The Concept of Operations for IUID-Enabled Maintenance in Support of DoD Materiel Readiness

Revision 1
January 2007

The Concept of Operations for IUID-Enabled Maintenance in Support of DoD Materiel Readiness

REVISION 1/JANUARY 2007

Executive Summary

The requirement for item-unique identification (IUID) is codified in various DoD policy documents; however, there is little guidance concerning the use of unique identification (UID) to support improved maintenance and materiel management processes. This document describes the improvements and benefits that can be derived from a fully implemented IUID-enabled information environment.

The Concept of Operations for IUID-Enabled Maintenance in Support of DoD Materiel Readiness describes

- the fundamental purpose of IUID and its position as an element of automatic information technology (AIT),
- the significance of uniquely identifying reparable items within supportability processes and life cycle events,
- how a fully optimized automated information system (AIS) can improve maintenance and weapon system support using serialized item management (SIM),
- the critical technical elements of this new environment, and
- who needs to become involved in its implementation.

Although this document is written at a user's level and is general in nature, its target audience is anyone holding key responsibility for supportability processes, including

- the program managers (PMs) charged with total life-cycle system management (TLCSM),
- the item managers who fulfill the tangible item requirements that sustain materiel readiness, and
- the maintenance managers who provide the requisite amount of materiel readiness when and where it is needed.

These key managers translate warfighter capability requirements into actionable, contractible, and measurable system performance and support processes. Accordingly, this maintenance IUID CONOPS directly supports DoD Directive 4151.18, *Maintenance of Military Materiel*, and explains how IUID-enabled data contributes to the accuracy and optimization within the weapon system sustainment processes—as described in the DoD supportability guide.[1]

To better explain actual IUID implementation processes, the CONOPS document includes (as an appendix) an implementation planning template. The template is a compilation of proven planning steps that have been used successfully by various DoD maintenance depots in their ongoing IUID implementation efforts. These planning steps embrace the essential elements of IUID implementation planning and are very relevant to any organization taking on the challenge of implementation. The template is also offered as tangible reinforcement of the current implementation of IUID and the DoD's commitment to IUID implementation.

The CONOPS document is not an implementation plan, a policy document, a system architecture, or detailed design. Rather, it sets the stage for what is operationally achievable using IUID technology and SIM methods. This document is intended to be a window into the future of DoD maintenance and materiel readiness—a future characterized by universal IUID and ubiquitous SIM in support of optimized sustained materiel readiness.

David V. Pauling
Assistant Deputy Under Secretary of Defense
Materiel Readiness & Maintenance Policy

[1] *Designing and Assessing Supportability in DoD Weapon Systems: A Guide to Increased Reliability and Reduced Logistics Footprint*, prepared by the Office of Secretary of Defense, 24 October 2003.

Contents

Figures

Tables

Chapter 1
About This Document

This document describes a high-level concept of operations (CONOPS) that explores the benefits provided by item-unique identification (IUID) within the Department of Defense (DoD) maintenance environment. This concept was developed by the Office of the Assistant Deputy Under Secretary of Defense for Materiel Readiness and Maintenance Policy (ADUSD-MR&MP) to illustrate the possibilities of an optimized, IUID-enabled maintenance and materiel management system. Although this concept is maintenance-centric, it is associated with and closely supports the core IUID concept of operations for the DoD logistics enterprise.[1]

THE CONCEPT'S FUNDAMENTAL FORMULA

The CONOPS notionally presents a future operational IUID-enabled maintenance system, with easily understood objectives and goals, using several envisioned "end-state" scenarios. The purpose of the envisioned end-state depiction is to foster a collective understanding as to what constitutes the fundamental elements of an IUID-enabled maintenance system and how that system supports overall DoD materiel readiness. It also guides those individuals tasked with implementing IUID and serialized item management in the evolution of DoD maintenance management and materiel management systems; thereby coalescing the individual service efforts into a more common approach.

The foundation of this common approach is easily articulated in a simple formula:

$$I + T = M, \text{ where}$$

I represents identification,
T represents tracking (condition, status, and location), and
M represents management.

In this concept document, we assume the *I* element already exists and has evolved to an adequate stage of implementation. Consequently, we do not elaborate on what appears to be already fairly well understood and supported (i.e., the marking of parts with IUID). Instead, we focus on defining and describing the *T* and *M* elements relative to maintenance management systems and processes used to sustain materiel readiness.

[1] As defined in *Concept of Operations for Using Machine-Readable, Globally Unique Item Identifiers in Strategic Serialized Asset Management within the Department of Defense* (Version 1.0, March 3, 2006), Under Secretary of Defense for Acquisition, Technology, and Logistics (USD-AT&L) Program Management Office for Unique Identification (PMO-UID).

This concept of operations deals with the use of IUID in maintenance and explains what maintenance tracking means and why it is vital to the DoD's transformation to a serialized item management (SIM) paradigm.[2] The concept also describes the critical role SIM plays within the overall maintenance operations, which brings into focus the definition of what the equation's equal sign (=) actually means.

Management is the performing function. For management to be effective, it must have a defined purpose that is punctuated with distinct and achievable performance requirements. These performance requirements are necessary to measure system effectiveness. They also define and facilitate optimization within the management function. Therefore, the equal sign represents the touchstone for what is called "actionable information." It is the equal sign that describes the conversion of the "who, what, when, and where" (provided by $I + T$) into accurate information. The *M* acts as the "how and why" catalyst of that information, which defines its "actionable" traits (i.e., those events, processes, or resources that need to be managed).

Although the $I + T = M$ formula emphasizes the concept of obtaining visibility for the purpose of doing something, it does not explain what exactly is to be done, or how well it can or should be done. So the explanation of what exactly constitutes the *M* in management for the future maintenance and materiel readiness environment is a key topic within this document.

THE SCOPE OF THE CONCEPT

The current DoD maintenance domain has many unique information processes and systems characterizing today's logistics environment. Many are essential for meeting current maintenance and materiel management information requirements. Therefore, it is logical to expect that these unique systems will continue to exist while new IUID-enabled systems are brought online and older systems are turned off or modified. However, tomorrow's logistics environment will bring to a close the use of these "stovepipe" systems as they are merged into or replaced by a shared data, single enterprise, IUID-enabled business system—virtual or actual—that is built on an information paradigm using standardized data sets, schemas, and serialized item management processes.

Regardless of the rate that existing systems are superseded, there is no "Big-Bang" event for the complete (DoD-wide) IUID implementation. Dual systems (IUID-enabled and non-IUID systems) must coexist during the transition phase. Ultimately, an effective transition to complete IUID and SIM processes is expected to take time, proceed incrementally, and require additional re-sources and

[2] Some logisticians consider "tracking" to be a function of distribution only, but we contend that tracking is much more when applied to maintenance management. The term "tracking" used inside distribution processes only denotes a portion of the visibility information needed. Associating data such as use information, maintenance event recording, or engineering specifications provides greater levels of tracking (and therefore visibility) for maintenance management.

management. The question now at hand is how much time, resources, and management. Therefore, the CONOPS assists the unique identification (UID) implementation managers with determining their portion of the overall implementation relative to a commonly defined "big picture."

Still, the duration and complexity of the transitional period during implementation must be dealt with on a one-to-one basis from service to service, system to system, and commodity to commodity. Consequently, the requisite details for the transition of each specific system cannot be represented or described within this document. Implementation and transition at the lowest levels must be planned and accomplished by those most familiar with the respective system.[3]

ADUSD-MR&MP recognizes that the transitional situation is a challenge for the maintenance and materiel managers who must work within today's business rules while attempting to implement and transition to the envisioned IUID-enabled end-state with new business rules and performance objectives. Therefore, implementation planning and execution issues beyond the scope of this document should be addressed in component-sponsored forums and working groups. ADUSD-MR&MP is committed to providing and coordinating assistance for these groups whenever possible.

To further illustrate the importance of effective planning to achieve the envisioned end-state described in the CONOPS, and to assist those faced with implementation planning, Appendix A contains a planning template used by the DoD maintenance depots. This template is a compendium of lessons learned from the successful planning efforts of several maintenance depots. Although it is depot-centric, the planning steps can be easily applied to most other maintenance organizations and facilities.

[3] The various roles and responsibilities of involved organizations and offices are further described in Chapter 6.

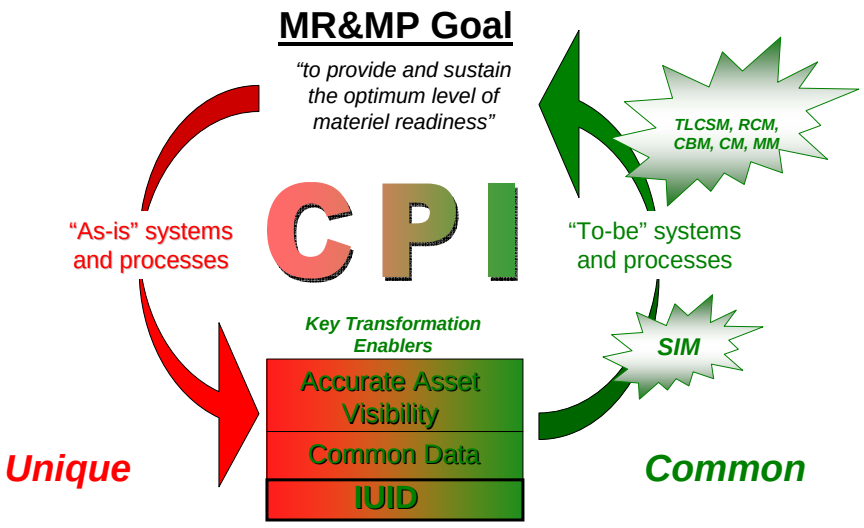
Chapter 2
The Case for IUID

Sustaining materiel readiness is the driving purpose behind almost all DoD logistics and business systems and processes. Providing effective materiel readiness produces the required levels of combat capability needed to meet DoD's strategic planning guidance. Since materiel readiness is a direct function of maintenance, both are sustaining elements of the DoD's combat capability.

Figure 2-1 depicts the current maintenance systems' transformation into the envisioned future system, directly supporting the overarching goal of sustaining materiel readiness. Essential to the $I + T = M$ formula are three key transformation enablers:

- Accurate asset visibility
- Common standardized data
- Standardized IUID.

Figure 2-1. Transformation Built on Three Key Enablers



In Figure 2-1, we see that optimized materiel readiness begins with the implementation of IUID and employment of common data sets, which in turn facilitate accurate asset visibility.

Achieving accurate asset visibility facilitates SIM processes within the new systems. This facilitates the advanced management functions for materiel readiness programs, such as the following:

- Total life-cycle system management (TLCSM)
- Reliability-centered maintenance (RCM)
- Condition-based maintenance (CBM)
- Configuration management (CM)
- Maintenance and materiel management (MM).

These programs provide the higher management functionality needed to fully optimize materiel readiness processes, which are necessary to effectively sustain combat capabilities. These are just some of the evolving programs and initiatives that begin to define the primary characteristics of a future maintenance and materiel readiness environment, as envisioned within this document. But common to all of these programs are their dependency on commonly defined data that are related to and associated with a specific materiel asset through use of IUID.

Another essential element of transformation depicted in Figure 2-1 is the continuous process improvement (CPI). CPI processes provide the organized method of reviewing, assessing, and optimizing this new environment as it evolves to new and different situations and conditions. Applying CPI methods, the program managers can identify and arrange the right elements within their materiel readiness value stream for the right amount of readiness and the right times.

BACKGROUND

In response to Government Accountability Office audit findings critical of the DoD's ability to physically and financially account for its spare and repair parts, and in support of the ongoing compliance requirements of the Chief Financial Officers' Act, the Office of the Secretary of Defense (OSD) undertook to improve its ability to account for DoD tangible items. The DoD vision for item identification was to implement policy, regulations, and supporting processes that enabled the service components to uniquely identify all significant tangible items in their inventories. This initiative is considered a strategic business imperative for the DoD.

In setting forth a UID policy, the OSD defined the following strategic outcomes:

- Data integration across DoD, government, and industry systems as envisioned by the DoD business enterprise architecture
- Improved item management and accountability

- Improved asset visibility and life-cycle management
- Clean audit opinions on the property, plant, and equipment and operating materiel and supplies portions of DoD financial statements.

In moving to achieve these strategic outcomes, certain issues emerge that must be identified and addressed. Most significant is orchestrating the right amount of transformation within the business processes, information systems, and management methods currently in place within the DoD enterprise. This transformation must be based on a SIM paradigm and system infrastructure that manages certain items at the individual level using IUID. All of these things are essential to effectively realize the mentioned outcomes.

A Strategic Return on Investment

It must be understood and recognized early on within implementation efforts that the application of IUID does not yield a great benefit in and of itself; nor is it expected to provide a direct return on investment (ROI) in all applications and situations. The ADUSD-MR&MP takes the position that a return on the investment of IUID is not just a function of economics; it is also a function of the amount of effective change that is ushered in by implementing IUID. Therefore, given the strategic nature of IUID, a direct ROI (relative to the costs incurred to establish IUIDs, mark parts, enter IUIDs into the registry, etc.) may not immediately appear at the operational maintenance levels that are typically tasked with its implementation. But in the long-term strategic perspective, IUID can produce significant ROI across the full spectrum of the business and logistics functions of the DoD.

The Case for Change

To better understand the case for implementing IUID, consider as an example a ROI analysis of three businesses implementing an e-mail system. These three businesses (referred to as Businesses A, B, and C) want to implement e-mail within their organizations. Currently, the businesses are postured accordingly:

- Business A functions purely on a paper-based mail system and does not employ the use of personal computers.
- Business B already functions partially by digital processes; it has personal computers, but they are connected only by a local area network—or intranet.
- Business C also partially uses digital processes and personal computers, but these computer are linked via the World Wide Web—the Internet.

Intuitively, the implementation of an e-mail system is significantly more costly for Business A than for Businesses B or C, which already use personal computers. Likewise, one might expect that the investment benefits are greater for Business C than for A or B.

But in reality, the greatest ROI belongs to the business that introduces the greatest amount of effective, positive change because of its new e-mail capability. If Businesses B and C elect to use e-mail only to supplant their current internal messaging processes, and Business A completely restructures itself and reengineers all information processes to conform with a net-centric, shared-data, real-time, fully digital system—coordinated and managed via e-mail procedures facilitated through that digital infrastructure—then Business A would produce the greatest ROI. But to the user of that email-enabled information system, most of the big benefits of using this system are almost invisible. The immediate benefit is perceived as merely a more modern process of doing the same job as before. But that perception may change once an individual is promoted or given a raise in salary due to the company's growth and prosperity.

The bottom line is the ROI on new technology integration directly correlates to how much change a business is willing to accept and implement relative to the full capability of the respective technology. What a business is willing to accept in terms of change is directly related to what they need to do to be the best viable alternative for their customers. The more efficient a business can become internally, the greater the external opportunities (to seize the competitive advantage).

Therefore, an investment cannot be calculated as just the cost of the new technology, especially if it is formulated as an attribute of the old processes it is placed into. It must be calculated as an integral part of the new processes and optimized system that it enables, supplants, supports, and interoperates with.

IUID is not just new technology for the sake of new technology; it is not change for the sake of change. It enables a revolutionary new management paradigm, one that instills optimal system efficiency and optimal process effectiveness throughout the DoD enterprise.

The application and implementation of IUID provides such a significant change to current maintenance operations and materiel readiness management that all of the benefits available may not be fully realized for years to come.

The combined effect of introducing much greater process efficiency and management effectiveness—throughout the DoD enterprise—is immeasurable. The only caveat to reaching these benefits is they cannot be obtained or optimized unless all implementing entities and maintenance activities are aligned to a single vision and a basic concept of operations.

Chapter 3
Concept Essentials

THE IMPORTANT ROLE OF VISIBILITY

Before the concepts for using IUID within maintenance and materiel management systems and operations can be meaningfully described, the fundamental principles of IUID must be explained and fully understood.

As explained in the previous chapters, IUID is essentially about providing accurate visibility. "Accurate" refers to eliminating error-prone input of asset identification processes and other data capture and data transfer between systems. Visibility refers to having precise intelligence about an asset when it is needed.

The definition of "accurate" is universally understood, but the definition of "visibility" is not; it varies somewhat based on its functional derivation. In the context of this document, "visibility" means seeing into all aspects of the complete life cycle of a system,[1] component, or item. Once accurate, timely, and reliable visibility is achieved, many other management and readiness optimizers can then be enabled and initiated.

THE THREE ELEMENTS OF VISIBILITY

Implementing IUID establishes accurate visibility as to the identity of a specific item for the purpose of associating relevant management data regarding its

- condition;
- handling requirements;
- design characteristics; and
- circumstances, incidences, and histories of the actual use and care of each unique item.

