Defense Standardization Program Journal

APRIL/JUNE 2016

Interoperability

The Case for Standards Interoperability

A Practitioner's Guide for Implementing DoD Parts Management

Building Obsolescence–Resistant Systems: How to Nip Obsolescence in the Bud

GIDEP—Mitigating a Risk to Interoperability

Defense Standardization Program Journal

Contents *April/June 2016*

1 Director's Forum

3 The Case for Standards Interoperability

11 A Practitioner's Guide for Implementing DoD Parts Management

16 Building Obsolescence–Resistant Systems: How to Nip Obsolescence in the Bud

21 GIDEP—Mitigating a Risk to Interoperability

Departments

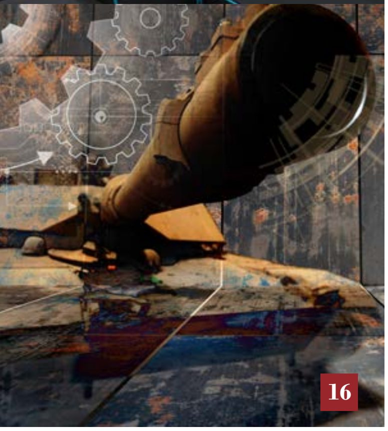
28 Program News

30 Events

32 People

3

11



16

The *DSP Journal* is available only in electronic form.

To receive issues, please subscribe at the DSP website, **www.dsp.dla.mil**, or e-mail DSP-Editor@DLA.mil and put "Subscribe" in the subject line.

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

Nicole Dumm
Editor, Defense Standardization Program Journal

Defense Standardization Program Office
8725 John J. Kingman Road, STOP 5100
Fort Belvoir, VA 22060-6220
703-767-6888
Fax 703-767-6876
dsp.dla.mil

Director's Forum

There is general agreement across the Department of Defense that standardization is a key enabler and multiplier of interoperability. Thanks to common standards, the services and allies and coalition partners of the United States are able to share ammunition, fuel, information, logistics support, and many other items and capabilities.

Somewhat ironically, an area where interoperability is sadly lacking is in the development and application of standards. A long-standing joke in the standards world is that there is no standardization in standards. This means that every standards developer, whether private sector or government, uses different processes and tools to create, maintain, and share standards, and they follow different formatting conventions. This creates significant challenges for organizations trying to share information and ensure that their design, manufacturing, and sustainment processes, as well as derivative works such as drawings, technical manuals, and other technical documentation, keep abreast of current versions of referenced standards, are consistent, and apply only the requirements needed for a particular application.

Often when people speak of interoperability, they talk about compliance to standards. But interoperability is not that simple. Standards typically have many options in them. How does a user necessarily know which options were selected, or even worse, which requirements in a standard may have been changed or waived? When a standard is changed, are we assured the item is backward compatible? And unfortunately, although parts and components may be marked as complying with a standard, in today's world counterfeit items abound, and the growing obsolescence issue just compounds this problem.

Gregory E. Saunders
Director
Defense Standardization Program Office

So what's being done to address these standards interoperability issues? Plenty. The National Information Standards Organization has an effort underway to standardize the identification and coding of information in standards across standards developing organizations (SDOs). The effect of this will be to make information interoperable without affecting each organization's formatting conventions. What is important is common definitions of content—whether referenced documents are called "referenced" or "associated" or some other term, the coding will identify them in the same way. From the “coded” document, a printed or machine-readable document (or table or drawing) can be produced in the user’s preferred format. There is also a new private/public-sector initiative called the Semantic Web for Interoperable Specifications and Standards that will transform standards into digital models and allow information to be fully and more easily integrated into design, manufacturing, and sustainment processes and to provide for cross-platform and SDO-independent interoperability. The Government-Industry Data Exchange Program is undergoing an information-sharing improvement that will help the department and defense suppliers better mitigate the interoperability risk posed by nonconforming, counterfeit, or obsolete parts.

These are exciting times, and at long last, the information revolution promises new tools to make the lives of standards developers and users even more productive, easier, seamless, and interoperable. Perhaps one day, we can put an end to the joke that there is no standardization in standards.

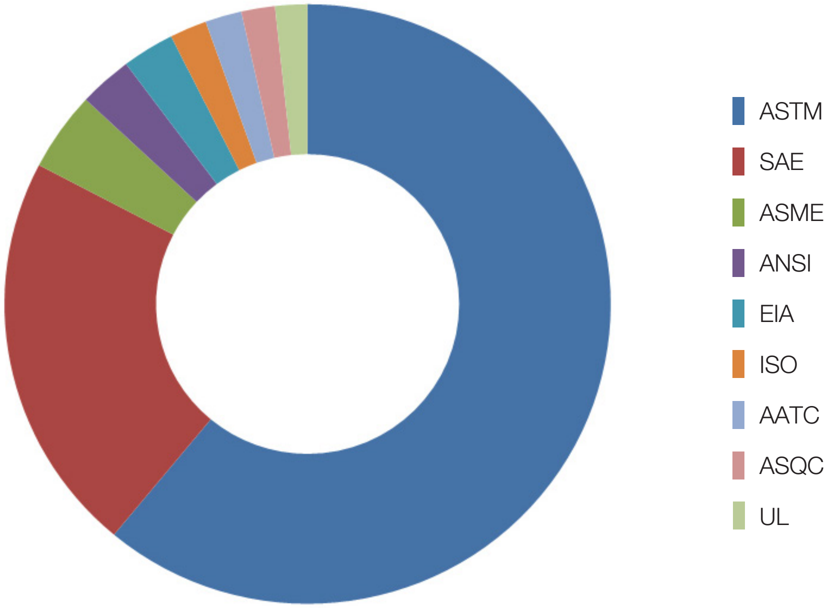
The Case for Standards Interoperability

By Rupert Hopkins, Robert Pokorny, and Andrew Bank

Specifications and standards define the parts, materials, and processes used in 80 percent of all traded products in the world.[1] DoD's Acquisition Streamlining and Standardization Information System (ASSIST) (https://assist.dla.mil) lists more than 100,000 documents including specifications, standards, and other technical requirements published by the U.S. government. There are 25,000 active specifications and standards in the ASSIST Library, and here's where it gets messy: 14,000 of these contain more than 85,000 references to other documents. While 60 percent of these references are to documents from government preparing activities, 40 percent refer to documents from more than 70 external standards-developing organizations (SDOs). And we haven't even mentioned the second-degree references yet: based on the average number of references per document and DoD's requirement to follow a reference for two degrees (or "hops"), we could expect those 85,000 references to refer to an additional 500,000 to 1 million documents. (For ASSIST-SDO references, see Figure 1.)

The lack of interoperability among this network of documents and among the millions of derivative documents that get created at the enterprise level (e.g., supplier specs, work instructions, requests for proposals [RFPs]) creates significant challenges for standards users to find the content they need, stay abreast of current versions, and apply the appropriate specs and standards to their particular application.

Figure 1. ASSIST-SDO References



[1] Organisation for Economic Co-operation and Development, https://www.oecd.org/tad/benefitlib/1955309.pdf.

The Problem with PDF

Standards are typically published by government preparing activities and SDOs as standalone PDF documents. Standards in PDF format were introduced around 1996 when most consumers were still buying plane tickets through travel agents. Since then, travel agents have nearly become extinct along with many newspapers, local bookstores, and land-line phones. But standards are still published and sold nearly the same way they were in 1996 despite their being used more than ever in complex and often digital enterprise processes and supply chains.

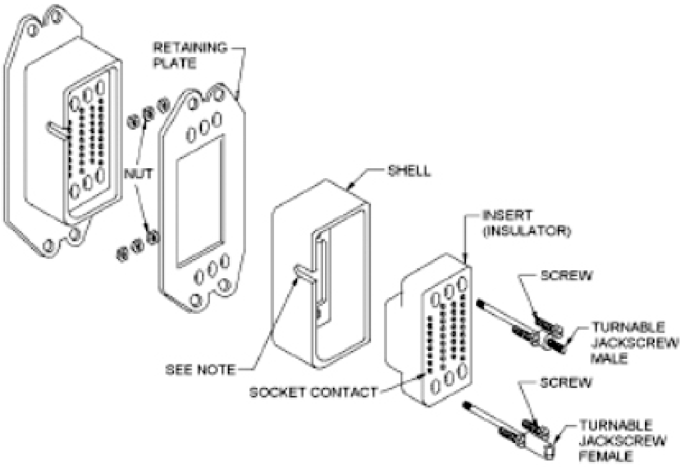
There are numerous shortcomings with standalone PDF documents or files that burden engineers and companies with enormous amounts of wasted time, unnecessary cost, potential risk, and, not least, frustration.

