Unclassified

U.S. Army

CBM^{+} Roadmap

13 December 2007

Deputy Chief of Staff, G-4

Headquarters, Department of the Army

DEPARTMENT OF THE ARMY
OFFICE OF THE DEPUTY CHIEF OF STAFF, G-4
500 ARMY PENTAGON
WASHINGTON, DC 20310-0500

REPLY TO
ATTENTION OF
DALO-MNN

13 DEC 2007

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Condition Based Maintenance Plus (CBM+) Roadmap

1. The Condition Based Maintenance Plus (CBM+) Roadmap provides an integrated and strategic vision for the development of CBM+ capabilities throughout the U.S. Army. This document builds upon existing guidance and further articulates a strategic vision for CBM+ along with identifying the attendant organizational responsibilities for achieving CBM+ capabilities across the U.S. Army. The pathway will not be simple or rapid and will require a collaborative effort to achieve this logistical vision of the future.

2. U.S. Army Commands are developing CBM+ guidance for their respective communities of interest. For example: the Combined Arms Support Command is developing a CBM+ Capabilities Requirements Document oriented toward combat developers and program managers, and the U.S. Army Materiel Command plans to publish a CBM+ Ontology in the near future to begin the process of data standardization.

3. The enclosed CBM+ Roadmap is a capstone document that complements and harmonizes these ongoing efforts. CBM+ Roles and Responsibilities are laid out in Section 4 of the Roadmap. Noteworthy is the establishment of a CBM+ oversight body to govern the implementation of this capability. The G-4 staff will announce the initial meeting of the CBM+ oversight body which is targeted to assemble in the 2nd Quarter Fiscal Year 2008.

4. The Logistics Innovation Agency is responsible for producing this document. Questions and comments should be directed to Mr Jerry Dolinish at commercial (717) 770-7083, DSN 771-7083, or e-mail: gerald.dolinish@us.army.mil. HQDA G-4 point of contact is Mr. Dan McDavid, DSN 224-1147, or e-mail: dan.mcdavid@us.army.mil.

Encl

ANN E. DUNWOODY
Lieutenant General, GS
Deputy Chief of Staff, G-4

DISTRIBUTION:
COMMANDERS:
UNITED STATES ARMY FORCES COMMAND
UNITED STATES ARMY MATERIEL COMMAND
UNITED STATES ARMY TRAINING AND DOCTRINE COMMAND
UNITED STATES ARMY EUROPE
UNITED STATES ARMY COMBINED ARMS CENTER
UNITED STATES ARMY COMBINED ARMS SUPPORT COMMAND
UNITED STATES ARMY CORPS OF ENGINEERS
UNITED STATES ARMY CRIMINAL INVESTIGATION COMMAND
UNITED STATES ARMY INTELLIGENCE AND SECURITY COMMAND
UNITED STATES ARMY MEDICAL COMMAND
UNITED STATES ARMY MILITARY DISTRICT OF WASHINGTON
UNITED STATES ARMY MILITARY ACADEMY
UNITED STATES ARMY NETWORK COMMAND
UNITED STATES ARMY PACIFIC
UNITED STATES ARMY RESERVE COMMAND
UNITED STATES ARMY SOUTH
UNITED STATES ARMY SPACE AND MISSILE COMMAND
UNITED STATES ARMY SPECIAL OPERATIONS COMMAND
UNITED STATES ARMY SURFACE DEPLOYMENT AND DISTRIBUTION COMMAND
UNITED STATES ARMY TEST AND EVALUATION COMMAND
UNITED STATES ARMY CENTRAL COMMAND
EIGHTH, UNITED STATES ARMY
UNITED STATES ARMY INSTALLATION MANAGEMENT AGENCY

Unclassified

U.S. Army

CBM$^+$ Roadmap

13 December 2007

Deputy Chief of Staff, G-4

Headquarters, Department of the Army

Executive Summary

This is a roadmap for the implementation of Condition-Based Maintenance—Plus (CBM$^+$) in the Army. It is structured to describe the key aspects of CBM$^+$ critical to the sustainment processes for military equipment. It is neither an implementation plan nor a technical design document; it only describes the pathway to effective implementation and design.

This roadmap also contains a high-level overview of the elements that drive transformation of Army logistics and maintenance, from many decades of practice of preventive maintenance to that of condition-based maintenance (CBM) and a future of increased readiness and lower maintenance costs.

It is important to distinguish between two terms, CBM and CBM$^+$. In a CBM environment, operating platforms, embedded sensors, inspections, and other triggering events determine when restorative maintenance tasks are required based on evidence of need.

Additional capabilities and infrastructure necessary to make use of this platform-generated information are embodied in the "+" of CBM$^+$. CBM$^+$ is a proactive equipment maintenance capability enabled by using system health indications to predict functional failure ahead of the event and take appropriate action. The capability marks an evolution from the earliest applications of embedded health management.

CBM$^+$ is also an umbrella initiative developed by the Office of the Secretary of Defense (OSD) to integrate "best of breed" maintenance strategies and concepts with innovative technologies to create a new maintenance environment.

Insight derived from CBM$^+$ capabilities provides operating commanders with unprecedented visibility into their fleet operating condition, enhancing force planning, and combat power. The information also feeds multiple business processes and provides performance information for problem analysis and performance optimization. Results include improved platform availability and reduced deployment footprint.

CBM$^+$ consists of three basic elements:

- A rigorous methodology for developing equipment maintenance task requirements, employing the structured decision logic process known as Reliability Centered Maintenance (RCM).[1] This methodology has four primary objectives:
  - Ensure realization of the inherent safety and reliability levels of the equipment.
  - Restore safety and reliability to their inherent levels when deterioration has occurred.

[1] Nowlan, F. Stanley and Heap, Howard F.; *Reliability-Centered Maintenance*, published by United Airlines for the (then) Office of the Assistant Secretary of Defense (Manpower, Reserve Affairs and Logistics), 29 December 1978. Government accession number in the Defense Technical Information Service (DTIC) is ADA066579, available only in microfiche format at http://handle.dtic.mil/100.2/ADA066579 (25 megabytes). The RCM methodology has been updated and simplified over the years since it was originally published, see as an example Moubray, John, *RCM II*, Industrial Press, Inc.,1997, Second Edition, available from Amazon.com.

- Obtain information necessary for design improvement of those items whose inherent reliability proves inadequate.
- Accomplish these goals at minimum cost, including maintenance costs and the costs of resulting failures.[2]

- CBM tasks. Tasks that are derived from the RCM methodology to monitor operating equipment to identify impending failure are called condition-monitoring tasks. When those tasks are inspected or supported through use of sensor technologies, the result is called CBM.

- Infrastructure to make use of sensor-based maintenance information. This infrastructure, consisting of numerous technologies and enablers, is what is meant by the "Plus" in CBM$^+$. Throughout this paper, the term CBM$^+$ connotes both the CBM tasks and the related infrastructure.

The management direction, Total Life Cycle Systems Management (TLCSM) strategy, and technical basis for CBM$^+$ all rest on the RCM foundation. CBM$^+$ is the fundamental capability[3] that will enable the Army to achieve the vision for predictive maintenance and anticipatory logistics for Focused Logistics[4] that was first articulated in *Joint Vision 2010*.[5]

The pathway to CBM$^+$ capability is neither simple nor rapid. Numerous interrelated issues must be solved over a long time horizon—more than ten years. Today, this vision is expressed in a number of foundational guidance documents that describe the transition to network-centric and Joint expeditionary warfare. The Focused Logistics Joint Functional Concept[6] is the principal document that describes the capabilities for logistics that CBM$^+$ fulfills.

CBM$^+$ is a set of capabilities rather than a system by itself; its enablers must be incorporated into any number of operating systems and support processes throughout the acquisition life cycle. Table ES-1 is a provisional set of actions for a variety of Army CBM$^+$ stakeholder organizations that will lead to a full CBM$^+$ implementation. Consult the basic roadmap, Section 4, for a complete listing. The actions will require extensive coordination and cooperation.

The roles and responsibilities in Section 4 address a wide range of topics that must be incorporated into a full-up CBM$^+$ implementation plan. Table ES-1 lists examples of the range of roles and responsibilities for the major stakeholders—the examples are not all-inclusive.

---

[2] Nakata, David, Vice President Consulting Services, EmpowerMX, *Can Safe Aircraft and MSG-3 Coexist in an Airline Maintenance Program?* White paper available at http://www.empowermx.com/whitepapers/CanSafeAircraft&MSG-3Coexist.pdf, undated, p. 2.

[3] A capability is a collection of operational tasks/activities, the information exchanged to enable the successful completion of those tasks/activities, a set of conditions and standards applied to the tasks/activities, and the necessary supporting system functionality and data exchange requirements.

[4] This Joint concept has been incorporated into *Army Vision 2010*, see http://www.army.mil/2010/focused_logistics.htm.

[5] The Joint Staff, *Joint Vision 2010*, available at http://www.dtic.mil/jv2010/jv2010.pdf, undated.

[6] Department of Defense, *Focused Logistics Joint Functional Concept*, Version 1.0, December 2003, available at http://www.dtic.mil/futurejointwarfare/concepts/jroc_fl_jfc.doc.

Table ES-1. Examples of CBM$^+$ Stakeholder Roles and Responsibilities

Action areas	Organization												
	ASA(ALT)	PEOs, PMs	G-4	LIA	G-6	TRADOC	CASCOM	AMC	LCMCs	ARDECs	AMSAA	LOGSA	ATEC
Policy	X		X		X								
Doctrine						X	X						
Requirements						X	X						
Research and development		X								X			
Metrics				X				X			X	X	
Architectures and standards			X	X		X	X					X	
Materiel solutions		X										X	
Simulation and modeling			X	X									
Verification and validation				X									X
Analytics		X		X					X	X	X	X	
Decision authorities	X	X	X		X	X	X	X	X				
Training Development			X			X	X						

Notes: AMC = Army Materiel Command, AMSAA = Army Materiel Systems Analysis Activity, ARDEC = Armament Research Development and Engineering Center, ASA(ALT) = Assistant Secretary of the Army (Acquisition, Logistics, and Technology), ATEC = Army Test and Evaluation Command, CASCOM = U.S. Army Combined Arms Support Command, LCMC = Life Cycle Management Command, LIA = U.S. Army Logistics Innovation Agency, LOGSA = Logistics Support Activity, PEO = Program Executive Officer, PM = program manager, TRADOC = U.S. Army Training and Doctrine Command.

The overall timeline for CBM$^+$ implementation is depicted in Figure ES-1 as a 10-year implementation horizon. Detailed implementation planning must engage multiple stakeholder communities, with a formal implementation plan to be issued following publication of this document.

This document is organized into four sections:

Section 1 contains the background, vision, and rationale for CBM$^+$. This section describes the key relationships between Reliability Centered Maintenance (RCM) and CBM$^+$.

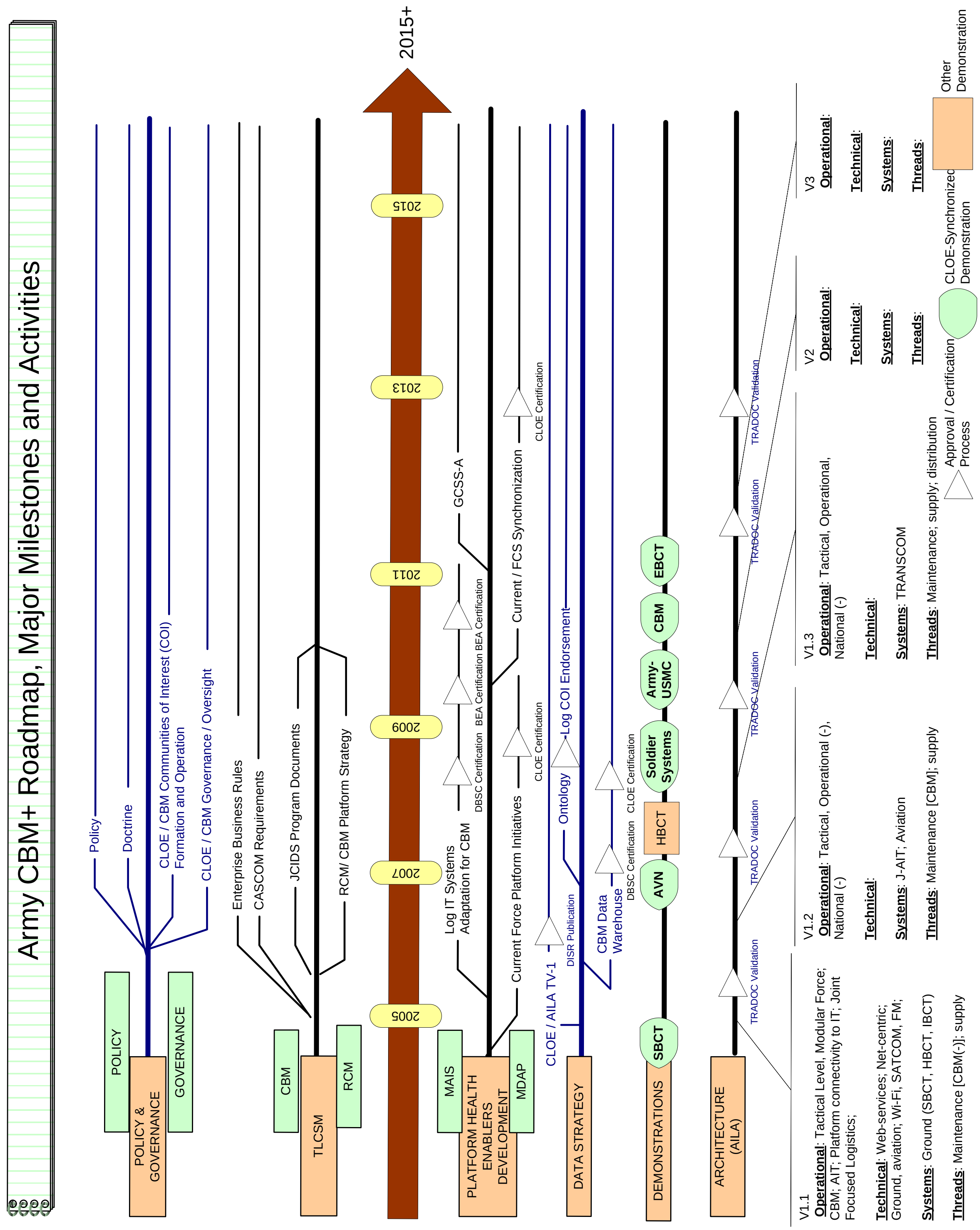
Section 2 is the CBM$^+$ roadmap, presented in a graphic format, with a “snapshot” assessment of current CBM$^+$ implementation status. The snapshot assessment points out instances where management and governance emphasis is required to achieve full CBM$^+$ functionality.

Section 3 describes essential elements of CBM$^+$, which when implemented will provide a functioning logistics common operating environment that is CBM$^+$-enabled.

Section 4 is a description of provisional CBM$^+$ roles and responsibilities, Army-wide, that facilitate CBM$^+$ implementation.

The roadmap will be available on the World-Wide Web at a Uniform Resource Locator (URL) address to be provided later.

Figure ES-1. Army CBM+ Roadmap, Major Milestones, and Activities



Contents

Figures

Tables

Section 1
Background and Vision

1.1 General

Condition-Based Maintenance (CBM) is a proactive equipment maintenance capability enabled by using system health indications to predict functional failure ahead of the event and take appropriate action. Potential actions range from “stop-now” to scheduling a repair at a time convenient to the mission profile. The capability marks an evolution from the earliest applications of embedded health management, as follows:

- *Diagnostic* capabilities are failure indications provided to the operating or maintenance crew by sensors or built-in tests (BIT) capabilities. The sensor or BIT indicates when something has failed. This is the level of capability included with the advisory caution lights in most modern automobiles: “Check Engine.” For military systems, it is what built-in test capabilities have provided for the past several decades.

- *Predictive* maintenance is based on trend analysis of historically collected data that, in the case of the Current Force equipment, uses sensors that were originally designed for diagnostic indications. Trend analysis is typically accomplished on-board in near-real-time circumstances or off-board by portable test equipment or at a data warehouse that archives sensor data. Off-board prediction is generally not a real-time process.

Predictive maintenance identifies impending failure, but does not predict when failure will occur.

The Army and the other military services are just now developing the capability for predictive maintenance.

Prognostics, on the other hand, are distinguished by being performed principally on-board as a real-time process, and are capable of analyzing component conditions and the prediction of failure based on the equipment’s real-time operating time-stress environment. The key difference between trend analysis of historical data and prognostic real-time analysis is that prognostic analysis is capable of estimating remaining useful life (RUL), including an accounting for the stress of operation that can significantly diminish calculated mean time between failure (MTBF). The Army, as are all military services, is evolving toward prognostic capability for CBM.

Diagnostic capabilities identify functional failures that have already occurred. Predictive capabilities identify impending functional failures without estimating remaining useful life, or time to failure. Prognostics capabilities identify impending functional failures with an estimate of time to failure, or remaining useful life.

This discussion of CBM does not attempt to describe in detail the distinction between predictive maintenance and prognostics, but it is an important distinction that the reader should be aware of.

Metrics for evaluating predictive and prognostic effectiveness are described in Section 3 as a part of the discussion about CBM$^+$ demonstrations in Tables 3-2 and 3-3.

1.2 The Distinction between CBM$^+$ and CBM

Two similar terms are used throughout this document. CBM is a maintenance paradigm. CBM$^+$ is a DoD initiative of many components that leverages the CBM concept and helps implement it. The following description may help to reinforce the distinction between the two terms.

CBM is most effective when accomplished in real-time, employing embedded health management sensors. However, CBM is routinely accomplished in the process control industry (oil, gas, chemicals, etc.) by at-system test tools in fixed plant installations. It involves a type of "condition monitoring" maintenance tasks, derived from Reliability Centered Maintenance (RCM).[1] CBM tasks are designed to identify the impending functional failure of operating equipment. The tasks can be accomplished by embedded sensors, special inspections or functional checks, or crew monitoring. CBM is focused on the portion of those tasks that can be automated through sensor installations.

CBM is a proactive equipment maintenance capability, enabled by using system health indications to predict functional failure ahead of the event and take appropriate action. Potential actions range from "stop-now" to scheduling a repair at a time convenient to the mission profile.

The CBM$^+$ initiative was established by the Deputy Under Secretary of Defense (Logistics and Materiel Readiness) (DUSD[L&MR]) and is aimed at enhancing the efficiency and effectiveness of CBM implementation through the application of enabling technologies, knowledge management, learning/training technologies, and life-cycle management processes.

Beyond the CBM tasks themselves, CBM$^+$ includes the additional infrastructures to make use of platform-generated information. This information provides operating commanders with unprecedented visibility into their fleet operating condition, enhancing force planning, and combat power. The information also feeds multiple business processes and provides performance information for problem analysis and performance optimization. Results include improved platform availability and reduced deployment footprint.

CBM$^+$ consists of three basic elements:

- *A rigorous methodology* for developing equipment maintenance task requirements, employing the structured decision logic process known as RCM. This methodology has four primary objectives:
    - Ensure realization of the inherent safety and reliability levels of the equipment.

[1] Nowlan, F. Stanley and Heap, Howard F.; *Reliability-Centered Maintenance*, published by United Airlines for the (then) Office of the Assistant Secretary of Defense (Manpower, Reserve Affairs and Logistics), 29 December 1978. Government accession number in the Defense Technical Information Service (DTIC) is ADA066579, available only in microfiche format at http://handle.dtic.mil/100.2/ADA066579 (25 megabytes). The RCM methodology has been updated and simplified over the years since it was originally published, see as an example Moubray, John, *RCM II*, Industrial Press, Inc., 1997, Second Edition, available from Amazon.com.

- Restore safety and reliability to their inherent levels when deterioration has occurred.
- Obtain information necessary for design improvement of those items whose inherent reliability proves inadequate.
- Accomplish these goals at minimum cost, including maintenance costs and the costs of resulting failures.[2]

- *CBM tasks*. Condition-monitoring tasks that are derived from the RCM methodology to monitor operating equipment to identify impending failure are called condition monitoring tasks. CBM is established when those tasks are monitored, with or without automation.
- *Infrastructure* to make use of sensor-based maintenance information. This infrastructure, consisting of numerous technologies and enablers, is what is meant by the "Plus" in CBM^{+}. Throughout this paper, the term CBM^{+} connotes both the CBM tasks and the related infrastructure.

The goal of CBM^{+} is to improve the availability of weapons systems throughout their life cycle and reduce cost. CBM^{+} supports not only the transition to an RCM/CBM maintenance strategy, but also provides the automation needed to improve maintenance productivity, reduce the deployed footprint required to provide maintenance services to combat units, and provide visibility of equipment status needed to implement anticipatory logistics concepts.

Office of the Secretary of Defense (OSD) has included the following enablers under its CBM^{+} initiative:

- RCM, from which CBM^{+} tasks are derived
- Diagnostics
- Prognostics
- Interactive Electronic Technical Manuals (IETMs)
- Data Analysis
- Automatic Identification Technology (AIT)
- Serialized Item Management/Item Unique Identification
- Integrated Information Systems
- Portable Maintenance Aid (PMA)

[2] Nakata, David, Vice President Consulting Services, EmpowerMX, *Can Safe Aircraft and MSG-3 Coexist in an Airline Maintenance Program?* White paper available at http://www.empowermx.com/whitepapers/CanSafeAircraft&MSG-3Coexist.pdf, undated, p. 2.

- Asset Visibility
- Interactive Training.

A new DoD Instruction 4151.XX is now in formal coordination and will mandate the implementation of CBM^+.[3]

This roadmap is focused on CBM^+ implementation. It minimizes references to basic CBM, except in instances where the two terms are contrasted, as in this section.

1.3 Maintenance Evolution toward CBM

CBM is not a new concept. It was articulated nearly 30 years ago, beginning with what is still regarded as a seminal study by Stanley Nowlan and Howard Heap[4] of maintenance practices in commercial airlines. Their book, published in the late 1970s, was based on commercial aviation experience and studies that began with the design of the Boeing 747 aircraft in the late 1960s. This work marks the origin of the term RCM. CBM is a process that has been used in industrial applications (outside commercial aviation) since the 1970s, and considered essential since the early to mid-1980s. In industry applications, the objective is to achieve maximum asset performance (availability) in order to realize maximum competitive advantage from a capital base. The same process is applicable to the military, with the distinction that mission requirements are usually more important than cost.

Development of CBM capabilities begins in the system design phase with a bottom-up assessment of equipment maintenance requirements (using RCM), informs the design process to design for reliability, and then designs for maintainability and CBM. This entails a rigorous assessment that must precede investment in CBM capabilities, as described below in the section describing the RCM context for CBM. Then the investment supports measures of effectiveness toward achieving enterprise goals, such as system operational availability. Appropriate goals and metrics are the key to evaluating the effectiveness of the investment.

The development process defines the way to assess, invest, measure, and obtain feedback about maintenance tasks and equipment performances until the desired goals are in hand. It is a continuous process for application through the equipment life cycle.