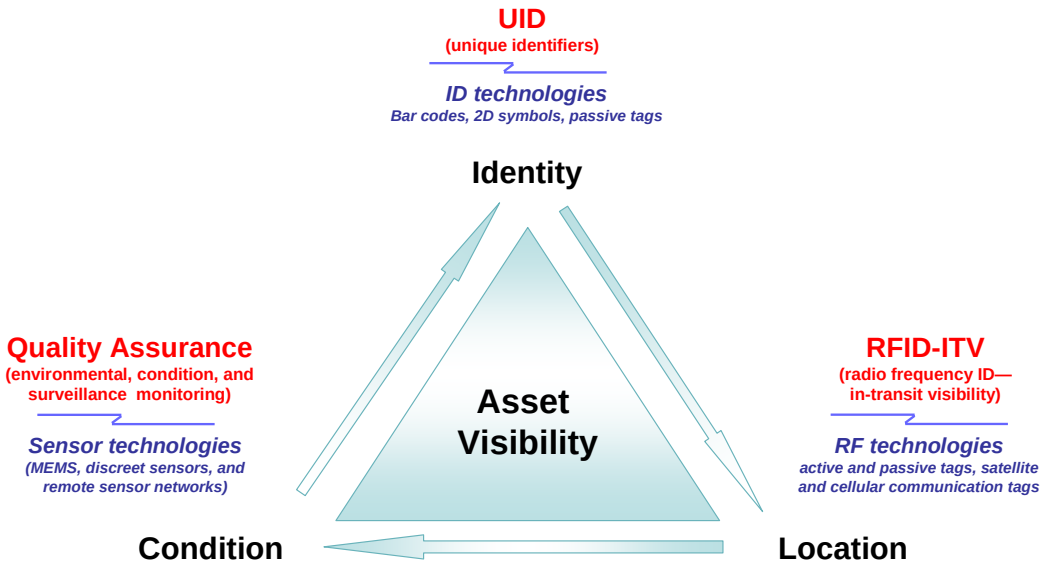
Visibility has three distinct elements: identity, location, and condition. Some might argue that time is also an element of visibility; but for this discussion, we consider time to be a variable of each of the other elements. Time is a variable in that it marks a measurable period (for example, right now, at some point tomorrow, or at some point last year) of identity, location, and condition. The location

[1] The term "system" includes the relevant subsystems, components, and parts comprising the system, as well as the associated materiel handling and business processes.

and condition of most materiel assets change frequently, and certain aspects of their identity (part number revisions, remanufacture, and software revisions) may also change, but this is all relative to what period they are being viewed.

Figure 3-1 shows the three elements of visibility relative to general asset visibility.

Figure 3-1. The Three Elements of Asset Visibility



In Figure 3-1, we see the three elements (black lettering) associated to some common automatic identification technology (AIT) (blue lettering), with the name of a known functional program they support (red lettering). It is the combination of the three elements that derives "complete asset visibility."

Not all processes or assets will require all three elements all of the time, but others will. A soldier in garrison may not be particularly concerned with the exact identity or condition of a bottle of window cleaner; he just needs to know where it is when he needs it. But an item manager for aircraft engines needs to know the specific identity, location, and condition of all engines (and the components inside those engines) he or she manages. Not knowing can have significant costs and consequences.

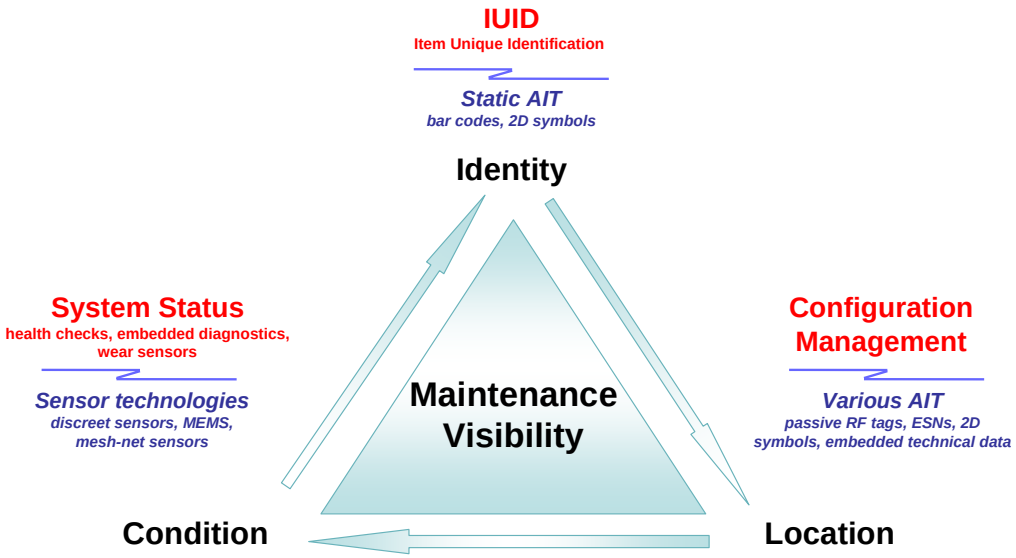
In considering the visibility triangle, a logical question is: If you drill down into a more specific functional area of logistics, do the three elements change? The short answer is no.

VISIBILITY ELEMENTS IN MAINTENANCE

Because the three elements of visibility are functionally non-parochial (i.e., universally used in many processes), they remain the same even though the supported programs, processes, and associated technologies change. In the case of maintenance (Figure 3-2), we see the functional purpose and programs have

changed and the types of technologies differ a bit, but the three elements of visibility remain the same. This is important because it supports the premise that the basic elements of visibility are common; they support and sustain high degrees of standardization and readily interoperate in all other functional areas.

Figure 3-2. The Three Elements of Maintenance Visibility



Note: ESN = electronic serial number; MEMS = micro-electromechanical systems; RF = radio frequency.

The point is visibility data may take a different name based on its function, purpose, and process placement. It may use different types of AIT to fully deliver a specific level of performance relative to a given process, but the three key elements remain common. Because they are common, the visibility data exchanges into and out of digital information systems can become common too.

THE SIMPLE DEFINITION OF IUID

Based on the preceding information, it can be stated that UID is essentially a standardized data construct that provides consistent, accurate, and automated unique item identification in a machine-readable (digital) language. As a data construct, UID needs a digital medium to communicate its message of unique identity. Any digital medium that conveys an identity message of itself, or of an item to which it is attached, can be considered an AIT. The application of UID onto a specific asset, entity, or item is then referred to as the IUID.

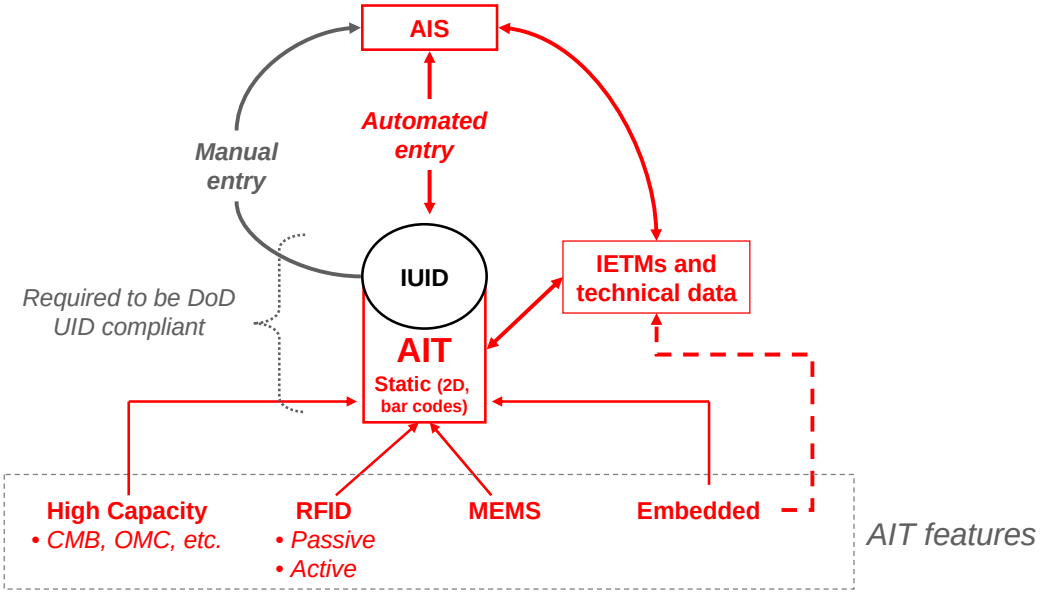
The Office of the Deputy Under Secretary of Defense for Acquisitions, Technology, and Logistics (ODUSD-AT&L) selected two main AIT media for conveying IUID: two-dimensional data matrix, commonly referred to as the 2D symbol, and one-dimensional bar code. These are simple and effective forms for expressing item identification. These types of AIT are considered static technologies and fall into the family of write once, read many (WORM) AIT media. However, many

other types of AIT, with a host of associated features, can be used in relaying IUID along with other necessary data elements for additional automated data acquisition processes.

THE CRITICAL RELATIONSHIP OF IUID WITH AN INFORMATION NETWORK

Figure 3-3 depicts the association of IUID to AIT, with the IUID being a resident element of what is essentially a static AIT medium. Below this, enclosed in a grey box, are the different types of media that constitute the more dynamic range of AIT. These different AIT, along with their associated features, may also use IUID data constructs depending on the functional application they support. But they derive their dynamic designation because they can store large amounts of data that can be changed or added as needed, or because they "transmit" their data and information to provide a stand-off read capability.

Figure 3-3. Relationships and Features of AIT



Note: OMC = optical memory card.

To be UID compliant, an IUID must be created using a 2D symbol or a bar code;[2] however, exceptions are allowed. Some exceptions involve the use of embedded AIT, such as electronic serial numbers found in a cell phone.

How an AIT must function and perform is relative to the functional requirements of the system that it supports. Automated information systems (AISs) are the information processors that accept, process, store, and pass AIT data. So, the types

[2] Refer to *Department of Defense Standard Practice, Identification Marking of U.S. Military Property*, MIL-STD-130M, 2 December 2005, for complete compliance standards and specifications.

and features of AIT that a system might use depend on how it is configured and how it must perform.

An AIS may also permit manual entry of an IUID, or the IUID may be passed into an AIS via an electronic technical data program or interactive electronic technical manuals (IETMs), as depicted in Figure 3-3. Many technical data functions are being integrated into a weapon's diagnostic system. Some weapon systems now use "self-reporting" (i.e., without human assistance) diagnostic systems that relay performance data by associated IUID directly into an AIS.

A process or a functional requirement can specify a precise AIT feature, so once that requirement is met, other questions arise:

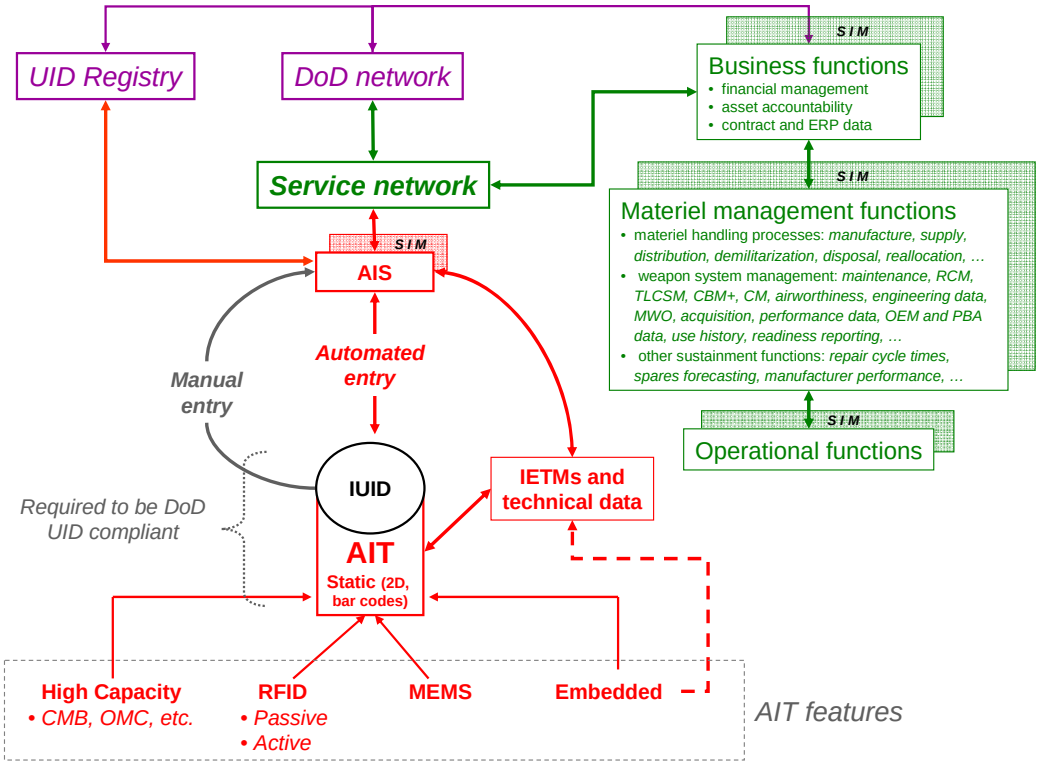
- What happens in the AIS once the IUID data is provided by the AIT?
- Where does the data go and for what purposes?
- What benefit does this data produce and for whom?

The answers to these simple yet important questions are planted firmly within the ODUSD-AT&L decision to implement IUID and the subsequent decision[3] by the ADUSD-MR&MP to implement serialized item management for reparable and intensively managed items.

In Figure 3-4, we see how the IUID is passed via an AIT into the supporting AIS. Inside the AIS, IUID data is processed using SIM methods to meet the functional requirements of that specific system and the assets or components it supports. The SIM information is then passed up into a service network, and on into the DoD network, in order to provide the requisite information for a multitude of functional purposes (marked in the green boxes).

[3] Department of Defense Directive Number 4151.18, USD(AT&L), Subject: Maintenance of Military Materiel, Paragraph 3.2.5, dated March 31, 2004.

Figure 3-4. The Relationships of SIM Information to Functional Processes



Note: MWO = modification work order; OEM = original equipment manufacturer; PBA = performance-based agreement.

From the DoD network, or in certain instances directly from the AIS, IUID data is pulled from or pushed to the UID Registry, which is the official DoD system that manages UID product data. Although greatly simplified, IUID data and other information is generally passed via the information network as depicted in Figure 3-4. But describing the technical elements of this vast system is not the purpose of this discussion. Instead, this concept of operations document focuses on describing the maintenance and materiel readiness functions listed in the middle green box.

THE CRITICAL FUNCTION OF IUID IN MAINTENANCE AND MATERIEL MANAGEMENT PROCESSES

An IUID is often referred to as an item's social security number (SSN) because it serves an identifying purpose much like an SSN. The number acts only as an identifier with which other relational data elements can be associated to derive more detailed and pertinent information about that specific item. For example, to ascertain the exact physical characteristics of a specific person, such as height, color eyes, or blood type of a specific person, the SSN could be accessed and associated to the medical records for that person. Or, the SSN could be associated to registrant data, like where a person works or lives. In any event, this is much like the data and information relationships of IUID to maintenance and

materiel management data. The number essentially makes it possible to find other sources of associative and relative data.

In the case of a reparable component, the term “associative data” means the ability to access pertinent technical data, such as maintenance and repair history, engineering data, and the operational use history. If this information is reliably accurate, a complete life-cycle perspective becomes visible, relative to that respective component. This leads to serialized item management (i.e., the management of a specific item relative to its exact conditions, requirements, and circumstances—rather than management based on assumed criteria generally applied to broad categories of similar components). Through IUID, we achieve SIM; through the use of SIM methods, we can achieve the following:

- Continuous process improvement
- Condition-based maintenance
- Accurate and complete cost and performance data for total life-cycle management functions of systems and components
- Reliability-centered maintenance
- Automated and highly accurate weapon system/component configuration management and system inventories
- More effective automated maintenance management (for example, fault-to-corrective action tracking, real-time status reporting, accurate technical data, accurate supply interfacing, component failure and performance rates, work order data, usage data, dispatching, warranty tracking, and mechanic proficiency tracking).

In the context of materiel management, the key benefit of IUID is the ability to associate specific assets to specific locations (or, if in transit, to specific transportation nodes), and then to the condition of the assets occupying those locations. The primary goal of materiel readiness and management is to ensure the right things are brought to bear at the right time, at the right place, in the right configuration, and in the best condition. If they are not, then the knowledge to adjust and correct an issue becomes paramount. For the materiel manager, IUID enables serialized item and asset management, which in turn achieves the following:

- Accurate supply inventories by specific configurations or criteria
- In-transit visibility at the lowest level of shipment
- Acquisition of the correct items and in the correct amounts
- Accurate and effective warranty management

- Effective retrograde operations
- Accurate accountability
- Automated transfer, issue, and receipt processes
- Deriving the remaining life of specific or entire populations of assets
- Improved repair cycle times
- Accurate disposal rates and conditions.

Visibility into the relational data associations of specific identities is primarily an attribute of the processing and networking capability of the AISs with which the AIT interfaces. These AISs acquire, pass, receive, collect, process, and store data for conversion into actionable information. In Figure 3-3, we depicted the relationship between IUID and AIT, and the interface between AIT and the AIS and pertinent technical data. In Figure 3-4, we depict the relationships and relevance of IUID data and SIM processes to an AIS and its higher service level and DoD networks. What was depicted in those figures can be summarized as follows:

- All elements of a system must work effectively in concert (interoperate) with each other.
- All sources of relevant data must be readily available to provide essential information for the essential functions as needed.
- And most important, it all starts with the accurate identification of an item using its IUID.

With instantaneous data exchanges available on demand, managers can have accurate visibility into all relevant aspects of the DoD enterprise. But what are the “relevant aspects” and how do they support the new maintenance and materiel management concept of operations? These questions are addressed in the next chapter.