- Documents from one standards authority may reference another authority's standard, but the standards are not connected in any convenient, user-friendly way; that is, users are unable to click easily from one document to another. They are not interoperable.
- Standards are more important than ever in many enterprise processes and supply chains, but integrating standards content is extremely challenging and risky. For example, engineers use equations, images, computer-aided design (CAD) drawings, tables of numbers, references, and sections of text contained in standards to prescribe vital steps in their work instructions, RFPs, manufacturing software, product life-cycle management systems, and much more. Getting that information into these various derivative work products often requires re-keying by hand, copying and pasting, or recreating content—all of which takes time and introduces human error (i.e., risk).
- It is difficult for engineers to be aware of changes made to standards; furthermore, it is even more difficult to assess the impact of those changes on any derivative work products. When a standard is revised or its content is modified in a change notice, engineers have no way to know all the places where that standard's information has been used throughout their enterprise or supply chain.

What if documents behaved more like an Internet of things where smart, connected products are revolutionizing the way we live?[2] Emerging semantic technologies and cloud-based repositories can provide improved interoperability by enabling a concept in one document or application to “know” that it is connected to a concept in another document or application and to know why the connection exists. It also knows if the concept in the downstream document or application has changed at the source and can alert the user of the change. Using this approach, standards become interoperable, smart connected documents that can dramatically change the way engineering content is created and exchanged.

To illustrate the requirement for standards interoperability, let’s examine MIL-DTL-28748. This defense specification defines 58 characteristics for a family of rectangular connectors and is the source document for more than 2,000 National Stock Numbers (NSNs) found on 455 weapon systems (source: Weapon System Impact Tool, https://wsit.xsb.com). MIL-DTL-28748, like many specifications, is not a standalone document. There are 17 active supplementary slash sheets for this specification, each defining a particular subcategory of connectors. Just one of these slash sheets, MIL-DTL-28748/4F (see Figure 2), references 15 other documents, which in turn refer to another 66 documents. These references total more than 200 pages from different DoD and SDO sponsors, including ASTM International, SAE International, and ASME. But, an engineer tasked with managing a single component may only need a small collection of facts hidden within these 200 pages. In fact, most engineers don’t need or read entire standards documents; they need answers to specific questions contained in just a few pages.

Figure 2. MIL-DTL-28748/4F



[2] Michael E. Porter and James E. Heppelmann, “*How Smart Connected Products are Transforming Companies*,” Harvard Business Review, October 2015, https://hbr.org/2015/10/how-smart-connected-products-are-transforming-companies.

When a MIL document references a test method from an SDO industry standard, the user must leave ASSIST and go to another website, download the referenced document, and navigate to the appropriate section. Although finding and obtaining standards has become easier due to better search engines and aggregated collections, users still must expend time to gain access to the right standard and then more time to ***find the relevant information within the standard***. This time-consuming effort is repeated for each reference as an engineer creates the work product. Making this information interoperable by linking the concepts within and between documents from different authorities and enabling engineers to embed these links in their work can ***reduce engineering parts management time by as much as 20 percent***.[3]

Once a standard is acquired by an engineer, what does the engineer "hire" the specification to do? What job is he or she trying to accomplish beyond reading the document? According to the Outsell Survey of Engineering End-Users of Standards and Standards-Related Information,[4] the most common uses of engineering standards are as follows:

- Regulatory conformance
- Design
- Specification of materials or components
- Definition of tolerance or performance
- Drawing.

Each of these uses requires the engineer to read through the network of documents and then cut and paste or manually reenter content from these documents into various enterprise tools used to support these tasks. This process is often repeated by different entities (design, production, procurement, test, etc.) within an organization and by different enterprises in the product supply chain. Each manual entry takes an incremental amount of time (often duplicating what someone else has already done) and introduces an opportunity for error, but worse, it leaves the content disconnected from the authoritative sources, creating future configuration management challenges. If the authoritative information changes or is cancelled, awareness of that change does not automatically propagate to downstream users or applications. In other words, engineers take a snapshot of information during a moment in time, but as that information changes, the snapshot remains the same to everyone and everything that initially received it. Currently, there is no automated way of integrating standards-based content in such a way that downstream users or applications can be made aware that important information has been cancelled or changed.

[3] Anectdotal claims from interviews with OEMs as well as a test plan creation benchmark study by XSB, Inc.

[4] Jo McShea and James Erickson, Outsell, Inc., *Engineering End-Users of Standards and Standards-Related Information*, December 2014, https://www.outsellinc.com/search/d7entity/47908.

Standards interoperability should enable engineers to rapidly identify and integrate standards-based content with the tools and systems they use. This should work regardless of the standards author and be done with minimum manual rework, maximum accuracy, and traceability. Further, interoperability should enable the engineering end product (drawing notes, work instructions, test plans, etc.) to link directly back to specific concepts in the authoritative source. Those links should alert the using engineer of changes, take him or her directly to the "redline" for the changed concept, and allow the engineer to determine what steps, if any, need to be taken as a result of the change. In this way, engineering content is not just text, but evolves to become smart, connected documents.

- Concepts in smart, connected documents link directly to concepts in other documents regardless of author.
- Each concept is aware of why it is linked to another document (the link represents a relationship based upon the part, material, or process concept).
- Each concept "knows" its status and the status of the document concept it links to (e.g., current, modified, or cancelled).

Today, there are two initiatives aimed at evolving standards documents into smart, connected documents.

National Information Standards Organization (NISO).[5] Different SDOs have independently developed publishing standards governing the format of their documents. According to NISO, this variety in standards publishing makes interoperability between organizations difficult and increases integration costs. NISO is addressing this through a working group to create a standard for standards. This effort focuses on standardizing the format of standards documents across SDOs. It is based, in part, upon the open International Standardization Organization standards tag set (STS).[6]

Semantic Web for Interoperable Specifications and Standards (SWISS). The Defense Logistics Agency (DLA) Research and Development Program funded the development of an open standard and platform to convert product, material, and process specifications to interoperable, smart connected document models.[7] These models may be used to put together a combined, tailored, and complete part requirement that virtually includes precise concepts from the authoritative sources of referenced documents. These models may be exported into a standard MIL-STD-961 form to be read by people or they could be queried through programming interfaces

[5] National Information Standards Organization, http://www.niso.org/workrooms/sts/.

[6] International Standardization Organization STS, http://www.iso.org/schema/isosts/.

[7] This material is based, in part, on research sponsored by the Defense Logistics Agency, Ft. Belvoir, VA, and the DLA Office of Operations Research and Resource Analysis, under contract number SP4703-13-D-5801.

by other automated systems. SWISS is guided by a technical working group with 20 representatives from government agencies, original equipment manufacturers (OEMs), and SDOs.

The SWISS project is developing “standards as digital models” that cover the top 80 percent of downloaded DLA Land and Maritime specifications. The program is also working with major nongovernment SDOs to convert their relevant specifications, and with design-centric OEMs to better understand their design processes. Additionally, the SWISS project is creating infrastructure to identify whether changes in referenced documents affect product requirements.

The developers of SWISS are also working with OEMs and SDOs to convert their content into standards as digital models, enabling the information contained within the standards to be more easily integrated into enterprise processes and supply chains.

NISO STS and SWISS will enable engineers to link concepts in their engineering work products directly to the authoritative source for those concepts. The interoperability gained through these technologies will dramatically reduce engineering time to knowledge and make it possible to provide truly tailored, targeted, engineering content that integrates both external and internal standards, supporting the workflow of end-users much more efficiently and effectively.[8]

[8] Jo McShea, Outsell, Inc., *Standards: 2016 Market Size, Share, Forecast and Trends*, April 2016, https://www.outsellinc.com/search/d7entity/51630.

