve the defense parts management community.

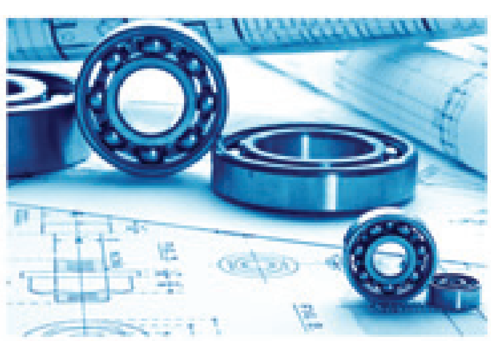
The DPMP is a new resource, a new marketplace, and a "one-stop shop" for parts management resources. It is a navigation tool, a communication and collaboration resource, and an information exchange. It gives you quick and easy access to the resources you need, saves you time and money, connects you to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





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 2011	Science and Technology
April/June 2011	Standardization Stars
July/September 2011	Materiel Readiness

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