Chapter 4
The Concept in Action

This chapter provides a full representation of typically defined, end-to-end maintenance and materiel readiness management processes used throughout the DoD components. These end-to-end processes entail the general maintenance and materiel management functions assumed to exist in a net-centric, shared information SIM environment. Therefore, the concept clarifies how the envisioned end-state (i.e., post-IUID implementation) operates, and it describes how certain benefits emerge for maintenance and materiel readiness activities, organizations, and operations throughout the DoD maintenance environment.[1]

We depict certain critical elements of an envisioned end-state for the concepts of future maintenance and materiel management using four scenarios:

1. Field-level operations
2. Sustainment-level operations
3. Life-cycle management
4. Performance-based agreements (PBA), contractor logistics support (CLS), and foreign military sales (FMS).

Although the scenarios are not complete, they do represent the general end-to-end processes used within all components. These are concepts and, therefore, they do not use or incorporate the specific lexicon and jargon of any one component. Likewise, we avoided using existing system names and concentrate on the role or function a system supports.

SCENARIO 1. FIELD-LEVEL OPERATIONS

Scenario 1 encompasses organizational and intermediate maintenance operations, supply interface, and engineering support. In this scenario, a mechanic is conducting a post-mission inspection of a weapon system. Using his common access card (CAC), he launches a maintenance management program (MMP) and enters his personal identification number (PIN) into his portable maintenance computer. Using the accompanying portable UID scanner, he scans the IUID for the weapon system, which is then communicated to the MMP. The MMP directs him to the appropriate technical information for that specific system.

[1] In this instance, the "environment" is defined as reaching from the lowest level of maintenance repair and disposal processes (usually organizational) up through the design, manufacturing, and component life cycle and system sustainment processes.

While conducting the inspection, the mechanic detects a hydraulic servo leaking fluid. Since the servo is an IUID-marked component, the mechanic scans the IUID of the servo and sends it to the MMP. The MMP validates the servo as an installed component on that weapon system and then automatically opens to the correct technical data and history for that servo. The mechanic enters the fault into the MMP, associates it to the servo, and is presented with the inspection criteria for assessing leaks. The mechanic concludes that no leaks are allowed and the servo must be replaced (noting that repairs must be performed at the depot).

Using the servo IUID as the initiating reference, he queries the MMP for replacement and is notified that a replacement is on-hand in organizational-level supply. He places the requisition for the new servo; it is transmitted wirelessly to the production control (PC) office where it is approved and routed to the unit supply computer.

The mechanic removes the unserviceable servo and prepares it for turn-in according to the MMP instructions. He makes the appropriate entry into the MMP confirming the removal; automatically all associated data and information regarding that servo is accurately annotated. The weapon system records are updated and all information regarding the servo fault, removal, and preparation actions are passed to the quality control (QC) office. Because the servo accumulated only a very low number of operating hours before it started to leak, the MMP checks to see if the item is warranted and passes a "premature failure" alert to the assigned engineering authority and program manager.

The PC office is simultaneously notified of the change in weapon system status, and all relevant information is passed to the service's maintenance database. The mechanic takes the old servo to supply and exchanges it for the new one. The supply clerk scans the IUID of the unserviceable servo as well as the new one.[2] The mechanic and clerk scan their common access cards, enter their PINs, and complete and document the transactions.

As the issuing action is registered by the supply clerk, the supply computer initiates its automated stock refill processes. The requisition is established, the refill assets are located, and a list of available servos that can be used in that specific weapon-system configuration is electronically provided to the PC office. The list associates all available servos by IUID to national stock numbers (NSNs), and it links to basic information pertaining to each available servo. If the unit's mission requires certain servos with a certain modification applied to them, or a specific time before the next scheduled maintenance event or overhaul, the PC office can select the one most appropriate for the weapon system being used by that unit. If there is no such requirement, the system automatically selects the first available replacement based on default criteria established by that unit.

[2] If the new servo is not already marked with an IUID, the automated supply management system will recognize by code the requirement for the IUID and will not release the servo for issue. Instead, the QC office will be notified; a qualified QC inspector will be assigned to create and apply the IUID according to approved marking procedures.

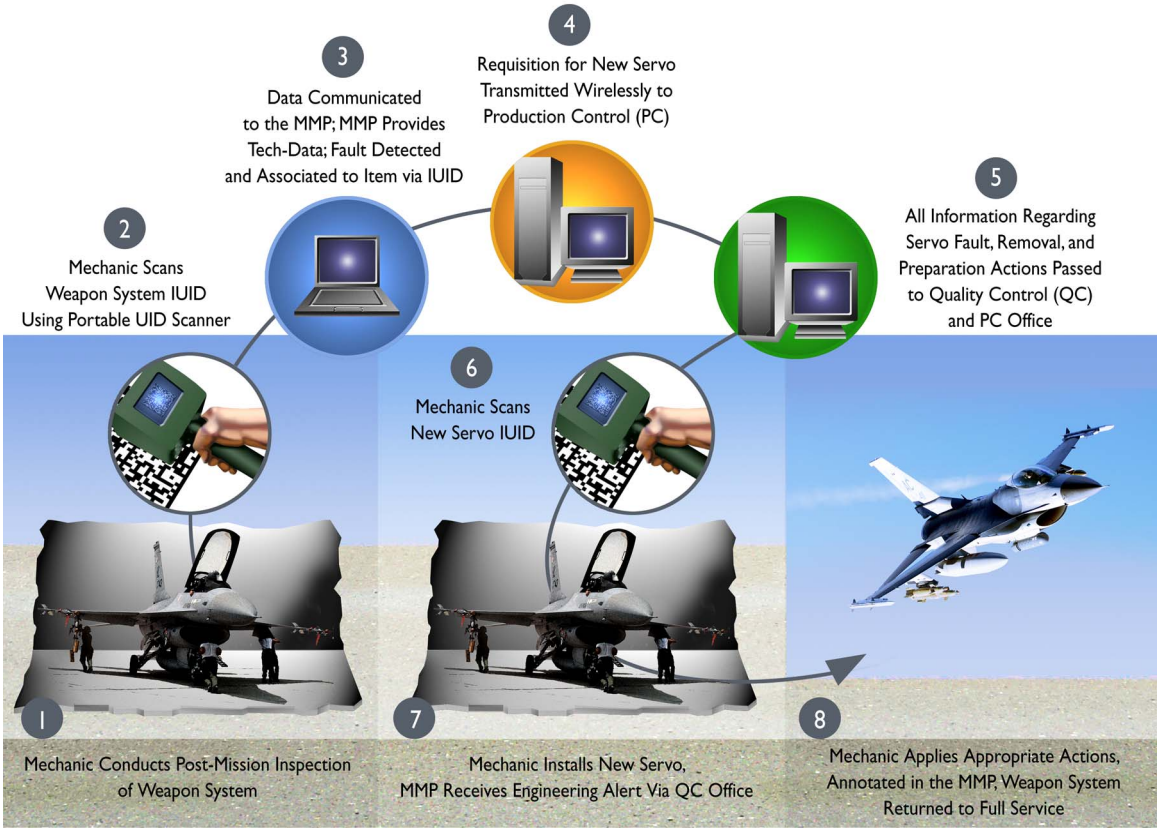
The new servo is taken back to the weapon system. The mechanic scans the IUID, which is then communicated back to the MMP. The MMP associates the IUID to the unique technical data for the servo and confirms the servo is compatible for that specific weapon system (based on the accurate weapon system build configuration and the "as maintained" inventory data). The servo is installed, and all pertinent information is passed to the QC and PC offices.

As the mechanic is finishing the replacement, the MMP receives an engineering alert via the QC office requesting an immediate inspection of shimming on the servo's support bracket. Because the "premature failure" alert was passed into the Service's maintenance database, the supporting engineering directorate was automatically alerted. The assigned engineer pulls additional maintenance data for that weapon system and verifies the servo replacement as an irregular event—noting this is the third time a servo was replaced on this weapon system—and, as such, it is identified as a potential problem.

The weapon system engineer checks the maintenance database for the IUIDs of the two previous servos that failed. Using IUID-associated maintenance histories, the engineer finds both servos were listed as "leaking" as the reason for replacement. Further research of depot tear-down analysis reports for these servos listed possible tensional loading—caused by improper shimming of the support bracket—leading to premature seal failure and leaking.

Back at the weapon system, the mechanic checks the bracket alignment and shimming using the engineering alert instructions and finds the bracket to be significantly out of tolerance. The correct shimming is applied and the appropriate actions annotated in the MMP. The weapon system is returned to full service. Figure 4-1 illustrates the sequence of events for this scenario.

Figure 4-1. Illustrated Sequence of Events for Field-Level Operations



In summary, scenario 1 describes the concept of automated maintenance management for field-level operations (the preponderance of field-level maintenance actions require mechanics to know the precise configuration of the weapon system, know the precise model of the subject component, and have immediate access to accurate and specific technical data).

This scenario illustrates the following benefits:

- The ability to automate (self-populate) a timely supply request with accurate information ensures the right part is ordered for the right system, and that it is delivered to the right unit.
- Specific replacement parts can be selected by maintenance managers to ensure supply replacement items are correct to unique end-system configurations.
- The ability to capture, track, and associate relevant information (e.g., use history, fault and corrective action data, and supply inventory data) can be fully automated (without human intervention) for maintenance to life-cycle management.

- Near-real-time readiness status reporting is ensured.
- Item-level visibility provides immediate benefits for the field maintenance manager and commander, with greater business information capability beyond the field level.

SCENARIO 2. SUSTAINMENT-LEVEL OPERATIONS

Scenario 2 encompasses depot operations, disposal processes, supply interfaces, and life-cycle management. In this scenario, the depot production manager uses a depot information system (DIS) to run the automated daily review of the supported services' maintenance databases. The review reveals that an unserviceable, repairable servo is being retrograded to that depot. The servo is identified by NSN and IUID. The DIS cross-checks the IUID with the service's information network (potentially linked through enterprise resource planning [ERP] software), which reports the servo is already in transit via a commercial carrier and provides a tracking number.

Using the tracking number, the DIS is programmed to automatically track the status of the inbound servo as it moves to the depot. The servo is expected to arrive within 1 week. Using the IUID provided, the production control manager opens a receiving and repair induction notice for the inbound servo.

Using the IUID included on the repair induction notice sent via the DIS, the induction manager has access to the maintenance history, fault data, QDR, and the depot maintenance work requirements (DMWR) of the expected incoming asset. He passes that information as an electronic advanced induction work package to an induction inspector, who reviews the materiel and tentatively routes the servo to a repair station as it arrives.

The work station's schedule is established by the production manager, which is based on visibility into the work flow for that station, the precise number of servos awaiting repair, the current and past demands for servos, any operational priorities (established by the weapon system manager or the item manager), the repair parts availability (pulled from the Defense Logistics Agency [DLA] information system), funding availability and special project codes, and the precise supply chain levels and inventory.

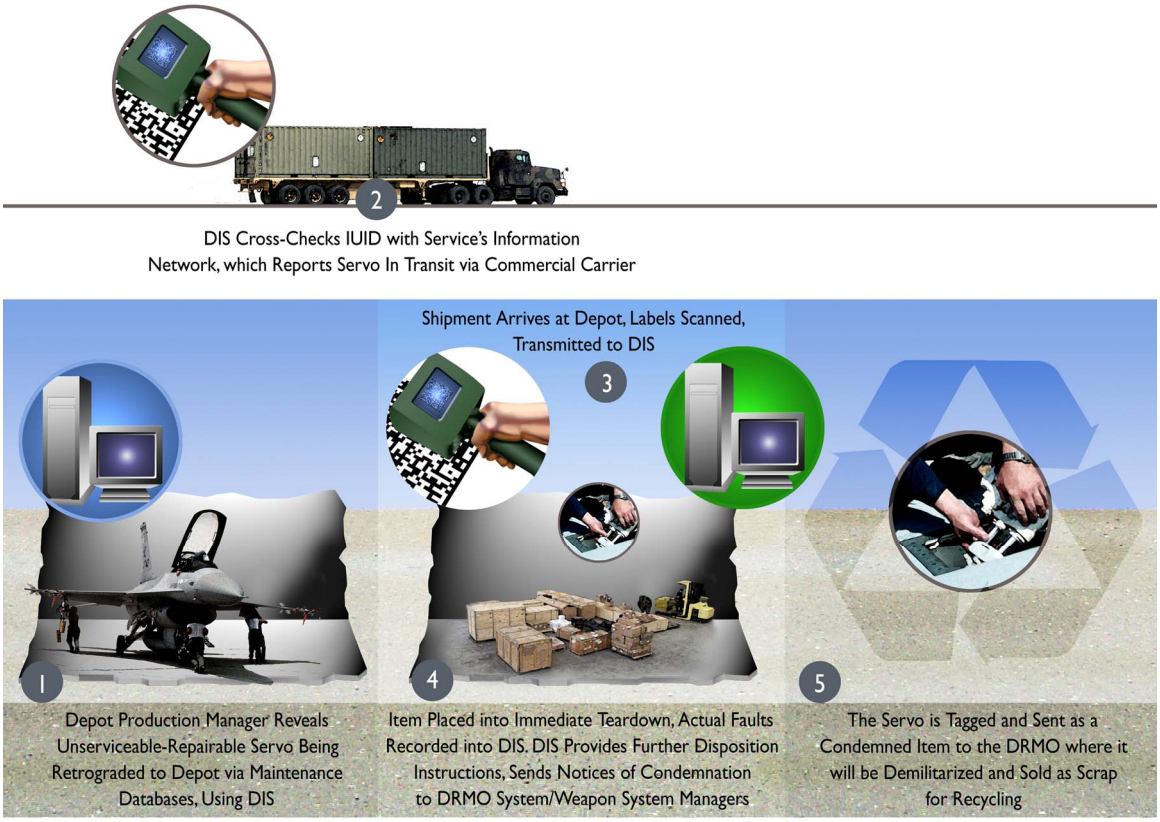
When the shipment arrives at the depot, the servo package shipping labels are scanned and transmitted to the DIS. The DIS identifies the shipping package as the expected in-bound servo and automatically associates it to its predetermined induction work-order package. Using the PIN of the receiving clerk, the servo is received within the DIS, and all open transportation actions associated by IUID and tracking numbers are closed. The receipt clerk is given instructions via the DIS to immediately route the package to the assigned repair station. Removing the servo from the shipping package, the repair station receiver scans the IUID and the shipping tag and transmits them to the DIS. The DIS verifies the servo

inside indeed belongs to that shipment package and completes all open supply actions for receipt-accountability of the servo.

Once inducted, the item is placed into immediate teardown, during which the actual faults and possible causes are recorded in the DIS. This is important because the original reported fault may be merely a contributing symptom of its actual cause; this is also relevant when the fault is no longer present or cannot be duplicated. This cause-and-effect relationship—between recorded symptom and actual fault—is captured as further teardown analysis reveals the internal diameter of the servo housing is worn beyond tolerance, rendering the servo non-reparable. At the repair station, the mechanic enters the teardown findings into the DIS, associates the findings to the servo's IUID, and assigns the "condemned" code. The DIS provides further disposition instructions and automatically sends notices of condemnation to the responsible Defense Reutilization and Marketing Office (DRMO) system, as well to the item and weapon system managers.

The servo is tagged and sent as a condemned item to the DRMO, where it will be demilitarized ("demil") and sold as scrap for recycling. The DIS automatically updates the UID Registry, showing the item was condemned by the depot and sent for demil to the DRMO. Using its IUID, the DRMO receives, demils, and scraps the servo, adding codes to the appropriate registry field. If the servo is inadvertently returned to supply, the UID Registry immediately identifies the servo as condemned upon attempting an electronic receipt transaction. Figure 4-2 illustrates the sequence of events for this scenario.

Figure 4-2. Illustrated Sequence of Events for Sustainment-Level Operations



To summarize, Scenario 2 describes the concept of automated maintenance management for sustainment-level (above field-level) operations. The preponderance of management actions requires the precise identity of the subject component because subsequent depot production control decisions are made relative to its maintenance and use histories.

This scenario illustrates the following benefits:

- IUID is used to associate item identities to shipment identities for supply and transportation actions and processes (such as in-transit visibility).
- By using IUID in the induction processes, all parties have immediate access to accurate and specific technical data, such as DMWRs and technical bulletins.
- IUID permits precise, automated receipt transactions and induction processing by associating the shipping information to the item.

- Incidences of disposal are accurately managed, and the potential for corrupt and counterfeit parts reentering the system is dramatically reduced.
- Accurate accountability of active stocks and inventories (along with the life remaining for those items in use) is factored into repair processes and priorities.

SCENARIO 3. LIFE-CYCLE MANAGEMENT

Scenario 3 encompasses national inventory control points, item and weapon system managers, engineer directorates, a manufacturer interface, and sustainment and field-level operations. In this scenario, the item manager (IM) is notified (based on the inputs from the DIS and service networks) that the servo was condemned and subsequently scrapped, reducing inventory by a quantity of one. Using IUID-enabled relational data, the IM pulls depot maintenance reports and supply data. Running a supply-analysis program the IM sees the demand rate for servos is five times greater than expected.

With analysis of the current rate of demand, repair cycle rate, and the condemnation washout rate, the IM concludes inventory levels are precariously low. A decision for an emergency acquisition of additional servos is required. Emergency procurement of those items is estimated to add 20 percent to the cost. He confers with the weapon system manager, who agrees that even if they separate the incidences of induced failures through improper shimming, the servos are not reaching their expected life. Moreover, they are being condemned at the depot at a disproportionately high rate.