About the Authors

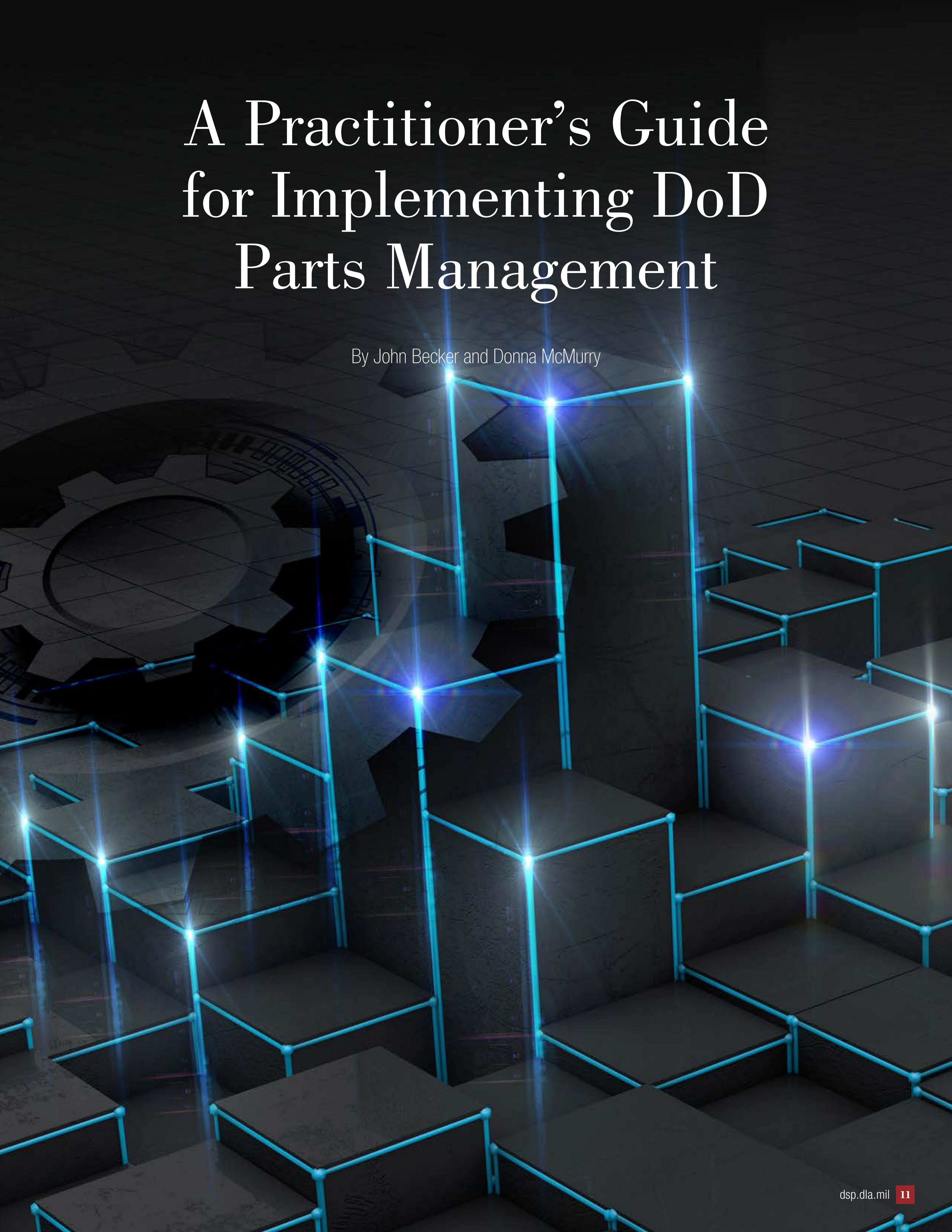
Rupert Hopkins is the founder of XSB. The company provides software and services for component product search, selection, management, and design. Its patented parts data management and semantic web-based solutions address the standardization problems and data inconsistencies commonly associated with integrating and managing large engineering product databases. Mr. Hopkins is co-inventor of the SWISS system.

Robert Pokorny has worked for XSB since the company was founded in 1998. He presently serves as XSB's software engineering manager, leading various development teams within the organization on projects focused on data aggregation and standardization. Dr. Pokorny draws on a wealth of experience in computer science and engineering to ensure the quality of the data produced by XSB's classification and extraction processes. He served as program manager for XSB on more than three dozen projects in support of DLA's logistics research and development effort. He also holds four U.S. patents and has published numerous technical papers on data quality.

Andrew Bank is an entrepreneur, growth strategy consultant, and co-founder of Techstreet, a digital standards aggregator. During his time at Techstreet, he pioneered PDF delivery, build-your-own subscriptions, and digital rights management for standards.

A Practitioner's Guide for Implementing DoD Parts Management

By John Becker and Donna McMurry



The DoD Parts Management Program is an integrated effort to streamline the selection of preferred or commonly used parts during the design of systems and equipment under an overarching systems engineering framework. The parts management process determines the optimum parts for an end item while considering all the factors that may affect program outcomes. Parts are the building blocks from which systems are created, and as such, they greatly impact hardware dependability and readiness. Because the reliability, maintainability, and supportability of the end item are dependent upon these building blocks, having an effective parts management program is an important contributor to defense readiness, while the nature of the process inherently provides cost savings and reduces inventory.

Parts Management Program Responsibility

The Defense Standardization Program Office (DSPO) is responsible for the DoD Parts Management Program. The DSPO has chartered the Parts Standardization and Management Committee (PSMC) to advise in the development of procedures and guidance related to parts management. The primary goal is to establish parts management best practices across DoD to increase system operational availability and reduce total ownership costs. The PSMC promotes effective parts management through information sharing between government and industry.

Standardization and Parts Management

Parts management is a mandatory standardization consideration, as stated in Department of Defense Manual 4120.24, “Defense Standardization Program Procedures,” dated September 24, 2014:

> Program offices must apply standardization processes to improve parts commonality, which may include cross program technical requirements and a business case analysis. Program offices should ensure that a parts management process is used to reduce the proliferation of parts and associated documentation and promote the use of parts with acceptable performance, quality, and reliability, as specified in MIL-STD-3018.

“MIL-STD-3018, Parts Management,” is a DoD standard practice document that provides requirements for the implementation of an effective Parts Management Program to support acquisition strategies and systems engineering practices. It provides performance-based parts management processes and practices that are intended to be adapted to individual program needs. The military standard and accompanying data item description (DID), “DI-SDMP-81748, Parts Management Plan,” are designed for placement on DoD contracts by acquisition program offices. “Standardization Document-19 (SD-19), Parts Management Guide,” provides additional information for defining and addressing parts management requirements in a contract.

Need for a Practitioner's Implementation Guide

Now that MIL-STD-3018 has been in use for several years, the PSMC has determined there is a need for more specific guidance to help defense industry practitioners understand how to create, document, and implement an effective parts management program in accordance with MIL-STD-3018. While many original equipment manufacturers (OEMs) have established effective parts management processes, by sharing information, others could benefit from their lessons learned, enabling standard practices. The PSMC formed an Implementation Subcommittee to develop a practitioner's implementation guide. The subcommittee has been gathering information from multiple defense providers on how they conduct their in-house parts management processes in compliance with MIL-STD-3018.

Specific Plans for the Practitioner's Guide

The primary goal of this effort is to develop and define "how to" procedures for defense industry practitioners to implement a viable parts management program that meets the requirements in MIL-STD-3018. The intention is to replicate best parts management practices across industry, not simply to reiterate the requirements included in MIL-STD-3018.

The approach of the Implementation Subcommittee involves three steps for each of the parts management elements defined in MIL-STD-3018:

- Define sample contract wording.
- Create sample processes and procedures. (Challenge: Manage differences between electrical and mechanical plans; also, detailed requirements for electrical component selection will not be addressed.)
- Implementation and checks and balances.

The procedures will address specific how-to elements, each one intended to provide a recommended generic practice for mechanical parts management.

Electronic Components Management Plan vs. Parts Management Plan

As previously noted, specific electronic component selection criteria will not be addressed in the guide, as those elements are typically embedded in each OEM's subtier processes. They include the following:

- Component application
- Component qualification

- Component quality assurance
- Component dependability
- Component compatibility with the equipment manufacturing process.

Following are the parts management elements that the selection guide will include.

Part selection baseline—parts selection list gives visibility to designers and subcontractors of the parts preferred for use.

Part selection and authorization—the management and organizational structure for standardization functions.

Obsolescence management—the plan must include procedures for obsolescence management, such as proactive obsolescence forecasting and mitigation for application part types.

Parts list or bill of materials—the plan must detail how and when the contractor submits initial and updated parts lists or bills of materials to the government, as required by contract.

Subcontractor management—the plan must describe contractor procedures for establishing and maintaining subcontractor participation to the extent necessary to ensure satisfaction of the parts management objectives.

Part and supplier quality—the plan must describe provisions for assessing part suppliers and part quality, such as statistical process control data, audits, and past performances.

Part-level documentation procedures—the documentation procedures must be detailed and consistent with the program's configuration management, logistics strategies, and total life-cycle requirements.

Substitute and alternate part procedure—the process for the management, definition, and documentation of substitute and alternate parts.