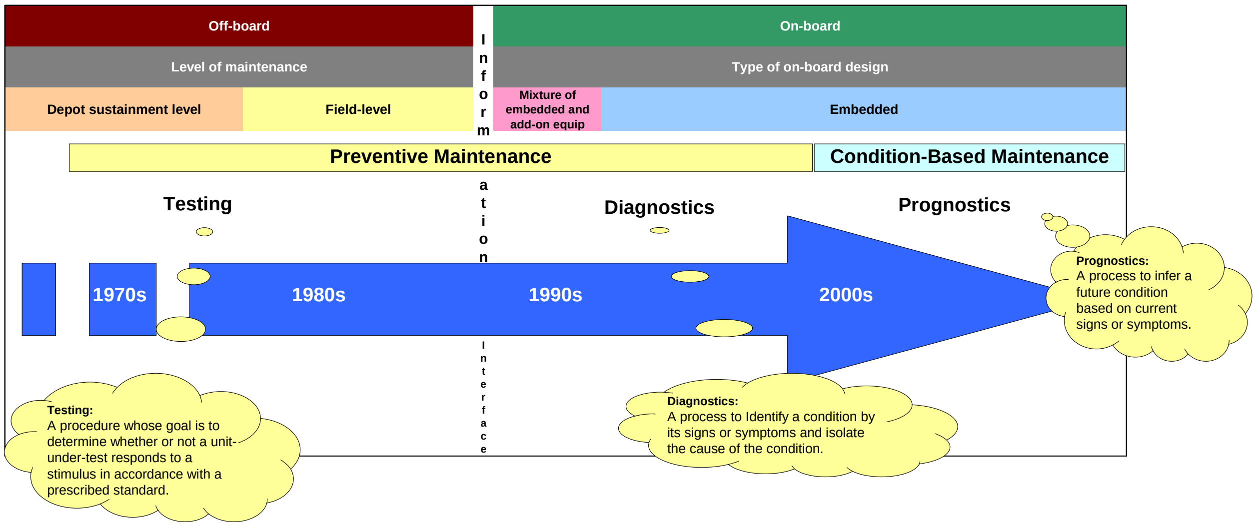
The process itself is under continual revision to reflect new management approaches, broader customer bases, and better application procedures.

Along the timeline from the 1960s to today, there have been a number of modernizing initiatives, from integrated diagnostics to embedded diagnostics and prognostics, as shown in Figure 1-1.

[3] Information about the OSD initiative is available at http://www.acq.osd.mil/log/mrmp/CBM%2B.htm.

[4] Nowlan, F. Stanley and Heap, Howard F.; *Reliability-Centered Maintenance*, ublished by United Airlines for the (then) Office of the Assistant Secretary of Defense (Manpower, Reserve Affairs and Logistics), 29 December 1978. Government accession number in the Defense Technical Information Service (DTIC) is ADA066579, available only in microfiche format at http://handle.dtic.mil/100.2/ADA066579 (25 megabytes). The RCM methodology has been updated and simplified over the years since it was originally published, see as an example Moubray, John, *RCM II*, Industrial Press, Inc.,1997, Second Edition, available from Amazon.com.

Figure 1-1. Military Maintenance Paradigm Progression



1.4 The CBM Maintenance Paradigm

CBM consists of a set of rigorously defined maintenance tasks, derived from RCM analysis. The tasks can be scheduled in response to accumulation of specified calendar time intervals or operating hours or mileage. Or they can be dynamically scheduled, based on the detection of a specified deterioration or operating condition.

Table 1-1 identifies the range of maintenance approaches that can be used to structure maintenance programs, including CBM.

Table 1-1. Maintenance Paradigms

Category	Reactive	Proactive		
	Run-to-fail	Preventive	Condition-based maintenance	
Sub-category	**Fix when it breaks**	**Scheduled maintenance**	**Predictive**	**Prognostic**
When scheduled	No scheduled maintenance	Static: based on a fixed time schedule for inspect, repair, and overhaul	Dynamic: based on current condition indicators	Dynamic: based on forecast of RUL
Why scheduled	N/A	Failure modes and equipment maintenance requirements predicted during design	Maintenance need is predicted, based on trend analysis of sensor data	Forecast of RUL does not support next mission
How scheduled	N/A	Modeling and simulation; no experience feedback loop	Continuous collection of condition-monitoring data	Based on real-time operating environment and stress loading indicators

1.5 CBM Purpose

The principal goal for CBM, in the military as in industry, is to achieve the highest possible return on capital assets. In the military, that goal translates to maximizing equipment operational availability while minimizing the logistics footprint and doing these things in a reduced manpower environment. Although specific return on investment data has historically been difficult to cite, recent instrumented tests in the Army aviation community indicate a four to five percent increase in operational readiness in CBM-capable aircraft. This translates to an increase in combat power by an additional battalion of aircraft available to an aviation brigade.[5] Similar results were obtained from simulation and modeling analysis performed in support of a Stryker Brigade Combat Team Proof of Enablers and Technical Test and Demonstration in the fall of 2004.[6]

Maximizing operational availability has two important facets. During equipment design, RCM applications minimize scheduled maintenance requirements and the out-of-service time required for inspections. During equipment operation, embedded platform health management capabilities can be applied to anticipate failure and take proactive action that results in a significant total maintenance time savings. A most powerful benefit of CBM is the compression of equipment non-available time. In a CBM enabled environment, Non-Mission Capable–Supply (NMCS) time will be significantly reduced as the prognostics initiate the request for repair part/support process prior to equipment failure while the system remains in an operational state.

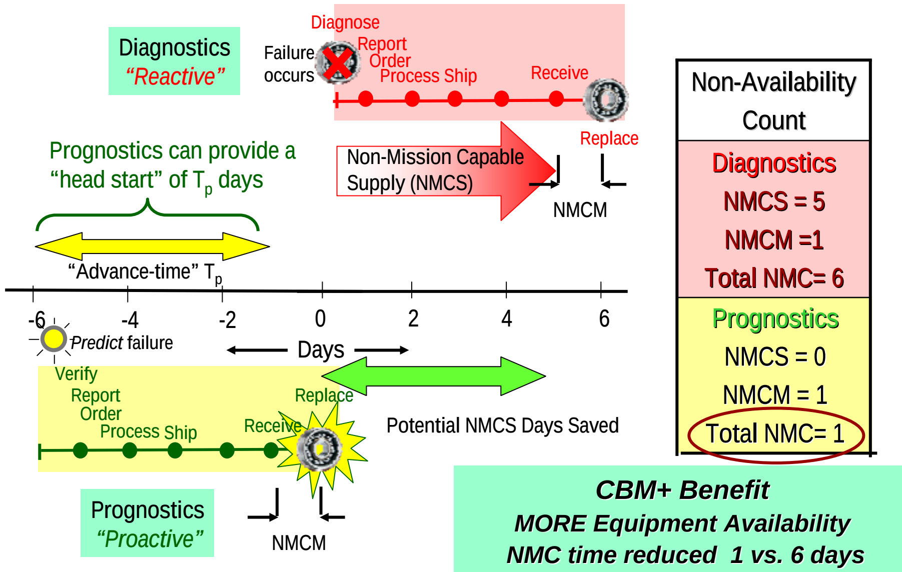
The impact of CBM on equipment availability is shown in Figure 1-2. As shown on the upper level of the timeline, in a current maintenance environment, an operating unit can experience an unanticipated failure and consume a total of 6 non-mission capable days, of which 5 of those days are supply days (processing and waiting for the part). However, in the lower half of the timeline, only a single day of readiness is lost because the CBM capabilities, along with the RCM analysis, predicted the failure of the part and ordered the part prior to failure while the system was still in an operational status. In this figure, the term “prognostics” is used in the generic sense of predicting a failure as a function of CBM.

---

[5] Chandler, Jerome Greer, “Condition-Based Maintenance,” *Overhaul and Maintenance Magazine*, The McGraw-Hill Companies, New York, 3 January 2007.

[6] U.S. Army Logistics Transformation Agency (now Logistics Innovation Agency), *Stryker Brigade Combat Team Proof of Enablers Technical Test and Demonstration, After-Action Report,* 9 June 2005, p. 7-5.

Figure 1-2. CBM Reduces NMCS, Increases Operational Availability



The benefits of increased combat power are also attributed to a reduction in maintenance operational test or test flight hours, vibration check man-hours, and overall inspection man-hours.

1.6 Relationship of CLOE to CBM+

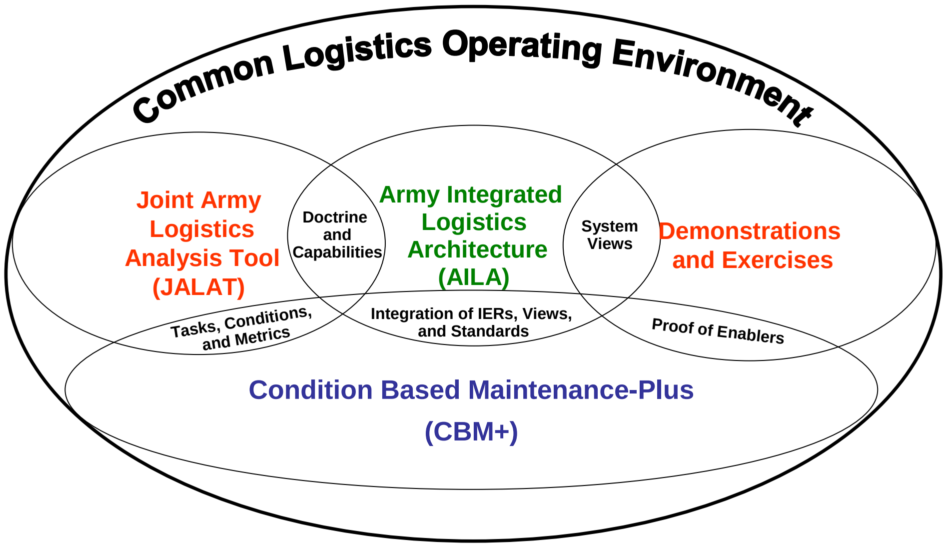
The Headquarters, Department of the Army, Deputy Chief of Staff (DCS), G-4, serves as the chief Army Sustainment Officer. Among other things, the G-4 is responsible for developing the Army Common Logistics Operating Environment (CLOE).[7] In turn, CLOE is based on an integrated DoD Architecture Framework architecture to comply with the Joint Capabilities Integration and Development system (JCIDS)[8] process. The G-4 has designated the Army Logistics Innovation Agency (LIA) as the lead for CLOE development. CLOE is engaged in developing the Army Integrated Logistics Architecture (AILA), which encompasses CBM+ functionality. CBM+ capability is integral to the AILA and that architecture is the bedrock upon which enterprise-wide CBM+ capability is built. Verifying CBM+ functionality on a platform-by-platform basis or as a function of enterprise operation is achieved by CLOE-compliant development and testing.

The CBM+ underpinning in the AILA is reflected in Figure 1-3. The information architecture is the means to integrate information exchanges that support CBM+ functionality with the rest of the Army sustainment system. CBM+ is also a capability that must be reflected in capability analysis and assessment (represented by the Joint Army Logistics Analysis Tool [JALAT]) as well as demonstrations and exercises that apply the capability. Taken together, these tools and processes assure CBM+ is an integral part of the Army common logistics operating environment.

[7] Headquarters, Department of the Army, Assistant Secretary of the Army for Acquisition, Logistics and Technology, (ASA[ALT]) Memorandum, DALO-SMM, Common Logistics Operating Environment Capabilities and Standards, 25 July 2003.

[8] Chairman of the Joint Chiefs of Staff Instruction 3170.01F, *The Joint Capabilities Integration and Development System*, 1 May 2007, available at http://www.dtic.mil/cjcs_directives/cdata/unlimit/3170_01.pdf

Figure 1-3. The AILA Builds-in Foundational CBM⁺ Capabilities



Note: IER = Information Exchange Requirement.

Section 2
CBM$^+$ Roadmap

2.1 Overview

The roadmap that is graphically displayed in Figure 2-1 lays out the elements of CBM$^+$ that were discussed in the previous section on a general timeline. Only the major elements of the CBM$^+$ strategy are shown here. A snapshot of where the Army is today is shown in Figure 2-1. These views will be refined as a part of the development of a CBM$^+$ implementation plan in the coming months. The plan will address overall timelines and implementation tracking that will be produced in response to this roadmap.

2.2 Suggested CBM$^+$ Path Forward

This roadmap is the first step in Army-wide implementation of CBM$^+$ capabilities. It will be the focal point for stakeholder coordination that will lead to the issuance of the CBM$^+$ implementation plan. Resource requirements from the plan will be considered for the Program Objective Memorandum (POM) exercise for fiscal years 2010–2015.

Several organizational and process tools will facilitate this process.

- Formation of an Army CBM$^+$ oversight body will serve to synchronize approaches and requirements in a structured process similar to a Joint Service user community. The DCS G-4 will lead the establishment and operation of this body.

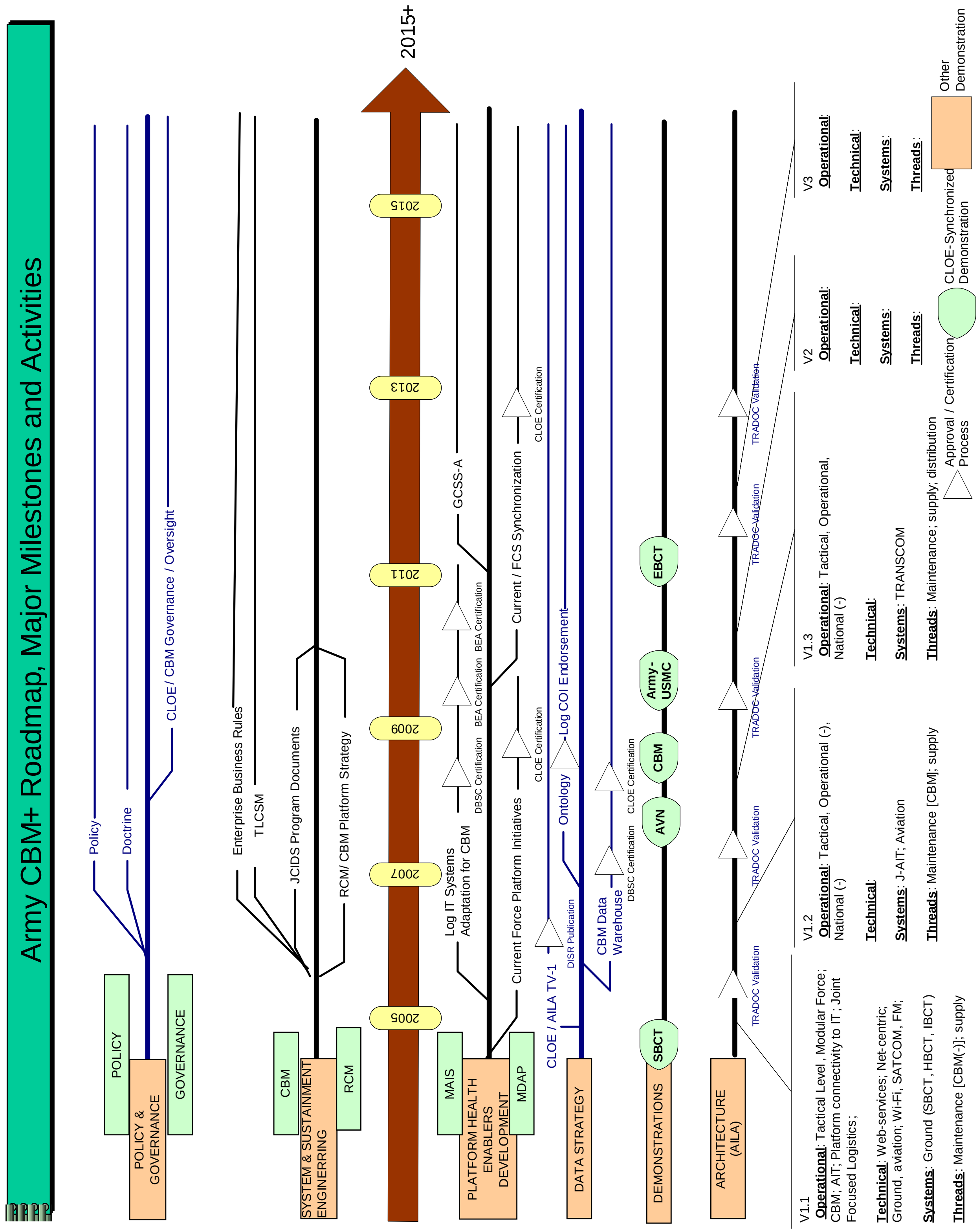
- Army Logistics Innovation Agency, in its role as the G-4 lead for CBM$^+$ implementation, will establish a means to track major initiatives and produce progress assessments.

- A CBM$^+$ implementation "dashboard" will assist in providing an assessment of implementation progress at various levels of indenture.

- Completion of major revisions to Army policy, doctrine, and capability requirements will support the POM initiative.

A major step in implementation of the CBM$^+$ concept will be the formative meeting of the Army logistics user community, to refine the roadmap elements and the detailed planning associated with a CBM$^+$ Implementation Plan.

Figure 2-1. Army CBM+ Roadmap, Major Milestones, and Activities



2.3 Milestones and the CBM$^+$ View Ahead

The roadmap graphic reflects a timeline from 2005 through 2015. The elements of the roadmap depicted in the lower half of the graphic, below the timeline, are technical in nature, including:

- System (Platform) Health Enablers
- Data Strategy
- Demonstrations
- Architecture.

In the upper half of the graphic, management and governance categories include:

- Policy and Governance
- Total Life Cycle Systems Management (TLCSM).

We briefly introduce each of these categories to orient the reader to Figure 2-1.

2.3.1 Policy and Governance

These two elements are intertwined, yet separate issues. Army policy for Condition-Based Maintenance and CBM$^+$ is being inserted into Army literature on many levels, placing increasing emphasis on the need to harmonize and de-conflict guidance. Publishing literature is one thing; establishing and operating collaborative management mechanisms and governance oversight bodies and then making them operational is another. The timeline in this category shows policy and governance development as an open-ended and continuous process.

2.3.2 Total Life Cycle Systems Management

TLCSM for CBM$^+$ has two significant branches, one of which is for reliability-centered maintenance (RCM), the other is for CBM$^+$ itself.

RCM is described in a later section as the up-front engineering analysis from which CBM$^+$ processes and CBM tasks are identified and described. For Major Defense Acquisition Programs (MDAPs), both RCM and CBM tasks must be described in DoD Acquisition System and JCIDS documents. The fundamental documents are the Systems Engineering Plan (SEP) and the Test and Evaluation Master Plan (TEMP). Each of these documents must be updated at Acquisition Milestones (MS) B and C, using the Capability Development Document (CDD) at MS B and the Capability Production Document (CPD) at MS C. This process is shown in Figure 3-17 in the next section.

The timeline in Figure 2-1 for TLCSM shows a need for these documents as a recurring element of MDAP planning for CBM$^+$ capability injection and the living document nature of RCM planning.

In addition to JCIDS document update cycles, business rules for CBM and requirements for acquiring CBM and CBM$^+$ capabilities need to be fleshed out. This is shown on the top half of the TLCSM timeline.

2.3.3 System (Platform) Health Enablers

The AILA acts as a guide and informs the systems engineering design process required for CBM^+ capability by incorporating embedded system health enablers (Major Defense Acquisition Programs) and Army logistics information technology (IT) systems (Major Automated Information Systems [MAIS]). Major increments and capabilities of the AILA are shown in this timeline.

CBM^+ requires synchronization between the Current Force and the Future Force, as well as synchronization between the warfighter and Business Mission Areas. The types of certification of interoperability in each Mission Area are shown on the timeline in this category.

2.3.4 Data Strategy

CBM^+ capabilities for MDAPs and MAISs are acquired by separate program or product managers (PMs), constrained for interoperability by the standards and interfaces that are embodied in the AILA. The CBM^+ capabilities support the development of a net-centric data strategy. This strategy is perhaps the single most important element necessary to achieve interoperability throughout the enterprise.

Policy for the DoD net-centric data strategy revises the old approach to data standardization accomplished by data administrators. The net-centric approach identifies visibility, accessibility, and understandability in addition to standardization.[1]

The net-centric data strategy is premised on new and unanticipated ways to access and use existing data. The central idea is to increase the potential for other systems to access data by "discovering" it when such data is needed.

The vision of the net-centric data strategy is predicated on these key elements:

- Metadata (descriptive data that identifies a data item as to use and meaning)
- Communities of Interest (COIs) to manage the metadata definition and tagging process
- Global Information Grid Enterprise Services (GIG ES) that enable data tagging, storing, sharing, searching, and retrieving.

The concept and employment of metadata is the basis for a net-centric data strategy. Metadata is data about data—a way to describe data to make it understandable and searchable, and also to make it rank-able, meaning that data can be rank-ordered from most-relevant to least-relevant.

The idea behind metadata is that a search engine, which is the principal tool today for searching the Web for content, must be able to sort out the relevant from the irrelevant for any given search criteria. It does that in part by using metadata. Where metadata exists today, it improves the quality of the search. When it's not available, and that is largely the case today, the search is less effective. We are flooded with information, but not enough metadata to organize it or make it navigable.[2]

[1] Department of Defense, Chief Information Officer (CIO), *Net-Centric Data Strategy*, 9 May 2003.

[2] Charles Goldfarb, *XML Handbook*, 4th Edition, Prentice-Hall, 2002.

The timeline in this category shows key process and certification milestones along the path toward full net-centric CBM^{+} capability.

2.3.5 Demonstrations

Demonstrations of system health management provide real-world test and measurement of CBM^{+} capabilities and interoperability. These demonstrations have been called proof of enabler (PoE) demonstrations. They test the accuracy and effectiveness of the architecture as well as the CBM^{+} capabilities and systems interoperability. At the present time (summer 2007), one PoE demonstration has been conducted for the Stryker brigade combat team (SBCT) and one is pending for Army aviation. Additional demonstrations are planned on a periodic basis as shown on the timeline for this category.

2.3.6 Architecture

The major strategic elements of the CBM^{+} roadmap are centered on the development of an integrated DoD Architectural Framework (DODAF) architecture for Army logistics, the Army Integrated Logistics Architecture. The AILA is being developed in increments, with increasing scope and depth as time progresses. The AILA first increment of CBM^{+} capability began with a focus on the tactical echelon and ground combat platforms operating in an SBCT. Subsequent increments of the AILA have expanded the AILA's scope, both horizontally (increasing equipment and systems reach, e.g., Joint Automated Information Technology [J-AIT], aviation) and vertically, including additional echelons above brigade.

2.3.7 Overarching Goals and Objectives

There are a number of overarching goals and objectives in a PoE demonstration, including:

a. Demonstrate the integration of Systems Architectures with the Operational and Technical Architectures for a given set of systems and CBM^{+} capabilities

b. Establish threshold functionality for Current Force embedded platform health management (EPHM) in operational deployment scenarios

c. Verify that information exchange requirements (IERs) for CBM are in place and work as planned

d. Measure the benefit of embedded health management and CBM for current force platforms

e. Promote technology maturation for promising platform health management efforts in Condition-Based Maintenance

f. Verify net-centricity and end-to-end connectivity throughout the Army logistics enterprise

g. Establish mechanisms for collaboration between PM-Future Combat Systems and Current Force PMs and Program Executive Officers (PEOs) to act as a risk-mitigation process for Future Combat Systems (FCS) technology spin-out to the Current Force.

2.3.8 Metrics Used in Demonstrations

- Compliance to IERs
- Operational availability rate (A_O)
- Mean-time-to-repair (MTTR)
- No-evidence-of-failure rate (NEOF)
- Customer wait time (CWT)
- Sortie-generation rate (SGR)
- Combat power
- Supply Chain Operations Model (SCOM)
- Balanced Scorecard.

Beginning in 2008, this roadmap reflects a cycle of annually testing, demonstrating, and evaluating the integration of Systems Views with AILA Operational and Technical Views to verify interoperability of the AILA constituent parts. This cycle of testing and demonstrating also verifies the synchronization of the AILA with joint logistics architectures and systems as well as successful architecture federation at the Operational and National-Strategic levels.

This process supports the Army portion of testing to ensure IER interoperability as required for the Director, Command, Control and Communications Systems, the Joint Staff (J-6) supportability certification.