The system manager contacts the depot quality control section, which queries the DIS for the IUID of all condemned servos, checking each for data surrounding their condemnation. The system manager finds that the majority were condemned due to higher-than-allowed tolerances of the inside diameter of the housing. The system manager contacts the weapon system engineering department and asks it to review the situation.

During their review, engineers discover the diameter tolerances cited in the DMWR were established to accommodate replacement of the encased seals. The seal is a common “garlock” seal, which costs approximately $10 dollars. Because the servo is provisioned with stability control circuitry and actuators, the complete servo assembly costs approximately $18,000. Allowing the housing to accommodate a slightly larger seal (by an additional 0.010 inch), in instances exceeding the allowed DMWR tolerances of over 0.010 but not exceeding 0.020, would eliminate most incidences of condemnation. The engineers also discover—through review of the IUID associated use and maintenance histories of all servos returned for depot repair—that most originated from units in Southwest Asia (SWA). Further investigation determines that teardown analysis revealed high degrees of abrasion of internal machined surfaces. The engineers conclude this is most likely caused by possible sand contaminants in the hydraulic fluid.

Additional field research reveals that maintenance crews are experiencing difficulty opening the reservoir lid for routine service of the weapon system without a significant amount of dirt and dust entering the reservoir. It was not believed to be an issue, because the primary first-stage filters are supposed to catch even microscopic particulates. However, the engineers find that in the SWA environment these filters are routinely overloaded and go into bypass, allowing unfiltered fluid into the second-stage filters, which can only filter much larger particles. Maintenance instructions require a flushing the hydraulic reservoir under these conditions of first-stage bypass, and not the entire system. Not flushing the entire hydraulic system is believed to be causing the high number of servo problems and other faults that require subsequent depot repairs.

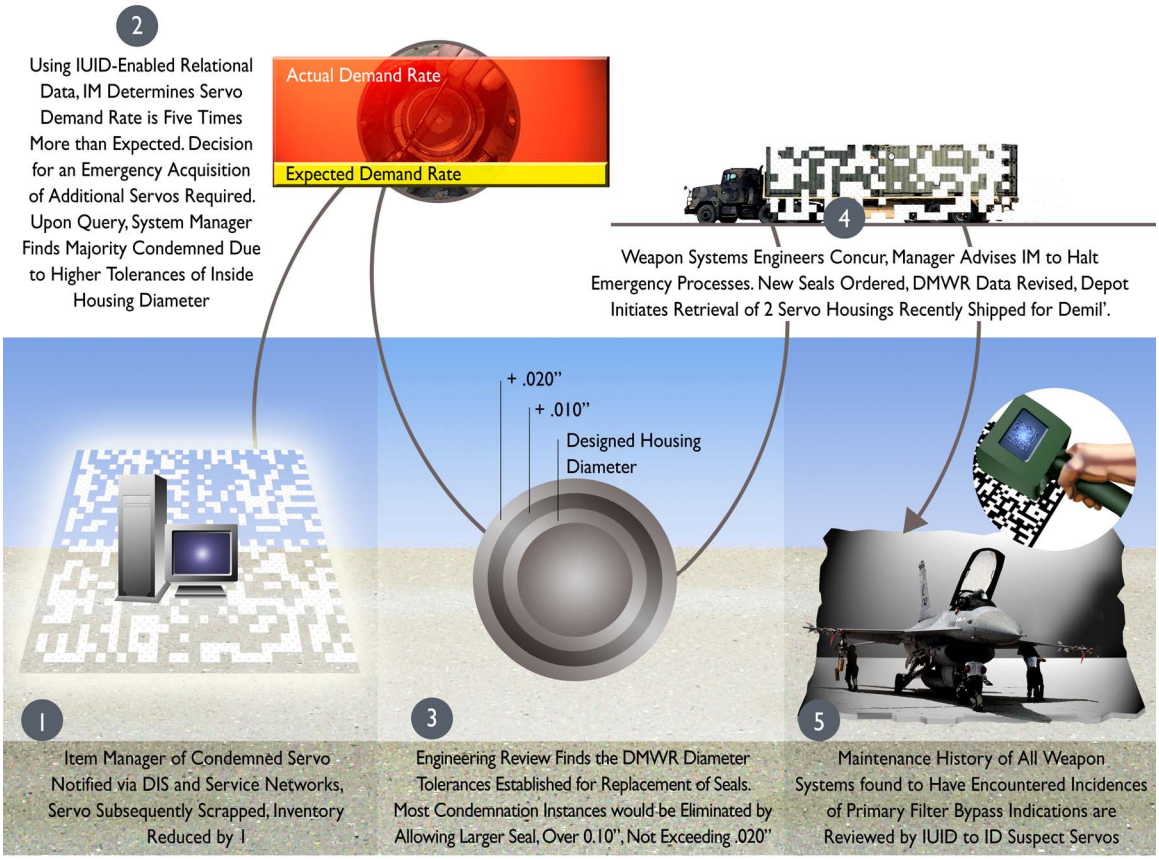
The system manager contacts the manufacturer of the servo, who concurs with the engineering review and adds that the servo housing can easily accommodate the larger seal. The manufacturer recommends a part number for another seal that fits the new criteria. With regard to contaminated hydraulic fluid, the manufacturer's engineers do not suggest any modification to the servo design. They suggest revising the maintenance procedures to include a full system flush upon entering bypass conditions of the primary filters.

The weapon system engineers concur; the weapon system manager advises the IM to not initiate procurement of any additional servos through emergency processes. The field maintenance procedures are immediately revised using an urgent technical bulletin. The depot production control orders the new seals and revises the DMWR data to include use of the new seal and inspection criteria. The depot immediately contacts the DRMO and initiates the retrieval of two servo housings by IUID that were recently shipped for demil.

The maintenance history of all weapon systems assigned, or having been assigned, to SWA is reviewed for incidences of primary hydraulic filter bypass. Those aircraft found to have encountered this situation are further reviewed to identify the servos by IUID. Those servos, which are quickly located by their IUID, undergo a one-time special inspection by an intermediate maintenance facility. All servos passing the one-time inspection have their "operating hours to overhaul" reduced by half of their remaining hours.

The depot, weapon system, and item managers are notified of the IUIDs of all affected servos and the circumstances and all historical data associated to each servo. Depot forecasting programs calculate best induction dates for depot work flow schedules. Figure 4-3 illustrates the sequence of events for this scenario.

Figure 4-3. Illustrated Sequence of Events for Life-Cycle Management



Scenario 3 describes the concept of automated maintenance management as it interfaces with weapon system and materiel management. Visibility information into the maintenance actions performed at field level is translated into actionable information required for fleet management and engineering analysis.

This scenario illustrates the following benefits:

- Accurate information regarding the use and maintenance histories of components can be readily associated to specific weapon systems or those in specific geographical locations.
- Visibility into inventory, demand trends, repair issues, and disposal rates are immediately available to the item manager.
- Engineering reliability analysis is immediately initiated using up-to-date trend analysis based on documented true and complete cause-and-effect relationships. The effectiveness of engineering corrective actions and redesign are monitored in near real time.
- Immediate revisions to technical data are controlled and implemented.

SCENARIO 4. PERFORMANCE-BASED AGREEMENTS, CONTRACTOR LOGISTICS SUPPORT, AND FOREIGN MILITARY SALES

The maintenance and support functions of the PBA, CLS, and FMS program vary somewhat from those provided in field-level and sustainment-level operations and during life-cycle management. Therefore, before describing this scenario, some further definition is needed.

The emphasis of PBA and CLS is to free the services of certain maintenance support duties in order to facilitate more efficient and effective support within the Services' maintenance environments. Under PBA and CLS, the onus is on the contractors to optimize support using whatever resources they have. The FMS program positions government-procured systems, equipment, and resources for sale to other countries. These systems are not necessarily "shared" systems, but they are similarly configured.

The primary purpose of IUID in PBA, FMS, and CLS is to provide automated, accurate asset accountability. Within CLS and FMS operations, SIM processes essentially follow the services' internal procedures. Within a PBA operation, SIM assets and maintenance management processes are under the control of the contractor, but there are points of interface into Service systems.

The servo in the preceding scenarios belonged to a weapon system that is part of a family of similar systems used throughout DoD. These systems are distributed throughout the Services and, although they have different mission design series designations, they share many common parts. The latest model of this weapon system is supported via a PBA. All other models have various arrangements of CLS in place. The earliest model of the weapon system is being removed from DoD inventory and is being placed into a FMS program.

The following subsections further explain how these support approaches operate and perform relative to IUID and SIM.

Performance-Based Agreements

Currently, weapon system support contracts do not use a standard definition for performance-based agreements (i.e., any support arrangement based on a performance driven outcome). Consequently, PBAs have many variations and unique facets. In the broadest and simplest definition, a PBA allows the service to concentrate on the use and application of the weapon system or subsystem and to delegate certain maintenance support to a contractor. Readiness is established as a performance requirement that the contractor agrees to provide. Therefore, the scenario for IUID within a PBA operation starts at the point of readiness reporting. But integrating that PBA support structure into the operational environment is still a challenge.

Under a PBA, accountability and tracking of government-owned or -leased assets used by the contractor may fall to the service. Delineating who owns or who controls what equipment is essential for both parties. In these cases, IUID facilitates the automated and accurate means to accomplish accountability and control.

In today's defense industry, a complete weapon system is seldom manufactured by a single company. Usually, a weapon system is composed of several proprietary subsystems that may not be included within the scope of the PBA contract (for example, aircraft engines may be supported and managed independent of the aircraft). These subsystems may be covered under a separate PBA or CLS contract, or supported by the service itself.

Under such circumstances, PBAs are established and executed in a manner that supports the information requirements for the entire system as a routine part of the contractor's performance. Essentially, this consists of contract clauses requiring information sharing and the use of common data exchange standards. These data standards permit the seamless migration of IUID-enabled maintenance data into other systems without loss or corruption of data integrity.

In this scenario, when the terms of performance for the PBA contract were negotiated, it was determined that the manufacturer of the new model weapon system had complied with the Defense Federal Acquisition Regulation (DFAR) guidelines and requirements for UID. In fact, the manufacturer had embraced the fullest extent of IUID application within its internal production processes and was able to provide an electronic "build" record, along with a digital operator's logbook, for the fielding of the new model weapon system.

Even though the support of this new system is performed under a PBA, this initial record establishes the exact configuration of the system "as built" and "as delivered" for the service's management system, accurately identifying all installed components and items. These digital records also enabled the accurate and automated accountability with the level of visibility to delineate all government-owned assets from contractor-owned assets used on or as part of the weapon system. This included contractor-provided ground support equipment used within the service's area of operations.[3]

[3] With regard to the contractor's support methods and operations, the contractor is free to move and use its non-IUID-marked government-supplied equipment (GSE) assets into and out of the service's area. However, if any GSE or support asset meets the established DoD criteria for marking items with UID and is used in direct support and in the operation of that weapon system while on a government installation, and if the asset is to remain unattended by the contractor and is secured or guarded by government personnel, it must be marked, registered, and tracked using the appropriate property management system (government or contractor). The intent is for the service to free itself from any extensive asset management, but still maintain accountability and security of all relevant assets placed into the service's tactical area of operations, regardless of ownership (e.g., equipment owned by the government but used by the contractor). In this instance, the government owns the weapon system but not the GSE, so accurate asset accountability is the motivating government concern, not life-cycle management.

Following the same IUID-enabled post-mission inspection requirement used in scenario 1, the sequence of events remain the same except that the contractor is using its own version of the maintenance management system. When a leak is discovered in the servo (commonly used in all models), and it is subsequently removed and replaced, the only element of the entire process visible to the service is the associated readiness and availability information. The contractor informs the service of the status and effect of the maintenance actions using the IUID-enabled standardized data exchange sets, which permits the seamless interface between the contractor and the government information systems. The government system passes the replacement transaction by IUID of the servos to its maintenance database. This permits an accurate update of the electronic "as maintained" record (initiated from the "as delivered" record) of that specific weapon system.

The contractor's maintenance management information system that tracks maintenance actions associates the IUID of the leaking servo to the weapon system's maintenance history. The system finds this servo was repaired four times before (once while on this model weapon system, three times while on older versions). The servo has demonstrated a tendency to develop leaks after operating in certain environments. The servo's reliability, based on its available mean time between failure (MTBF) data is reaching only 19 percent of its expected service life.[4] Engineers are concerned because all servos are averaging only 84 percent of their calculated service life.

The breakout by individual performance analysis shows this servo is a significant statistical outlier, which is significantly affecting overall reliability averages. The servo is labeled a "bad actor" within the maintenance system, and it is no longer allowed to be repaired. It must be sent back to the engineering department for further analysis.

Through the IUID, the engineering department identifies three other servos with extremely low MTBF. These three servos are installed on PBA-supported weapon systems. Using IUID-associated manufacturer data, research reveals that all prematurely failing servos were machined and assembled at a specific station, at a specific plant, and on the same day. The production database identifies that a total of five servos were produced that day. The other two servos were procured by DLA as spares for the earlier model weapon system. IUID data show the two servos were issued to a service supply organization but were never installed. They are located using IUID-associated supply transaction data in the service's intermediate-level supply warehouse.

The production manager at the manufacturing plant is contacted. She informs the engineers that the machines used in the production of the five servos lost power on the day in question. The machines were reset; apparently these servo housings were not pulled from the line during the reset process and inadvertently made it through assembly. This is an isolated incident involving only these five servos.

[4] An individual component's reliability can be assessed using relational data that is associated to its IUID, which is visible using SIM methods.

Using their IUIDs, the three installed servos are "tagged" with a technical bulletin alert within the Service's maintenance database. Upon entering scheduled maintenance or exhibiting a leak (whichever occurs first), the servos are replaced by the contractor, and the bad ones are sent to the engineering department. The other two servos are recalled from inventory by IUID; replacements are provided at no cost to the service. By removing the three failing servos and replacing the two spares, the average reliability of the total population of these servos is now expected to achieve 99 percent of their engineered reliability and service life.

This PBA scenario describes the concept of automated maintenance management as it interfaces with the weapon system and materiel management. Visibility information about the maintenance actions performed by the contractor is translated into actionable information required for fleet management and engineering analysis. This scenario's illustrates the following benefits:

- Accurate information about the use and maintenance histories of components in and out of the PBA support system is associated to specific weapon systems and geographical locations.
- Visibility into inventory, demand trends, repair issues, and disposal rates are immediately available to the PBA provider, resulting in greater maintenance productivity at less cost with better reliability.
- Engineering reliability analysis is immediately initiated using up-to-date trend analysis based on documented true and complete cause-and-effect relationships.
- Affected parts and systems are easily identified and corrective actions and replacements are readily dispatched.

Contractor Logistics Support

CLS provides experienced weapon system and logistics support. Maintenance CLS contracts often provision the contractor as an augmenter to the uniformed or DoD civilian workforce. Because CLS contractors augment the existing DoD capability, they are usually integrated with the component information management systems. Of course, there are exceptions and variations, but usually the CLS approach matches the service's capability, but with a higher level of dedicated resources. Therefore, CLS contractors are expected to generate, use, and transfer the same maintenance data required and used by the respective component.

Under most CLS arrangements, all processes and procedures remain the same as in the scenarios 1–3. In some instances, the contractor may use its own information management systems, but it still is required to capture, record, archive, and transfer all data and event information to the service AIS (as if using a pure service system). No service-required information or data are lost; the contractor has

access to the information needed for support functions and can use a system that serves its own processes and requirements.

CLS use of IUID follows the DoD component requirements and business rules. Asset information and materiel management interoperability between CLS providers and their respective supported component is effective and continuous through standardized IUID-enabled processes. Other benefits are essentially the same as in scenarios 1–3.

Foreign Military Sales

The sale of defense equipment and systems by the FMS program usually does not require tracking components outside the DoD environment. Exceptions are most often based on the type of technology present in the respective commodity. However, some countries may wish to implement automated asset tracking and SIM programs in participation with U.S. programs, while other countries may explicitly forbid any form of outside visibility into the systems and equipment used by their defense forces that are not required by stipulation of the FMS program. In certain cases, a customer country may purchase U.S. logistics support for the respective system as part of the FMS package.

Although any IUID-enabled maintenance or materiel management system could use the IUID, the primary purpose of marking FMS components is to register their existence in order to properly exit them from the DoD accountability system. Marking parts that are leaving the DoD may seem counterintuitive to the intent of IUID, but this is an essential step in accountability. In addition, because many parts used on foreign systems are common to U.S. systems, it is important to control the procurement of counterfeit parts and stem the reentry of foreign parts with unknown histories back into the DoD.

If the part placed onto the FMS platform was not procured through DoD acquisition and procurement channels, and if the part is not common in fit and function to U.S. systems—meaning there is no concern that the item may inadvertently return to the DoD system—it may not be necessary to mark these items (if not explicitly requested and provisioned to do so by the customer country).

In the FMS scenario, a service maintenance depot was awarded the task of converting the earliest model weapon system for placement into the FMS program. As the system is refurbished to its specified configuration, a new servo is placed onto the weapon system. In accordance with DoD requirements, the servo is appropriately assigned and marked (as in Scenario 1) when it is issued to the depot maintenance team. The servo's IUID is now associated to the weapon system as it is installed.