Replacement process—the contractor must ensure that the program is consistent with the intent and application of systems engineering disciplines (configuration management, quality, logistics, etc.).

Customer-contractor teaming—the parts management plan must address customer teaming to allow for continued insight into processes for program verification.

Counterfeit parts—address the detection, mitigation, and disposition of counterfeit parts, including electronic, electrical, and mechanical parts. SAE International's AS5553 should be used as guidance for electronic parts. AS6174 should be used as guidance for mechanical parts.

Lead-free electronic parts—the parts management plan must address the process to manage the risk associated with using lead-free parts. TechAmerica GEIA-STD-0005-1 may be used as guidance for lead-free electronic parts.

Additional elements—the process for addressing those additional elements, as identified by contract, must be defined.

While the Implementation Subcommittee has a ways to go before the Practitioner's Implementation Guide is published, here is an example of the type of requirement that may be included for contract wording.

EXAMPLE

The contractor shall establish and maintain a Parts Management Program in accordance with MIL-STD-3018 for all new designs or modified equipment. This program will ensure that the use of parts meets the contractual requirements, reduces proliferation of parts within and across DoD weapons systems and equipment through standardization, enhances reliability and supportability to meet material readiness objectives, and reduces total-life-cycle costs. Also, the contractor shall describe how the parts management process is validated, how process improvements are incorporated, and how process variation is controlled. The contractor shall document the plan in accordance with Data Item Description DI-SDMP-81748 and deliver the plan in accordance with the Contract Data Requirements List (DD Form 1423).

Summary

A mandatory standardization consideration, parts management is an effort to select preferred parts during the design of weapon systems and equipment to enhance standardization, reliability, and supportability and reduce total ownership costs. MIL-STD-3018 and its accompanying DID provide a contractual tool that delineates parts management requirements. SD-19 offers helpful guidance for defining and addressing parts management in acquisition contracts. The parts management implementation guide for practitioners being developed now is intended to clarify and share effective processes of applying MIL-STD-3018 requirements to implement a company's parts management program. Once the guide is completed, the PSMC's Implementation Subcommittee plans to make it available online for the benefit of all interested parts management practitioners.

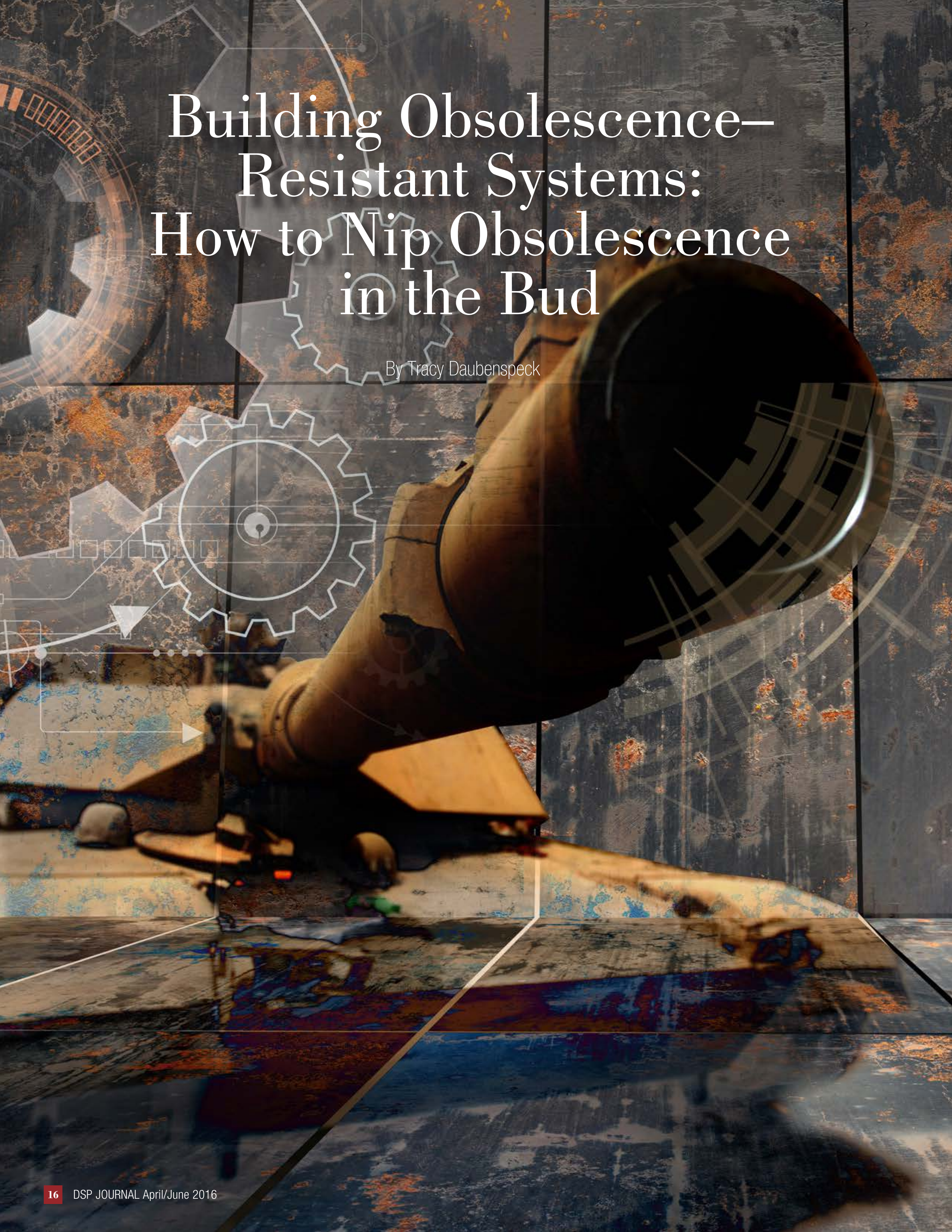
About the Authors

John Becker is working at United Technologies Aerospace Systems as engineering support for corporate commodity teams. He is also currently supporting a corporate-wide effort in mechanical parts standardization and has been actively involved in the PSMC since the mid 1990s. Mr. Becker has an extensive background in component engineering, engineering standards, quality engineering, and supplier quality.

Donna McMurry is a member of the DSPO staff. She serves as the program manager for DoD parts management and has 35 years of defense acquisition, logistics, and standardization experience.

Building Obsolescence–Resistant Systems: How to Nip Obsolescence in the Bud

By Tracy Daubenspeck



Nearly everything is subject to obsolescence. Companies go out of business or change product lines, technologies evolve over time and old technologies are abandoned, materials are phased out due to regulations or because of improvements; the list goes on. Military systems are subject to obsolescence and because they typically have long life cycles and particularly long acquisition periods, the problem is often exacerbated. Diminishing Manufacturing Sources and Material Shortages (DMSMS) management is a multidisciplinary process to identify issues resulting from obsolescence, loss of manufacturing sources, or material shortages; to assess the potential for negative impacts on schedule and/or readiness; to analyze potential mitigation strategies; and then to implement the most cost-effective strategy.[1] Because conventional wisdom tells us that 70 percent of the total life-cycle cost of a system is in the sustainment phase, and because those costs are essentially locked in during the design phase,[2] it makes sense to apply the principles of DMSMS management during the design phase to ensure that the most obsolescence-resistant products are used in the design and to continue to reinforce that strategy as the system is built, delivered, sustained, and upgraded.

As stated above, DMSMS management is a multidisciplinary process and is typically handled by an integrated process team often referred to as the DMSMS Management Team (DMT). The composition of the DMT may vary as a system progresses through the life cycle but a typical team is composed of members from engineering, logistics, and supply, technicians, the prime contractor, DMSMS specialists, and, potentially, ad hoc members from other groups such as contracting or legal. Early in the life cycle, when designs are being vetted for use in a system, there are three key activities. The first is to establish a DMT, its associated processes, and a DMSMS management plan. The second is to get DMSMS management requirements in contracts. The last is to evaluate design proposals to ensure that the designs will be as DMSMS resistant as possible. “SD-22, DMSMS: A Guidebook of Best Practices for Implementing a Robust DMSMS Management Program” covers all three of these topics; we will focus on the last two.

The importance of good contract language cannot be overstated. In my experience working with more than 70 different programs during the past 10 years, one of the biggest problems facing DMSMS managers is in the area of contracts. Many contracts make no

[1] Defense Standardization Program Office, “SD-22, Diminishing Manufacturing Sources and Material Shortages (DMSMS): A Guidebook of Best Practices for Implementing a Robust DMSMS Management Program,” 2016, https://acc.dau.mil/CommunityBrowser.aspx?id=46237.