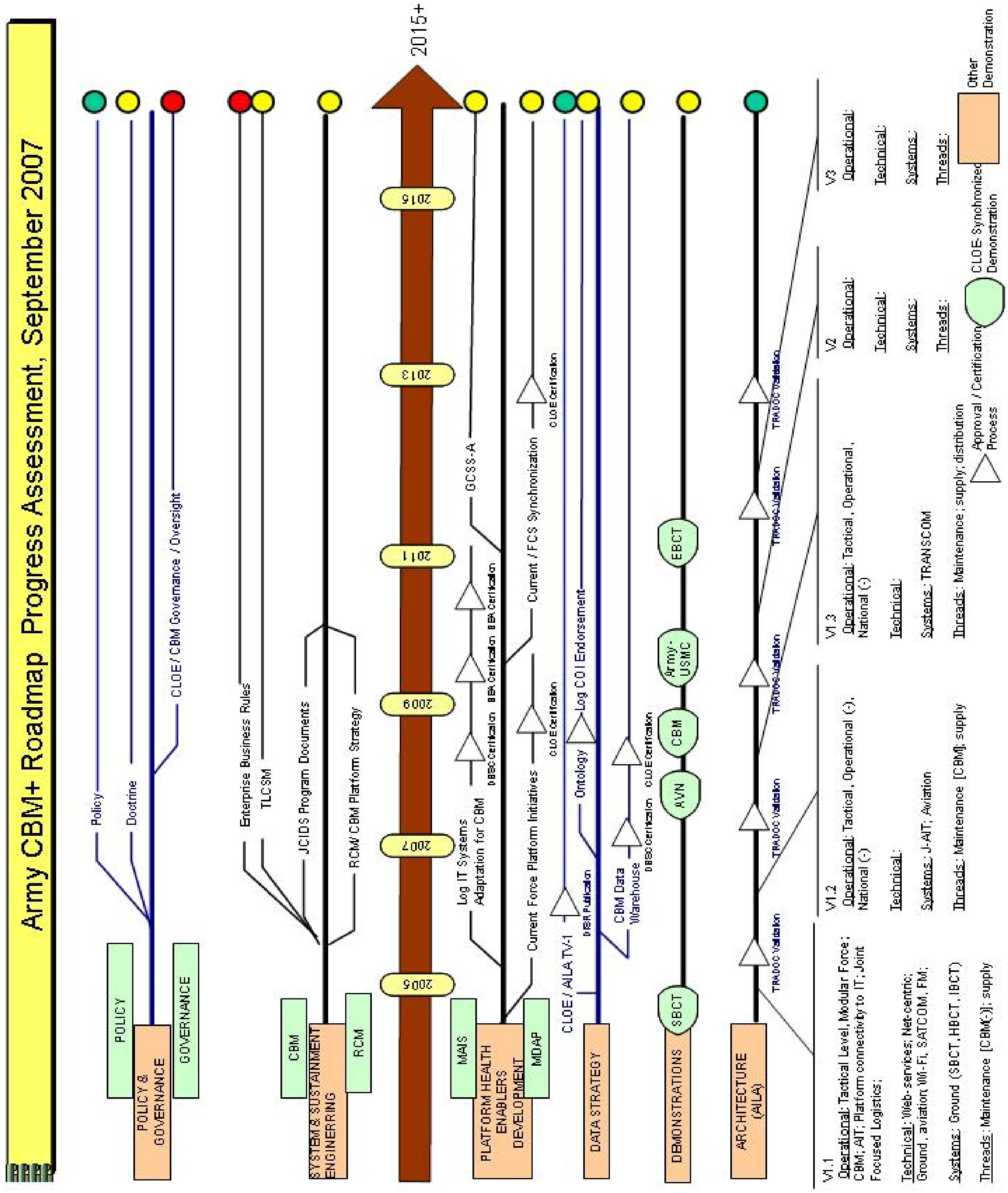
2.4 Snapshot Assessment Rationale

Figure 2-2 portrays a “snapshot” assessment of Army CBM$^+$ implementation status, as of summer 2007. The snapshot is based on current working knowledge of each element within the CLOE program. The following summary provides a capsule rationale for each of the red-amber-green assessments in the figure.

- Policy—Development is well underway with revisions in work or completed for a substantial range of Army policy documents.
- Doctrine—Doctrinal development is in process.
- CLOE/CBM Community of Interest—Not yet formed. CBM Integrated Product Team (IPT) chaired by Logistics Support Activity (LOGSA) is a first step toward full Army IPT structure.
- CLOE Governance/Oversight—Established but not yet exercised on an Army-wide basis.

- Enterprise Business Rules—Not yet defined, particularly as applied to funding (e.g., definition of serviceable credit for remaining useful life).
- Combined Arms Support Command (CASCOM) Requirements—In process.
- JCIDS Documentation—Functional concepts and individual programs are just beginning to address appropriate requirements in JCIDS process.
- RCM Platform Strategy—Pending implementation of Office of the Secretary of Defense and Army RCM instructions and guidance.
- Logistics IT Systems Adaptation for CBM–Integration of information exchange requirements for CBM^+ with AILA in work.
- Current Force Platform Initiatives—Cohesive program integration planning is in work but only partially programmed. Current to future force synchronization is a work in progress.
- CLOE/AILA TV-1—Published with several revisions, vetted with other Army programs and the Army G-4 and CIO/G-6 Chief Information Officer.
- Ontology—AILA OV-7 and SV-11 development on schedule; CBM Ontology IPT in progress; Logistics Ontology to be determined.
- CBM^+ Data Warehouse—Demonstrations ongoing with implementation to follow.
- Demonstrations—SBCT demonstration complete; aviation demonstration complete; Heavy Brigade Combat Team (HBCT) COBRA demonstration being planned; and CBM^+ data demonstration also being planned.
- Architecture (AILA)—Being developed on schedule and on budget, being fully coordinated with CASCOM and Army Training and Doctrine Command (TRADOC) and being coordinated with Army and Joint stakeholder organizations.

Figure 2-2. Snapshot Assessment of Army CBM⁺ Implementation Status



2.5 Implementation Considerations

As shown in the two previous figures, CBM^+ implementation is a complex multi-year endeavor, representing an objective that is mid-term and beyond (2010–2015 plus) in the Army's transformational journey.

Successful implementation depends on synchronization of a number of interdependent actions. Although CBM^+ is not a "system" *per se*, its many components must be treated in a systematic fashion, spanning from system design to sensors in equipment to data warehouses to analytic and decision support tools in life cycle sustainment management at the enterprise level. CBM^+ is a transformational concept for enterprise sustainment. The CBM^+ implementation lanes focus on policy and governance, platforms and technology, and integration into an end to end architecture.

CBM^+ is designed to be more effective in a "net-centric" environment. It supports net-centric warfare concepts by enabling near-real-time visibility of platform operating status and improving mission reliability. CBM^+ relies on the exchange of platform data to various places throughout the enterprise and its supporting architecture. The milestones and activities along the CBM^+ implementation timeline will require full enterprise depth and integration to enhance support to the warfighter with aligned maintenance processes and redefined business processes.

The end state for CBM^+ implementation is a transformational maintenance concept where maintenance planning, maintenance execution at both the Field and Sustainment levels, and the supporting business processes are based upon condition-based approaches, while preventive and reactive maintenance tasks are fewer and less frequent. Near-term system readiness is clear and visible with a minimized maintenance footprint.

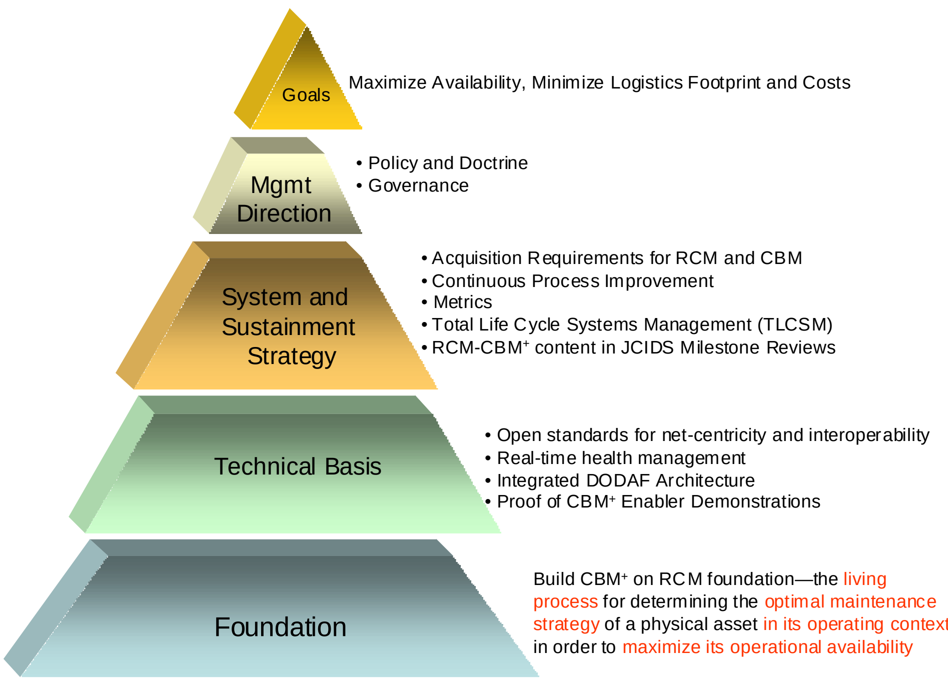
With that background, Section 3 addresses the essential elements of a CBM^+ implementation, and Section 4 addresses the roles and responsibilities for successful implementation.

Section 3
Essential Elements of Condition-Based Maintenance Plus

3.1 Overview

The management strategy for achieving the transition to CBM+ is depicted in Figure 3-1. The strategy is based on establishing Army policy for Reliability Centered Maintenance (RCM) as the foundational process that analyzes, selects, prioritizes, and refines CBM+ tasks and processes throughout the equipment production, deployment, sustainment, and operational phases.

Figure 3-1. CBM+ Strategy



As the figure depicts, the management direction, systems and sustainment engineering strategy, and technical basis for CBM+ all rest on the RCM foundation. The remainder of this section addresses each element of the strategy in turn.

This section addresses an approach to achieving CBM+ capabilities in the Army, leaving the "how" to be addressed in a follow-on implementation plan.

3.2 RCM Foundation

3.2.1 General

Reliability Centered Maintenance (RCM) analysis establishes the operational importance of the equipment in an organizational/mission context. It does so as it assesses the consequences of equipment failure. In that light, RCM can be described as setting the business case for CBM task selection—it is the process by which applicable and effective tasks are selected to mitigate failure consequences.

In RCM, the impact of equipment failure is assessed at the bottom line (both financial and operational). Failure modes that impact operational availability determine the nature of the maintenance task. Tasks that are most critical to operational availability are the ones that will justify installation of embedded sensors and become CBM tasks, e.g., predictive maintenance tasks.

RCM guidance is currently published in multiple documents, including those from the Society of Automotive Engineers (SAE) International,[1] the Naval Sea Systems Command,[2] the Naval Air Systems Command,[3] and the National Aeronautics and Space Administration.[4] Naval Air RCM guidance mirrors the SAE RCM standard. A recent revision to Army Regulation 750-1, *Army Materiel Maintenance Policy*,[5] also mandated the SAE standards.

3.2.2 The RCM Context for CBM

RCM is a master set of principles and processes by which an enterprise analyzes its physical assets and determines the optimum maintenance strategy for them, including how and where to implement CBM. Figure 3-2 illustrates the elements of the RCM process.

The hub of the figure is RCM itself. RCM uses a structured decision process to assess how equipment can fail and what happens when it does. The process assigns “applicable and effective” maintenance tasks to mitigate or avoid failure consequences and provides feedback to the equipment design process when maintenance tasks alone will not ameliorate the risk of failure.

For the purposes of the graphic, the RCM process generates maintenance tasks that can be characterized as preventive, corrective, or alternative. Alternatives include a continual search, based on operating performance history, for better “applicability and effectiveness” over the operating life cycle of the platform or system. Sometimes, that kind of analysis leads to requirements for changes in configurations (e.g., installation of a new sensor), in addition to adjustment and refinement of existing maintenance task requirements.

---

[1] SAE International, Surface Vehicle/Aerospace Standard JA1012, *A Guide to Reliability-Centered Maintenance*, revised 2002; and Surface Vehicle/Aerospace Standard JA1011, *Evaluation Criteria for Reliability-Centered Maintenance (RCM) Processes*, 1999.

[2] MIL-P-24534A, *Planned Maintenance System: Development of Maintenance Requirement Cards, Maintenance Index Pages, and Associated Documents*, dated 07 May 1985.

[3] Naval Air Systems Command (NAVAIR), NAVAIR Management Manual 00-25-403, *Guidelines for Naval Aviation RCM*, 1 July 2005.

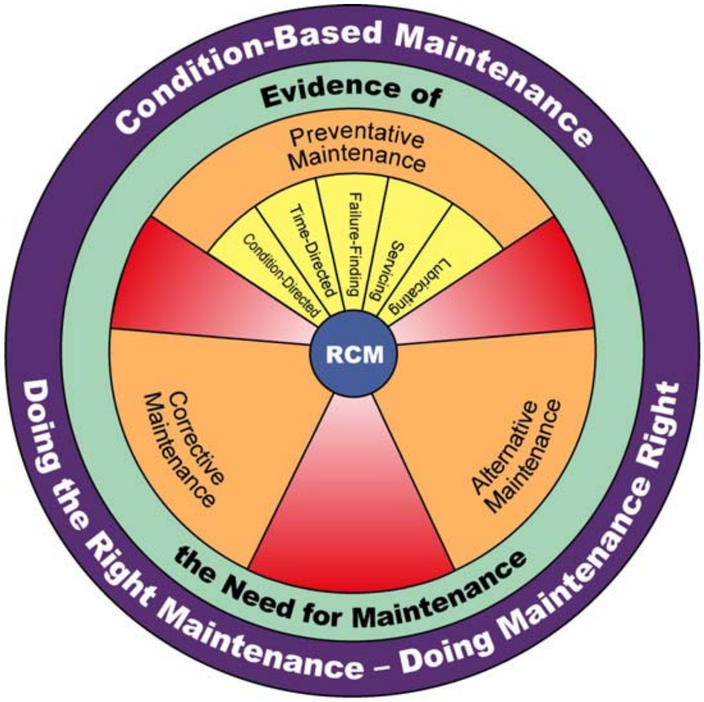
[4] NASA, *Reliability-Centered Maintenance Guide for Facilities and Collateral Equipment*, February 2000.

[5] Current version available at http://www.apd.army.mil/series_range_pubs.asp?range=750.

Ideally, maintenance tasks are triggered by evidence of need rather than a "just in case" approach. For tasks that support CBM, that evidence can be provided by the embedded health management system, or through off-board analysis of performance data.

Taken together, these elements support a robust CBM implementation.

Figure 3-2. Reliability Centered Maintenance Is the Hub of CBM



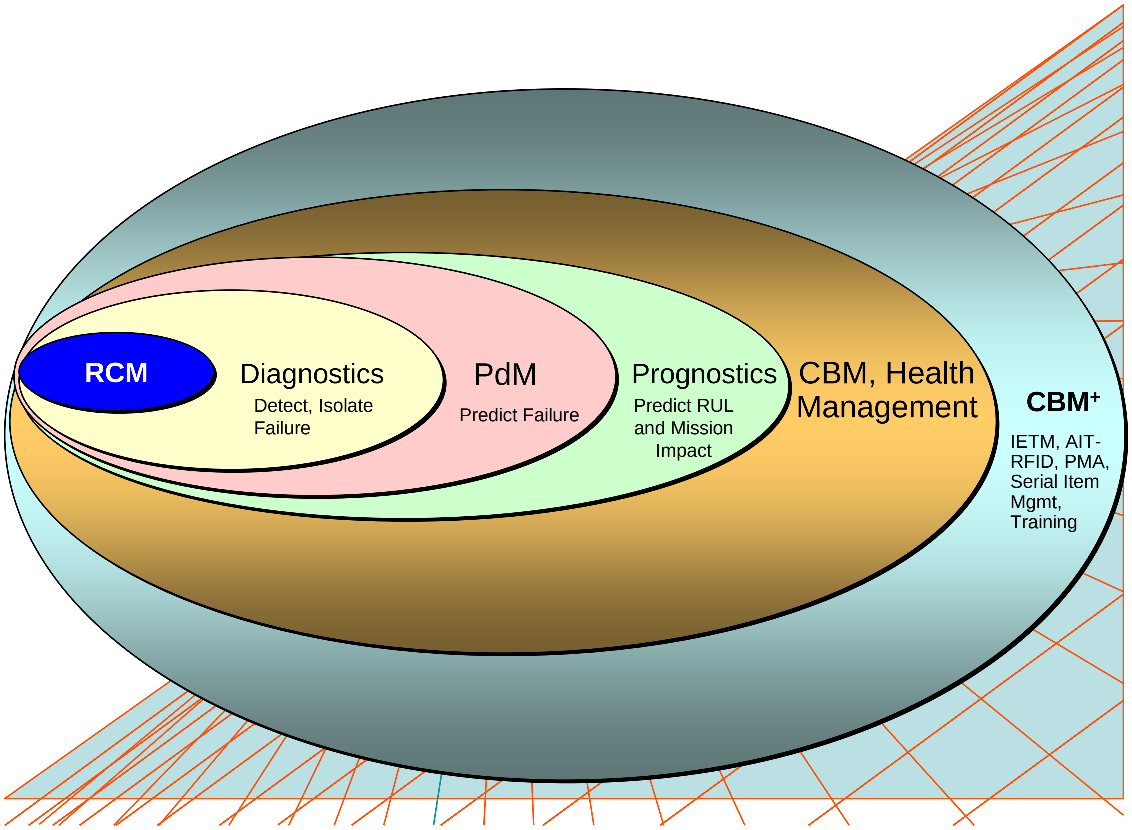
Source: Jacobs, Kenneth, U.S. Naval Sea Systems Command, Surface Ship Maintenance Division.

CBM as a maintenance strategy is typically applied to high-value failures—which are not necessarily the same as high-value components. High-value failures have the greatest impact on the metric of choice, whether cost of operation, mission performance, operational availability, or some other value basis. It is also possible to use manual inspection techniques (e.g., visual inspections or functional tests) to perform classic CBM tasks. The decision to automate a CBM maintenance task by installing platform sensors should be based on a cost-benefit analysis as a part of equipment design.

Systems and platforms that are not equipped with embedded sensors can still benefit from the off-board analysis of operating performance, using CBM analytic processes.

RCM is the foundational platform analytical process for logistics analysis and life-cycle support. It helps determine a maintenance strategy to include when and how to apply CBM^+ techniques to platform systems and subsystems. The relationship of RCM to CBM and CBM^+ is shown in Figure 3-3.

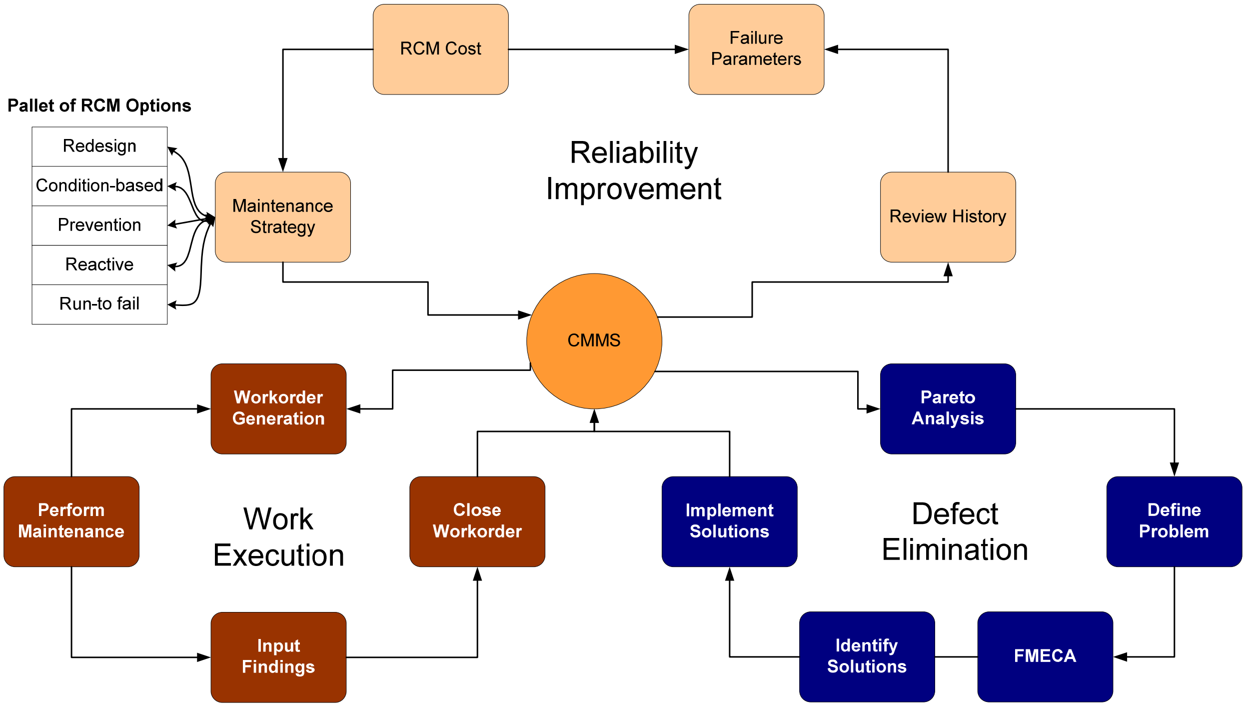
Figure 3-3. Envelope of RCM, CBM, and CBM+ Capabilities



Notes: IETM = Interactive Electronic Technical Manual; PdM = Predictive Maintenance; PMA = Portable Maintenance Aid; RFID = Radio Frequency Identification; RUL = Remaining Useful Life.

RCM is a living process that begins during the design phase of acquisition and continues through the operations and maintenance phase of the equipment life cycle. Life cycle applications depend on continuously collecting and analyzing failure and performance data for feedback and root cause analysis. The analysis supports identification of adverse trends, “bad actors” and other performance degraders, and initiates remedial actions that can include component redesign for increased reliability, as well as selecting or revising the appropriate maintenance strategy for a given failure mode. The process is depicted in Figure 3-4.