Upon completing the refurbishment, an electronic "build" record is compiled of all associated parts installed on that weapon system. The weapon system is delivered to the customer along with an "as delivered" record of its pertinent components. Upon

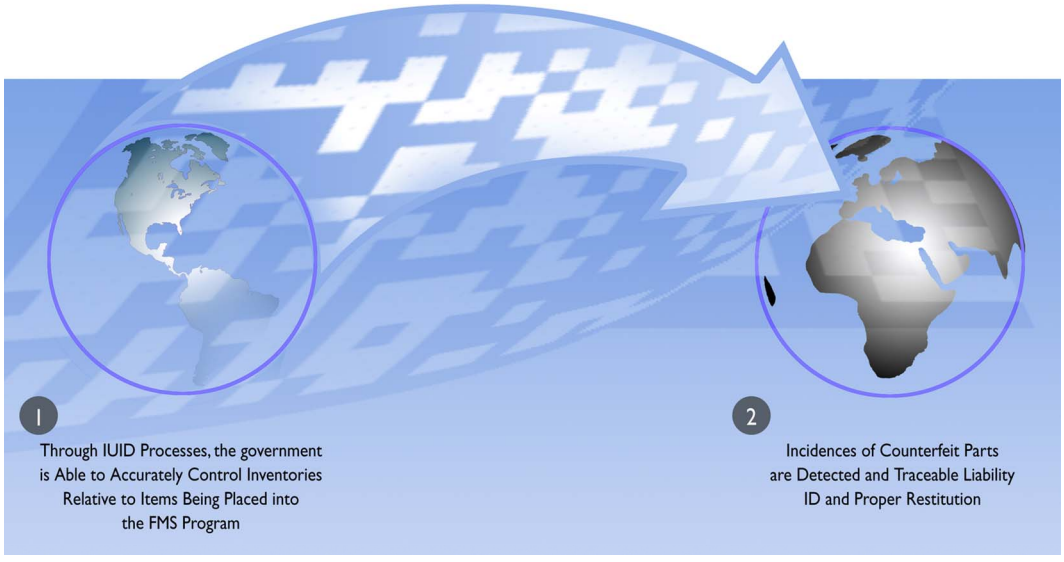
receipt by the customer, all associated IUID-marked components are annotated as being removed from U.S. inventory within the UID registry.

Several years later, due to heavy battle damage of the U.S.-deployed weapon system, the servos' item manager initiates a reorder for the procurement of 20 additional servos from the manufacturer. As per DFAR requirement, the new servos are delivered and receipted using IUID. Upon receipt at DLA, the servos' IUID marks are scanned and entered as new items into the UID registry. Through this process, one of the servos is flagged as being duplicated within the UID registry. Through linked databases, research reveals that the IUID belongs to a servo listed as having been assigned to an FMS system.

The manufacturer is informed of the situation and quickly launches an investigation. Using global databases, the servo housing is traced to a vendor dealing primarily with overseas customers. The servo housing was recovered from the disposal processes initiated by the FMS customer country. The vendor repaired the damaged housing using unauthorized repairs and engineering specifications and returned it to his inventory as a new housing. The servo housing was sold back to the original manufacturer, who no longer manufactures that model housing. The servo is recalled by the manufacturer and another legitimate servo is provided. Legal actions are taken against the errant vendor.

To summarize, through IUID processes, the government can accurately control its inventories relative to items being placed into the FMS program. The program enables detection of incidences of counterfeit parts and traceable liability identification (ID) and proper restitution. Figure 4-4 illustrates the concept.

Figure 4-4. Controlling DoD Inventories and Identifying Counterfeit Parts Relative to the FMS Program



Chapter 5
Making the Concept Work

THE NEED FOR COMMONALITY AND STANDARDS

The respective weapon system manager must establish correct milestones for implementation of IUID. One of the milestones is determining the level of items required to be marked before achieving a "critical mass" necessary to convert a specific system to fully IUID-enabled processes.[1] Once the conversion is made, it becomes the point of "no return." In other words, after obtaining a certain level of IUID implementation, it becomes almost irreversible with regard to the system's information processing that is now inextricably configured to operate using IUID.

A positive effect of achieving critical mass is it becomes the point at which benefits start to emerge (as the item management system begins to effectively operate with a fully IUID-enabled information capability). In this sense, it is imperative that weapon system managers understand that, ultimately, the benefits of IUID are more an attribute of SIM.

Achieving a point of critical mass is no small feat. This document makes no attempt to persuade anyone into believing the transition to this point is easy or an insignificant effort. Moving to an IUID-enabled SIM paradigm is truly a transforming event for all elements of the DoD's business, operational, and logistics functions. However, it is not the focus of the maintenance concept to describe each element of transition or to define the critical mass points for each system. In this section we just want to point out the "nuts and bolts" that hold the concept together.

COMMON PIECES OF THE CONCEPT

Several common elements hold the concept together, allowing maintenance and materiel readiness management to move far beyond the capability of current systems. These common elements are as follows

- Common data
- Assigned uniqueness at the item level
- IUID data standards

[1] "Critical mass" is the specific point in implementation that permits a system to begin to fully operate or derive expected benefits by using IUID.

- Tracking of maintenance data events
- Data interchanges.

Common Data

As stated throughout this document, it's all about visibility; and visibility is all about the data. If common data are not defined and used, then all the other things that may be common—the service you work in, the ERP system you use, the AIT equipment you use—become exponentially complex, expensive, difficult, and cumbersome. Without a common data structure, interoperability is not achieved.

Common data are analogous to U.S. dollars in our society. It is the medium by which all businesses work. One cannot go to the store and buy food without American money. The storekeeper has no interest in exchanging food for Yen, or euros, or your best pig. Even if the euros were equivalent to dollars, the shopkeeper does not want them because they are not common to him; it is too difficult for him to change them into something that is—dollars. And the pig may be worth far more than the goods you are buying, but the store owner has no way to evaluate that fact; he has no perspective of what any pig is worth. Likewise, data has to be in the form of a common digital medium, something that others can universally recognize and use.

Assigned Uniqueness at the Item Level

In the past century, the DoD has moved from text on paper to text in computers, but the concept of common data has yet to take hold. The UID policy from the Office of the Secretary of Defense for Acquisitions, Technology, and Logistics (OSD-AT&L) is the latest and best attempt to define some common data. This is a social security number (SSN) concept in which the IUID is the permanent identity of the item, regardless of where it lives or where it works. The item gets a distinctive IUID when it is born, and that IUID is never reissued. It is this unique identification that becomes the foundation for all future materiel management systems throughout the DoD and its supply chain.

IUID Data Standards

To create common data, one must define the "core" data elements to determine the common definition and common attributes of the data. For example, what is meant by "part number"? Is it the service's part number, the NSN, the integrator's part number, or the manufacturer's part number (e.g., Boeing installs a Honeywell part onto a Boeing system)? "Part number" cannot mean *all* those things, because all those numbers are different; they are not common. So the definition has to be agreed upon first (typically the manufacturer's part number), and then the attributes need to be identified and adhered to.

Is the part number 10 characters long, 15 characters, or 50 characters? Are lower case letters the same as upper case letters? What special characters are to be recognized? Applications and databases cannot be created until those things are defined.

Defining the core data elements—the definitions and the attributes—begins the formation of a common data dictionary that the DoD needs before it can move forward. Politically and practically, this will be very hard to accomplish, and the core data elements that demand commonality should be kept to an absolute minimum.

While the IUID is an excellent piece of standardized, common data, it is not enough. It is a necessary but insufficient element in the real world. Essentially the IUID is a "virtual" number. It resides in computer databases and in machine-readable code on an item. But in the austere environments of a combat theater, there are no guarantees for electrical power, system connectivity, or hardware replacement. Therefore, people sometimes need to intervene, and they need to read something other than codes and computer language.

Those individual human-recognizable data elements used to create the IUID (part numbers, serial numbers, enterprise IDs, etc.) also need a common definition and attributes that both humans and computers can use to conduct business in contingency situations.

Tracking of Maintenance Data Events

Once the identity of a common item can be created (the concatenated UID number in the computer), the next step is to define and gather data on common maintenance events that are significant in the life of the item (install, remove, overhaul, repair, etc.). Such events constitute a basic traceability of the item: where it has been, where it has worked, and what has been done to it. Such standards already exist in the commercial world.

Defining these maintenance events adds a significant degree of complexity to the process of defining what is common, because there are many different kinds of items and many different things that define an event for any particular item. Defining these maintenance events requires a balance—or, better yet, a combination—between a tightly defined set of common processes that is good to know about every item, and the flexibility to handle all the particular variations for any given item. "Freedom with the structure" is the philosophy that needs to be applied to successfully handle the needs of the computers, the millions of parts, and the people involved.

These data definitions for the basic traceability of life-cycle events (in and out of maintenance) form the basis of the data exchanges (DEXs) that represent the "resume" of the part: where has it worked and what have been the significant events in its life. These form the basic history and current capability of the item.

Data Interchanges

While defining the core set of maintenance events, along with their corresponding data, it also is necessary to create the means to capture the total visibility for tracking and managing the item. Items move from the original equipment manufacturer (OEM); to warehouses; to organizational- (O-), intermediate- (I-), or depot- (D-) level locations; and then onto a weapon system or into an operational environments. From there, they move back and forth again and again in a continuous loop of life-cycle events until they are disposed. Therefore, the traceability of the item becomes dependent on dozens, if not hundreds, of geographically dispersed and disparate computer systems all "playing well" with each other. This is where the core commonality of a minimum number of data elements really comes into play.

It is estimated that the DoD and its supply chain partners have 100,000 computer systems, all of which have to play well together. This is possible only by having common data. Even in the smaller circle of an item moving from OEM to warehouse to O-level and D-level locations, common data, common DEXs, and then a common way to interchange the data are needed.

Defining one single interchange mechanism is not practical in light of the vast array of different computer systems, their age, their hardware capabilities, their software capabilities, and all the different interchange mechanisms. But each maintenance or logistics system gathering data about an item as it passes through its control must have a way to extract the common data from the system and send it to some external source. Without this capability, even simple visibility is impossible to achieve, and the "DoD Transformation" concept is all but dead. The term "visibility" is thrown around very loosely without being well defined. The key concept behind "visibility" is that visibility is common and widespread—not parochial within one computer system, one facility, or one service.

Visibility means many people can see what a specific item is, where it is, where it has been, and what its condition is relative to the events and locations to which it has been subjected. That knowledge alone enables huge albeit simple benefits to be achieved. When people have even the simplest information, such as an item's location, they can adjust their plans appropriately. Typically, there is tremendous flexibility in management actions and decision processes if the truth is known. Lacking that truth—lacking accurate visibility—people and systems develop alternative plans and secondary efforts that result in a significant amount of "churn." It the classic case: A worker needs to create a work-around process to compensate for poor system performance or inadequate processes. Without visibility, no asset management system is capable of producing reliable, consistent results.

When visibility is common, all parties can know the truth; and if there are problems to be solved, the common visibility ensures a single solution can be developed. Simple, common visibility in our distributed world could help solve 80 percent of the materiel handling and management problems without developing more sophisticated technology or business processes.

In one specific logistics functional arena, commercial shippers (e.g., FedEx, UPS) achieved that common visibility for the merchant, the shipper, and the customer. But they did it in a closed system in which the data, the AIT, data interchange, and computer systems are all within their control or influence. Achieving visibility is not a hard problem to solve given those circumstances. The DoD has a far more difficult problem, because its systems are not under single control, nor do they support standardized processes.

CONCEPT REALIZATION

We know the fundamental pieces required to achieve visibility are common data, common identity, common traceability, and the ability to move the data around. A variety of data interchange mechanisms is available, including open data base connectivity, web services, Structured Query Language connections, and file transfer protocol; however, many applications and databases were never designed to exchange data with other systems. This is the core problem that needs to be fixed if even limited amounts of visibility are to be achieved. But how is it fixed?

Certain tasks must be undertaken and successfully achieved to reach the goals of a fully interoperable, IUID-enabled, common data system. The tasks include the following:

- Integrate with automated information systems.
- Modify the databases.
- Create external system interfaces.
- Address cultural change.
- Employ common reader technology.
- Establish new IUID- and SIM-derived requirements.

Assessing the degree of modifications, in all aspects of system-to-business processes, requires an understanding of what happens next. Usually the modifications involve changes to information systems and their integral components, but some changes also must take place within the human interface with these systems. The following subsections detail the typical modifications.

Integrate with Automated Information Systems

Arguably, the UID effort began with a primary focus on the new requirement of having a 2D symbol or bar code on the part. Although that may have been what attracted the most attention, it is not the substance of IUID. The substance comes from having good, shareable data in AISs, and few companies were ready to gather, store, and use the data before they started marking parts. At its best, part

marking was integrated into the regular production process on new manufactured items; at its worst, it was considered as a stand-alone, isolated process and the data may not get integrated until new AISs are built.

The first order of business should be to figure out how IUID data will enter the mainstream of existing systems and databases. The actual integration plans may be years in the future, but not having a plan wastes substantial effort. It is easier to modify and adjust a plan than it is to create one in the eleventh hour of implementation. To gain the greatest benefits from IUID data, AISs need to be modified to gather the basic IUID data elements. This may take more time than one might expect because, unlike the commercial world, the DoD implementer and user of IUID probably do not own or control the AIS that supports operations or facilitates functional requirements.

The challenge comes in having the AIS or database serve the business need while handling both IUID and non-IUID data. DoD has defined and permitted two data strings in order to construct a compliant IUID. Construct 1 provides for serialization of items within an enterprise, and Construct 2 provides serialization by a specific manufacturer and part number.

For companies choosing a Construct 1 approach to part marking, this is fairly simple. User interface screens already capture the three basic unique item identifiers—CAGE code, serial number, and current part number—so few changes need to be made. One additional data entry field or database field needs to be created, however, to indicate whether this particular set of data represents an IUID item. Otherwise, IUID and non-IUID data will look the same in the database. Without the ability to differentiate, the marking effort is substantially wasted and the databases will again contain enough garbage data to render them ineffective.

For companies choosing the Construct 2 approach to part marking, the AIS-conversion task is slightly harder. Data entry screens and databases will have to add another part number field to handle the original part number used in the Construct 2 approach. That number can be the same as the current part number at birth into the UID Registry, but after the first part number roll (after a modification), the information will be wrong for a crucial piece of data used by nearly everyone dealing with that part.

We do not go into further depth in this document, but it is crucial to address key details like this to gain the greatest benefit from IUID. In other words, numerous critical details must be understood before a well laid plan can be developed.

Modify the Databases

Before one can make a definitive statement about a database's capability to handle UID data, one must know the type, structure, and age of that database. However, most databases require some modification to handle even a minimum of UID data effectively. Moreover, during a transitional period, maintenance databases must be

structured to enable the mixed use of IUID and non-IUID data. At an absolute minimum, a Construct 1 database that uses only CAGE codes would need one additional field to indicate the record represents IUID data. More sophisticated application-level logic needs to be added to then handle the data correctly, interface with the UID registry, and so on.

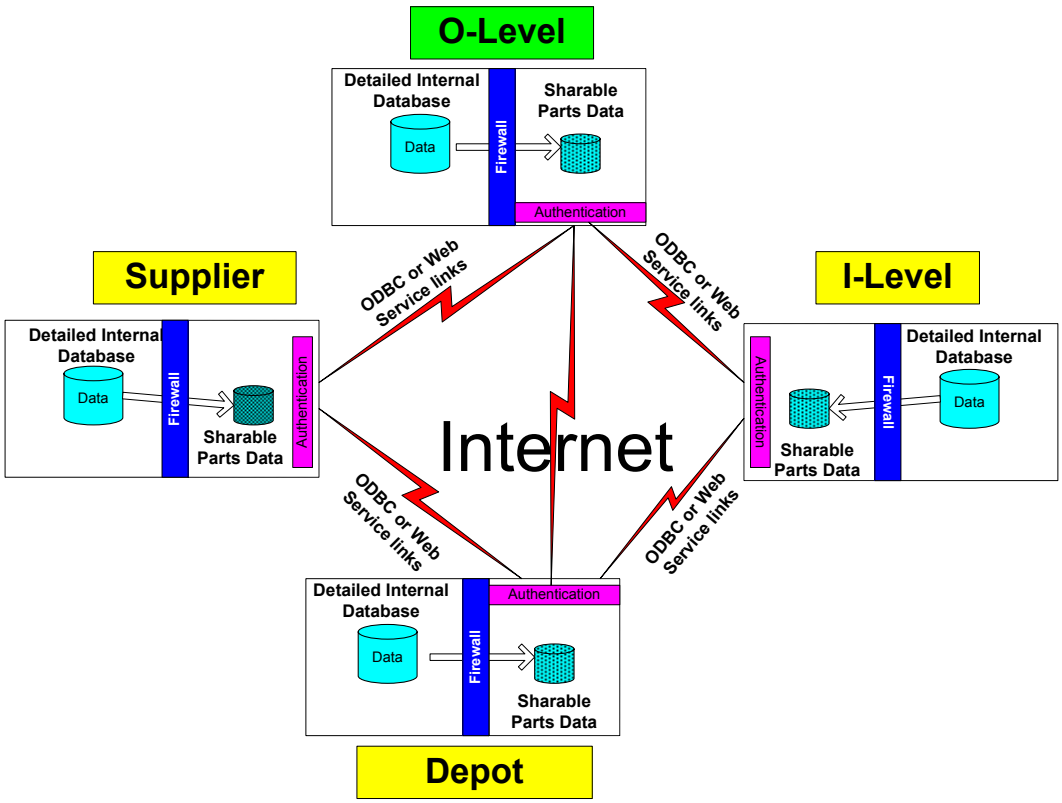
The database modifications are much more complex for a Construct 2 company wanting to handle CAGE, DUNS, and European Article Numbering–Uniform Code Council numbers, along with original part numbers needed to create the IUID number. The complexity comes not from adding a few more data fields, but in checking and modifying the different applications that use that data as well as the core maintenance applications that must be upgraded. Of equal importance are the business rules that identify when and who must populate or extract data from the data fields.