[2] Capt. Gary Jones, Lt. Col. Edward White, and Lt. Col. Jonathan D. Ritschel, “Investigation into the Ratio of Operating and Support Costs to Life-Cycle Costs for DoD Weapon Systems,” Defense Acquisition Research Journal, January 2014, http://dau.dodlive.mil/2014/01/01/investigation-into-the-ratio-of-operating-and-support-costs-to-life-cycle-costs-for-dod-weapon-systems.

mention of DMSMS management. Many more have vague references that often result in limited or no action on the part of suppliers. Good DMSMS contract language has several key elements: responsibility for DMSMS management is spelled out, DMSMS management requirements are flowed down to subtier suppliers, and DMSMS data requirements are detailed. Getting this language in place ensures that DMSMS is considered and managed during designs and that subtier suppliers are engaged as well. In addition to "SD-22, SD-19 Parts Management Guide," and "MIL-STD-3018 Parts Management," contain information pertinent to DMSMS contract language. A Navy memo from the Assistant Secretary of the Navy (Research, Development and Acquisition) dated May 12, 2006, and titled "DMSMS Guidance for Developing Contractual Requirements," also has good content. While in the ideal, DMSMS contract language is in place from day 1, it is never too late to get proper contractual language in place.

Key considerations for DMSMS management activities during design include standards-based designs, open architecture, the use of newer but mature technologies, the selection of parts with multiple suppliers, and considering the health of the supply chain. The first three activities listed fall into the realm of engineers and technicians with experience in the technical area being evaluated, while the last two are most typically handled by logisticians.

There are many types of standards to consider, including international standards, industry standards, and government standards, each with their own strengths and weaknesses. The important thing with standards, with regards to DMSMS, is to select the one that will give the system the most benefits in terms of a long life cycle and availability of parts. A good example is the PCI Express serial computer expansion bus standard. This standard was formalized in 2004 and has continued to be maintained and upgraded. The latest version, 4.0, is scheduled to be published in 2017. This standard has maintained a great deal of backwards compatibility over the years while increasing speed by a factor of 4 and throughput by a factor of 7.[3] In computer hardware terms, this is a very durable standard and is probably still a good choice for future designs.

Open architecture, similar to standards, is a design method that uses interfaces that have defined interconnections and communication protocols. Any device that is similarly designed should fit appropriately and be able to "talk" with the other devices in the system. Open architecture applies to both software and hardware. In open architecture software, software modules in an application or the application itself have documented interfaces that allow other developers to design modules that "bolt on" and work correctly.

There appears to be a tendency among designers to use familiar products in their designs. While this is no doubt more efficient, it is not always the best choice when developing a system expected to last decades. Most products fall into a predictable life-cycle curve starting with

[3] Wikipedia article, "PCI Express," 2016, https://en.wikipedia.org/wiki/PCI_Express.

introduction, progressing through market acceptance, and ending in discontinuance. In a perfect world, system designers would select long life-cycle parts that have just passed the market acceptance point in their cycle.

HOW NOT TO USE STANDARDS

Many years ago, while working as the lead of a circuit card manufacturing shop, I worked on a project to build some first article cards for testing. The production run went fine and the cards were ready for in-house testing when the project was stopped. When I investigated to determine the cause of the stop in production, I was told that the designer of the card had used an early version of the PCMCIA memory cards in the design and that the memory cards were no longer available. The PCMCIA standard was well established at the time that these cards were designed and built, and the replacement product met the specifications of the standard. However, the designer had used a feature of the memory card that was not part of the standard. The new memory cards did not have this feature and it rendered the circuit cards unusable. The entire run had to be scrapped and months passed before a new design was finalized and new circuit cards were delivered.

–Tracy Daubenspeck

Vendor and supply chain health considerations should also be examined for each part being evaluated. This evaluation is risk based with criticality, cost, and lead time of a part being one set of considerations and the health of the supply chain being another. If the part is only available from a single vendor, is a special order part, or contains exotic materials, the health of the company and its supply chain are very important. If the part is a commercial off-the-shelf item available from several vendors, the health of a given supplier may not be so important. When selecting a part that is high risk, it is often a good idea to document approaches to mitigate that risk, for instance, buying the technical data package and/or the rights to the manufacturing process, or considering a contractual option to obtain those data rights and/or technical data package once a company is ready to discontinue support.

As long life-cycle systems are typically upgraded periodically during their life, the actions detailed above should be used during the design phase of the upgrades as well. In addition, a database that keeps track of all parts used in a system, the rationale for their selection, and information related to their expected life cycle is an invaluable tool to aid in future obsolescence mitigation activities.

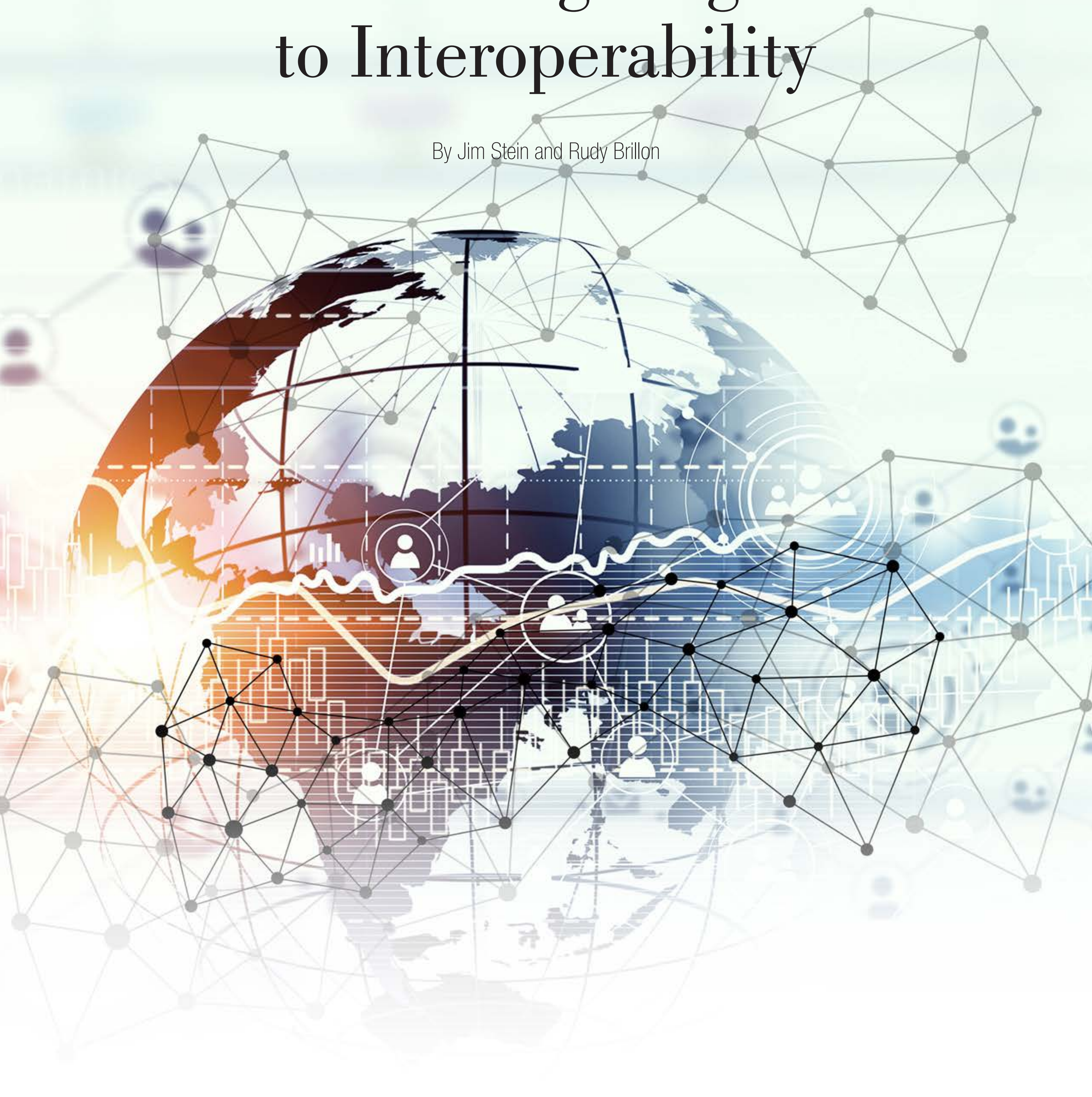
I have focused this article on ways to avoid obsolescence problems later in the life cycle by designing obsolescence-resistant systems and ensuring that sound suppliers are used. However, no amount of effort in the design phase can ward off obsolescence for the entire life of a typical military system. A good, proactive DMSMS program and an effective DMT will discover and handle most obsolescence well in advance of an impact from that obsolescence and before options like last-time procurements run out, avoiding redesigns where possible and allowing for planned redesigns or technology refreshes when not. DMSMS management practices have a proven track record for avoiding unnecessary redesign costs and schedule delays and ensuring that obsolescence issues are not the cause of availability problems.