Figure 3-4. The RCM Process

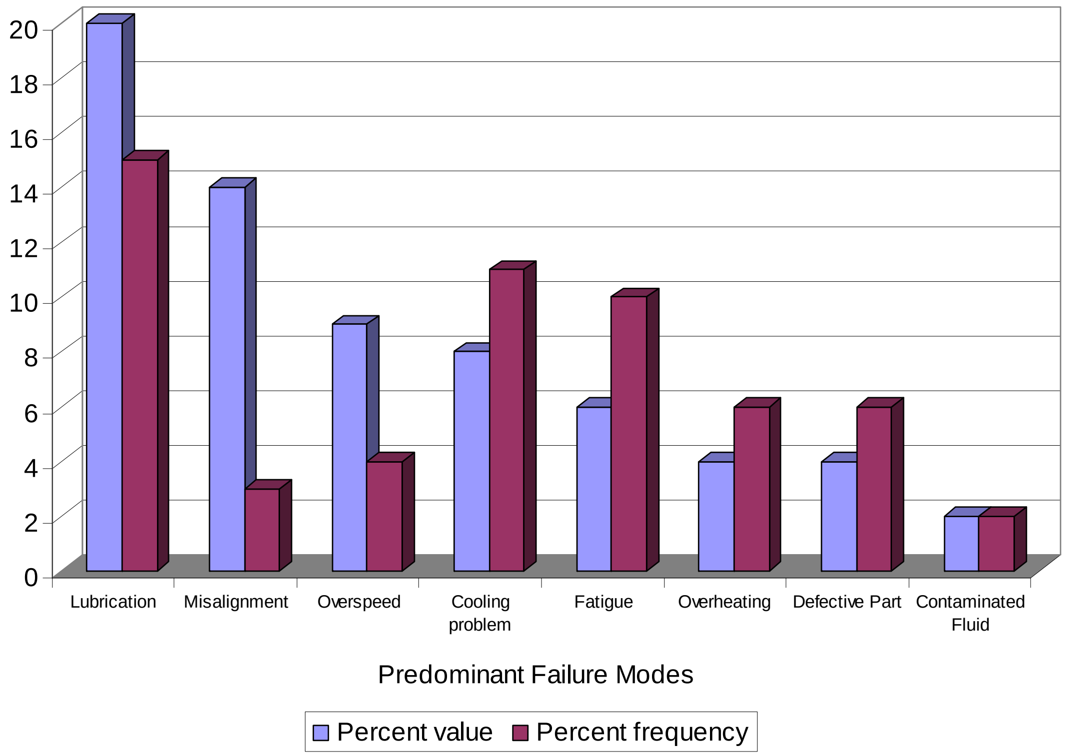


Source: M. Drew, Reliability Tools, Asset Reliability, and Maintenance Specialists (ARMS) Reliability Engineers, Ltd.
Note: CMMS = Computerized Maintenance Management System.

The first objective of RCM is to realize the inherent safety and reliability levels that have been built into a platform or system. One aspect of this objective is to identify and eliminate defects that degrade that inherent level of performance. The process of defect elimination is underpinned by a Pareto analysis that partitions failures into classes by value, weighted by some metric, typically cost or operational impact. This leads to a root cause analysis that identifies the reasons for the failure identified as having the greatest impact on whatever metric was used for evaluation.

In Figure 3-5, percent value indicates how much value a particular failure mode contributes to poor operation, high cost, etc., relative to the enterprise. The figure, as an example, portrays lubrication problems not only cause the most damage, they occur with the greatest frequency.

Figure 3-5. Pareto Distribution of Values and Frequency of Failure Modes



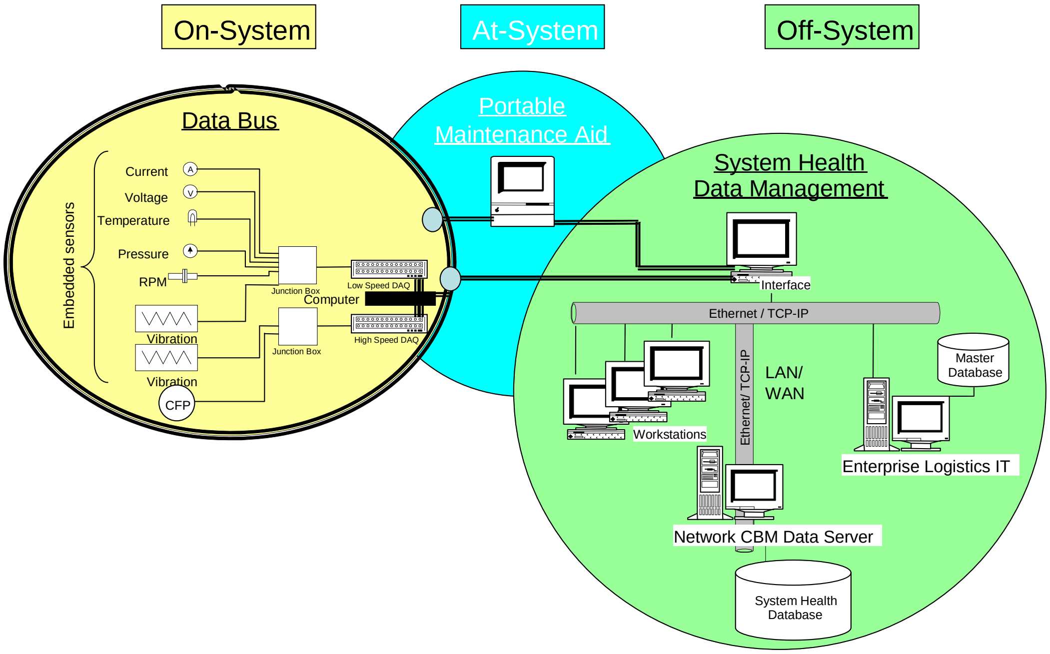
Source: SmartSignal Corporation.

3.3 Technical Basis for CBM$^+$: Major Capabilities Required to Implement CBM$^+$

3.3.1 General

CBM$^+$ is a collection of systems which are connected and made interoperable through an integrated common logistics operating environment (based on DODAF architecture) that ranges from on-board sensors and related hardware and software in platform equipment to off-board information warehouses and decision support tools in life cycle management centers at the enterprise level. The three basic levels in the CBM$^+$ "system" are illustrated in Figure 3-6.

Figure 3-6. CBM$^+$ System Block Diagram



Notes: A = amperage, CFP = Common Fieldbus Protocol, DAQ = data acquisition, LAN = local area network, RPM = revolutions per minute, TCP-IP = Transmission Control Protocol-Internet Protocol, V = voltage, WAN = wide area network.

3.3.2 On-At-Off System Components

3.3.2.1 On-System

Embedded software on platforms and major components assesses the "condition" of the equipment using information from built-in test equipment, sensors, and other usage data. This information is shared with command and control (C2) systems to permit automated status feeds to the tactical and logistics common operating pictures (COP and LCOP). Information shared with the platform C2 system is generally exceptional/report data, and does not include all available CBM$^+$ data. Software on the system interprets sensor readings and other operating parameters to indicate existing or potential malfunctions. Operating and maintenance data is captured and stored for future analysis off-platform.

3.3.2.2 At-System

Portable maintenance aids augment the on-board systems, although they typically do not operate in real time. They support both condition-based and corrective maintenance tasks. The suite of maintenance aids could include portable computers, portable test equipment, and software. Maintenance aids support both operator-level and maintainer-level maintenance tasks. Aids for maintainers provide capabilities to perform tests and analyses not available from on-board systems.

Maintenance aids include both on-system software and portable computers and software used at-system. The at-system portable computer used by maintainers is called a Portable Maintenance Aid (PMA) in CBM$^+$ policy documents. The PMA hosts the software used by maintainers to carry out at-system maintenance tasks such as condition monitoring, diagnostics, prognostic analysis of platform data, and fault isolation and repair.

3.3.2.3 Off-System

Data pulled from platforms and equipment is used at the field level to schedule maintenance and manage readiness. The data is also passed over the communications/information infrastructure to a national-level data warehouse. Life cycle managers, original equipment manufacturers, and others use analysis and decision support tools to “mine” the data to identify adverse trends, improve diagnostic routines, identify targets for product improvement programs, refine maintenance plans, establish budgets and inventory levels for repair parts, issue maintenance bulletins, and to plan and budget rebuild and reset programs.

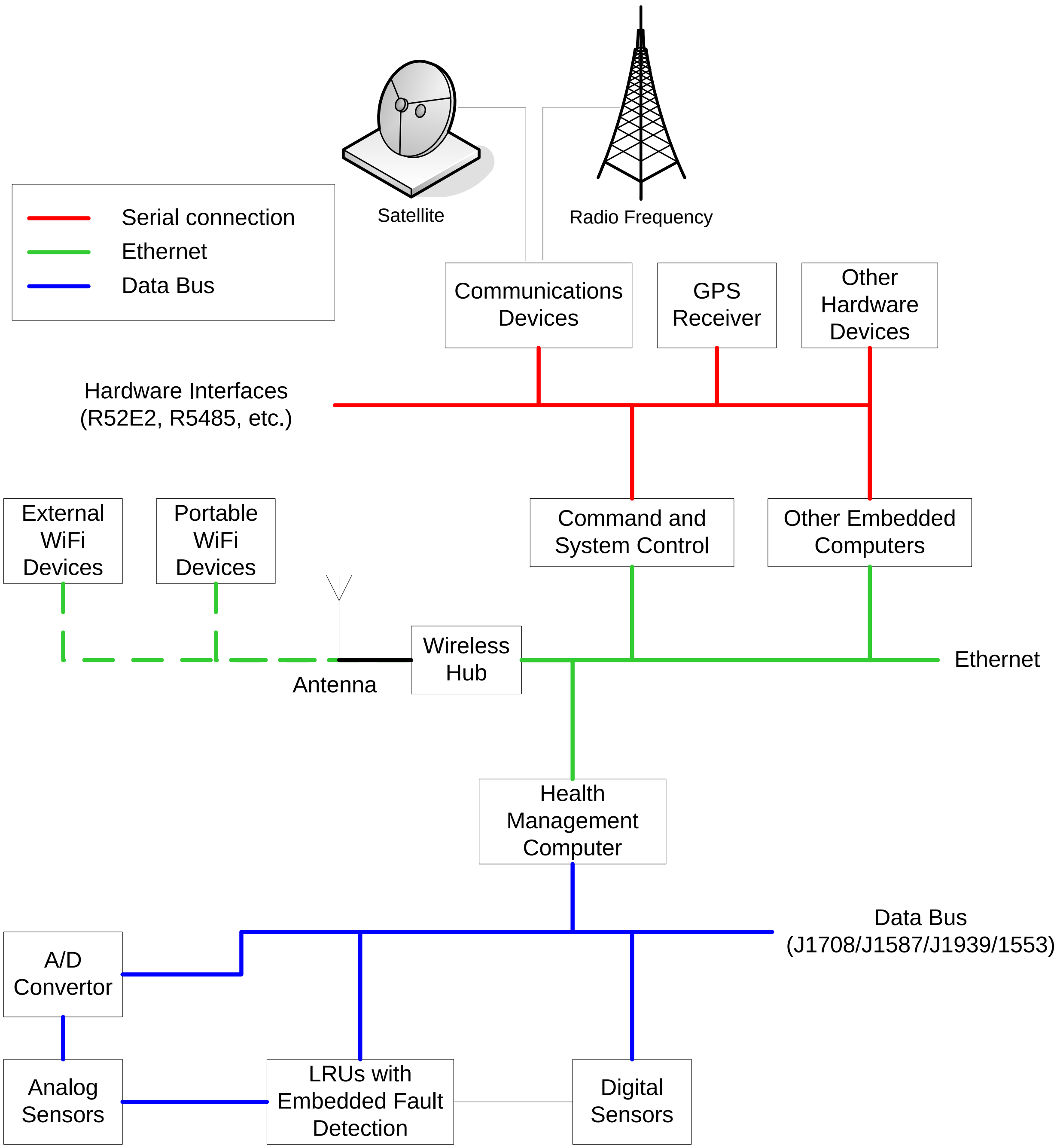
3.3.3 CBM$^+$ Structure—Platform Infrastructure

CBM$^+$ begins as an embedded design for platform system health management. This platform infrastructure is enabled by an on-board network of sensors coupled with a computer that hosts the interfaces and software to perform embedded system health management. Subsequently, this platform infrastructure connects to on-board communication systems that transmit maintenance data to the integrated information enterprise in three directions:

- Health status to the logistics common operating picture
- Actionable maintenance data to the logistics enterprise information technology (IT) systems
- Filtered raw sensor data to a CBM$^+$ data warehouse for further information discovery.

Figure 3-7, Figure 3-8, and Figure 3-9 show the infrastructure and functional views of platform CBM$^+$ components.

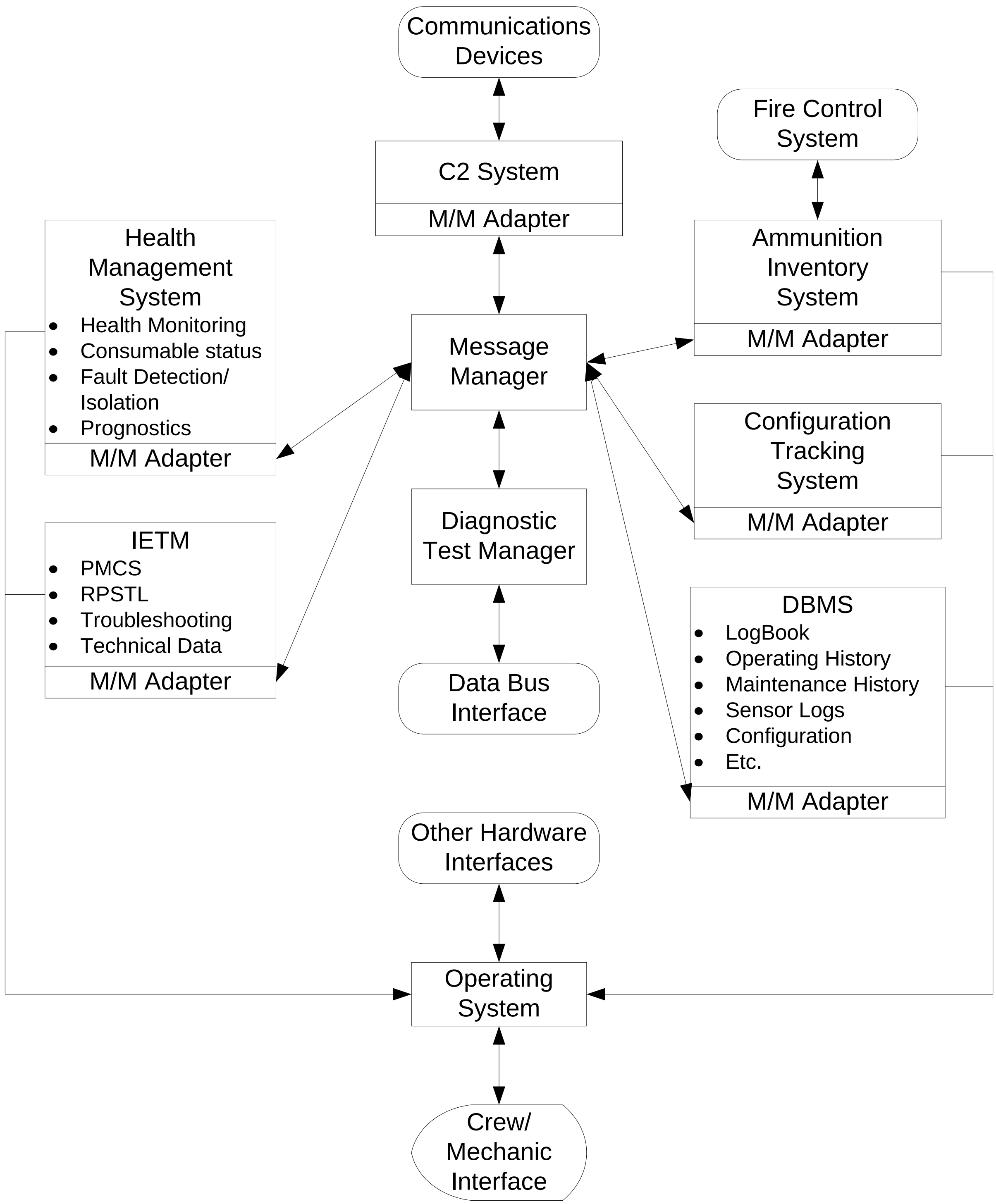
Figure 3-7. Platform Block Diagram of CBM+ Hardware Components



Notes: A/D = analog/digital; GPS = Global Positioning System; LRU = line replaceable unit; WiFi = Wireless Fidelity.

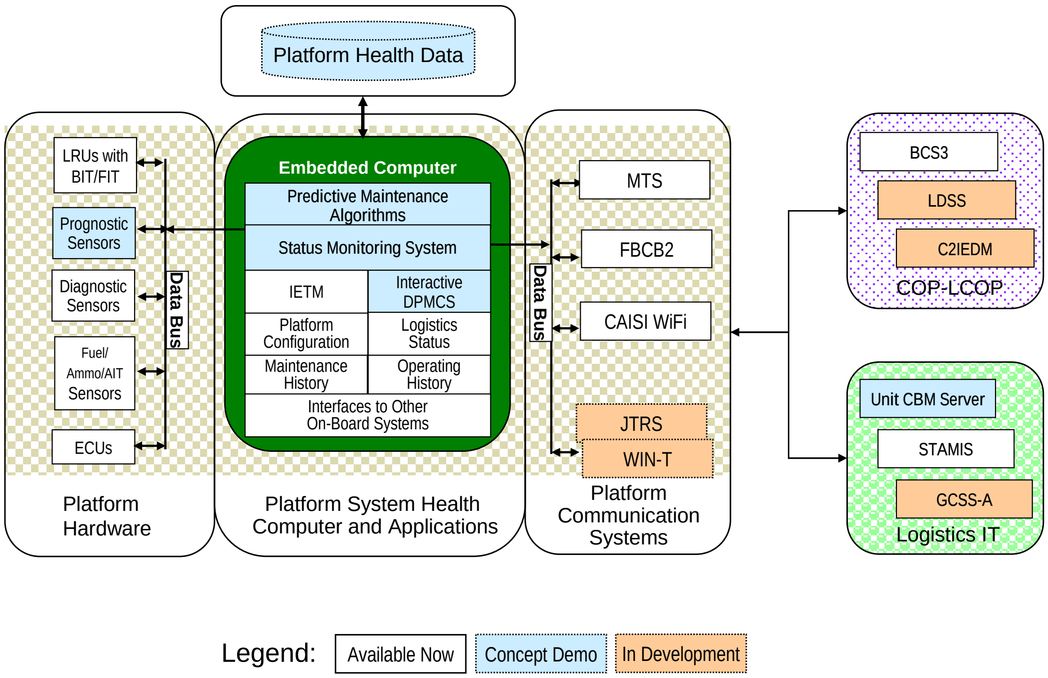
Other Embedded Computers = Other embedded computers are any and all computers residing on the platform for any purpose, such as those controlling weapon subsystems, displays and night vision devices, avionics subsystems, protection systems, etc.

Figure 3-8. Platform Block Diagram of CBM+ Software Components



Notes: C2 = command and control; M/M = Message Manager; PMCS = preventive maintenance checks and services; RPSTL = repair parts and special tools list.

Figure 3-9. Platform CBM+ Components Functional Systems Diagram



Notes: BCS3 = Battle Command Sustainment and Support System; BIT = built-in test, C2IEDM = Command and Control Information Exchange Data Model; CAISI = Combat-Service-Support Automated Information Systems Interface; ECU = electronic control unit; FBCB2 = Force XXI Battle Command, Brigade-and-Below; FIT = fault isolation test; GCSS-A = Global Combat Support System—Army; JTRS = Joint Tactical Radio System; LDSS = Logistics Decision Support System; MTS = Movement Tracking System; STAMIS = standard Army management information system; WIN-T = Warfighter's Information Network—Tactical.

3.3.3.1 On/At-System Software and Hardware Infrastructure

There is a set of key enabling software or hardware/software infrastructure applications which serve to facilitate CBM+. These enablers can be stand-alone applications, or can be run as either on-system or at-system processes. These applications include:

- Automatic identification technology
- Configuration management
- Operational history
- Digital Logbook
- Message Management (e.g., a publish and subscribe process for network management of event-driven messages)
- Interactive Electronic Technical Manuals (IETMs)—A Class 5 IETM represents a combination of test equipment and technical manual that can interrogate the platform data bus and incorporate real-time sensor information into the troubleshooting and repair process. Because of this capability, a Class V IETM can store cause-effect data in an on-board database called a System Health Data Store.

The on-or-at system enablers facilitate Systems Health Management. IETMs can be classified by their functional capabilities and are grouped into one of five classes of functionality. Classes 1–4 function as an electronic analogy to a paper manual, with increasing degrees of navigation sophistication.

- Sensor infrastructure—typically, the sensor infrastructure is based on either an open-system industry standard, such as the Society of Automotive Engineers (SAE) or a Military Standard, which define a networked data bus and sensor grid.

- System health management computer—The health management computer may be embedded on-board or may be an at-system PMA. The principal software that resides on the health management computer performs many functions:

  - Monitoring equipment health and consumable status through the embedded sensor grid (whether on-board or at-system, the computer connects to the sensor grid via an embedded data bus)

  - Predicting impending failures via trend analysis of collected sensor data or through model-based reasoning software

  - Providing the crew with platform health information

  - Providing platform health and consumable status to the C2 system for situation awareness reporting

  - Providing the logistics IT systems with actionable supply and maintenance information.

These capabilities have analogs at higher levels of the logistics enterprise architecture. They also have significant implications for doctrine, organizations, training, leader development, materiel, personnel, and facilities (DOTMLPF). Among other things, they will require new skills to support embedded software systems. These new DOTMLPF requirements should be addressed in focused planning.

Some of these applications may be accessible from a portable computer or portable display carried on the platform. This gives the operators the ability to use applications such as the logbook or digital preventive maintenance checks and services (DPMCS) while moving around the platform.

The ultimate goal for CBM$^+$ platform computing capability is to enable real-time embedded system health management capabilities. At-system CBM$^+$ is a limited form of CBM$^+$ that can only detect and forecast impending failures at the times when CBM$^+$ test equipment is available and/or scheduled for use. While at-system capabilities may be adequate for some unit missions, it will not be a real-time process and will miss many of the benefits that will accrue to a fully integrated system.

The foundation of CBM$^+$ is capturing and analyzing data from systems and components. At the platform level, the data supports platform health management functions. At the field level, managers use the data to maximize the readiness of their equipment. At the enterprise level, life cycle managers analyze the data for the entire fleet of platforms. The results of the analysis flow down to the field level for use by maintenance managers in predicting component failures and scheduling maintenance. The results of fleet-level analysis of CBM^+ data are also used to improve diagnostic routines used by embedded health management systems and maintainers. An effective system to manage CBM^+ data includes several key elements:

- *CBM^+ data warehouse* (as a part of the Logistics Information Warehouse) provides a single master data archive for a fleet of equipment and the associated data required for CBM^+ analysis. Approved users can access the data store for maintenance management, life cycle management, and related purposes.

- *Common maintenance data schema* enables a bi-directional flow of operational and maintenance information between operations, maintenance, and related decision support systems. The standards developed by the Machinery Information Management Open Systems Alliance (MIMOSA)[6] provide, in part, the open-protocol interface foundation for the required common schema. The CLOE-developed net-centric data strategy also applies.

- *Analysis and decision support tools* help users mine the data warehouse for CBM^+ analysis; to support product improvement efforts; to identify gaps in training for maintainers, operators, and supervisors; and to help maintenance managers to plan and schedule condition-based maintenance tasks.

Business processes and business rules need to be consistent with this maintenance approach. For example, business rules must support replacement of components before failure. Processes for turning in removed components, inspecting them, repairing them, and returning them to the supply system will need to be revised to support a CBM^+ approach. Maintenance planning processes and the supporting business systems will need to be modified to incorporate condition-based approaches and remove unnecessary preventive maintenance procedures. Operating procedures for preparing for deployment will need to incorporate CBM^+ principles to help the unit maximize the readiness of its equipment during the anticipated mission.

Table 3-1 contains a capability checklist for overall CBM^+ implementation.

[6] The MIMOSA web site is at http://www.mimosa.org.