Create External System Interfaces

Another large shift needs to take place for IUID data to fully benefit the DoD community. Data that once was the sole responsibility of a particular service, depot, or function must become much more flexible and shareable with other entities. Older systems generally were not designed to share data with other systems. At best, they interfaced with a flexible report-writer application, but more often, the reports were hard coded into the application and were not very easy to change or adjust.

The raw data needs to move easily between systems. Extracting data manually from one system and sending it via a formatting application to another system will no longer be acceptable. DoD needs something like a data grid in which data are transparently shared with authenticated systems. The idea, as depicted in Figure 5-1, is to use a Google-like capability to find all the related data and have it pass transparently to the approved, authenticated systems that need it, without people being involved. Here again, the concept of a common data dictionary is crucial for all systems and databases to "play well together" in the future. The technology to do this exists, but execution of the concept is probably a decade away.

Figure 5-1. Information System Interchanges



Address Cultural Change

One more significant effort needs to be addressed: the cultural shift that must happen to help people understand the importance of data accuracy. This is absolutely crucial when the IUID birth record data are initially entered into the system. And it is only slightly less important during the rest of the component's life. In the past, an instance of bad data was simply that, one instance. But with data being shared and moved among systems, now one piece of bad data can easily get replicated in dozens of different databases. We know from experience that bad data almost never gets fixed, and the data certainly never gets fixed at all the many places to which it may have moved.

It is a classic battle between the real world of "production" and the virtual world of "recording" what has been produced. Maintenance mechanics have an affinity for just getting the job done and making the system work again; they do not enjoy recording data about that job.

That conflict must be addressed on several fronts. First, the workforce, at all levels, must understand that the data is very important and that bad data are worse than no data at all. Second, the use of bar code technology will prevent the typographical errors that corrupt the IUID data, but a lot of other data will still have

to be entered.[2] Third, the data must be fed back to the mechanic so he can do his job better, faster, or easier. This will provide the incentive for the mechanic to enter accurate data, ultimately making the accuracy problem self-correcting.

Employ Common Reader Technology

In implementing the infrastructure and reengineering processes to capture, create, pass, store, and use IUID data, the logical question will be asked, "What kind of equipment is needed to optimize IUID within my systems and processes?" The answer to this seemingly easy question requires consideration of the end-to-end asset management processes. In many instances, direct part marking is the method of choice within maintenance and materiel readiness operations. The part is marked, and that mark remains for the life of the part, regardless of the harsh environment imposed on it during operational use or maintenance. An easy application, right? Not if you do not have a reader to consistently and accurately read that mark when needed.

Consider a part that may have come from an operational environment requiring that it have a passive radio frequency (RF) tag as its source of IUID. What does that do for the depot worker holding a laser scanner at the receipt point? Ideally, only one form of AIT would be used as the IUID, but, as discussed earlier in this document, that may not be the case. The type of IUID and the manner in which it is applied and read are process driven; but this process cannot be isolated to just one local instance. "Process driven" means the most advantageous relative to the entire scope of life-cycle events and processes associated to a specific item.

Rather than having multiple IUID AIT marks, labels, and devices—each one requiring a different infrastructure and interface technology—one type of IUID reader is needed. It should be a reader that can be used by all services at all locations for all types of AIT and any type of IUID construct.

Establish New IUID- and SIM-Derived Requirements

When a new technology is introduced into a process or functional area, there is always a question of how to fully optimize it. Although many approaches center on the technology itself, the highest degree of optimization comes from revising the performance requirements of current standards. This presents the question of whether policy enables the optimal changes in technology, or does technology enable the optimal changes in policy? The answer is a balance of both.

Consider an AIT initiative that placed a passive RF tag on every weapon held in an Army unit's small-arms room. The intent was to reduce the unit's inventory time and to provide better accountability. The project was a huge success in terms

[2] This can be greatly facilitated by using a barcode reader and providing barcode menus for the mechanic or data entry person, or by restructuring the user interface on the application to provide pull-down menus.

of the technology; however, the regulation still required that every weapon be physically touched and that its serial number be manually read and manually annotated. Without changing that requirement, there was little advantage to using AIT.

Likewise, the property book sensitive item inventory was required every 90 days. That requirement recognized the burden of the time and effort imposed on the unit, and it settled for a blanket level of mediocre visibility based on what was achievable 40 or 50 years ago. However, with the new AIT-enabled capability, visibility could be optimized by increasing the requirement to a daily or weekly inventory.

Several questions needed to be asked of the unit's arms room: What is the intent of the regulation? What are the performance requirements based upon? If the intent is to always know what weapons are in or out of the arms room, then current requirements are inadequate. Is the purpose of the process to verify actual quantities of weapons by serial number, or is it to physically inspect the weapon? If the intent is to verify serial numbers, AIT would greatly improve this process.

In looking at how to assess and approach changes, some consideration must be given to requirements, new business rules, and the level of discipline necessary to enact and sustain the approach. The following are some areas of interest:

- *Develop new AIS processes to deliver data back to end user.* When a mechanic is recording a serial number that went into a repaired system, he is the only person who knows the correct information, and we need to get and deliver more and better data to him digitally. The entire man-machine interface has to be improved over what we knew two decades ago.

- *Define and extract common data for engineering analytics* (e.g., reliability). Commercial industry has defined parameters and processes to accurately measure and calculate reliability data standards. Reliability-centered maintenance is a concept that needs to be more broadly embraced by the various services, and the foundation for that is the reliability data itself. Reliability data ("how good something is") provide the greatest ROI from both a technical and a business point of view.

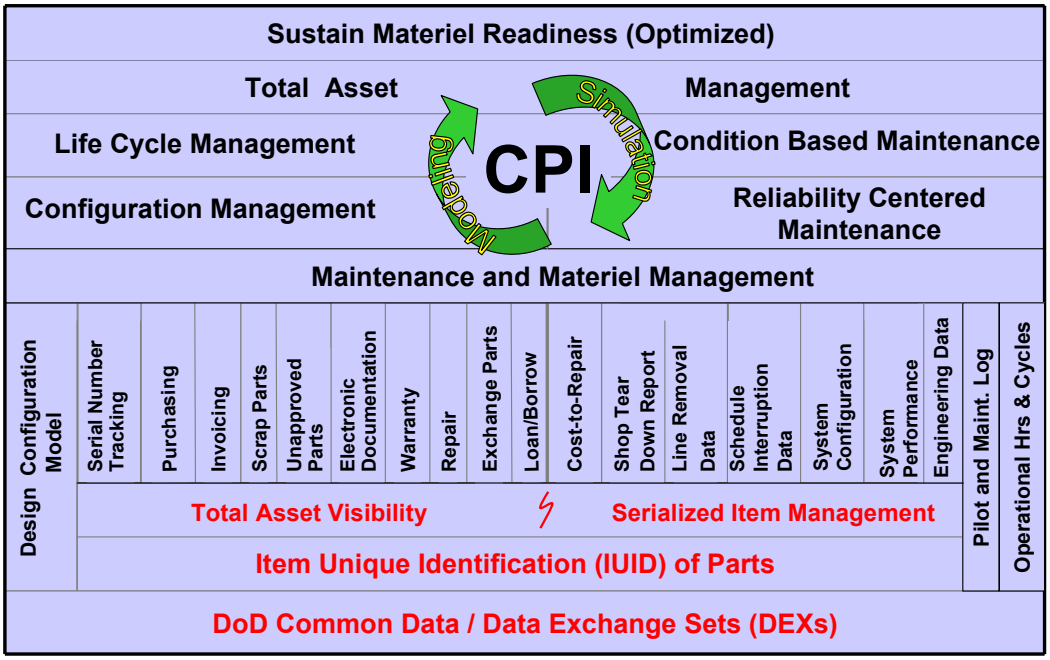
- *Integrate applications (via common data) between acquisition, logistics, maintenance, and engineering, and define core DEXs for those interfaces.* As the DoD's maintenance functions get reorganized around IUID data and other common data elements, data evangelism needs to continue across the entire supply chain from the acquisition function and suppliers, to the logistics and engineering functions. The entire data supply chain needs to define sets of DEX standards centered on the common IUID data elements.

- *Continue to demand that core data elements be common in all new applications across all services at all locations—a basic application architecture standard based on IUID data.* Before it was disbanded, the DoD's Future Business Systems Architecture group was attempting this very thing. One hopes that a new group has picked up this function. The chief information officer cannot mandate and structure higher level applications and business processes, but it is both reasonable and possible to mandate that all new systems developed across the supply chain adhere to a handful of key data elements, based on the UID data.

SUMMARY

Figure 5-2 depicts a materiel readiness structure built on a solid foundation of common data sets, IUID data elements, and the principles of SIM (along with total asset visibility) to achieve many related benefits.

Figure 5-2. Materiel Readiness Built on Common Data and IUID



The tremendous benefits made possible with IUID and SIM can be finally realized if the focus is on gathering accurate data from the maintenance technician on up, and sharing the data among the interested parties. Moreover, the philosophies and automated management methods formulating the programs, systems, and processes providing these benefits are optimally adjusted using CPI techniques, which are supported using simulation and modeling methods, to sustain the highest levels of materiel readiness.

Chapter 6
Roles and Responsibilities

To complete the concept of operations, this chapter describes the roles and responsibilities of the organizations involved with the institutionalization, sustainment, and use of IUID. Because this document is not intended to be an implementation plan, this chapter does not assign responsibilities or create "taskers" for achieving specific milestones. The primary intent is to describe the diverse organizations, offices, and the typical interrelationships involved with the implementation and use of IUID. This is done to describe the areas of responsibility and specific roles within those areas, along with certain limitations of those respective entities, in the context of the newly described IUID environment.

Achieving an IUID-enabled SIM environment is not a one-person or a one-organization show. It takes a sustained, coordinated effort among many different and dedicated entities to implement this concept; but the result will be well worth it. Realization of this concept will induce benefits at all management levels throughout the DoD, but the motivation for IUID implementation should always remain on the soldiers, sailors, marines, and airmen maintaining the military force in order to provide reliable, accurate support for the services' missions and operations.

To further illustrate the challenges and complexities of implementing IUID, Appendix A contains a template used by DoD maintenance depots to effectively plan the implementation of IUID. Although this template is depot-centric, it provides very relative information for all organizations, activities, and facilities tasked with planning the implementation of IUID into information systems, weapon systems, or materiel readiness processes. The planning template addresses an effective, incremental approach to planning and executing IUID implementation.

We strongly encourage your review of Appendix A!

TWO IUID CAMPS

Essentially two main aspects of the DoD logistics environment influence the implementation and use of IUID:

- Business processes
- Materiel readiness.

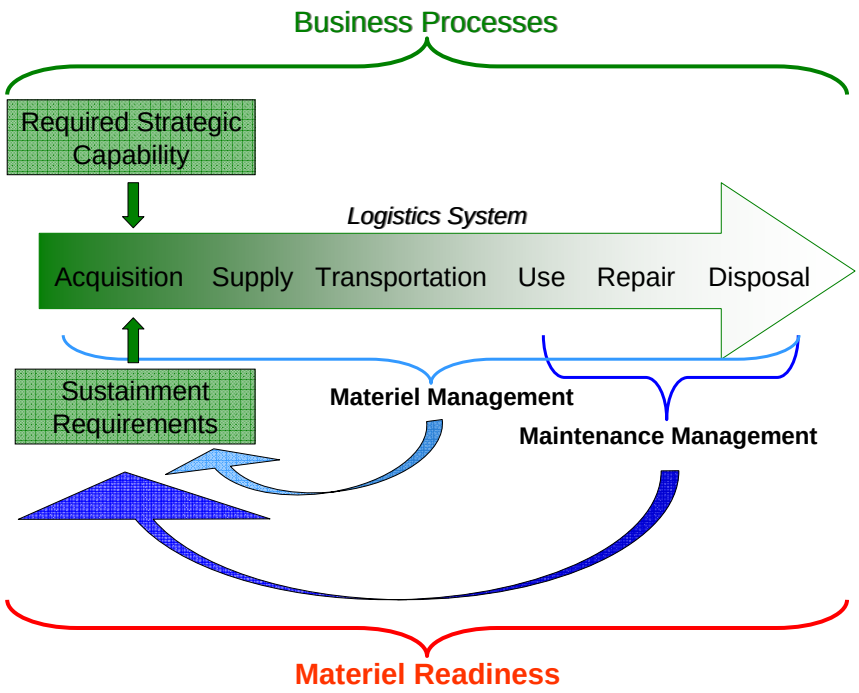
Although business processes support materiel readiness, they are not necessarily focused on the same things. The business processes of the DoD enterprise must account

for the location and inventory of assets, assess the value of those assets, and ensure DoD remains on top of all resources and property entrusted to it.

Materiel readiness is how the DoD ensures its assets are sustained to a specified level of capability in order to support our country's defense forces. Materiel managers ensure this capability is sustained (provided and replenished at the appropriate times and levels) for all operations. In other words, materiel management functions link to the appropriate business processes that facilitate meeting the needs and requirements of the operational forces.

Figure 6-1 depicts how a required strategic capability drives the acquisition function. This essentially is the entry point for procured assets that are placed into the DoD logistics system. Materiel management involves all functions of the logistics system, whereas maintenance is specifically concerned with the use, repair, and disposal functions. Materiel and maintenance management combine to derive sustainment requirements, which drive the acquisition function. All functions and processes are enveloped by the business processes that must account and pay for all materiel and services placed into or that support the logistics system.

Figure 6-1. The Division of IUID's Functional Purpose



If it effectively performs all these functions and processes, the DoD achieves materiel readiness. Therefore, business processes contribute to readiness, but they do not directly control it. Sustaining materiel readiness is the direct result of effective materiel and maintenance management, which identifies, defines, and passes accurate sustainment requirements into the logistics system.

Without both aspects working in unison, readiness cannot be effectively or efficiently achieved. This is why those implementing IUID and SIM into materiel and maintenance management processes must be cognizant of the associated business processes that also require the capture and use of IUID data.

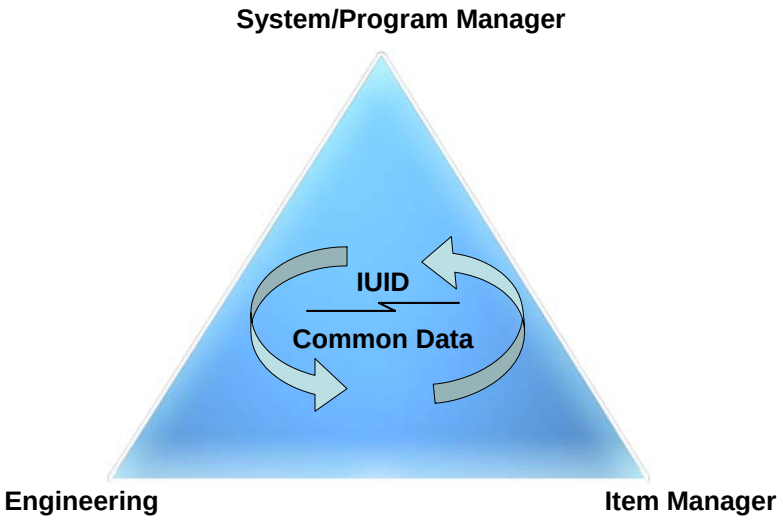
Organizing both business and materiel readiness process requirements into coordinated, effectual business rules is essential to integrating IUID into the entire logistics system. But this chapter's focus is on the materiel readiness aspect; the business aspect must be described by whomever is responsible for those functions.

THE IUID IMPLEMENTATION TRIAD

There is no single "owner" of all the maintenance and materiel systems used within the DoD environment. Maintenance—performed at an equally diverse number of facilities, organizations, and geographical areas—is a routine requirement of such an extremely diverse group of weapon systems, assets, and equipment that no one entity can expertly speak for all these systems. The ADUSD-MR&MP has responsibility for DoD materiel readiness and maintenance policy, but system processes are an attribute of operational and organizational requirements. Therefore, it is the people who are intimately involved with and best understand the intent of these processes and requirements that are key to IUID implementation.

Materiel passes through, to, and from every logistics functional area. Each must be considered when implementing information technologies such as IUID, and with new SIM information processing. But almost every system, part, item, asset, and piece of equipment has an item manager, is or is part of a system, and will have some sort of engineering element to oversee certain specifications. These three key entities form a "triad" for planning and managing the implementation of IUID. Figure 6-2 depicts the arrangement of key implementation roles and responsibilities as they form around standardized IUID and common data.