About the Author

Tracy Daubenspeck is a technical project manager for the Obsolescence Management Division at Naval Undersea Warfare Center in Keyport, WA. In that capacity, he manages the execution of obsolescence management projects in the division. Mr. Daubenspeck is a co-chair of the DoD DMSMS Working Group's Problem and Solution Committee and an active participant in both the Navy's and NAVSEA's DMSMS working groups, where he works to develop DMSMS management best practices. He was a major contributor to the revised SD-22 DoD DMSMS Guidebook that was published in 2012 and revised in 2015 and 2016. He worked with the DoD DMSMS community and the Department of Commerce to develop a DMSMS cost metrics survey that was conducted in 2014. The results of that survey were published in early 2015.

GIDEP—Mitigating a Risk to Interoperability

By Jim Stein and Rudy Brillon



Interoperability, as defined by DoD policy, is the ability of systems, units, or forces to provide data, information, materiel, and services to, and accept the same from, other systems, units, or forces; and to use the data, information, materiel, and services so exchanged to enable them to operate effectively together.

Standardization facilitates interoperability. Using the same parts and materials allows for interchangeability. Using common commercial parts and materials allows for reducing costs while enabling interoperability. However, using a common set of commercial parts and materials introduces the risk of a single nonconforming part or material affecting multiple systems. This risk becomes even greater when the threat of counterfeit is introduced.

In 2007, the Naval Air Systems Command (NAVAIR) asked the Department of Commerce (DOC) to conduct a defense industrial base assessment of counterfeit electronics. This request was motivated by NAVAIR's suspicion of an increasing number of counterfeit electronics infiltrating the DoD supply chain. In January 2010, DOC published its findings in ***Defense Industrial Base Assessment: Counterfeit Electronics***.[1] On the basis of interviews with major segments of the U.S. supply chain, DOC found that "39 percent of companies and organizations participating in the survey encountered counterfeit electronics" and that there had been "an increasing number of counterfeit incidents being detected, rising from 3,868 in 2005 to 9,356 incidents in 2008."

Subsequent independent studies identified electronic parts—in the DoD supply chain and used in the development of multiple DoD systems—as counterfeit.

What Can Be Done?

The DOC, in its report, went on to provide general findings and recommendations on how the U.S. government could "inhibit the circulation of counterfeit electronics." Two of those recommendations were (1) "report all suspect and confirmed counterfeit components to federal authorities and industry associations" and (2) "consider establishing a centralized federal reporting mechanism for collecting information on suspected and confirmed counterfeit parts for use by industry and all federal agencies."

So, to help mitigate this risk, there is a need for system designers, developers, operators, and maintainers to be able to share their experiences so that others can benefit from their lessons learned.

[1] Botwin et al., *Defense Industrial Base Assessment: Counterfeit Electronics*, U.S. Department of Commerce Bureau of Industry and Security Office of Technology Evaluation, January 2010.

How Information Sharing Has Proven Effective in the Past

The concept of information sharing is one that was recognized back in the late 1950s by the U.S. Army, Air Force, and Navy. Engaged in similar assessments in support of the Ballistic Missile Program, the services realized that through information sharing they would be able to reduce duplicate testing being conducted on the same parts, components, and materials. Thus was born the concept of establishing a government program to facilitate the sharing of information between government and its industry partners to increase systems' safety, reliability, and readiness while reducing development, production, and ownership costs. By 1970, this concept had grown into the Government-Industry Data Exchange Program, or GIDEP. Through the years that followed, GIDEP continued to expand its membership to include the National Aeronautics and Space Administration, the Canadian Department of National Defence, and the Department of Energy, as well as many other federal agencies and industry partners. GIDEP also continued to expand its roles and responsibilities. In 1991, it received the designation as the federal government's repository for information concerning nonconforming products and materials (Office of Federal Procurement Policy Letter 91-3), and in 1995 it was designated the DoD obsolescence information repository for Diminishing Manufacturing Sources and Material Shortages (DMSMS).

GIDEP Today

Today, GIDEP is a DoD program, managed by the Defense Standardization Program Office, that serves all U.S. government, the Canadian Department of National Defence, the Canadian Space Agency, and their industry partners. GIDEP provides its membership with a web-accessible database for the exchange of a variety of data. Relevant to this discussion are the three data types known as failure experience, suspect counterfeit, and DMSMS.

- **Failure experience data** provides information regarding nonconforming parts and materials discovered during the design, test, integration, manufacture, and support of government and industry systems. A nonconforming part is a part that does not meet the technical requirements of the contract or advertised characteristics. Failure experience reports (known as alerts, safe alerts, problem advisories, agency action notices, and lessons learned) inform the GIDEP members that a problem exists and help prevent the use of the problem parts and materials. This information assists GIDEP information users in improving the availability, reliability, maintainability, quality, and safety of their systems and equipment. The use of failure experience data has resulted in significant cost avoidance and, more importantly, has prevented injuries and saved lives.

- **Suspect counterfeit data** contains information on suspect counterfeit parts and materials. GIDEP members provide fact-based reports on items that, after having undergone inspection and, in many cases, extensive testing and analysis, are suspected to be counterfeit. Because counterfeit parts jeopardize the integrity of a system, these reports are important to GIDEP members as the knowledge allows them to actively screen their inventories for these items. These reports also help to prevent the recirculation of counterfeit parts back into the supply chain.
- **DMSMS data notices** are generated when a part manufacturer announces that a part or a production line will be discontinued. This information is frequently augmented with value-added cross-reference data, and then it is stored in GIDEP. The majority of GIDEP DMSMS notices have been issued on piece parts, especially in the electronics area (primarily microcircuits); however, DMSMS notices are also released at the module, component, equipment, or other system indenture level. There is also a great deal of discontinued part information on non-electronic types of commodities such as fasteners, software, valves, and filters. The GIDEP database contains information on parts manufactured in accordance with military or government specifications and commercial parts. GIDEP DMSMS information assists users in implementing their obsolescence management programs.

The use of the same nonconforming, counterfeit, or obsolete parts in multiple systems adds to the risk to interoperability. The use of GIDEP data helps to mitigate this risk. However, even though GIDEP has proven to be a successful tool for its members, there is room for improvement.

In March 2010, the Senate Armed Services Committee (SASC) announced its investigation into the issue of counterfeit parts in the DoD supply chain. At the conclusion of this investigation, the SASC conducted a hearing on November 8, 2011, to refine its understanding of its findings. One finding, germane to this discussion, was the following:

> Another place where the defense industry is coming up short is in reporting cases of counterfeit parts. Our investigation uncovered approximately 1,800 cases where parts suspected to be counterfeits have been identified by companies in the defense supply chain. However, the vast majority of those cases appear to have gone unreported to the Department of Defense or criminal authorities. In addition, too few contractors and distributors consistently file reports with the Government Industry Data Exchange Program (GIDEP). … That has to change. Failing to report suspect counterfeits and suspect suppliers puts everyone at risk. We need to make sure our regulations require contractors who discover suspected counterfeit parts in a military system to report that discovery to the military right away. We should also require DoD and contractors to report cases of suspected counterfeits found in the supply chain into GIDEP, so that others are alerted.[2]

As part of its response to the SASC findings, DoD published its Counterfeit Prevention Policy in April 2013, which included the following direction regarding the reporting of counterfeits:

[2] Carl Levin, "Opening Statement at SASC Hearing on Counterfeit Electronic Parts in DoD Supply Chain," November 8, 2011.

> Document all occurrences of suspect and confirmed counterfeit materiel in the appropriate reporting systems including the Government-Industry Data Exchange Program (GIDEP).[3]

GIDEP can only share the information that is being submitted. Even though the program, processes, and system are in place to meet the challenge, GIDEP is not being fully utilized.

GIDEP Tomorrow

Due to the criticality of this information, new DoD and federal regulations have been and are being put in place requiring government and industry to screen GIDEP information and to report discoveries of nonconforming parts and materials and suspect counterfeits to GIDEP. It is anticipated that the implementation of these regulations will result in significant increases in GIDEP membership and information exchange.