Table 3-1. Summary of Required CBM+ Capabilities

CBM+ element	Required CBM+-related capabilities
Platform hardware	Single on-board computer capable of hosting embedded health management system and related CBM+ enablers adaptable to systems such as EPLARS, SINCGARS, and FBCB2
	On-board non-volatile memory for up to 90 days of operating history data
	Platform hardware architecture supports real-time reporting of equipment status, consumable status, and mission-critical faults
	Platform architecture supports LRU-level embedded diagnostics/built-in test, as well as platform-level health status monitoring, anomaly resolution, and fault detection/isolation
	Platform supports Serialized Item Management (SIM) for Materiel Maintenance
Platform software	Platform software architecture supports publish/subscribe interface among platform applications and between platform and applications at unit level and above, compliant with MIMOSA OSA-CBM and OSA-EAI[a] standards
	Embedded health management system with fault detection, fault isolation, and failure prediction capability
	Capture operating history (events, faults, usage stresses, sensor logs) in MIMOSA OSA-EAI compliant format
	Capture/store configuration of major components; configuration data includes nomenclature, national stock number, manufacturer's part number, unique identification/serial number, and installation date
	Capture, maintain, and store software configuration; configuration data includes software title, version number (with patches and updates), host computer, and install date
	Level 5 IETM with DPMCS and Integrated Parts Selection
	Automatically download operating history and configuration data when reporting threshold is reached and WiFi connection available
	Compress data for transmission
	Receive updates of tech data, predictive algorithms, etc. from log network over WiFi
Platform interface	Digital interface between health management computer and platform sensors, data buses, electronic control modules, and control system
	Ethernet interface between health management computer and other major computers on the platform (C2, Fire Control, etc.)
	WiFi compatible with Army standard WiFi system; external antenna provides capability to connect platform to authorized WiFi hub when in range
	Maintainer's computer capable of connecting to platform, hosting IETM, and connecting to business system over Army standard WiFi, compliant with MIMOSA OSA-EAI
	Class 5 IETM compliant with S1000D (international specification for technical publications utilizing a common source database) for each platform and end item
	IETM on maintainer's computer supports interfaces with platform data buses, "intrusive" diagnostic tests, and interfaces with test equipment; IETM provides integrated parts selection and shares XML data with the materiel management standard system and other applications through a publish/subscribe interface
	IETM supports automated tracking of maintenance man hours and consumption of small parts, lubricants, and other items used during a maintenance action. IETM supports capture of troubleshooting logs and related maintenance history data
	At-platform capability to analyze usage data when needed to augment on-platform capability
	Develop platform maintenance program using RCM analysis

Table 3-1. Summary of Required CBM+ Capabilities

CBM+ element	**Required CBM+-related capabilities**
C2	Tactical C2 System provides integrated set of products for combat platforms, aircraft, and Combat Support/Combat Service Support platforms
	Tactical C2 System has publish/subscribe interface with platforms
	Tactical C2 System provides automated status reporting of fuel, ammo, equipment health, critical faults
	Tactical C2 System provides automated reporting of quantitative log data (system health, urgent faults, fuel quantity, ammo inventory by type, inventory of other consumables, other critical tracked items list items) to log net
	Tactical C2 System publishes data from fault messages to maintenance management system
	Full data exchange between Tactical (e.g., FBCB2 data) and Log C2 Systems (e.g., SAMS-E, and BFT) through a publish/subscribe interface
	Platform health data is extracted from Tactical C2 Systems and integrated with data from business systems in log C2 Systems to provide timely, accurate logistics situation awareness
IT infrastructure	Unit level local area network (LAN) with Army standard wireless Ethernet
	Router/server/file transfer capabilities at company level
	Broadband connection to wide area network (WAN) in the field at battalion level
	Server with file backup capability at node with WAN connection
	Optional automatic dual communications medium switching capability.(i.e. auto-switch to cellular technology when out of range of WiFi)
Data warehouse	Storage capacity for current and historical data from entire fleet
	Receive automated data feeds from platforms in the field; verify receipt so temporary data stores can be erased
	Accepts incoming data feeds in MIMOSA OSA-EAI compliant formats and provides data exports/queries in MIMOSA OSA-EAI compliant formats including the Common Relational Information Schema (CRIS) Object Registry Data Model and CBM+ CRIS Reference Library
	Data base structured to facilitate analysis; supports both on-line analytical processing and on-line transactional processing of data
	Links to related data, such as maintenance history, personnel data, cost data, etc.; pull data needed routinely for CBM+ analysis
	Permission-based levels of access
	Accessible through Army Knowledge Online (AKO)
	Stores RCM life-cycle information through the product life cycle
Analysis and decision support	Supports application of advanced data mining and feature extraction tools
	Interface structured to facilitate analysis
	Parse complex data sets by key variables such as system, organization, location, etc.
	Efficient query across multiple data warehouses (CBM+, business, financial, personnel, engineering, etc.)
	Ability to extract data to support related analyses such as modeling and simulation
	Supports RCM analysis of maintenance tasks
	Generate maintenance scheduling factors based on analysis of CBM+ data; scheduling factors include upper and lower control limits, flags or alerts, key usage indicators, etc.
	Generate refinements to failure models and other diagnostic and predictive algorithms based on analysis of fleet level data
	Accepts incoming data feeds in MIMOSA OSA-EAI compliant formats and provides data exports/queries in MIMOSA OSA-EAI compliant formats including the CRIS Object Registry Data Model and CBM+ CRIS Reference Library

Table 3-1. Summary of Required CBM+ Capabilities

CBM+ element	**Required CBM+-related capabilities**
Maintenance management system	Embedded logbook application synchronized with master records in MMS. Interface between logbook and other platform applications to permit data sharing in a publish/subscribe environment
	Maintain master hardware and software configuration file (current and historical) for each platform
	Automatically synchronize master records in MMS with records on platform
	Support real-time wireless interface to maintainer's computer; provide a MIMOSA OSA-EAI compliant interface with the IETM and other maintainer applications to support integrated parts selection and automation of routine maintenance tasks
	Support condition-based maintenance scheduling as well as reactive and preventive maintenance approaches
	Fleet management capabilities at the battalion and brigade levels
	Share maintenance data with CBM+ data warehouse (national-level in potentially a distributed or echeloned fashion across multiple locations)
	Accepts incoming data feeds in MIMOSA OSA-EAI compliant formats and provides data exports/queries in MIMOSA OSA-EAI compliant formats including the CRIS Object Registry Data Model and CBM+ CRIS Reference Library

Notes: BFT = Blue Force Tracking; EPLARS = Enhanced Position Location and Reporting System; OSA-CBM = Open Systems Alliance–Condition Based Maintenance; OSA-EAI = Open systems Alliance–Enterprise Architecture Integration; SAMS-E = Standard Army Maintenance System–Enhanced; SINCGARS = Single Channel Ground and Airborne Radio System; XML = eXtensible Markup Language.

[a] Machinery Information Management Open Systems Alliance, Standard OSA-EAI V3.1, available at http://www.mimosa.org.

3.3.4 DODAF Architecture for CBM+

The current DoD acquisition system and the Joint Capabilities Integration and Development System (JCIDS)[7] are based on the development of an integrated information architecture as defined by the DODAF.[8]

The DODAF defines a common approach for DoD architecture description development, presentation, and integration for both warfighting operations and business operations and processes. The framework is intended to ensure that architecture descriptions can be compared and related across organizational boundaries, including Joint and multinational boundaries. The Logistics Domain has identified the Army Integrated Logistics Architecture (AILA) as the Army G-4's overarching logistics architecture, which is DODAF compliant. The AILA informs, guides, and supports decisions for the CBM process and assists the Army logistics community in achieving integration interoperability in the logistics and warfighter domains. The AILA assists the effort by identifying producers and consumers of the logistics information and assists in eliminating

[7] Chairman of the Joint Chiefs of Staff Instruction 3170.01E, *The Joint Capabilities Integration and Development System*, 11 May 2005, available at http://www.dtic.mil/cjcs_directives/cdata/unlimit/3170_01.pdf.

[8] DODAF Working Group, *DoD Architecture Framework*, Version 1.0, 15 August 2003. See DoD Architecture Framework description at http://en.wikipedia.org/wiki/Department_of_Defense_Architecture_Framework. The actual framework is available for download at http://www.aitcnet.org/dodfw/.

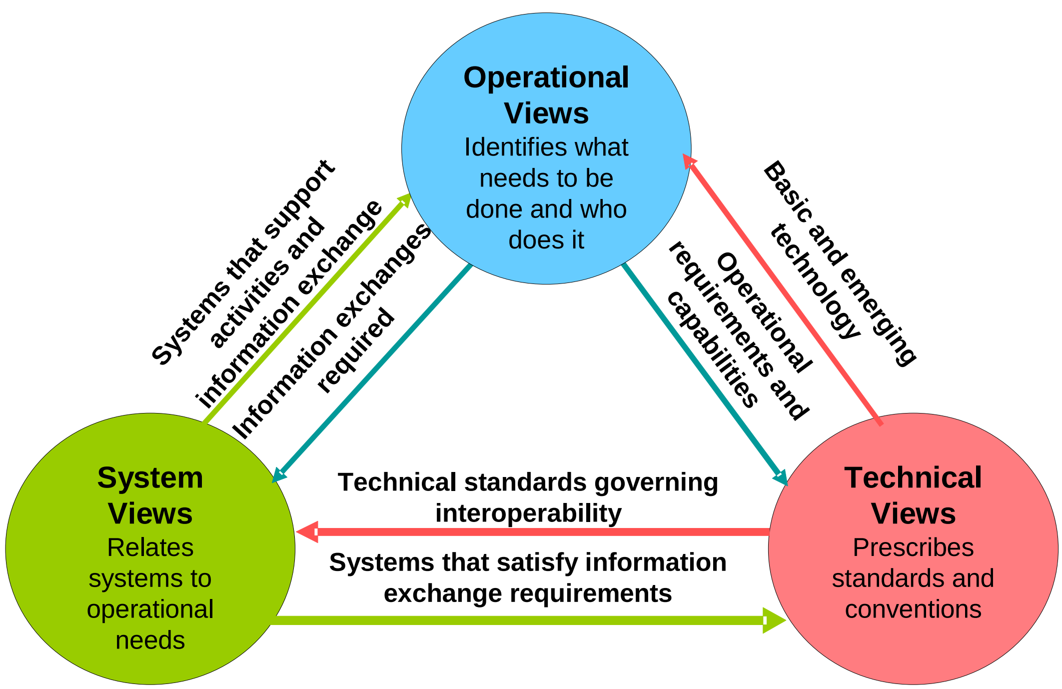
redundant and/or stovepipe IT investments. CBM+ and Sense and Respond Logistics (S&RL)[9] depend on the ability to connect the operating platform to the network.

The sustainment functional concept describes capabilities needed to apply the focused logistics Joint functional concept to the Army. One of the Joint functional concepts requires the capability for the collection, storage, and transmission of platform operating and maintenance data to enable implementation of CBM practices.

Open, modular software architecture permits data to be exchanged among applications without the effort and expense of maintaining dozens of separate interface control documents. The open architecture requires server-level software, such as message mangers and data base management systems. Server operating system software and related commercial products provide this functionality. The standards and supporting tools for the open software architecture must be tailored for use in the Army's operating environment. For example, an extensible markup language schema (based on the MIMOSA OSA-EAI standard) must be utilized. Message topic structure must be defined and MIMOSA OSA-EAI compliant reference data tables and formats must be developed to support the AILA.

The development of an integrated architecture requires the integration of the three types of architecture views in the DODAF: the operational (OV), technical (TV), and systems (SV) views. Figure 3-10 depicts the DODAF Architecture Product Relationships for the basic concepts.[10]

Figure 3-10. DODAF Architecture Product Relationships



[9] U.S. Army Combined Arms Support Command, Concepts and Doctrine Directorate, *Sense and Respond Logistics White Paper*, 10 October 2005. Also known as Adaptive Logistics in the Army.

[10] Extracted from Defense Acquisition University, *Defense Acquisition Guidebook*, Chapter 7, DoD Architecture Framework, available at http://akss.dau.mil/dag/DoD5000.asp?view=document&rf=GuideBook\IG_c7.2.4.1.asp.

Architecture development has several purposes. The process is fundamentally centered on documenting information flows and their attributes, but also includes management processes that support portfolio management and gap analysis. A fully integrated architecture has multiple applications in capability assessment.

The integration process is made more challenging by the fact that the responsibility for development and integration of the separate architecture view types (OV, TV, and SV) is led and governed by separate Army agencies.[11]

By both DoD mandate and good engineering practice, this integration process is based on industry-standard open-architecture specifications and data models. The technical aspects of this architecture are expressed in the Technical Standards Profile, the TV-1.

3.3.5 Data Strategy

3.3.5.1 Open Standards

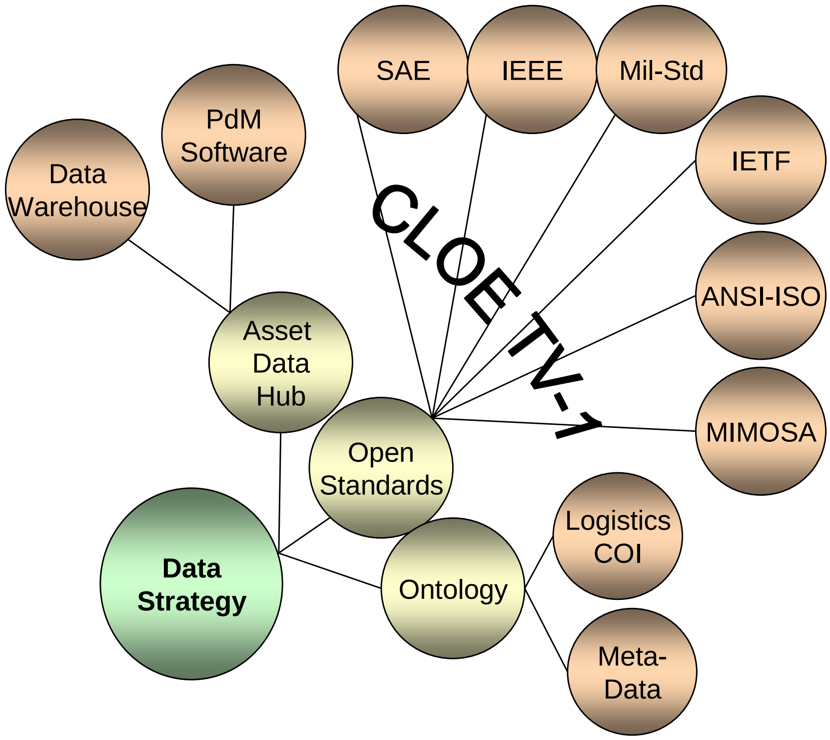
Open standards and data models underpin well-designed information domains. The interchangeability of components that is possible in an "open" architecture environment yields several benefits:

- System capability can be extended by adding conforming components
- System performance can be enhanced by adding components with improved or upgraded capabilities.

Figure 3-11 shows a pictorial view of the CBM$^+$ Data Strategy. The CLOE TV-1 containing standards from multiple sources, including American National Standards Institute (ANSI), International Organization for Standardization (ISO), Institute of Electrical and Electronics Engineers (IEEE), Internet Engineering Task Force (IETF), military standards (Mil-Std), Machinery Information Management Open Systems Alliance (MIMOSA), and the Society of Automotive Engineers–International (SAE).

[11] Headquarters, Department of the Army, Vice Chief of Staff Memorandum, "Architecture Development and Approval," 8 October 2004.

Figure 3-11. Elements of CBM+ Data Strategy



A basis for defining the open CBM+ information domain has been established by the ISO standard 13374-1, *Condition-Monitoring and Diagnostics of Machines*.[12] This standard describes the data flow hierarchy for CBM+ information exchange.

MIMOSA[13] has established specifications and data models in support of ISO 13374-1. These standards have been included in the technical standards profile (TV-1) of the architecture for the Common Logistics Operating Environment (CLOE) to support CBM+.

3.3.5.2 Ontology

There are five tenets of net-centric data strategy—make data visible, accessible, understandable, trusted, and interoperable. Ontology as applied to IT systems is the process of defining data and meta-data for the purpose of making data understandable and interoperable across the logistics user community. It is easy enough to define the structure of logistics data ontology. The real work lays in the formation and operation of the logistics user community, which at this time has not been formed.

[12] International Organization for Standardization (ISO), ISO Standard 13374-1:2003, *Condition Monitoring and Diagnostics of Machines—Data Processing, Communication and Presentation*, available at http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=21832&ICS1=17&ICS2=160&ICS3=.

[13] *Op cit.*

3.3.5.3 Net-Centricity

A network-centric data strategy underpins army transformation. The DoD mandates for net-centricity are encompassed by Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6212.01D[14] and DoD Instruction (DODI) 4630.8.[15] These mandates apply to CBM$^+$ Information Exchange Requirements, and compliance is assured through integration of these requirements with the CLOE OVs and TV-1.

CBM$^+$ is a "net-centric" maintenance concept. It supports net-centric warfare concepts by enabling near real-time visibility of platform operating status and improving mission reliability. CBM$^+$ relies on the movement of platform data to various places in the enterprise. This movement requires a supporting communications and information systems infrastructure. Key elements of the infrastructure include:

- Server functionality at the unit (limited) and battalion (robust) to support movement of CBM$^+$ data from the platform to other users. These capabilities provide "publish and subscribe" services and manage file transfers and related movement of data up and down the system.
- Reliable local area network (LAN) and wide area network (WAN) coverage provides the basic network backbone needed to support movement of CBM$^+$ data and automation of other maintenance and logistics tasks.

3.3.5.4 Asset Data Hub (or CBM$^+$ Data Warehouse or Logistics Information Warehouse)

From an open, non-proprietary data strategy viewpoint, an overriding concern is to ensure that all CBM$^+$ systems, including the CBM$^+$ data warehouse, conform to the open architecture data standard formats published by MIMOSA entitled *Open Systems Architecture for Enterprise Application Integration* (OSA-EAI). This specification mirrors the data flow hierarchy in ISO 13374-1.[16] This is the international standard that MIMOSA implements for condition monitoring and other CBM$^+$ applications as shown in Figure 3-12. The figure shows key industry and military standards that apply to the various levels of the ISO/MIMOSA data flow hierarchy. This depiction is for automated (sensor-based) data entry. This interface specification is referenced in the CLOE-AILA TV-1.

---

[14] Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6212.01D, I*nteroperability and Supportability of Information Technology and National Security Systems*, 8 March 2006.

[15] DODI 4630.8, *Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)*, 30 June 2004.

[16] International Organization for Standardization, ISO 13374-1:2003, *Condition Monitoring and Diagnostics of Machines—Data Processing, Communication and Presentation—Part 1: General Guidelines*, available at http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=21832.

Figure 3-12. Selected Industry Standards that Address the ISO 13374/MIMOSA CBM^{+} Data Flow Hierarchy

			Platform Hardware and Software Infrastrucure			
			Type	**Example**	**Industry Standard**	**Data Interface Specification**
	Layer 0	**Embedded Computing**	**Win; Linux; VME**	**DT-3000**	**Win; Linux; Posix; VME**	
ISO 13374 Schema	**Layer 1**	**Data Acquisition**	**Sensors**	**Control, Operational, Diagnostic**	**IEEE 1451**	**MIMOSA OSA-CBM** **MIMOSA Tech CDE** **MIMOSA OSA-EAI** **Mimosa CRIS XML Object Registry Data Model**
			DATA BUS	**Aircraft avionics and weapon systems; Fighting vehicle turret subsystems**	**Mil-Std-1553**	
				Automotive	**SAE J1850**	
				Heavy-Duty Diesel-Powered Vehicles	**SAE J1708;** **SAE J1939 (family of standards);** **XTP**	
	Layer 2	**Data Manipulation**	SOFTWARE	**Embedded Diagnostics**		
				Configuration Mgmt	**Java Msg Service API; OSA-MSG services**	
				Operating History		
				Logbook		
				AIT		
				IETM		
				Message Manager		
				CBM+ Data Store		
	Layer 3	**State Detection**		**Predictive Health Management**		
	Layer 4	**Health Assessment**				
	Layer 5	**Prognostic Assessment**		**Prognostic Health Management**		
	Layer 6	**Advisory Generation**		**LCOP-Asset Data Hub-Logistics IT Systems**		**STAMIS**
	Layer 7	**COM**	**Hardware and Software**	**FBCB2 ICD**	**FBCB2 v 6.4.1**	
				WiFi Applications	**IEEE 802.11**	

Note: AIT = Automated Identification Technology; API = Application Programming Interface; CBM = Condition Based Maintenance; CDE = common data environment; COM = Communications; Config = Configuration; CRIS = Common Relational Information Schema; DT-3000 = Data Translation computer model; EAI = enterprise application integration; FBCB2 = Force XXI Battle Command, Brigade-and-Below; ICD = Initial Capabilities Document; IETM = Interactive Electronic Technical Manual; LCOP = Logistics Composite Operating Picture; MIMOSA = Machinery Information Management Open Systems Alliance; Msg = message; OSA = Open System Architecture; Posix = Portable Operating System Interface (IEEE Standard 1003.1); STAMIS = Standard Army Management Information System; Tech = technical; VME = Virtual Machine Environment; Win = Microsoft Windows; XML = eXtensible Markup Language.

3.3.6 Hardware and Software Infrastructure for CBM$^+$

3.3.6.1 General

The computing infrastructure for CBM$^+$ can be divided into three main categories:

- Equipment infrastructure (e.g., the operating platform)
- Enterprise infrastructure (e.g., the logistics IT systems that manage supply, maintenance, and distribution and the C2 Systems that provide the commander operational and situational visibility, including the status of equipment health and consumables)
- Enterprise information storage, analysis, and decision support—an asset data hub.

The computing infrastructure for equipment is built upon the equipment's analog or digital electronics contained within a platform. There are two ways to accomplish CBM$^+$ for the platform:

- On-system (e.g., embedded on the platform)

At-system (e.g., through the use of a portable computer that runs many of the same software applications that might otherwise be embedded on the platform).