Figure 6-2. The IUID Implementation Triad



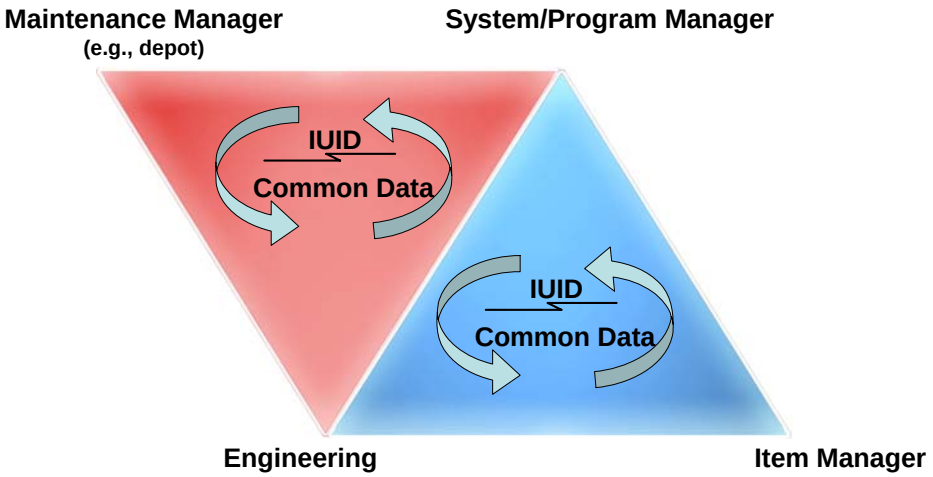
The item manager must define the information requirements of an asset relative to its appropriate and applicable management processes while the asset is off the weapon system. The system or program manager defines the information requirements while the asset is on (installed or assigned to) the end-item system. The engineering directorate or department (sometimes this is the manufacturer or the program manager) defines engineering information requirements. In addition, the engineering directorate must consider the information requirements of both the system and item managers in order to select the appropriate IUID media relative to all requirements.

THE MAINTENANCE MANAGEMENT PROCESS TRIAD

As items are marked or are being marked, certain material-handling functions and processes must align with IUID implementation to meet their information requirements. Obviously, maintenance is one such functional area, as is supply and transportation. Therefore, the system and item managers must coordinate information and material handling requirements with the appropriate maintenance organizations (such as the respective depot or repair facility). This ensures maintenance processes are properly provisioned in capturing requisite IUID data and associating it to relevant maintenance events. It also ensures that the maintenance managers have a proactive role in the integration of IUID into the maintenance systems and materiel processes.

Figure 6-3 shows the triad of responsible participants for integrating IUID into maintenance systems and processes as they form around standardized IUID and common data. This triad combines with the first and continues to connect the responsible entities via their use and need for common IUID-derived data.

Figure 6-3. The Maintenance Management Triad



THE MATERIEL MANAGEMENT TRIAD

As with the maintenance management systems and processes, other functional areas need to contribute to implementing and integrating a single IUID solution. Transportation managers, supply system and facility managers, DRMO managers, training and doctrine managers, and information system managers may have requirements and processes that support or are supported by IUID. Therefore, coordinating with the appropriate representatives is essential.

In Figure 6-4, we see how this continuing association of responsible organizations, facilities, systems, and functional entities combine and collaborate to successfully implement IUID into all information and materiel handling requirements. This collaborative effort is critical to providing optimal logistics system performance in order to achieve optimal materiel readiness. The space between these connecting lines is occupied with standardized IUID and common data sets that enable SIM and fulfill all other functional processes. This acts as the life-blood of the new materiel readiness environment.

Figure 6-4. The Linking of Responsible Triads

Figure 6-4 depicts the joining of the relevant triads (e.g., the responsible organizations, offices, facilities, and information systems) into a geodesic half-sphere representing all functional areas contributing to materiel readiness. This in turn links to another half-sphere that is formed by the collaborative arrangements of financial managers, acquisition executives, accountable officers, policy makers, strategic operations offices, and governing offices that represent the complete end-to-end business information and process requirements for the DoD. Together, the two half-spheres combine and make a single, fully connected information sphere that is sustained by standardized IUID and common data.

Although it is not within the purview of this document to define the roles and responsibilities of the business processes, general responsibilities can be described. Combined with the maintenance and materiel management roles already presented, a general picture of the scope of full involvement emerges. Table 6-1 presents a general list of the roles and associated responsibilities germane to IUID.

Table 6-1. General Roles and Responsibilities

Roles	Responsibilities
Program managers	◆ Define population of individual items to be marked, tracked, or serial managed ◆ Work with engineering community, item managers, contractors, and depots to mark items ◆ Work with information systems to develop IUID-enabled SIM processes for advanced management functionality
Contracting officers	◆ Get IUID requirements on contract ◆ Insert IUID clause in all supply contracts ◆ Develop and insert appropriate SIM information requirement clause for applicable contracts
Supporting contractors	◆ Deliver IUID and register pedigree data ◆ Maintain stewardship of government-furnished property ◆ Provide accountability of contractor items placed into government installations and facilities
Defense Contracting Management Agency	◆ Inspect and accept IUID items ◆ Provide oversight of government-furnished property ◆ Provide oversight of initial IUID-enabled SIM information requirements per contract clauses ◆ Provide program and technical support using IUID associated data for analyzing the cost, schedule, and technical performance of contractor programs and systems
UID Registry administration	◆ Establish interfaces with Wide Area Work Flow and Property Systems ◆ Maintain the UID Registry ◆ Establish interfaces with item history, maintenance, system configuration, and other pertinent technical databases
Supply systems	◆ Issue receipt, transfer, and storage transactions involving IUIDs
Transportation systems	◆ Track reparable asset shipments and transportation transactions using IUID
Top-level accountability systems	◆ Receipt transactions involving IUIDs ◆ Maintain IUID accountable property records current and correct in the applicable system of record. Report lost, destroyed, or expended IUIDs to the appropriate information systems and databases
Maintenance activities	◆ Incorporate IUID processes into all relevant transactions ◆ Mark legacy items as required ◆ Associate maintenance events to IUID items ◆ Coordinate the development of IUID processes and SIM requirements with the appropriate information systems
Defense reutilization and marketing offices	◆ Receipt transactions involving IUIDs ◆ Report disposition of IUIDs
Component headquarters	◆ Provide oversight of respective maintenance and materiel management IUID efforts ◆ Establish effective policy and business rules for the use of IUID-enabled SIM processes within maintenance and materiel management processes

Appendix A
The Maintenance Depot IUID Implementation Planning Template

This appendix contains the *Item-Unique Identification: Implementation Template for DoD Maintenance Depots* in its entirety. The "Planning Template" was originally designed as a stand-alone document, but it may be desirable to separate it from the CONOPS for ease of use. However, care should be taken when separating it from the CONOPS to ensure the integrity and context of the higher level vision, goals, and functionality of IUID applications within maintenance operations are maintained.

ITEM-UNIQUE IDENTIFICATION

Implementation Template

for

DoD Maintenance Depots

November 2006

Contents

Figure

Item-Unique Identification

PURPOSE

This document is designed to aid DoD maintenance depots in implementing item-unique identification (IUID). Its purpose is to help depots plan for IUID, achieve their first parts marking milestones, and establish a full parts-marking capability.

INTRODUCTION

This template captures the culmination of experience gained from actual DoD implementation efforts. The initiative for those efforts was a report prepared by the Office of the Secretary of Defense, Materiel Readiness and Maintenance Policy, in May 2005: *Approach to Unique Identification Initial Operating Capability at DoD Maintenance Depots*.

Vanguard efforts, such as IUID implementation efforts at the Air Force Oklahoma City Air Logistics Center and at the Corpus Christi Army Depot, have produced effective planning documents that are guiding other depots to an initial capability and beyond. Those documents highlighted several seminal features of their successful approaches to planning and executing IUID programs; some of those features are incorporated into this template.

The common fundamental elements of these features are arranged into succinct and concise steps that together form a simple template for the planning and execution of IUID at DoD maintenance depots. The template also includes a checklist that allows implementation managers to chart their organization's progress toward IUID capability.

BACKGROUND

DoD has concluded that asset accountability, valuation, and life-cycle management of all tangible items would improve if it had the capability to uniquely identify those items. In support of that conclusion, the Under Secretary of Defense for Acquisition, Technology, and Logistics created the Unique Identification (UID) Program.[1] That program has established and is refining DoD policy, acquisition requirements, and

[1] According to DoD Instruction 5000.64, "Defense Property Accountability," UID policy applies to all items acquired through purchase, lease, or other means, including transfer or fabrication if the unit acquisition cost is $5,000 or more; the item is either a serially managed, mission essential, controlled inventory piece of equipment; the item is a reparable item, or it is a consumable item or material where permanent identification is required; or the item is a component of a delivered item that the program manager has determined must be uniquely identified for management purposes.

marking criteria for the implementation of UID throughout DoD's logistics and business environments.

As part of the UID Program, separate initiatives have evolved to focus attention onto the specific functions, processes, and activities essential to its implementation. One of the initiatives that is key to the UID Program in DoD's maintenance environment is IUID, which uses a unique item identifier (UII).

IUID is the method of implementing UID standards, instructions, and policies for tangible assets and items. The resultant identifying symbol or mark on a component or item is referred to as the UII. The UII contains the identification data string that is globally unique and unambiguous, yet it is standardized for full interoperability among automated information systems (AISs). This uniqueness of the data ensures integrity and quality throughout the life of the item, and supports multifaceted business applications and users.

IUID will help differentiate marked items in the supply chain, bringing DoD one step closer to realizing a full serialized item management (SIM) program for all tangible items through all life-cycle phases. As such, the maintenance depots, where most legacy parts currently in inventory will be marked, are in a position to contribute significantly to this transformation of DoD's information management capability.

OUTCOMES

The rationale for a depot to implement IUID extends beyond meeting any government requirement; it comes from an intimate awareness of the importance of near- and long-term outcomes from UID. Those outcomes include the following:

1. Depot IUID processes and associated doctrine

2. Capability to uniquely mark UID items identified by their respective management offices and commands using DoD-sanctioned serialization schemas and parts marking techniques

3. Capability to automatically capture, modify, and query UID data in a local database and to transmit that data to a central DoD registry.

After the depots establish these outcomes and begin to advance their UID Programs, they can realize additional benefits. In the initial phases of UID, depot, item, and program managers will have better visibility of item location and value. But when UID is fully institutionalized across the services, the capabilities will provide these managers with a means to share other vital information, such as item reliability data and maintenance events, and further improve life-cycle management. Improvements in the availability and quality of data would give depots the information they need to realize greater efficiencies in depot operations, thus approaching the intent of SIM.

BENEFITS

Although IUID is viewed as a strategic imperative and a key enabler for benefits across the spectrum of DoD materiel readiness processes, it will offer depots several specific benefits.

It will facilitate direct improvements in depot productivity (such as reducing repair cycle times); process efficiency (automating tedious and labor-intensive tasks); inventory efficiency (reducing depot inventory and support equipment); and record and administration management (reducing the amount of time spent using slow, inaccurate paper-based systems).

Even small gains in productivity and efficiency in an operation as large as a depot are significant. Such gains will result in lower support costs and ensure higher states of readiness and availability for the warfighters. This gives the depot a competitive advantage in performance-based weapon support options and other industry partnerships.

APPROACH

This template provides succinct guidance to DoD maintenance depots in planning and establishing a full parts-marking capability. The guidance is presented in three phases:

1. Conducting preliminary research and planning efforts

2. Determining the new business environment and developing a marking plan for initial items targeted for IUID

3. Executing the marking plan and developing a full implementation plan for the remaining IUID items.

Each phase presents a list of actionable tasks. Because of the differences in individual depot environments and requirements, the lists may not capture all the tasks necessary for achieving the objectives at every facility. However, they do offer a good foundation for comprehensive IUID planning.

Although many of the tasks could be addressed concurrently, the template still addresses them in the context of three phases. The tasks that could be performed concurrently depend extensively upon a depot's resources and capabilities.

It is important to note that a depot is not the sole responsible agent for marking DoD items. In fact, the depot is merely the executing agent that provides a certain marking capability, which is defined by program managers and service commands for their applicable items. It is in this capacity as the key executing agent that the planning and subsequent achievement of an efficient marking capability becomes a depot-centric operation.

Obtaining a positive outcome for IUID implementation within DoD will occur only through the due-diligence and collaboration of joint efforts and organizations. But maintenance depots are uniquely situated to positively influence how quickly IUID is implemented and how quickly these other organizations can achieve the associated benefits. In taking an active and proactive approach, as described in this template, depots should be able to reduce the physical and financial burden of marking and create efficiencies across the implementation process. Therefore, effective teaming is the catalyst for positive results, and it is continually emphasized throughout all implementation planning steps.

IUID Implementation Phases and Tasks

Phase I. Conduct Preliminary Research and Planning Efforts

This phase includes developing the basic steps to define the scope of effort, establish a collaborative path, and designate the organizational elements needed for proper oversight and execution. Its minimum steps are described below:

1. *Establish a depot IUID team*. An integrated process team (IPT) should be established to develop the depot IUID implementation plan. The steps outlined throughout this template should be addressed by depot personnel, such as technicians, engineers, shop managers, and process owners, and possibly augmented by outside personnel with IUID experience.

   The depot should inform industry partners and significant suppliers of its decisions to ensure consistency with new item marking solutions whenever possible. As part of this step, the depot should designate a point of contact to serve as the liaison to outside organizations. In addition to depot representation, the Depot IPT should include representatives from item and program management offices, service commands, and other organizations with a vested interest in the depot's implementation approach.

2. *Initiate preliminary research and planning efforts*. The Depot IPT should initiate preliminary research and planning efforts, including the following:

   a. Develop a Depot IPT Plan of Action and Milestones.

   b. Research program and item managers' candidate items for IUID marking at the depot.

   c. Research parts marking sourcing options, whether organic or contract.

d. Coordinate with program and item managers to determine local serialization schema alternatives, such as the data construct of the marking (serial number, cage code, and manufacturer identification).[2]

e. Initiate engineering analyses to determine best marking alternatives relative to engineering requirements associated with parts marking (e.g., the type of mark, where and how to apply the mark, and what level of approval is needed before application). Those analyses should address the technical data requirements (e.g., changes to engineering drawings, material specifications, and standards) needed for the depot marking processes and they should investigate parts-marking resource requirements for materials, equipment, automatic information technology (AIT), facilities, and training. This include exploring the following:

   i) Local database requirements[3]

   ii) Communication interface options associated with the DoD UID registry

   iii) Facility provisions

   iv) Training requirements.

f. Explore material process flow options as well as associated data and information requirements.

g. Determine quality control requirements.

h. Initiate associated costs analyses and define funding responsibilities.

3. *Map current processes*. The depot should map its existing maintenance, repair, overhaul, and manufacturing processes at a high level to determine how and where to insert parts marking capabilities.[4]

Phase II. Determine the New Business Environment and Develop a Marking Plan for Initial IUID Items

In Phase II, the Depot IPT should use the information garnered during the first phase to determine the new business environment. It should also select the first

[2] All data constructs should be consistent with DoD policy in Military Standard 130M.

[3] Initial UID data transactions should be able to report changes in inventory locations and item value. This communication should be automatic and not involve manual data entry.

[4] The existing process should serve as the baseline for IUID integration and employment within the depot. It defines the scope of implementation in the context of training, resources required, and business process reengineering required to upgrade any process models. Planning for those models should consider the impact on shop flow, training requirements, management and administrative requirements, and quality control measures.

candidate parts for marking and establish a marking plan for these particular items. The steps in Phase II are defined below:

1. *Develop an implementation schedule for initial items targeted for IUID*. This schedule should include selecting best candidate items from those identified by program offices for initial depot IUID parts marking and setting production goals and timelines.

2. *Implement a coordinated local serialization schema*.

3. *Address parts marking technical requirements and coordinate implementation technical approach with the respective engineering office*. This action should include the following:

    a. Obtaining the correct and approved technical data.

    b. Ensuring the defined engineering instructions adequately address depot process requirements that determine where and how to mark each item.

    c. Developing and obtaining approval of necessary changes to depot processes, material specifications, standards, and engineering documentation. (Note: Design authority for engineering drawings may reside outside of depot purview, so all changes to internal IUID depot processes may need to be reviewed by other technical elements.)

4. *Establish sourcing option (organic or contract)*. If a depot has decided to procure or outsource any part of its IUID implementation process, it should initiate the required contracting actions in a timely manner to ensure the necessary resources are on hand when they are needed.

5. *Determine and map the layout of the new business environment*. This layout should include material process flows, equipment locations, and data and information requirements.

6. *Ready parts marking capability*. This capability should include the following:

    a. Establishing a local database for IUID data or to integrate IUID processes into an existing system

    b. Developing or obtaining a communications interface with the DoD UID registry for both depot manufactured and legacy parts

    c. Obtaining other necessary materials, supplies, and equipment

    d. Addressing facility requirements

    e. Training operators.

7. *Establish the depot IUID implementation management structure*. This structure should define the roles and responsibilities necessary to manage and execute the depot's IUID implementation effort relative to a definitive capability (such as an expected degree of performance or outcome).

8. *Draft depot doctrine*. This doctrine should consist of instructions, management plans, standard operating procedures, performance metrics, and other guidance, as required.

9. *Establish quality control processes*. These processes should include methods for documenting parts-marking progress and monitoring performance metrics.