The need to share this information extends beyond the borders of the United States and Canada. With the globalization of the supply chain, it is not uncommon to find U.S. and Canadian industry partners having to turn to companies in other countries for support. Under GIDEP's current information distribution policy, GIDEP information cannot be shared with these organizations. This is due to the fact that some of the information contained in GIDEP reports may be subject to the International Traffic in Arms Regulations and the Export Administration Regulations export restrictions and the fact that GIDEP members have shared their information with the understanding that it would be kept within the GIDEP community. New processes and methods of sharing information will be required in order to adhere to these regulations while meeting the expectations of the GIDEP community.

GIDEP is in the process of "modernizing" its policies, procedures, and information technologies to better meet these demands.

[3] DoDI 4140.67, A.2, "DoD Counterfeit Prevention Policy."

Conclusion

As can be seen by the above, GIDEP provides a valuable forum for system designers, developers, operators, and maintainers to be able to share their experiences so that others can benefit from their lessons learned. Their active participation in GIDEP helps mitigate this risk to interoperability.

HOW CAN YOU HELP?

Join GIDEP! Become a member of the team. Membership is free. Simply access www.gidep.org/join/requirements.htm and submit your application today. By becoming a member, you will become part of the community that is tackling these critical issues. By submitting your data, others will benefit from your experiences, and by downloading their data, you will benefit from theirs. It is through this interactive sharing of information by people like you that GIDEP will be able to help protect the benefits of interoperability while helping to mitigate the risk!

About the Authors

Jim Stein is the GIDEP program manager. He has 32 years of experience in the federal government in logistics, engineering, and program management.

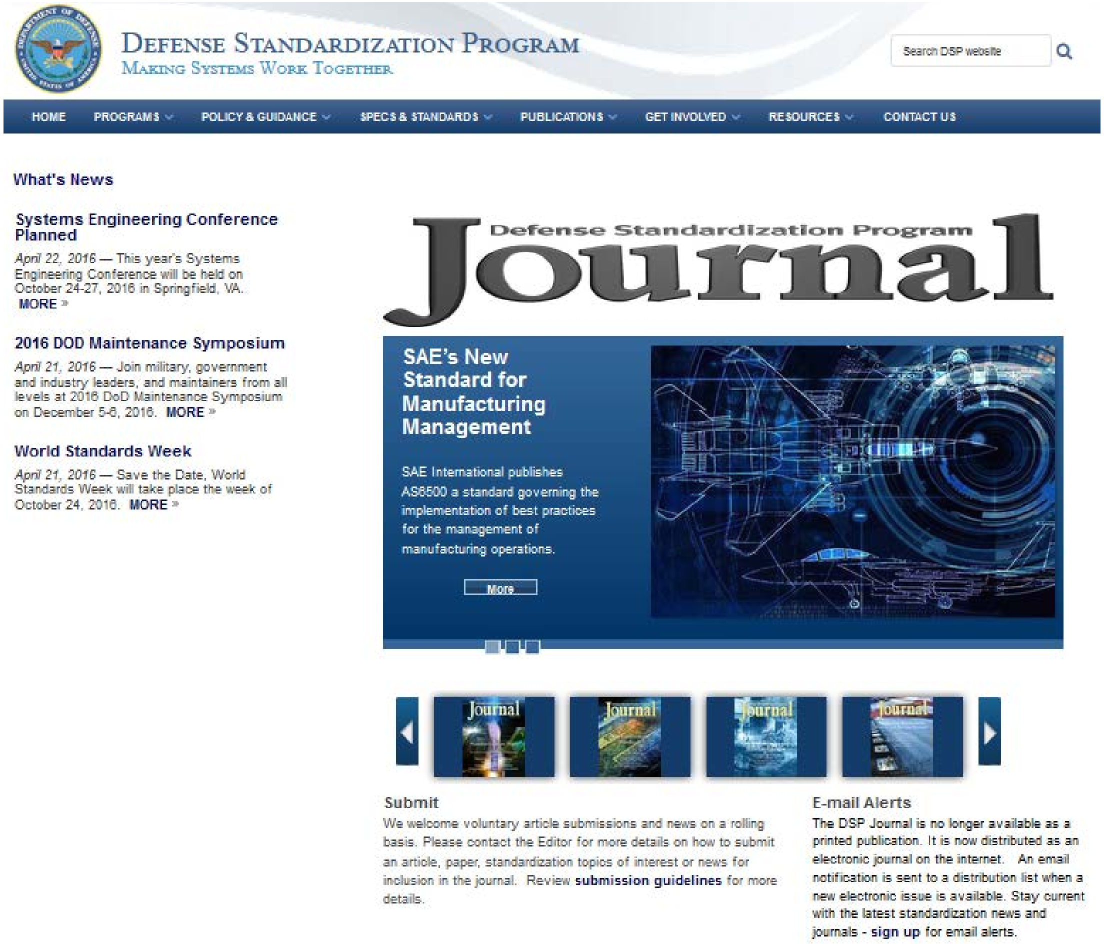
Rudy Brillon is the GIDEP Operations Center director. With a background in information technology, he has spent the past 31 years developing, implementing, operating, and maintaining information systems in support of DoD maintenance, configuration, logistics, ordnance, and metrology management.

Program News

Topical Information on Standardization Programs

Check Out Our New Website

The new and improved Defense Standardization Program Office (DSPO) website made its debut on May 27, 2016. The website began to gradually migrate to the AFPIMS (American Forces Public Information Management System) web platform in January 2016 and was led by dedicated DSPO team members LaTasha Beckman, Stephen Lowell, and Joseph Delorie. DSPO program managers have been trained to maintain their programs' areas of the website.



What's News

Systems Engineering Conference Planned

April 22, 2016 — This year's Systems Engineering Conference will be held on October 24-27, 2016 in Springfield, VA. **MORE** »

2016 DOD Maintenance Symposium

April 21, 2016 — Join military, government and industry leaders, and maintainers from all levels at 2016 DoD Maintenance Symposium on December 5-6, 2016. **MORE** »

World Standards Week

April 21, 2016 — Save the Date, World Standards Week will take place the week of October 24, 2016. **MORE** »

SAE's New Standard for Manufacturing Management

SAE International publishes AS6500 a standard governing the implementation of best practices for the management of manufacturing operations.