3.3.6.2 Communication Systems

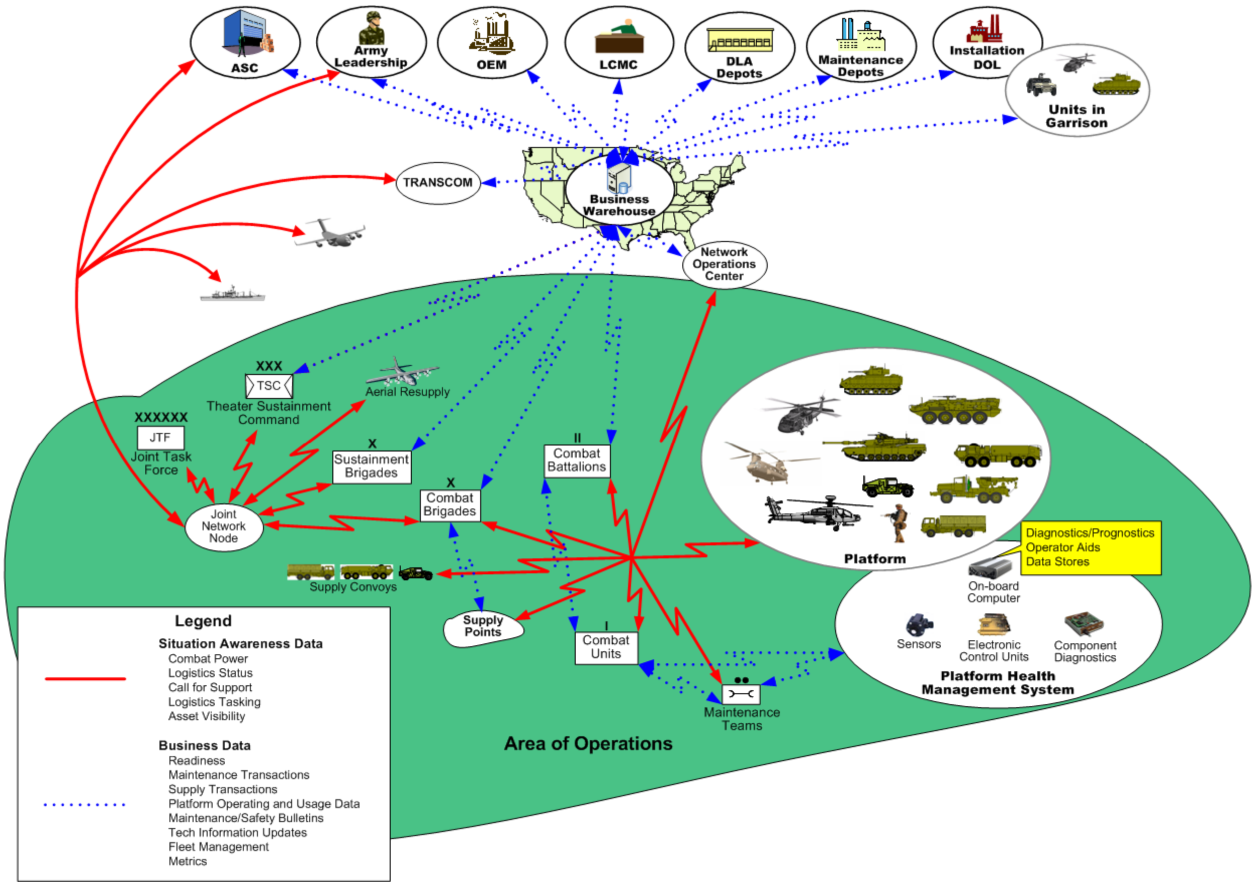
CBM$^+$ capabilities depend on the ability to transmit business process, platform status, and equipment performance data. The principal means for platform over-the-horizon communication is by frequency modulated (FM) radio or satellite. Current Force systems include:

- FM radio: Single Channel Ground-Airborne Radio System (SINCGARS)
  - Used in combination with the Enhanced Position Location Reporting System (EPLRS)
  - Used by the C2 application entitled Force XXI Battle Command Brigade and Below (FBCB2)
- Satellite: Movement Tracking System (MTS)
- Wireless Fidelity (Institute of Electrical and Electronics Engineers [IEEE] 802.11b/g wireless networking) (WiFi)
- Combat Service Support Automated Information System Interface (CAISI). CAISI is an example from a growing family of tactical wireless local area networks (LAN). CAISI employs third-party encryption and access control technology for secure computing capability
- FBCB2-based Blue Force Tracking (BFT).

From a CBM+ standpoint, CAISI offers a capability to shift data transmission bandwidth for sensor health data related to equipment performance from limited FM radio or satellite communication to the more expedient WiFi, albeit with transmission distance limited to a few miles.

The overview of data flow over various communication media is shown in Figure 3-13.

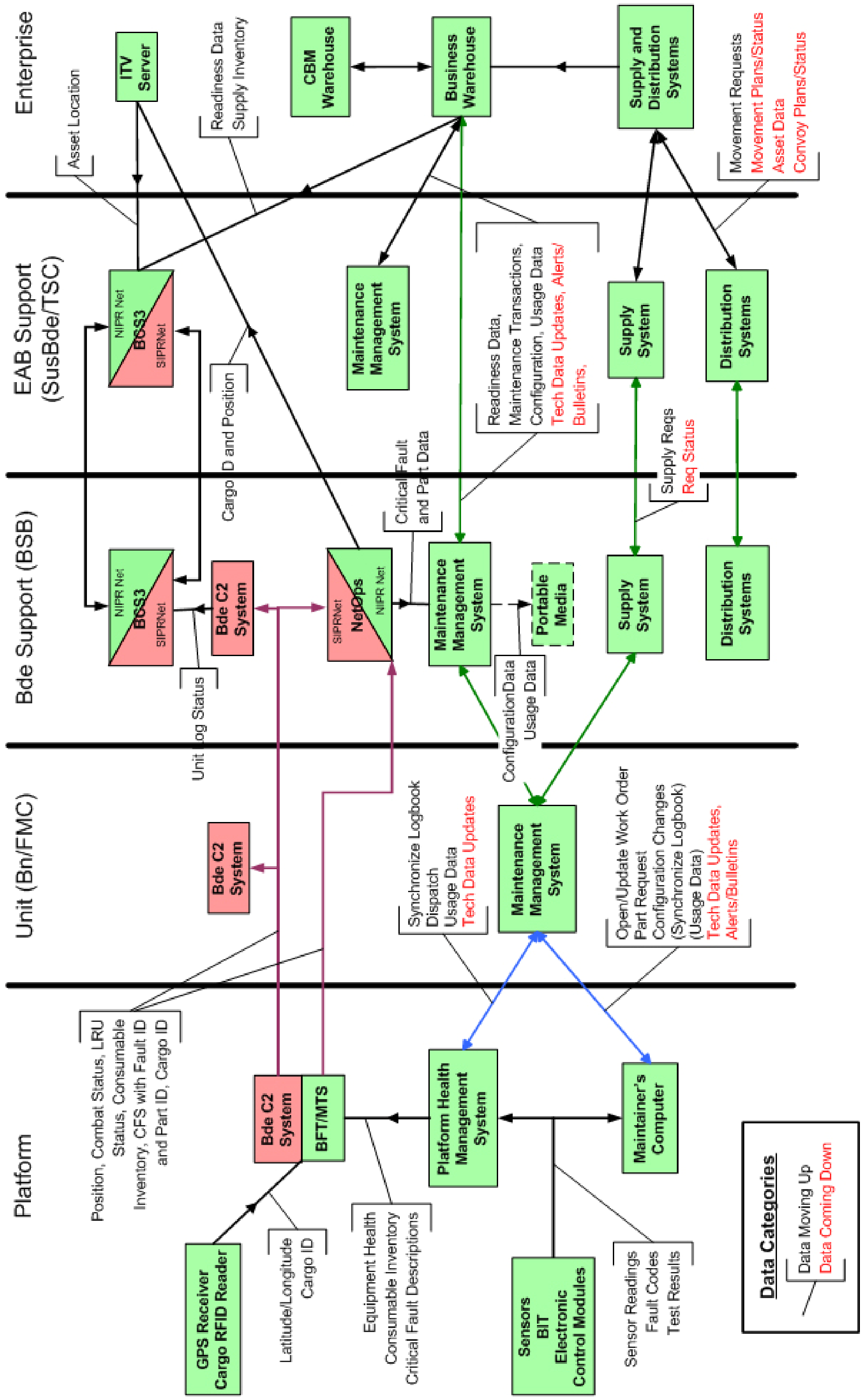
Figure 3-13. CBM+ Data Communication Overview



Notes: ASC = Army Sustainment Command; DLA = Defense Logistics Agency; DOL = Director of Logistics; LCMC = Life Cycle Management Command; OEM = Original Equipment Manufacturer; TRANSCOM = Transportation Command.

CBM+ information flow from the platform throughout the logistics enterprise is shown in Figure 3-14. The platform is shown to have an on-board health management computer, with an at-system portable maintenance aid (PMA, the maintainer's computer).

Figure 3-14. CBM+ Information Flow from the Platform through the Logistics Enterprise



Notes: CFS = call for support; FMC = forward maintenance company; SIPRNet = secret internet protocol router network; TSC = theater support command.

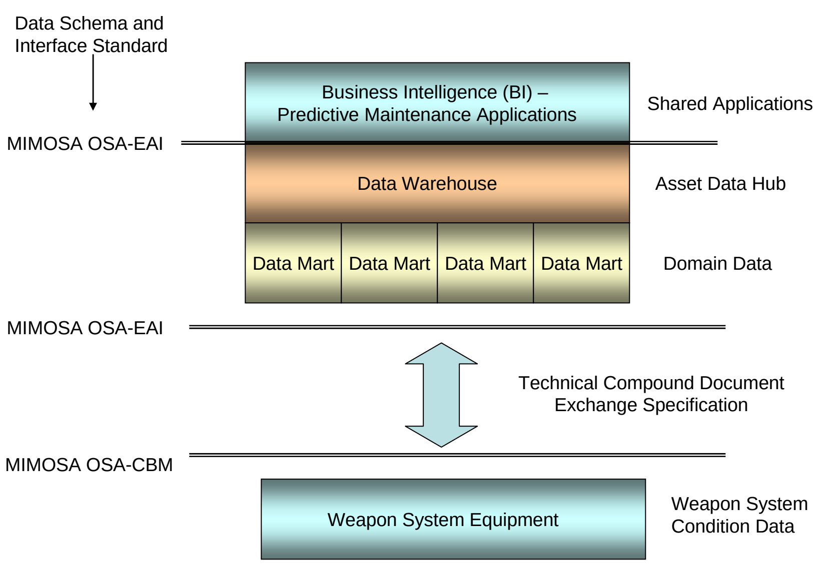
3.3.6.3 Logistics Enterprise Infrastructure

The logistics enterprise-level infrastructure for CBM$^+$ is comprised of logistics information technology (IT) systems and C2 Systems for logistics that provide the commander with logistics situational awareness, including the status of equipment health and consumables.

3.3.6.3.1 Data Warehouse and Predictive Maintenance

The enterprise-level capability for CBM$^+$ applications in logistics centers on the ability to provide, populate, and manage an asset data hub for system health data—a CBM$^+$ data warehouse. A data warehouse can be comprised of smaller, domain-specific data bases called data marts (e.g., with respect to CBM$^+$ data, a data mart could support a particular class of vehicle or a set of commodity-specific platforms such as aircraft). Software applications that extract information from a data warehouse are generically termed business intelligence (BI) systems. In the case of a CBM$^+$ data warehouse, the BI applications that operate on the data are the applications for predictive maintenance. Figure 3-15 depicts the relationship.

Figure 3-15. CBM$^+$ Data Warehouse and Shared Applications



The CBM$^+$ data warehouse supports a data aggregation process that can be performed at any level above the platform (e.g., tactical, operational, or national-strategic echelons). The higher the level of the CBM$^+$ data warehouse, the more global the information it contains. For example, a tactical echelon CBM$^+$ data warehouse may predict failures from the entire set of similar vehicles in a given unit. A CBM$^+$ data warehouse at the national-strategic level can assess and predict failures for an entire class of vehicles that account for different geographical regions, different climate and weather patterns, different area of responsibility (AOR), operational tempo (OPTEMPO), etc.

3.3.6.3.2 Server/Portal Strategy

In addition to a national CBM$^+$ Data Warehouse, the Army CBM$^+$ operating concept envisions an echelon server concept, employing servers in the theatre of operation down to the battalion/ brigade level. The echelon-servers act as CBM data concentrators, filters, and intermediate data warehouses, putting local data immediately in the hands of the unit and also forwarding aggregated data to higher echelons/national servers.

The echelon server concept is similar to the off-board service application (OBSA) of the United States Marine Corps (USMC) Embedded Platform Logistics System (EPLS) and the overarching Autonomic Logistics (AL) System. EPLS and AL employ U.S. Navy Joint Technical Data Integration (JTDI) servers at unit, theater, and national echelons.

In the Army current force Enterprise Information Systems (EIS) environment, the logistics and maintenance systems (e.g., Standard Army Maintenance System—Enhanced [SAMS-E], Unit Level Logistics System [ULLS], and Standard Army Retail Supply System [SARSS]) process transaction data only. These systems are not equipped to host CBM^+ data nor act as a CBM^+ data warehouse. As a result, the Army current force logistics applications require a hardware and software augmentation for CBM^+ functionality that will integrate with GCSS-Army as the Single Army Logistics Enterprise replaces current force logistics systems.

At echelons below the national-strategic level, augmentation amounts to an additional server to host both the CBM^+ data warehouse and the predictive maintenance software applications that act on the stored CBM^+ data and can convert it to the kind of transaction data that the logistics systems will accept. The data repository has multiple applications that do not always entail business transactions, including fleet-level trending, root cause analysis, etc. This system of communications and data is defined by an information architecture. Within logistics, that is the Army Integrated Logistics Architecture (AILA).

3.3.7 CBM^+ Demonstrations and Operational Evaluations

3.3.7.1 General

The CLOE program plans and conducts proof of enabler (PoE) demonstrations and operational evaluations of the AILA to demonstrate:

- CBM^+ capabilities for Focused Logistics;
- Platform CBM^+ interoperability with logistics IT systems;
- Verification that platform systems meet OV interoperability requirements for CBM and CBM^+;
- Benchmarks for metrics that evaluate the effectiveness embedded system health management and CBM^+; and
- Selected aspects of the net-centric data strategy for CBM^+.

3.3.7.2 Demonstration Objectives

- Establish threshold functionality for Current Force Embedded Platform Health Management in operational deployment scenarios
- Verify that Information Exchange Requirements for CBM^+ are in place and work as planned

- Measure the benefit of embedded health management and CBM$^+$ for current force platforms

- Promote technology maturation for promising platform health management efforts in CBM$^+$ applications.

- Verify logistics and maintenance net-centricity and end-to-end connectivity for CBM$^+$ functionality in the Single Army Logistics Enterprise (SALE)

- Work with Program Manager (PM)–Future Combat Systems (FCS)—Experimental Brigade Combat Team and PM–Modular Brigade Enhancements, act as a Risk-Mitigation Process for FCS Technology Spin-out to the Current Force.

3.3.7.3 Metrics for Measuring Demonstration Objectives

Compliance with demonstration objectives should be assessed using metrics derived from the following topical areas:

- Compliance to information exchange requirements (IERs)

- Operational availability rate (A_O)

- Mean-time-to-repair (MTTR)

- No-evidence-of–failure rate (NEOF)

- Customer wait time (CWT)

- Sortie-generation rate

- Combat power

- Supply Chain Operations Reference Model (SCOM)

- Balanced Scorecard

- Test equipment and repair parts densities (footprint).

Table 3-2 and Table 3-3 describe metrics and effects applicable to CBM$^+$ demonstrations.

Table 3-2. CBM^+ Metrics and Effects for Focused Logistics

Focused logistics effects	Metric	Effect sought
Reduce cycle time	CWT	Decrease
Supply, maintenance, and platform-soldier health visibility (LCOP)	Information latency from time of platform report to display on warfighter systems for BCS3, FBCB2, and BFT	Near-real-time information display
Operational availability	Operational readiness rate	Increase
Logistics footprint	Mean-time-between-removals	Decrease
	NEOF False removal rate (e.g., tests good at next higher support echelon)	Decrease
	Distribution-based (Theater/Tactical Supply Stock Piles)	Decrease
Repair time	MTTR	Decrease

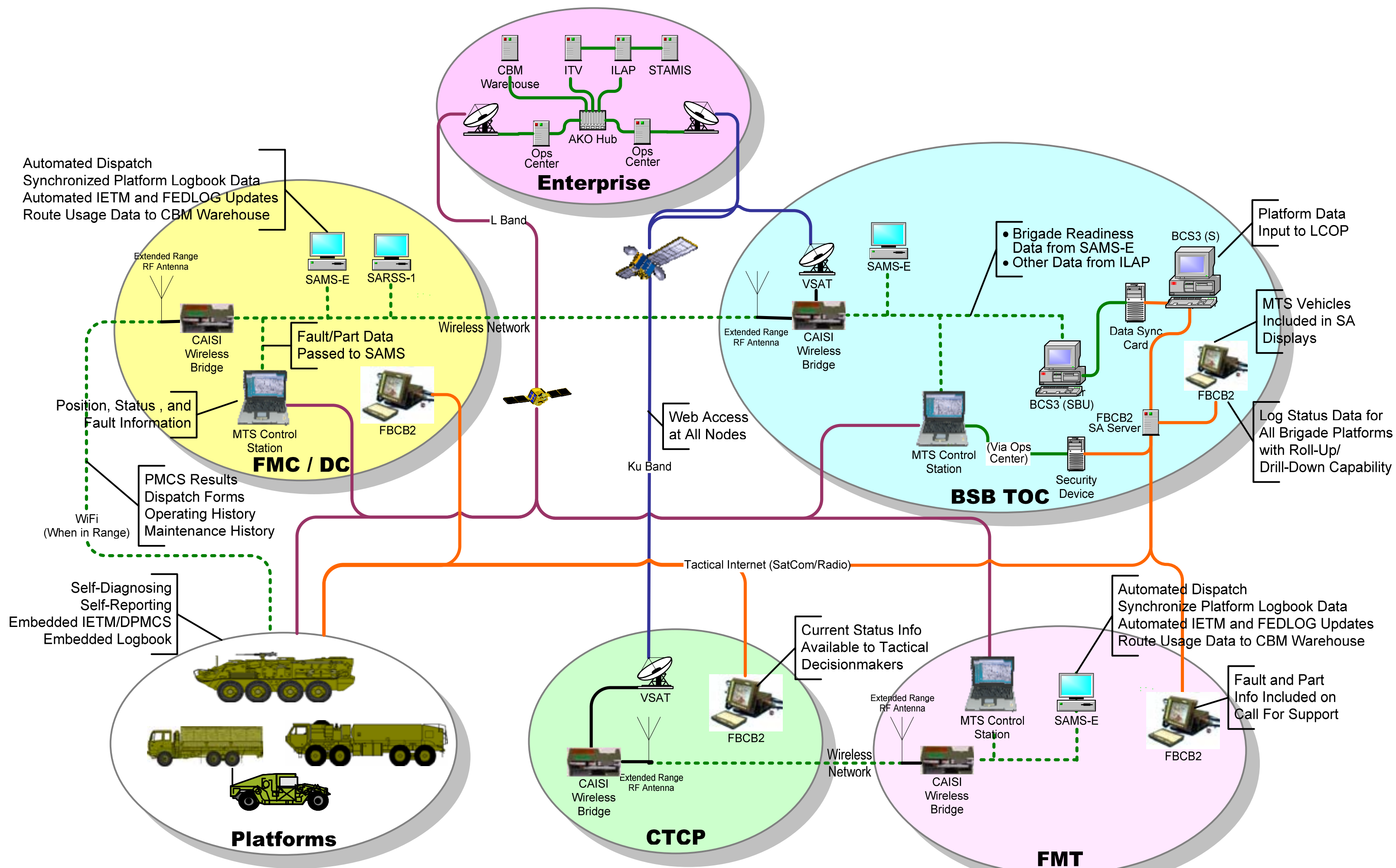
Table 3-3. Evaluating Prognostics

Metric	Effect
PFDphm: Percentage of Correct Automatic Detections, from the set of detectable failures	Threshold varies; objective 100%
PFIphm: Percentage of Correct Automatic Isolation from the set of correct detected failures	Threshold varies; stated in terms of the number of components in the isolation group; objective is 100% to one component
False Alarm Rate	Threshold varies; objective is zero
Mean Time Between False Alarms	Threshold varies; objective is infinity
RULMSphm: Remaining Useful Life of Component Maintenance	This is a measure of platform health management effectiveness for maintenance planning purposes; the lowest bound represents the “latest” notification requirement to be made aware that a component is about to reach a failed state

3.3.7.4 Connecting the On-, At-, and Off-System CBM^+ Components to the Logistics Enterprise

Coupling CBM^+ processes to the Army logistics enterprise entails the development of a DODAF integrated logistics architecture which identifies and connects the platform CBM^+ infrastructure to the logistics IT systems and logistics common operating picture (LCOP) systems. Figure 3-16 is a detailed Operational View, OV-1 in a Stryker brigade combat team (SBCT) context, and was demonstrated during the SBCT PoE demonstration at Fort Hood, Texas, in November 2004.

Figure 3-16. SBCT Operating Concept for CBM+



Notes: AKO = Army Knowledge Online; BCS3 = Battle Command Sustainment and Support System; BSB = Brigade Support Battalion; CAISI = Combat-Service-Support Auto-mated Information Systems Interface; CBM = Condition Based Maintenance; CTCP = Combat Trains Command Post; DC = Distribution Company; DPMCS = Digital Preventive Main-tenance Checks and Services; FBCB2 = Force XXI Battle Command, Brigade and Below; FEDLOG = Federal Logistics Record; FMC = Field Maintenance Company; FMT = Field Maintenance Team; HQ = Headquarters; IETM = Interactive Electronic Technical Manual; ILAP = Integrated Logistics Analysis Program; ITV = In-Transit Visibility; Ku = Kurtz (under band of the electromagnetic spectrum); L = portion of the microwave band of the electromagnetic spectrum; LCOP = Logistics Common Operating Picture; MTS = Movement Tracing System; Ops = Operations; PMCS = Preventive Maintenance Checks and Services; RF = Radio Frequency; S = Secret; SA = Situational Awareness; SAMS-E = Standard Army Main-tenance System–Enhanced; SARSS-1 = Standard Army Retail Supply System–One; SBU = Sensitive But Unclassi-fied; STAMIS = Standard Army Management Information System; TOC = Tactical Operations Center; VSAT = Very Small Aperture Terminal; WiFi = Wireless Fidelity (Institute of Electrical and Electronics Engineers 802.11b wireless networking).

3.4 CBM$^+$ System and Sustainment Engineering

The implementation, management, and oversight functions performed by the designated program manager, are conducted through the Total Life Cycle Systems Management (TLCSM) process. All activities associated with the acquisition, development, production, fielding, sustainment, and disposal of a DoD weapon system across its life cycle are reviewed and evaluated through the TLCSM process.[17]

3.4.1 Development Strategy for CBM$^+$ Involves Six Key Initial Actions

- Establishing a business case for CBM implementation in accordance with Assistant Secretary of the Army (Financial Management) (ASA [FM]) Army Cost and Economics Manual.[18] The basis for the CBM solutions and related tasks is the criticality of equipment failures that deadline equipment, coupled with the criticality of the equipment required for mission accomplishment. RCM analysis will be the foundation for the CBM tasks and benefits supporting the CBM business case.

- Establishing business rules for supply, maintenance, and Army Single Stock Fund transactions that deal with line replaceable unit (LRU) and shop replaceable unit (SRU) repair parts that have remaining serviceable life, though removed from use due to predicted failure.

- Establishing the linkage and requirements for RCM, CBM$^+$, and CLOE in a TLCSM perspective and then linking that to JCIDS milestone reviews and required documentation. AR 70-1 requires program and product managers to describe how embedded prognostics/diagnostics, and embedded training systems will be incorporated into the acquisition. For Current Force systems that will not trigger further JCIDS milestone reviews, the linkage will occur as a part of modification planning within Integrated Logistics Support.

- Establishing a Verification and Validation (V&V) plan for testing the DODAF architecture for CBM$^+$, followed by the incorporation of CBM$^+$ test elements within the Intra-Army Interopability Certification (IAIC) program.

- Establishing metrics in system acquisition planning documents (e.g., JCIDS Initial Capability Document [ICD]) as well as metrics at the Army level to assess overall CBM$^+$ capability progress.

- Establishing CBM$^+$ driven Doctrine, Organizations, Training, Materiel, Leader Development Personnel, and Facilities (DOTMLPF) changes, including requirements for acquisition and sustainment efforts.

Figure 3-17 shows the integrated acquisition, technology, and logistics life cycle documents which need to reflect RCM and CBM$^+$ content at each stage of the JCIDS review process.

