Introduction

The implementation of a Military Message Handling System (MMHS) is a large project, typically extending over a significant period of time and involving large numbers of organisations and individuals.

The movement towards modern MMHS solutions introduces a new and often confusing array of terminology and applicable standards. Understanding this new technology and how it may best be implemented is challenging. To achieve the expected return on an investment of this scale, an understanding of the requirements, capabilities, management and use of the technology is essential.

Nexor has devised its MMHS Seminar to support organisations and individuals who need to understand the technology and the concepts involved. This reference manual is provided to delegates and is intended to supplement the information supplied during the seminar.

Why is an MMHS needed?

Legacy systems for passing information from one location to another are typically very manually intensive, requiring intervention by a relatively large number of individuals. These telex-based systems with paper audit trails are becoming increasingly expensive and are prone to error. The time taken for a message to travel from originator to recipient is also unacceptably long. It is essential that an organisation's communication system is at least as efficient as those of others of a similar nature, using modern technology, and, as cooperation becomes more commonplace, that the systems are capable of communicating with each other using standard protocols.

Over time, requirements have changed. From the initial need to transmit simple, text based messages, it is now necessary to send complex documents, diagrams, photographs and sometimes audio messages, all with the same basic requirements for efficient low-cost guaranteed delivery.

What is involved in implementing an MMHS?

In the commercial world, the technological advances in the electronic transmission of messages have accelerated in recent years. These new technologies can form the basis of an effective MMHS but they require careful enhancement and configuration to ensure that all the additional requirements of a military system can be met.

In addition to defining requirements for technology, the software and hardware components that form the tangible elements of an MMHS, other elements must be considered. These include the potential to expand and enhance the system in the future, the requirement for training of both those who will manage the system and those who will use it and the accessibility of experts in the relevant fields who can assist in ensuring that maximum benefit is obtained from the investment made.

What is the purpose of this manual?

Following attendance at the Nexor MMHS Seminar, and with the aid of this reference manual, a broad understanding of an MMHS will be gained. In particular, the components forming an MMHS, organisational and user requirements of an MMHS and the terminology used to describe them will be understood.

This reference manual assumes minimal prior knowledge and is organised in the following manner:

- “Introduction”, beginning on page 9

  Describes the purpose behind this document and the associated seminar, outlining the contents of each chapter within the book.

- “Messaging”, beginning on page 13

  A brief history of messaging, describing the two distinct variations of X.400 messaging and Internet messaging, based on SMTP. The two different standards are discussed and an overview of their features is included.

- “Directories”, beginning on page 23

  The concept of using a directory to store information required both by people and by other applications is discussed. An overview of the security methods forming part of the X.500 standards is given, together with a brief insight into the technology behind a modern X.500 directory.

- “Security Issues”, beginning on page 35

  Security is of paramount importance within an MMHS and an entire chapter is devoted to the methods used to ensure that the required standards are met. An introduction to the terminology and an understanding of the basic concepts is provided in this chapter.

- “Military Message Handling System”, beginning on page 57

  This chapter describes the detailed requirements of an MMHS, contrasting it with a basic, non-military MHS.

- “Overview of the Components of an MMHS”, beginning on page 65

  An overview of the components forming a modern MMHS is given in this chapter, showing the interaction between them.

- “Backbone Components”, beginning on page 67

  The backbone of the MMHS is the area giving it structure, interconnecting the various section separated by purpose or by geography.

  There is little or no direct interaction with end-users at this level; this is the domain of systems administrators.

- “Local Components”, beginning on page 71

  The hub of a local portion of the MMHS, serving a particular geographic or functional unit. The components in this section may vary, depending on local and national requirements.

- “Workstation Components”, beginning on page 79

  The portion of the MMHS that is the most visible, with direct interaction from end-users who will be composing, releasing or reading messaging, depending on their level of responsibility.

  Applications to enable appropriate individuals to update the contents of a directory or to manage features such as mailing lists may also be accessible from workstations.

- “Border Components”, beginning on page 85

  The components described in this section sit on the border between the MMHS and other messaging systems. Border components may also be found within a single organisation, at the border between high and low security zones.

- “The Future of the MMHS”, beginning on page 89

  This chapter takes a look at emerging technologies and how these may be deployed to further enhance the capabilities and usability of the modern MMHS.

  The possibilities discussed include the use of XML, the use of additional encoding and transport mechanisms and advances in security.

- “Standards”, beginning on page 93

  Listings of applicable messaging, directory and military standards are available, providing a quick reference to relevant information.

- “List of Acronyms”, beginning on page 97

  A list of acronyms is provided to assist in recognising and understanding those used extensively within messaging, and within an MMHS in particular.

About Nexor

Nexor provides policy directed messaging solutions to government, military and enterprise sectors. Founded in 1990, the company specialises in delivering solutions for situations where it is absolutely critical that the message gets through, where the value of communications is high and where the need for secure, reliable and auditable message handling is paramount.

Nexor’s messaging solutions build on existing COTS (Commercial Off-The-Shelf) infrastructure to facilitate high levels of message security, information integrity and adherence to organisational policies. Organisations that use Nexor solutions benefit from improved conformance to standards, reduced risk and high levels of interoperability. Nexor enables organisations to address security needs and apply accountability, traceability and control to their existing messaging solution with a low overall cost of ownership.

Nexor is proud to count amongst its customers some of the world's largest government, military and commercial organisations, including the British MoD and other UK Government departments, the Australian Department of National Defence, US military and intelligence agencies including the Army, Navy, and NSA, Canadian Crown agencies and departments, Barclays Bank, BT, CSFB, and 22 European state banks including the Bundesbank and the Bank of England. Nexor, IBM and Cogent have been chosen to deliver the next generation messaging system for the NATO alliance.

Partnerships

Partnerships with major systems' integrators such as Fujitsu, EDS, Syntegra and Lockheed Martin enhance Nexor's reputation and standing in the industry. We are a Microsoft Certified Solution Provider and part of the Entrust Alliance Developer Program. We also provide OEM technology to companies such as Novell and CommPower.

Industry forums

Nexor are active members of the Armed Forces Communications and Electronics Association (AFCEA), the European Electronic Messaging Association (EEMA), the Internet Engineering Task Force (IETF), the Organisation for the Advancement of Structured Information Standards (OASIS) and the Open Group.

Contact Nexor

Nexor has office locations in:

- Nottingham, UK (Head Office)
- Washington DC, USA
- Ottawa, Canada
- Sydney, Australia

Further information on Nexor's solutions may be obtained from our website: www.nexor.com