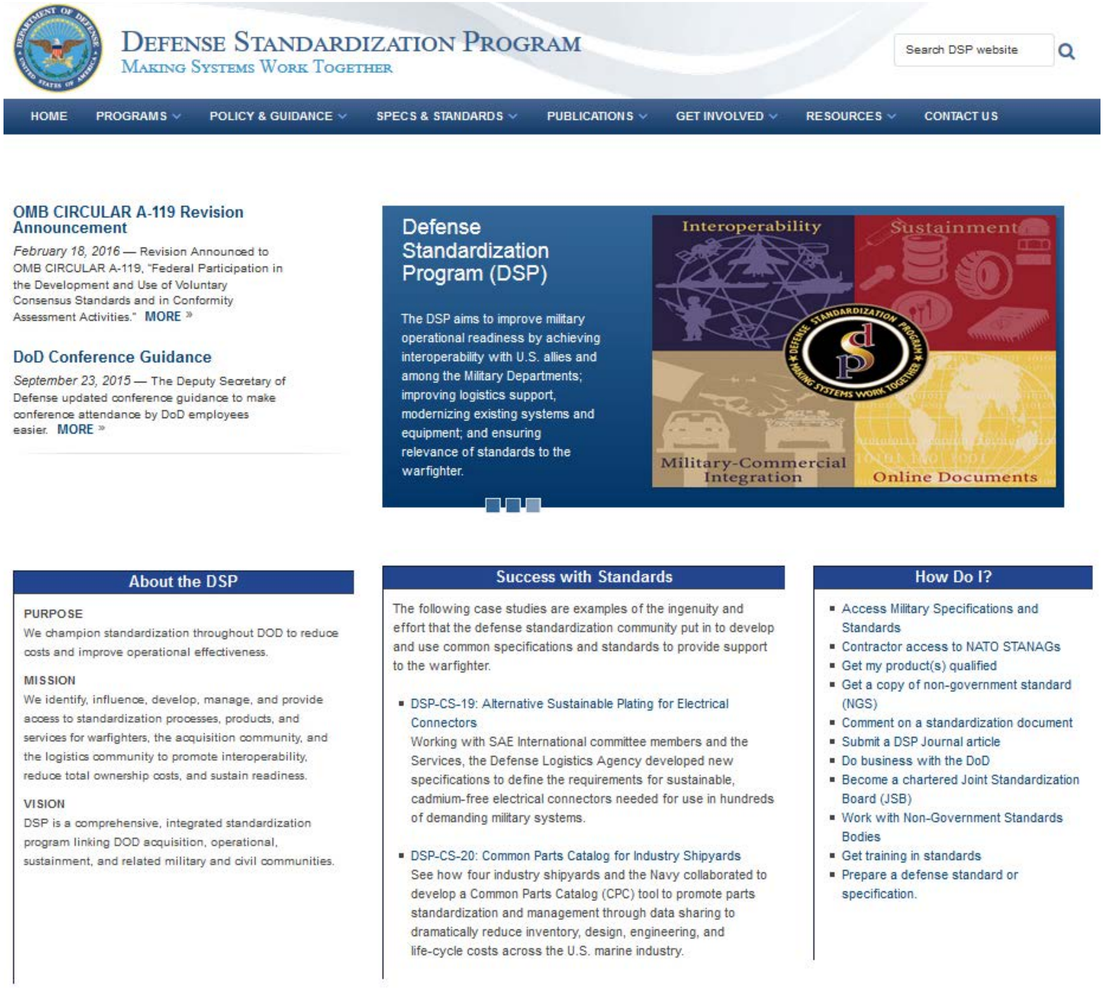
Submit

We welcome voluntary article submissions and news on a rolling basis. Please contact the Editor for more details on how to submit an article, paper, standardization topics of interest or news for inclusion in the journal. Review **submission guidelines** for more details.

E-mail Alerts

The DSP Journal is no longer available as a printed publication. It is now distributed as an electronic journal on the internet. An email notification is sent to a distribution list when a new electronic issue is available. Stay current with the latest standardization news and journals - **sign up** for email alerts.

The website features a fresh, modernized layout with user-friendly navigation links. The home page displays featured news from the standardization community as well as a “How Do I?” section for frequently visited topics. Current and previous ***DSP Journal*** issues can be found under the “Publications” tab.



OMB CIRCULAR A-119 Revision Announcement

February 18, 2016 — Revision Announced to OMB CIRCULAR A-119, “Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities.” MORE »

DoD Conference Guidance

September 23, 2015 — The Deputy Secretary of Defense updated conference guidance to make conference attendance by DoD employees easier. MORE »

Defense Standardization Program (DSP)

The DSP aims to improve military operational readiness by achieving interoperability with U.S. allies and among the Military Departments; improving logistics support, modernizing existing systems and equipment; and ensuring relevance of standards to the warfighter.

About the DSP

PURPOSE

We champion standardization throughout DOD to reduce costs and improve operational effectiveness.

MISSION

We identify, influence, develop, manage, and provide access to standardization processes, products, and services for warfighters, the acquisition community, and the logistics community to promote interoperability, reduce total ownership costs, and sustain readiness.

VISION

DSP is a comprehensive, integrated standardization program linking DOD acquisition, operational, sustainment, and related military and civil communities.

Success with Standards

The following case studies are examples of the ingenuity and effort that the defense standardization community put in to develop and use common specifications and standards to provide support to the warfighter.

- DSP-CS-19: Alternative Sustainable Plating for Electrical Connectors
  Working with SAE International committee members and the Services, the Defense Logistics Agency developed new specifications to define the requirements for sustainable, cadmium-free electrical connectors needed for use in hundreds of demanding military systems.
- DSP-CS-20: Common Parts Catalog for Industry Shipyards
  See how four industry shipyards and the Navy collaborated to develop a Common Parts Catalog (CPC) tool to promote parts standardization and management through data sharing to dramatically reduce inventory, design, engineering, and life-cycle costs across the U.S. marine industry.

How Do I?

- Access Military Specifications and Standards
- Contractor access to NATO STANAGs
- Get my product(s) qualified
- Get a copy of non-government standard (NGS)
- Comment on a standardization document
- Submit a DSP Journal article
- Do business with the DoD
- Become a chartered Joint Standardization Board (JSB)
- Work with Non-Government Standards Bodies
- Get training in standards
- Prepare a defense standard or specification.

Please visit the new website at http://www.dsp.dla.mil.

Events

Upcoming Events and Information

October 24–28, 2016, Washington, DC
World Standards Week

World Standards Week will take place October 24–28 at several locations in Washington, DC. This is an annual event where members of the standards and conformity assessment community come together in the spirit of cooperation and collaboration. A comprehensive week of both meetings and events has been planned and this is a must attend for all standards professionals. For more information and event updates and locations, go to http://www.ansi.org/wsweek.

October 27, 2016, Washington, DC
World Standards Day Celebration

The World Standards Day Celebration (exhibition, reception, and banquet) will take place Thursday, October 27, at the Fairmont Hotel in Washington, DC. The U.S. Celebration of World Standards Day is an event that recognizes the critical role of various stakeholders across the standards community, including business leaders, industry, academia, and government. Aside from the exhibition and reception, the event will include the presentation of the 2016 Ronald H. Brown Standards Leadership Award, which is named after the late U.S. Secretary of Commerce and honors an individual who has effectively promoted standardization as a key tool in the elimination of global trade barriers. The winners of the 2016 World Standards Day Paper Competition will also be announced. For more information on this event, go to https://www.ansi.org/meetings_events/wsw16/wsd.aspx.

November 1–3, 2016, Torrance, CA
PSMC Fall 2016 Meeting

The Parts Standardization and Management Committee (PSMC) will hold its fall 2016 meeting at Honeywell in Torrance, CA. Primary topic areas to be addressed include parts management contracts, procedures, and guidance; counterfeit parts and risk mitigation; and parts management tools and data. Attendance is open only to PSMC participants. If you are interested in becoming a PSMC participant, please contact Donna McMurry at Donna.McMurry@dla.mil or 703-767-6874.

November 28–December 1, 2016, Denver, CO
DMSMS 2016

The 2016 Diminishing Manufacturing Sources and Material Shortages Conference will be conducted simultaneously with the Defense Manufacturing Conference, joining together their exhibitions to bring participants a diverse knowledge base in the manufacturing world and more networking opportunities, all in one location. While each conference will have its own unique agenda, focus its program to its specific conference audience, and

Events

Upcoming Events and Information

have a separate registration procedure to attend, one registration fee will give access to both conferences. DMSMS 2016 registration is open to defense industry, military, and government personnel. See http://www.dmsmsmeeting.com/pages/registration.html#.

December 5–8, 2016, Albuquerque, NM

2016 DoD Maintenance Symposium

The mission of the 2016 DoD Maintenance Symposium is to create an environment that enables attendees to share relevant information, identify critical issues, discuss key topics, and increase their awareness of Department of Defense maintenance initiatives. Join military, government, and industry leaders and maintainers from all levels at this distinctive, first-class event—the maintenance community's primary venue for networking and content sharing. For more information or registration details, go to http://www.sae.org/events/dod.

People

People in the Standardization Community

Hails

After 27 years as a U.S. Marine, **Paul D'Antonio** joined Headquarters Air Force (HAF) for Planning and Force Posture Issues Worldwide. As a Marine helicopter pilot, he was deployed to the four corners of the earth flying off ships, in the jungles, and especially in the desert. As a senior officer, he was on the United States European Command staff and Joint Force Command Naples as a planner. As a North Atlantic Treaty Organization (NATO) officer, he gained a great appreciation for his allied partners, and he desired greatly to continue that relationship into a retired civilian job. On HAF, he handled U.S. Air Force NATO policy for 6 years. He is excited to be the U.S. air standardization representative and to continue to work in and around NATO.

Farewells

Robert Bamberg is stepping down as chief of the U.S. Air Force International Standardization Office after 7 years. During his time as the chief, he oversaw the coordination and implementation of international agreements (NATO standardization agreements and Air and Space Interoperability Council air standards) and directed the budget supporting Air Force international standardization. He was the U.S. representative to both the NATO Military Committee Air Standardization Board and the Air and Space Interoperability Council.

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
July/September 2016	Standards Policy
October/December 2016	Agency Standardization
January/March 2017	Warfighter Support
April/June 2017	Standardization Stars

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, STOP 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
Journal
Science and Technology
Defense Standardization Program
Journal
Systems Engineering
Defense Standardization Program
Journal
Biometrics Standardization
Secure Biometric Information
Compact Biometric Messages
The Biometrically Enabled Coalition

DEFENSE STANDARDIZATION PROGRAM
dsp
MAKING SYSTEMS WORK TOGETHER