---

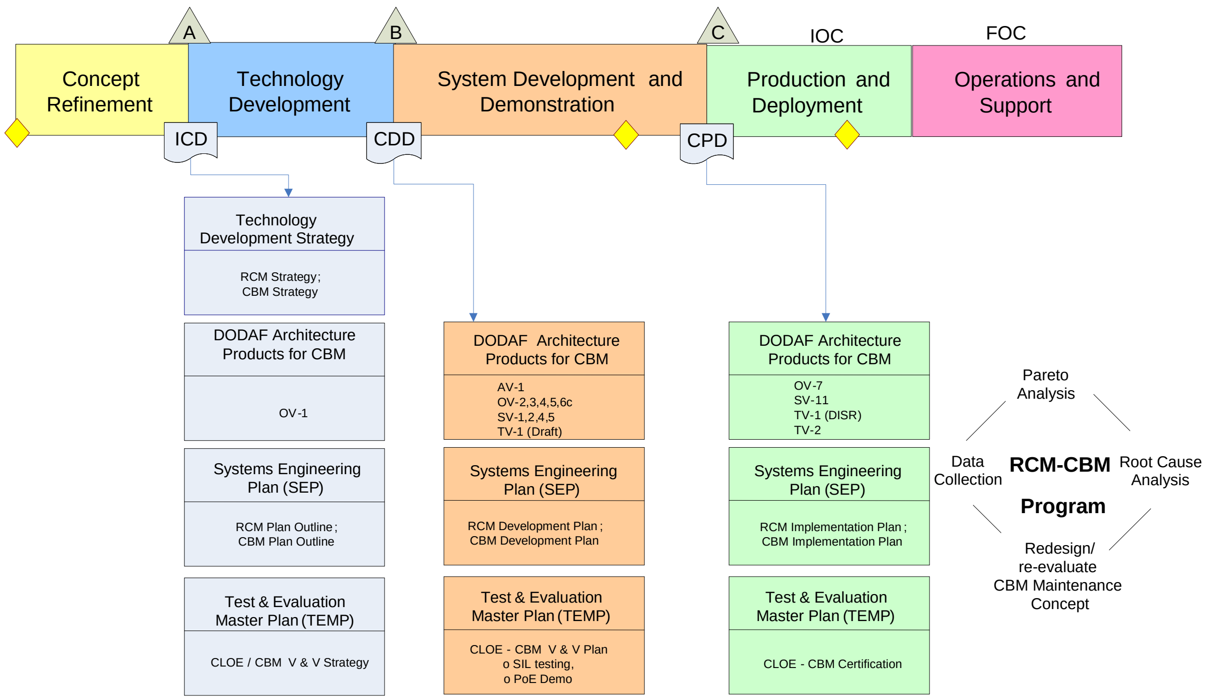
[17] DoD, *Focused Logistics Roadmap*, Volume 1, page 3-15, September 2005.

[18] AR 750-1 Army Maintenance Policy, page 80, Section 7-4e.(2), 20 September 2007.

Figure 3-17. JCIDS Process and Document Content for RCM and CBM+ by Phase

System-Level JCIDS Planning Requirements for RCM—CBM Capability

The goals for Focused Logistics include predictive maintenance, anticipatory logistics fulfillment, reduced Logistics footprint and time-definite delivery. CBM is the capability that achieves these goals.



CBM capability is expressed in broad operational terms in the format of an Initial Capabilities Document (ICD) or a DOTMI PF change recommendation.

In materiel proposals , the definition progressively evolves to DOTMLPF performance attributes identified in the Capability Development Document (CDD) and the Capability Production Document (CPD).

Notes: FOC = full operation capability; IOC = initial operation capability.

3.4.2 Verification and Validation Strategy

As part of the CBM+ development strategy during System Development and Demonstration (SDD), a V&V strategy should be articulated in the Test and Evaluation Master Plan (TEMP).

V&V of CBM+ functionality is tied to the DODAF architecture products that are developed and described in the Concept Development Document (CDD), as prescribed by CJCSI 6212.01D. V&V of these DODAF architecture products is not done individually, but rather as an integrated architecture that integrates the information exchange requirements of the DODAF operational views with systems views that then govern the systems that accomplish that data exchange. That data exchange is accomplished in conformance with the DODAF technical standards views as described in the TV-1.

Initially, this process is a matter of developing the models of the processes and then the modules themselves. V&V is first a simulation and modeling exercise of transmitting CBM+ data between models, accomplished in a Systems Integration Laboratory (SIL) setting. As the SDD phase proceeds and the applications for software exchange are developed, V&V may be accomplished between the platform and remote sites by live demonstration.

3.4.3 Certification

In CBM$^+$, as in other logistics IT applications, there is an Army oversight and approval function which is manifested in various levels of review and certification. There are three basic kinds of processes that require certification: DODAF architecture, CBM$^+$ functionality, and RCM functionality. Table 3-4 provides examples of IT certification and/or other forms of RCM and CBM$^+$ validation or certification.

Table 3-4. Types of CBM$^+$ Certification

Type of RCM/CBM$^+$ initiative	System or architecture		Certification authority		Certification requirement
	Type	**Application**	**Business mission area (logistics domain)**	**Warfighter mission area (focused logistics domain)**	
DODAF	Architecture	AILA		TRADOC, ASA(ALT), CIO/G-6, J-6	Architecture views (OV, TV, SV) and integrated architecture
Standards profile	Architecture	CLOE-AILA TV-1		CIO/G-6/ DISR	DISR mandated/emerging standards requirements
Ontology	CBM$^+$ data	Net-centric data strategy		Logistics User Community	KPPs
IT CBM$^+$ functionality	LOG IT	SALE (GCSS-A, PLM+)	DBSMC	CLOE	Business Enterprise Architecture (BEA)/ CLOE interoperability
		CBM$^+$ data warehouse		CIO/ G-6	Information Assurance (IA) Certification
Platform CBM$^+$ functionality	Embedded Platform Health Enablers	Platform or major end item (MDAP), hardware and software		CIO/G-6	Information Assurance (IA) Certification
				CLOE	CBM$^+$ functionality; interoperability
	DODAF system views	Integration into AILA		Combined Arms Support Command; PEOs/PMs, CIO/G-6, J-6	DODAF products required for JCIDS ICD, CDD, CPD
	CBM$^+$ plan in systems engineering plan (SEP)	JCIDS, net-centricity		CASCOM, ASA(ALT), G-4, J-4	Compliance with CBM$^+$ standards; JCIDS ICD, CDD, CPD (3170 and 6212)
	CBM$^+$ V&V plan in Test/Evaluation Master Plan (TEMP)	JCIDS, net-centricity			JCIDS ICD, CDD, CPD ISP
RCM foundation	RCM plan in SEP	JCIDS		CASCOM, ASA(ALT), G-4, J-4	Compliance with RCM standards; JCIDS ICD, CDD, CPD

Notes: BEA = Business Enterprise Architecture; CASCOM = U.S. Army Combined Arms Support Command; DBSMC = Defense Business Systems Management Committee; DISR = DoD Information Technology Standards and Profile Registry; T = Information Technology; ISP = integrated support plan; KPPs = key performance parameter; LOG = logistics; Log = Logistics; MAIS = major automated information system; MDAP = Major Defense Acquisition Program; PEO = Program Executive Officer; PLM+ = Product Lifecycle Management–Plus; TRADOC = Training and Doctrine Command.

The reviewing, approving, and certifying authorities depend on whether the application domain falls under the Business or Warfighter Mission areas, or both.

The system owner has significant responsibilities in achieving CBM^+ Information Assurance (IA) Certification. IA requires a DoD Information Assurance Certification and Accreditation Process (DIACAP) for all Information Systems, for which almost any system that processes or transmits data qualifies. Governing policy is contained in:

- Interim DoD Certification and Accreditation (C&A) Process Guidance, July 2006
- AR 25-2, 24 October 2007.

CBM^+ systems fall into two of the four types of IT system categories:

- Automated Information Systems
- Platform IT Interconnections.

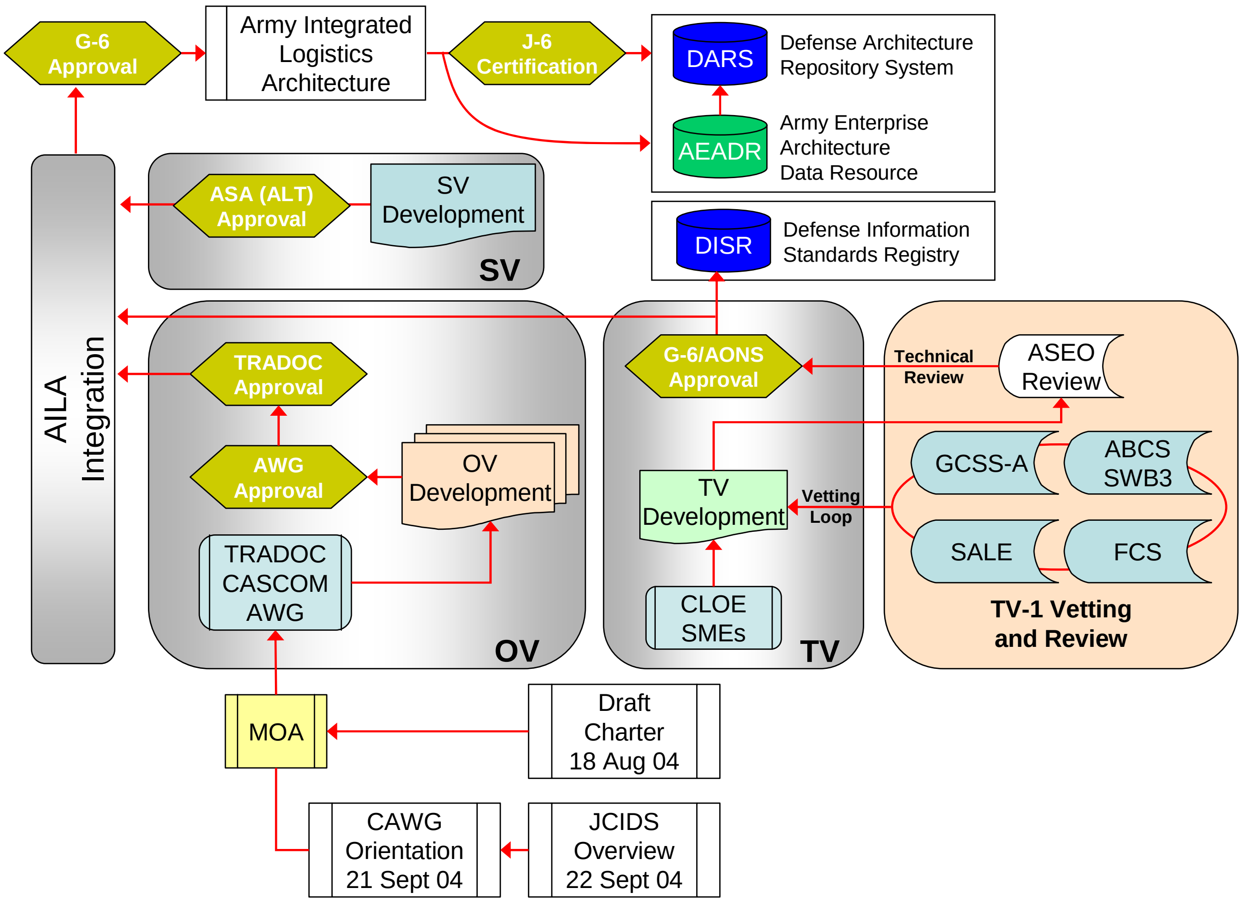
According to this viewpoint, CBM^+ information systems need to be certified and accredited in accordance with AR 25-2 which has a similar framework of four phases:

- Definition
- Verification
- Validation
- Post Accreditation.

A key element to the IA process is the System Security Authorization Agreement (SSAA), and SSP (System Security Policy) which are referenced in AR 25-2.

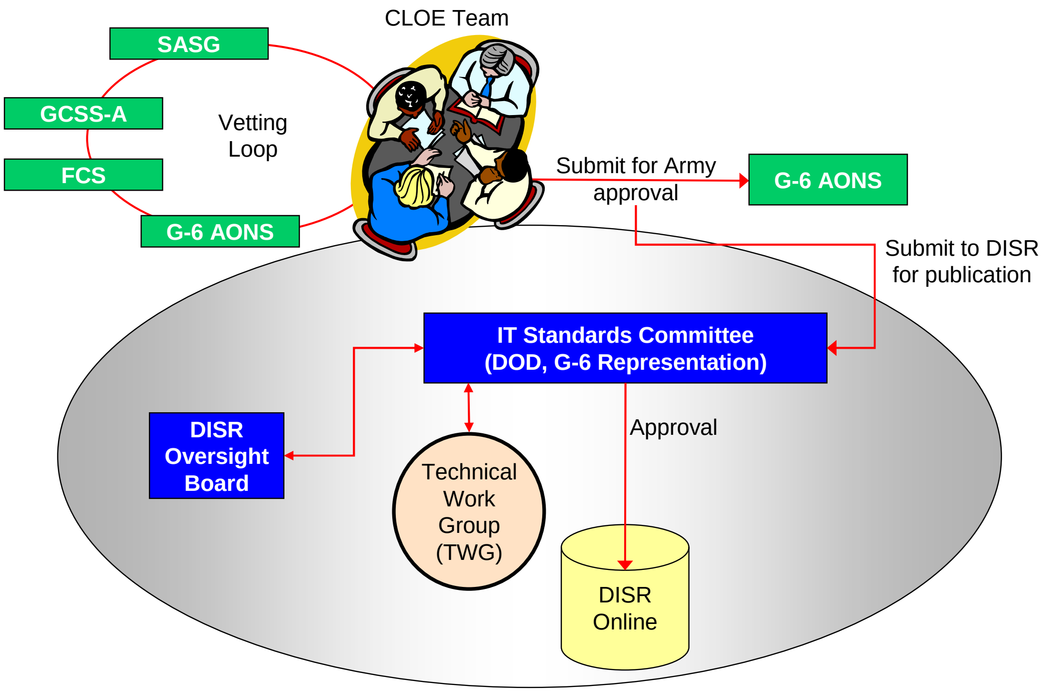
Figure 3-18 and Figure 3-19 depict the Army Integrated Logistics Architecture development, review, and approval processes which include CBM^+ functionality as an integral component.

Figure 3-18. AILA Oversight and Approval Process



Notes: ABCS = Army Battle Command System; AILA = Army Integrated Logistics Architecture; AONS = G-6 Office of Architectures, Operations, Networks and Space; ASA(ALT) = Assistant Secretary of the Army for Acquisition, Logistics and Technology; ASEO = Army Systems Engineering Office; AWG = Architecture Work Group; CASCOM = Combined Arms Support command; CAWG = CASCOM Architecture Working Group; CIO/G-6 = Office of the Army Chief Information Officer; CLOE = Common Logistics Operating Environment; FCS = Future combat Systems; GCSS-A = Global Combat Support System–army; J-6 = Command, Control, & Communications Systems Directorate, the Joint Staff; JCIDS = Joint Capabilities Integration and Development System; MOA = memorandum of agreement; OV = operational view; SALE = Single Army Logistics Enterprise; SMEs = subject matter experts; SV = system view; SWB3 = Software Block 3; TRADOC = Training and Doctrine Command; TV = technical view.

Figure 3-19. CLOE TV-1 Standards Process (including CBM+ Functionality)



Note: DISR = DoD Information Technology Standards and Profile Registry; DOB = DISR Oversight Board; FCS = Future Combat Systems; CIO/G-6 AONS = Office of the Army Chief Information Officer, Office of Architectures, Operations, Networks and Space; GCSS-A = Global Combat Support System–Army; IT = information technology; SASG = Strategy, Architecture and Standards Group.

3.5 Management Direction Policy

Current CBM+ policy is described in the following Department of the Army regulations and pamphlet:

- AR 700-127, *Integrated Logistics Support* http://docs.usapa.belvoir.army.mil/jw2/xmldemo/r700_127/cover.asp, 27 September 2007
- AR 711-7, *Supply Chain Management* http://docs.usapa.belvoir.army.mil/jw2/xmldemo/r711_7/cover.asp, 19 November 2004
- AR 750-1, *Army Materiel Maintenance Policy* http://docs.usapa.belvoir.army.mil/jw2/xmldemo/r750_1/cover.asp, 20 September 2007

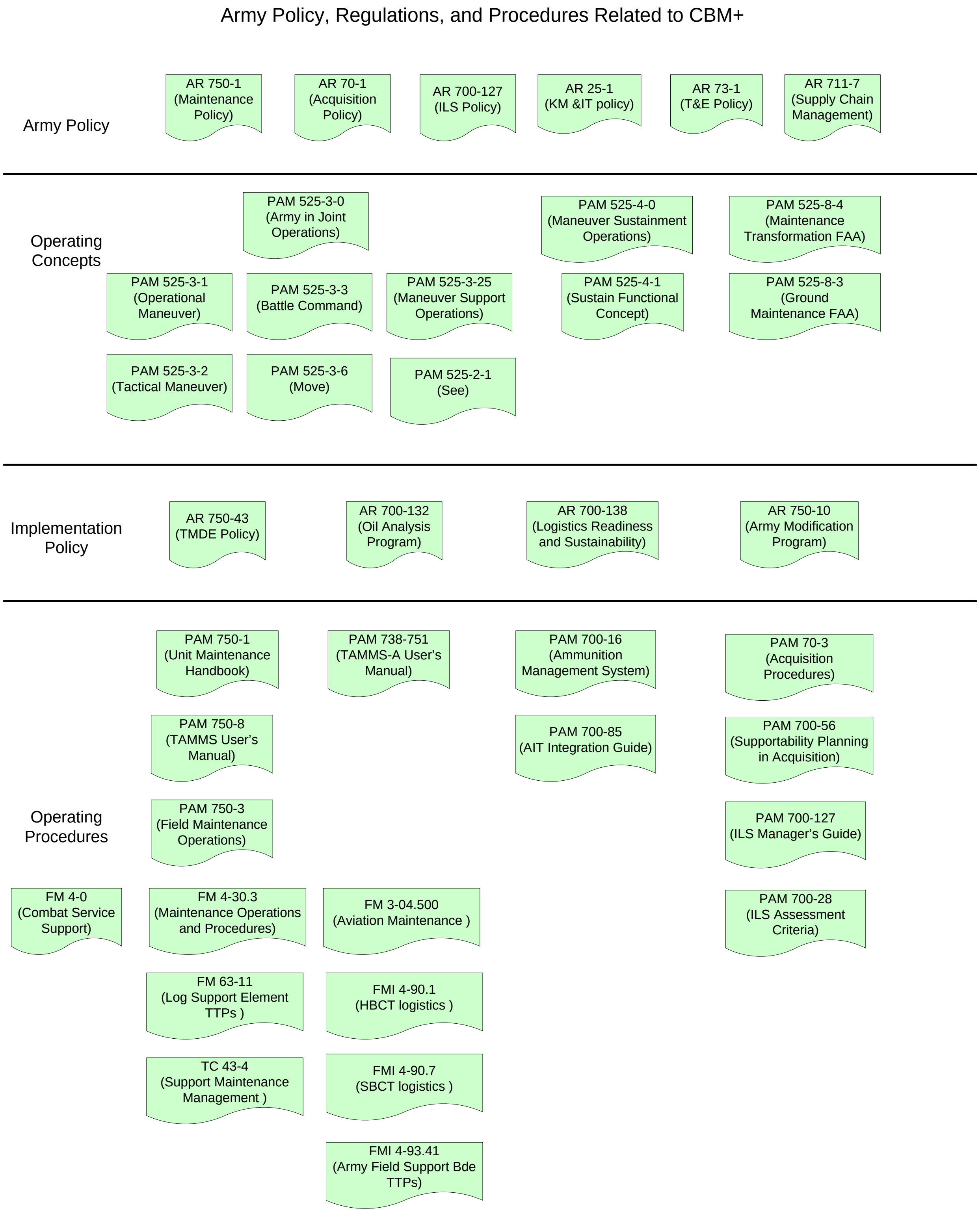
- AR 750-43, *Army Test, Measurement and Diagnostic Equipment* http://www.army.mil/usapa.epubs/xml_pubs/r750_43/cover.xml, 3 November 2006

- DA Pam 700-56, *Logistics Supportability Planning and Procedures in Army Acquisition* http://docs.usapa.belvoir.army.mil/jw2/xmldemo/p700_56/cover.asp, 21 April 2006.

The Deputy Under Secretary of Defense (Logistics and Materiel Readiness) (DUSD [L&MR]) has issued interim CBM$^+$ policy available at http://www.acq.osd.mil/log/msmp/CBM%2B.htm.

Figure 3-20 illustrates the range of current Army policy, regulations, and procedures that relate to CBM$^+$.

Figure 3-20. Army Policy and Doctrine for CBM+



Note: AR = Army regulation; FAA = functional area analysis; FM = field manual; FMI = field manual interim; HBCT = heavy brigade combat team; ILS = integrated logistics support; KM&IT = knowledge management and information technology; PAM = pamphlet; T&E = test and evaluation; TAMMS = The Army Maintenance Management System; TC = training circular; TMDE = test, measurement and diagnostic equipment; TTP = tactics, techniques, and procedures.

Army Logistics Enterprise policy has also been established for CLOE[19] and CBM$^+$.[20] Army policy for RCM was originally published in 1982[21], but subsequently cancelled. A recent revision to Army Regulation 750-1 invoked the RCM standards published by the Society of Automotive Engineers–International.[22]

Additionally, Army regulations contain guidance to the System Acquisition community for embedded diagnostics/embedded prognostics (ED/EP).[23]

Published CBM$^+$ policy has gaps and redundancies across the spectrum of memoranda and regulations. The need exists to harmonize published guidance for ED/EP and CBM$^+$ consistency.

RCM policy guidance needs to be updated and re-published, tying RCM to CBM$^+$ program plans and linking both RCM and CBM$^+$ to Total Life Cycle Systems Management in the Joint Capabilities Integration and Development System (JCIDS).[24] CBM$^+$ is now being mandated by the impending DoD CBM$^+$ Instruction (Appendix B), and it is likely that Army implementing policy will reflect the connection between RCM and CBM$^+$.

3.6 Governance

3.6.1 General

CBM$^+$ applies across many diverse Army organizations, interests, and policy domains. In particular, CBM$^+$ is influenced by decisions made in the oversight of Logistics Information Technology Portfolio Management and the allocation of resources in many areas impacting CBM$^+$ hardware, software, and communication infrastructure, as well as analytic and decision processes.

3.6.2 Logistics User Community

The premise of net-centricity as articulated in CJCSI 6212.01D[25] and the Network-centric Operations and Warfare–Reference Model[26] is founded on the formation and operation of communities of interest to define common sets of standards and data descriptions. These interface and data standards apply to CBM$^+$ as well as to other applications, in particular to logistics IT Portfolio

---

[19] Assistant Secretary of the Army (Acquisition, Logistics, and Technology) (ALT), memorandum, "Common Logistics Operating Environment Capabilities and Standards," 25 July 2003; and a memorandum jointly signed by Headquarters, Department of the Army, Deputy Chief of Staff, G-4, and the Military Deputy to the Assistant Secretary of the Army (ALT), "Implementing the Common Logistics Operating Environment (CLOE)," 5 May 2005.

[20] Assistant Secretary of the Army (Acquisition, Logistics, and Technology), memorandum, "Condition-Based Maintenance Plus," 17 August 2005.

[21] Department of the Army Pamphlet, 750-40, *Guide to Reliability Centered Maintenance (RCM) for Fielded Equipment*, 15 May 1982. Rescinded 1 July 2006.

[22] SAE International, Surface Vehicle/Aerospace Standard JA1012, *A Guide to Reliability-Centered Maintenance*, revised 2002; and Surface Vehicle/Aerospace Standard JA1011, *Evaluation Criteria for Reliability-Centered Maintenance (RCM) Processes*, 1999.

[23] Department of the Army, AR 70-1, *Army Acquisition Policy*, 31 December 2003; and AR 750-43, *Army Test, Measurement, and Diagnostic Equipment*, 14 December 2004.

[24] Chairman of the Joint Chiefs of Staff Instruction 3170.01E, *Joint Capabilities Integration and Development System*, 11 May 2005.

[25] Chairman of the Joint Chiefs of Staff Instruction 6212.01D, *Interoperability and Supportability of Information Technology and National Security Systems*, 8 March 2006.

[26] Described at http://en.wikipedia.org/wiki/NCOW.