10. *Prepare depot budget estimates, define depot fiscal responsibility, and communicate and coordinate funding issues*.

11. *Create a marking plan for initial parts targeted*. This plan should include developing a process for documenting progress.[5]

Phase III. Execute Marking Plan and Develop a Full Implementation Plan for Remaining IUID Items

In this phase, the depot should execute the transition plan for the initial items targeted to be marked and, from the lessons learned from this experience, develop an implementation plan for all other items requiring IUID marking. The knowledge gained from the first IUID parts marking experiences should enable the depot to finalize its processes and doctrine. When those processes and doctrine are developed, the depot will have the groundwork in place for executing parts marking on all other items, leading the way for ongoing IUID management. IUID processes should be continually reassessed and improved upon through the depot's continuous process improvement (CPI) initiatives. The steps in Phase III are described below:

1. *Implement the marking plan for initial items targeted*. The plan should include:

    a. Executing parts marking on targeted items and registering associated data in the UID registry

    b. Documenting experiences

    c. Measuring any performance outcomes identified in Phase 2 Steps 7 and 8.

[5] The marking plan should exercise as many parts-marking capabilities (labels, plates, direct parts marking) as feasible because it will serve as the foundation for the depot's UID program.

2. *Develop a full implementation plan for all other IUID items based on coordinated input from item and program management offices*. The full plan should incorporate lessons learned from the depot's first parts-marking experiences.

3. *Finalize depot doctrine*.

4. *Review and adjust funding requirements as necessary*.

5. *Execute the implementation plan*. This implementation plan should be the depot's IUID program.

6. *Initiate a continuous process improvement program*. This program should capitalize on experiences from other IUID implementation programs.

SPECIAL CONSIDERATIONS

Although this template draws extensively from preceding guidance to document high-level actions and events support IUID implementation, it also addresses several areas that deserve special consideration. Those areas are addressed below:

1. *Alignment within the service*. Implementation of IUID should be well coordinated and implementation managers should think about the materiel and information requirements when they apply to an end-to-end life-cycle management approach. Since depots are just one part of DoD's logistics and materiel readiness process, their IUID efforts should be well coordinated. Effective coordination requires participation in other IPTs and implementation workgroups. Similarly, the depots should assign organizational responsibility to research issues and propose paths to resolution. Depot managers should publicize their points of contacts for IUID implementation and continually seek to reinforce implementation with supportive organization and management actions.

2. *Single solution*. An IUID implementation solution conceived for a local or unique process may not "fit" with processes from other organizations. A collective or "holistic" solution also may not be possible, or it could be cost prohibitive. As a result, depots should implement isolated solutions only when absolutely necessary and carefully consider the long-tern effects of all solutions. However, intelligent decisions must be made whenever it is deemed necessary to isolate processes by use of a single solution and these decisions must be made with a full understanding of future ramifications. Depots should also strive to mark as many parts as quickly as possible and begin transformation to a fully integrated information enterprise with full visibility of unique items (i.e., SIM).

3. *Information flow*. The use of IUID will facilitate accurate identification of unique items within an automated system, and parts identity data will

eventually coalesce with other data (technical and business) to become actionable information. These capabilities should form foundations for depots to establish relevant, accurate, unique item-level data for shared enterprise-wide use. Depot IPTs should consider the interoperability of their systems architecture when designing IUID capabilities.

4. *IUID IPT*. When implementing IUID within a depot, IPTs should address and coordinate (1) internal issues, such as training depot artisans, and (2) external issues that affect or are affected by the application of IUID (such as standards, funding, engineering specifications, compatibility with industry partners and suppliers, and AIS reengineering). To create a service or program approach to IUID, item and program managers and service representatives should be included on the depot IPT. In addition, outside sources, such as industry experts and relevant academia, should assist in evaluating implementation plans and processes. Similarly, the depot IUID IPT lead should seek out opportunities to share knowledge and coordinate with other implementation efforts. Taking a proactive stance and clearly understanding and articulating the depot's capabilities and limitations during the implementation effort should significantly minimize the burden and intrusiveness to the depot and other involved offices and organizations.

5. *AIS interface*. The item, system, and logistics process owners seldom have complete control or ownership of the AISs used in support of materiel management. As a result, depot IPTs should seek effective interfaces with the depot's AISs. Similarly, when IUID becomes the key enabler of increased efficiency and other benefits across the service and DoD enterprises, AIS interface requirements should become fairly common. Depot IPTs should look to assess the availability of interface hardware and software used in like organizations and processes and minimize development or procurement costs whenever practical.

6. *Roles and responsibilities*. When considering the role of its IPT, the depot should stress effective coordination and collaboration with stakeholders and other involved organizations and offices. However, since many of the programmatic and technical decisions required for a depot's implementation of IUID lie outside its control and purview, the depot should recognize those instances where implementation responsibilities go beyond its control. But these instances should not be viewed as points of impasse where all depot implementation action is stopped.

   One of the key points of organizing an IUID implementation plan with a depot-centric approach is that it quickly defines the issues, separates the noise from the important messages, and offers considerable promise for achieving positive results. DoD's depots are uniquely positioned with their expertise and knowledge of pertinent materiel handling processes and technical procedures. This position places them at the critical points of interface between responsible executing organizations and policy and decision authorities, which

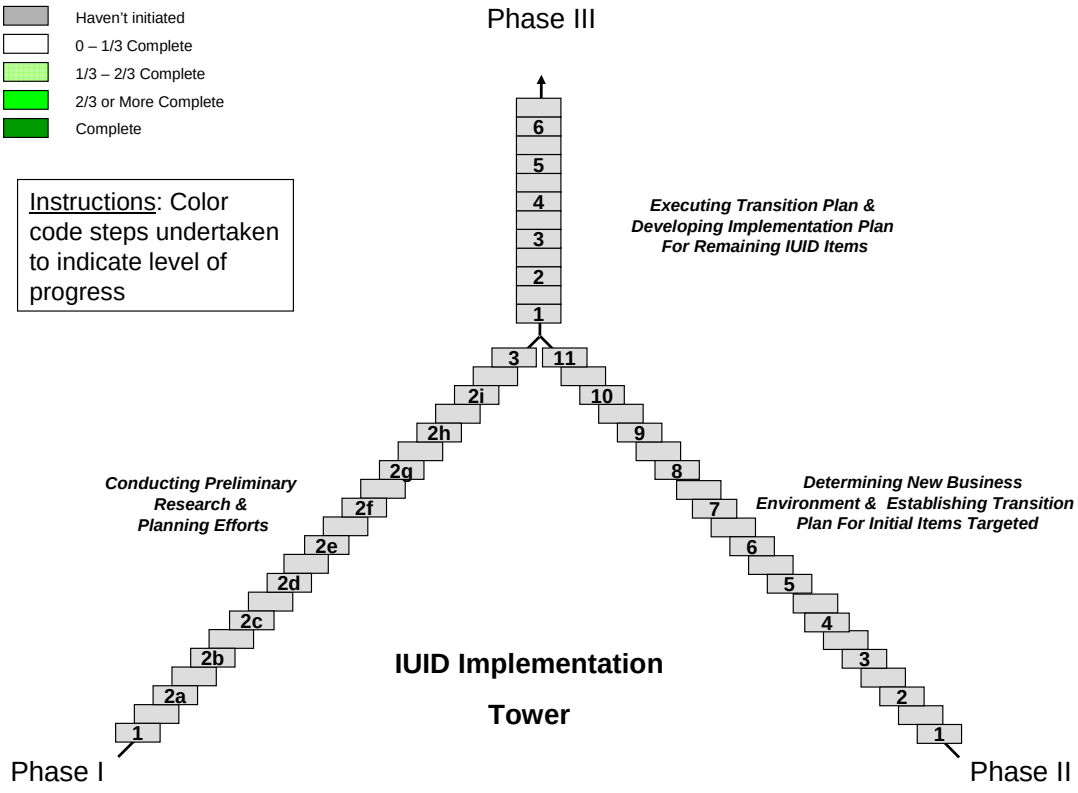
means that even though a depot may not hold decision authority, it has the responsibility to define and articulate issues and to assist supported organizations in finding the right solution for their decision processes.

MEASURING PROGRESS

Figure 1 shows a common tool that depots should use to map and communicate their IUID progress, both internally and externally. Each leg in this figure represents one of the three phases described in this template. The blocks represent the associated steps. When IUID is being implemented, the depot's IPT should indicate its progress by color coding the blocks corresponding to the steps in the template. For example, using the legend at the top left of the diagram, the lightest green color would indicate that one third of the effort associated with a particular step had been accomplished; the next darker shade would indicate that between a one and two thirds of the work had been accomplished, and so forth.

As depicted in this figure, both Phase I and II serve as the foundation for a depot to realize a full parts-marking capability.

Figure 1. IUID Implementation Tower



The appendix presents a replica of this figure for depot use.

SUMMARY

The tasks identified in this document form a template for DoD's maintenance depots to implement IUID. These tasks are not all inclusive and additional actions may be necessary as deemed appropriate by internal implementation teams. However, they are considered minimum essential tasks. By following these basic steps, depot managers can simplify and organize their initial implementation efforts and to collectively articulate and discuss their implementation issues and solutions. By preparing and organizing their implementation efforts, depots should be able to fully implement parts marking processes and exploit the benefits of economies of scale in an effective IUID program.

The tasks in this template are based on the lessons learned from successful implementation efforts and experience. In order to provide utility to an audience with diverse backgrounds, they are presented in a generalized fashion.

An implementation effort as comprehensive and large as the application of IUID has many aspects that have no precedence, so many unknowns exist. The best path to success is to share experiences and issues throughout the depot community. By following the intent and concept of this template and by maintaining good communications across the services and offices, the depot IPTs should be able to take full advantage of the business and information transformation that IUID offers.

Please visit http://www.acq.osd.mil/dpap/UID/ for more detailed information and guidance in implementing IUID.

REFERENCES

[1] Office of the Assistant Deputy Under Secretary of Defense–Materiel Readiness and Maintenance Policy, *The Concept for IUID-Enabled Maintenance in Support of DoD Materiel Readiness*, October 2006.

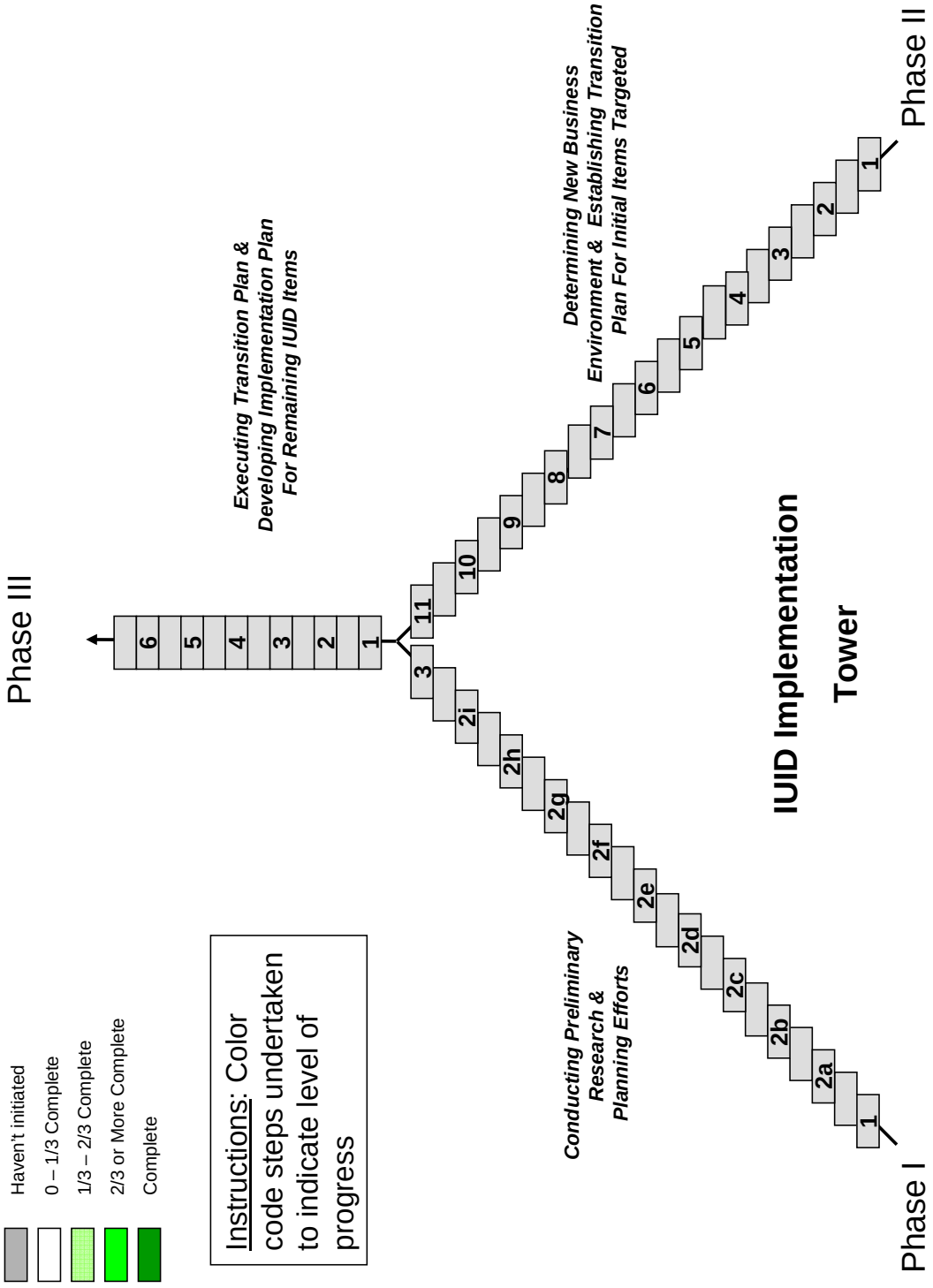
[2] Office of the Assistant Deputy Under Secretary of Defense–Materiel Readiness and Maintenance Policy, *Approach to Unique Identification Initial Operating Capability at DoD Maintenance Depots*, May 2005.

[3] Under Secretary of Defense for Acquisition, Technology, and Logistics UID Web site: http://www.acq.osd.mil/dpap/uid.

[4] IUID Toolkit, http://www.iuidtoolkit.com.

[5] Defense Acquisition University UID Special Interest Area, https://acc.dau.mil/CommunityBrowser.aspx?id=18007.

APPENDIX. IUID IMPLEMENTATION ACHIEVEMENTS



Appendix B
Abbreviations

ADUSD-MR&MP	Assistant Deputy Under Secretary of Defense for Materiel Readiness & Maintenance Policy
AIS	automated information system
AIT	automatic identification technology
CAGE	commercial and government entity
CBM	condition-based maintenance
CLS	contractor logistics support
CM	configuration management
CPI	Continuous Process Improvement
DEX	data exchange
DFAR	Defense Federal Acquisition Regulation
DIS	depot information system
DLA	Defense Logistics Agency
DMWR	depot maintenance work requirements
DRMO	Defense Reutilization and Marketing Office
DUNS	Data Universal Numbering System (Dun & Bradstreet)
ERP	enterprise resource planning
ESN	electronic serial number
FMS	foreign military sales
ID	identification
IETM	interactive electronic technical manual
IM	item manager

IUID	item-unique identification
MEMS	micro-electromechanical systems
MMP	maintenance management program
MTBF	mean time between failure
NSN	national stock number
ODUSD-AT&L	Office of the Deputy Under Secretary of Defense for Acquisitions, Technology, and Logistics
OEM	original equipment manufacturer
OSD	Office of the Secretary of Defense
PBA	performance-based agreements
PC	production control
PIN	personal identification number
QC	quality control
QDR	quality deficiency report
RCM	reliability-centered maintenance
RF	radio frequency
ROI	return on investment
SIM	serialized item management
SSN	Social Security number
SWA	Southwest Asia
TLCSM	total life-cycle system management
UID	unique identification
VIN	vehicle identification number
WAWF	Wide Area Work Flow

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
01-2007	Revision	

4. TITLE AND SUBTITLE
The Concept of Operations for IUID-Enabled Maintenance in Support of DoD Materiel Readiness (Revision 1)

5a. CONTRACT NUMBER
R26N.R706.LR502

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Durant, Ronald W
Andreson, Jon

5d. PROJECT NUMBER

5e. TASK NUMBER
LG603.50

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
LMI
2000 Corporate Ridge
McLean, VA 22102-7805

8. PERFORMING ORGANIZATION REPORT NUMBER
LMI-LR502C7 Revision 1

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
ADUSD-MR&MP
3500 Defense Pentagon
Room 5A712A
Washington, DC 20301-3500

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
A Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
This document describes a high-level concept of operations for using Item Unique Identification (IUID) within the Department of Defense (DoD) maintenance environment. This concept was developed by the Office of the Assistant Deputy Under Secretary of Defense-Materiel Readiness and Maintenance Policy (ADUSD-MR&MP) in order to establish the goals and objectives of an optimized, IUID-enabled, maintenance and materiel management system. Although this concept is maintenance centric, it is associated to and closely supports the core IUID concept of operations for the DoD logistics enterprise.

15. SUBJECT TERMS
IUID; item unique identification; concept of operations; maintenance system; IUID-enabled

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**	Unclassified Unlimited	82	Nancy E. Handy
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED			**19b. TELEPHONE NUMBER** *(include area code)* 703-917-7249