Management. As we show in the next section, the stakeholders must organize and agree to a common path forward for both the CLOE and CBM$^+$ data strategy to work efficiently across the enterprise.

3.6.3 DoD CBM$^+$ Governance

In a policy memorandum issued by the Deputy Undersecretary of Defense for Logistics and Materiel Readiness, the Materiel Readiness Senior Steering Group (MRSSG) was tasked to monitor DoD CBM$^+$ initiatives and programs and to provide a forum for the exchange of information and ensure DoD efforts in CBM$^+$ are coordinated across the military services.[27]

A Joint Service CBM$^+$ Integrated Product Team (IPT) assists the Office of the Secretary of Defense (OSD) in monitoring and coordinating CBM$^+$ research and implementations, reviewing service progress, sharing, and warehousing information, recommending action, and conducting focused activities, as directed.[28]

3.6.4 Army CBM$^+$ Governance

Army CBM$^+$ policy and governance responsibilities are currently distributed among the Deputy Chief of Staff, G-4; ASA(ALT); and the Army Materiel Command (AMC). The AMC CBM$^+$ governance function is embodied by the operation of the Business Process Council which reports to the AMC Principal Deputy G-3 as part of the Single Army Logistics Enterprise (SALE).

The Army Logistics Innovation Agency (LIA) serves as the CBM$^+$ lead for the DCS, G-4. The principal program fulfilling this LIA responsibility is the Common Logistics Operating Environment (CLOE); the principal process and product of CLOE is the Army Integrated Logistics Architecture (AILA), as well as a series of technical tests and demonstrations. AILA is both the CBM$^+$ technical foundation and the principal management tool for oversight of many logistics interoperability and net-centricity requirements.

The CLOE-AILA provides the DoD Architecture Framework (DODAF)[29] architectural foundation for CBM$^+$ information exchange. Capability requirements development is the responsibility of the U.S. Army Training and Doctrine Command (TRADOC), and its subordinate Combined Arms Support Command (CASCOM).

A consolidated approach to CBM$^+$ governance similar to that established for OSD is needed to drive stakeholder coordination across the Army. The need exists across Army organizations to de-conflict resource requirements and differing technical approaches for CBM$^+$ as well as to harmonize development efforts at the DODAF architectural level. Additionally, a consolidated Army governance function for CBM$^+$ needs to speak with a consistent voice to the OSD CBM$^+$ IPT and MRSSG, rather than have potentially conflicting views generated by different Army organizations. The AILA is a principal tool for that governance function.

---

[27] Department of Defense, Deputy Under Secretary of Defense for Logistics and Materiel Readiness (DUSD[L&MR]) Memorandum, Subject: Condition-Based Maintenance Plus, 25 November 2002.

[28] Department of Defense, Assistant Deputy Under Secretary of Defense for Materiel Readiness and Maintenance Policy, Condition-Based Maintenance Plus Integrated Product Team Charter, undated from November 2005 time frame, available at http://www.acq.osd.mil/log/mrmp/cbm+/CBM+_Charter.pdf.

[29] DODAF Working Group, *DoD Architecture Framework*, Version 1.0, Deskbook, 9 February 2004.

The Army governance structure also needs to support programmatic actions for capabilities that do not currently exist within Army organizations. In particular, these include analytic capabilities for CBM^{+} data, and decision support structures to make use of the data. The combination of policy, doctrine, and requirements (with supporting cost-benefit analysis) make up the essential elements to justify resource allocations in the Army Planning, Programming, Budgeting, and Execution System (PPBES).

3.7 Incremental Approach to Achieving CBM^{+} Capabilities

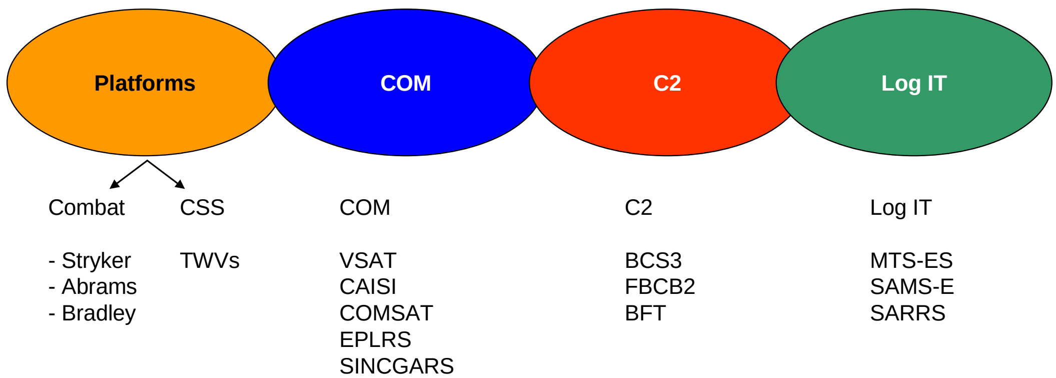
The CLOE program recommends a phased approach similar to software blocking for CBM^{+} implementation which requires that many separate program and project initiatives be grouped into implementation packages, called Increments.

Three principal Increments are currently outlined, linking CBM^{+} capabilities into software blocking packages that synchronize capacities of the following four major elements with the master schedule for Software Blocking:

- Combat platforms and combat support platforms
- C2 Systems
- Logistics IT systems
- Communication systems.

Increment One is comprised of the elements identified in Figure 3-21. The figure shows graphically that a software blocking strategy can be grouped into three major categories, one each for platforms, C2 Systems, Log IT systems, and communications systems. The other increments follow a similar process, bundling CBM^{+} system enhancements as shown in Table 3-5.

Figure 3-21. CBM^{+} Increment One Implementation System of Systems



Notes: C2 = command and control; CAISI = Combat Service Support Automated Information Systems Interface; COM = communications; COMSAT = communications satellite; CSS = combat service support; EPLRS = Enhanced Position Location and Reporting System; IT = information technology; LOG = logistics; MTS-ES = Movement Tracking System – Ehnhanced System; SAMS-E = Standard Army Maintenance System–Enhanced; SARRS = Standard Army Retail Supply System; SINCGARS = Single Channel Ground-Airborne Radio System; TWVs = tactical wheeled vehicles; VSAT = very small aperture terminal.

Increments two and three, pending publication at this writing, expand the systems list in each of the four categories, taking a system-of-systems approach for all systems that are employed within a Brigade Combat Team (BCT) or are external to it that exchange information with the BCT. These systems are also a part of the master Software Blocking Schedule and include GCSS-A, Net-enabled Combat Command (NECC) and other communications systems, including the Joint Tactical Radio System (JTRS) and the Warfighter Information Network-Tactical (WIN-T).

Table 3-5. Increment One, CLOE-CBM^{+} System Enhancements

System	Modified for Increments 1 Fielding	Enhancements
Platforms		
Stryker	Y	Logistics information transferred from the platforms to FBCB2 system Fuel, equipment, and LRU status (ICD message #s 22, 23, 25, 37)
Bradley	Y	
Abrams	Y	
TWVs	N	
C2 Systems		
BCS3	N	
FBCF2	Y	Rolls up equipment status and logistical information from the platforms and distributes via a LOG distribution list within the brigade SITREP, CFS, and LOGSTAT (VMF messages: K05.14, K07.12, KO7.03)
Logistics Support Systems		
MTS	N	
SAMS	Y	SAMS-E will combine SAMS—1 and ULLS-G functionality
SARSS	N	
Communication Systems		
VSAT	N	Existing communication systems expected to support planned functionality
CAISI	N	
COMM SAT	N	
EPLRS	N	
SINCGARS	N	

Notes: LOGSTAT = logistics status report; SITREP = situation report; VMF = variable message format.

Section 4
CBM+ Roles and Responsibilities

This is an initial set of actions for a variety of Army CBM+ stakeholder organizations that will lead to a full CBM+ implementation. The actions will require extensive coordination and cooperation.

The actions address a wide range of topics that must be incorporated into a full-up CBM+ implementation. Table 4-1 lists examples of the range of roles and missions for the major stakeholders—the examples are not all-inclusive.

Table 4-1. Examples of CBM+ Stakeholder Roles and Missions

	Organization												
Action areas	**ASA(ALT)**	**PEOs, PMs**	**G-4**	**LIA**	**CIO/G-6**	**TRADOC**	**CASCOM**	**AMC**	**LCMCs**	**ARDECs**	**AMSAA**	**LOGSA**	**ATEC**
Policy	X		X		X								
Doctrine						X	X						
Requirements						X	X						
Research and development		X								X			
Metrics				X				X			X	X	
Architectures and standards			X	X		X	X					X	
Materiel solutions		X										X	
Simulation and modeling			X	X									
Verification and validation				X									X
Analytics[a]		X		X					X	X	X	X	
Decision authorities	X	X	X		X	X	X	X	X				
Training Development			X			X	X						

Notes: PM = program manager, TRADOC = U.S. Army Training and Doctrine Command, AMC = Army Materiel Command, LCMC = Life Cycle Management Command; ARDEC = Armament Research Development and Engineering Center, AMSAA = Army Materiel Systems Analysis Activity, LOGSA = Logistics Support Activity, ATEC = Army Test and Evaluation Command.

[a] In this table, the term "analytics" merits further explanation. The term is meant to encompass the range of analytic tools and processes that will be applied to CBM data. Examples include data mining, triggers and alerts, trending, and other forms of data presentation to support decision making for improved sustainment. The term applies to any management level with a requirement to assess system performance and identify potential areas for improvement.

4.1 Assistant Secretary of the Army (Acquisition, Logistics, and Technology) (ASA[ALT])

- Provide CBM^+ guidance for acquisition policy to focus the direction of CBM^+ implementation across platforms and systems.
- Ensure performance-based logistics and other contract sustainment support providers provide CBM^+ data to the Logistics Information Warehouse, regardless of the contract structure employed.
- Pursue development of prognostic capabilities as science and technology initiatives.
- Provide representation to the CBM^+ oversight body.

4.2 Deputy Chief of Staff, G-3/5/7

- Provide representation to the CBM^+ oversight body.

4.3 Deputy Chief of Staff, G-4

- Serve as Army lead for CBM^+ implementation.
- Revise Army maintenance program to CBM^+ which includes governance and strategy based upon RCM analysis.
- Develop the CBM^+ implementation requirements with major stakeholders for Army-wide implementation.
- Develop policy to mandate CBM^+ implementation as well as realign sustainment engineering resource applications.
- Develop a strategy with TRADOC for doctrinal development to support CBM^+ implementation.
- Lead development of CBM^+ business processes and information exchanges and ensure they are reflected in the Army Integrated Logistics Architecture (AILA).
- Synchronize CBM^+ within the larger Army logistics user community.
  - Establish an oversight body to assure cross-functional interests are represented and addressed.
  - Serve as CBM^+ oversight body chair to govern CBM^+ implementation. Membership to CBM^+ oversight body should include; ASA(ALT), TRADOC G-3/5/7, CIO/G-6, G-8, AMC, TRADOC, and others on an as required basis. The oversight body will be supported by a subordinate body such as a CBM^+ Council of Colonels to execute the cross enterprise CBM^+ governance and implementation. Because

CBM$^+$ is a rapidly developing area in the Army, the CBM$^+$ Council of Colonels will meet monthly and the CBM$^+$ oversight body quarterly.

  - Direct the establishment of an Army center of excellence for CBM$^+$ methodologies and best practices.

- Identify and validate resource requirements for CBM$^+$ implementation on enterprise-wide basis within the Army Planning, Programming, Budgeting, and Execution System.

- Facilitate resource synchronization in coordination with DCS, G-8, ASA(ALT) and DCS, G-3, to identify resource requirements for CBM$^+$ implementation across all applicable platforms, organizations, and business information processes.

- Synchronize CBM$^+$ with Army Transformation initiatives.

- Manage the Logistics IT Portfolio to support CBM$^+$ implementation and initiatives, as guided by:

  - Office of the Under Secretary of Defense (Logistics and Materiel Readiness), *Business Mission Area, Logistics Domain Advocacy Review Plan*, Version 1.0, 25 August 2004

  - U.S. Army Chief Information Officer CIO/G-6, *Army Enterprise Capabilities-Based Information Technology Portfolio Management Process Guidance* (Working Draft), Version 3.0.

- Develop CBM$^+$ policy in conjunction with ASA(ALT) that will serve to focus the Army implementation of CBM$^+$ to emphasize RCM, predictive maintenance, and the transition to prognostics, adaptive logistics, and software agents.

- Assess the adequacy of Army logistics IT systems to implement CBM$^+$ on an enterprise-wide basis

  - Identify gaps in CBM$^+$ capability in logistics IT systems; in particular, identify the CBM$^+$ data aggregation and server strategy to achieve fleet-wide health management and feedback

  - Recommend IT Portfolio investment alternatives within the combined logistics user community to address CBM$^+$ capability gaps.

- Assess CBM$^+$ and logistics IT interoperability between Current Force platforms and FCS-unique platforms

  - Identify gaps in functionality and interoperability

  - Recommend gap resolution mechanisms in both Architecture and Systems development.

- Evaluate CBM^+ data collection and decision support methodologies.
- Develop a modeling and simulation capability that can verify and validate CBM^+ functionality and platform embedded system health management systems effectiveness.
- Integrate the evaluation of embedded system health management and CBM^+ capabilities, business processes, and functionality at both the platform and the enterprise logistics IT-level.
- Establish metrics and benchmarks against which to measure the effectiveness of CBM^+ and platform embedded system health management.
- Develop an Army-wide CBM^+ implementation plan consistent with the deliverables described above for the CBM^+ roadmap, including stakeholder steps and milestones.
- Develop training requirements and plan for acquisition, sustainment program managers, and maintainers.
- Identify capabilities and enablers for CBM^+ implementation.
- Determine gaps and requirements for establishing a Logistics Common Operating Environment PM supporting CBM^+ integration

4.4 Chief Information Officer, CIO, G-6

- Issue policy guidance to the Army on the application of approved information technology architectures to support CBM^+.
- Provide oversight of Army integrated architectures.
- Incorporate Technical Architecture views and related technical interchange standards into the Army Technical Architecture to assure interoperability of CBM^+-enabled systems and platforms.
- Develop the Army's Technical Standards Profiles.
- Review/approve IT architectures prior to investment and ensure adequate information resources are applied to sustain required capabilities for CBM^+.
- Provide architectures standards waivers as required.
- Provide representation to the CBM^+ oversight body.

4.5 Deputy Chief of Staff, G-8

- Provide guidance and support for preparation of successful resourcing effort in the PPBES.
- Provide representation to the CBM^+ oversight body.

4.6 U.S. Army Logistics Innovation Agency (LIA)

- Serve as G-4 lead for CBM$^+$ implementation, RCM application, and the transition to prognostics and adaptive logistics.
- Establish an Army center of excellence for CBM$^+$ methodologies.
- Establish a CBM$^+$ interoperability certification process to assist PM acquisition for embedded system health management technologies.
- Develop a platform-by-platform spreadsheet of current force capabilities for embedded system health management with retrofit schedules for unit Army Force Generation cycles.
- Develop a blocking strategy for developing and acquiring upgraded embedded system health management enablers.
- Assist synchronization and integration of the platform Systems Architecture for embedded system health management with the operational and technical views to create an instance of the Army Integrated Logistics Architecture (AILA).
- Establish a business case for CBM$^+$ implementation.
- Establish liaison and interface with the CBM$^+$ stakeholder community systems integration laboratories and process centers.
- Research, evaluate, demonstrate, and integrate analytic methodologies for CBM$^+$, including applications of simulation and modeling capabilities.
- Provide membership and support to the CBM$^+$ oversight body to assist the G-4 in the CBM$^+$ implementation efforts.

4.7 U.S. Army Materiel Command (AMC)

- Support Science and Technology initiatives for CBM$^+$ capabilities.
- Work with PEO Enterprise Information Systems to integrate tactical unit level logistics systems and capabilities with national level systems.
- Establish analytic and decision support capabilities for application at all levels from the operating platform through Army-wide CBM$^+$ assessments and provide support to stakeholder organizations, through the Life Cycle Management Commands (LCMCs) and the Research, Development, and Engineering Command, as well as product support integrators.
- Ensure both current and future platforms are equipped with requisite CBM$^+$ capabilities in hardware (health management computer, real time sharing, SATCOM or radio links, and WiFi capability, etc.) and in software (embedded IETM, DPMCS, logbook, and predictive health monitoring, etc.).

- Establish and support CBM$^+$ analysis and decision processes within current force systems in LCMCs.
- Create and operate new capabilities within the Logistics Information Warehouse to support CBM$^+$ data storage and retrieval.
- Provide assessments of CBM$^+$ data to stakeholder organizations.
- Provide representation to the CBM$^+$ oversight body.

4.8 U.S. Army Training and Doctrine Command (TRADOC)

- Approve Army Operational Architectures (the Army Integrated Logistics Architecture).
- Coordinate with ASA(ALT) to establish the JCIDS milestone requirements to certify CBM$^+$ methodologies.
  - Review and revise existing acquisition doctrine and literature where appropriate.
  - Incorporate CBM$^+$ requirements in Total Life Cycle System Management (TLCSM).
- Develop the Operational Architecture supporting CBM$^+$.
- As the principal Army combat developer, ensure that CBM$^+$ capabilities are considered in the JCIDS process for all new equipment, weapon systems, and information systems.
- Assess the adequacy of policy, standards, and requirements governing CBM$^+$ implementation.
- Identify gaps in adequacy of CBM$^+$ doctrinal requirements.
- Recommend changes to doctrine and literature to address CBM$^+$ implementation.
- Establish business rules for supply, maintenance, and Army Single Stock Fund transactions that deal with issues stemming from CBM$^+$ application, such as line replaceable unit (LRU) and shop replaceable unit (SRU) repair parts.
- Provide representation to the CBM$^+$ oversight body.

4.9 U.S. Army Test and Evaluation Command (ATEC)

- Support testing and evaluation relating to CBM$^+$ capabilities.
- Verify/validate current and future CBM$^+$ applications, data system functionality, RCM applications, and decision support processes meet the intent of systems requirements.

Appendix
Abbreviations

AAE	Army Acquisition Executive
AID	analog digital
AILA	Army Integrated Logistics Architecture
AIT	Automatic Identification Technology
AKO	Army knowledge online
AL	autonomic logistics
ALT	Acquisition, Logistics & Technology
AMC	Army Materiel Command
AMSAA	Army Materiel Systems Analysis Activity
ANSI	American National Standards Institute
AO	Operational Availability rate
AOR	area of responsibility
AR	Army Regulation
ARDEC	Armament Research Development and Engineering Center,
ARMS	Asset Reliability, and Maintenance Specialists
ASA (FM)	Assistant Secretary of the Army (Financial Management)
ATEC	Army Test and Evaluation Command
BEA	Business Enterprise Architecture
BFT	Blue Force Tracking
BI	business intelligence

BIT	built-in test
C2	command and control
CAISI	Combat Service Support Automated Information System Interface
CASCOM	U.S. Army Combined Arms Support Command
CBM	Condition-Based Maintenance
CBM^+	Condition-Based Maintenance—Plus
C&A	Certification and Accreditation
CDD	Concept Development Document
CIO	Chief Information Officer
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CLOE	Common Logistics Operating Environment
CMMS	Computerized Maintenance Management System
COI	community of interest
COP	common operating pictures
CPD	capability production document
CRIS	Common Relational Information Schema
CWT	Customer Wait Time
DAS	Defense Acquisition System
DBMSC	Defense Business Systems Management Committee
DCD	Directorate for Combat Development
DCS	Deputy Chief of Staff
DIACAP	DoD Information Assurance Certification and Accreditation Process

DISR	DoD Information Technology Standards and Profile Registry
DODAF	DoD Architectural Framework
DODI	DoD Instruction
DOTLMPF	Doctrine, Organizations, Training, Leader Development, Materiel, Personnel, and Facilities
DPMCS	Digital Preventive Maintenance Checks and Services
DTIC	Defense Technical Information Service
EAI	Enterprise Application Integration
ED/EP	embedded diagnostics and prognostics
EIS	Enterprise Information Systems
EPHM	embedded platform health management
EPLRS	Enhanced Position Location Reporting System
EPLS	Embedded Platform Logistics System
FBCB2	Force XXI Battle Command Brigade and Below
FCS	Future Combat Systems
FM	frequency modulated
GCSS	Global Army Combat Support Systems
GIGES	Global Information Grid Enterprise Services
GPS	global positioning system
HBCT	Heavy Brigade Combat Team
HUMS	health unit monitoring system
IA	Information Assurance
IAIC	Intra-Army Interopability Certification

ICD	Initial Capability Document
IEEE	Institute of Electrical and Electronics Engineers
IER	Information Exchange Requirement
IETF	Internet Engineering Task Force
IETM	Interactive Electronic Technical Manual
ILS	Integrated Logistics Support
IPT	Integrated Product Team
ISO	International Organization for Standardization
IT	information technology
J-AIT	Joint Automated Information Technology
JALAT	Joint Army Logistics Analysis Tool
JCIDS	Joint Capability Integration Development System
JTDI	Joint Technical Data Integration
JTRS	Joint Tactical Radio System
LAN	local area network
LCMC	Life Cycle Management Command
LCOP	logistics common operating pictures
LIA	U.S. Army Logistics Innovation Agency
LOG	logistics
LOGSA	Logistics Support Activity
LRU	line replaceable unit
M/M	Message Manager

MDAP	Major Defense Acquisition Program
MHIS	Major Automated Information Systems
Mil-Std	military standard
MIMOSA	Machinery Information Management Open Systems Alliance
MRSSG	Materiel Readiness Senior Steering Group
MS	milestone
MTBF	mean time between failure
MTS	Movement Tracking System
MTTR	Mean-Time-to-Repair
NAVAIR	Naval Air Systems Command
NECC	Net-enabled Combat Command
NEOF	No-Evidence-of–Failure
NMCS	non-mission capable–supply
OBSA	off-board service application
OEM	original equipment manufacturer
OPTEMPO	operational tempo
OSA	Open Systems Architecture
OSD	Office of the Secretary of Defense
OV	operational view
PdM	predictive maintenance
PEO	Program Executive Officer
PLM+	Product Lifecycle Management–Plus

PM	program manager
PMA	Portable Maintenance Aid
PMCS	preventive maintenance checks and services
PoE	proof of enabler
POM	Program Objective Memorandum
PPBES	Planning, Programming, Budgeting, and Execution System
RCM	Reliability Centered Maintenance
RFID	Radio Frequency Identification
RPSTL	repair parts and special tools list
RUL	remaining useful life
S&RL	Sense and Respond Logistics
SAEMS	Society of Automotive Engineers
SALE	Single Army Logistics Enterprise
SAMS	Standard Army Maintenance System
SARRS	Standard Army Retail Supply System
SBCT	Stryker brigade combat team
SCOM	Supply Chain Operations Mode
SDD	System Development and Demonstration
SEP	systems engineering plan
SGR	Sortie-generation rate
SIL	Systems Integration Laboratory
SIM	Serialized Item Management

SINCGARS	Single Channel Ground-Airborne Radio System
SRU	shop replaceable unit
SSAA	System Security Authorization Agreement
SSP	System Security Policy
SV	systems view
TEMP	Test and Evaluation Master Plan
TLCSM	Total Life Cycle Systems Management
TRADOC	U.S. Army Training and Doctrine Command
TV	technical standards view
ULLS	Unit Level Logistics System
URL	Uniform Resource Locator
USMC	United States Marine Corps
V&V	Verification and Validation
W3C	World-Wide Web Consortium
WAN	wide area network
WiFi	wireless fidelity
WIN-T	Warfighter Information Network-Tactical
XML	eXtensible Markup Language