Chapter X

A Standards-Based Common Operational Environment

Jaroslav Blaha
NATO ACCS Management Agency, Belgium

INTRODUCTION - THE NEED FOR A COE

NATO as an international organization consists of representatives from 19 nations and has to satisfy the political, operational and technical requirements of all members. In addition to the development of specific NATO information systems, it has to consider and support means for interoperability with national systems. Taking into account the life-cycle-cost aspects, it becomes clear that a standardization policy must consider the cost-effective maintenance, upgrade and replacement of system components and their interfaces.

Standardization of NATO specific interfaces is a well-established process, which results in ‘Standardization Agreements’ (STANAGs). Those are specifications of proprietary standards or of adaptations of international (e.g. ITU, ISO) standards. STANAGs have two major disadvantages: First, the process to develop a new or to modify an existing standard is lengthy; the process to get the specification ratified by the relevant nations is even longer. This can result in STANAGs, which do not reflect the state-of-the-art of standards. Second, as STANAGs often specify standards that are different from international or commercial standards, there is very little market and product support. This leads naturally to increased development and procurement costs.

In military terms a Command, Control and Information System (CCIS) is the equivalent to a Management Support and Information System (MSS/MIS) in the commercial domain.

The COE efforts originated with the simple observation that in command, control and information systems certain functions (e.g. message exchange, tasking, communication interfaces) are so fundamental that they are required for virtually every CCIS. Yet these functions are built over and over again, in often-incompatible ways, even for systems with almost identical requirements. If such common functions could be extracted, implemented as a set of extensible building blocks, and made readily available to system designers, development schedules could be...
accelerated and substantial savings could be achieved (although the quantitative demonstration of cost effectiveness is a complex problem). Moreover, interoperability would be significantly improved because common software is used across systems and the functional capability only needs to be built correctly once rather than for each project (DII-COE, 1999).

The COE currently focuses on CCISs and mostly ignores special-to-purpose systems outside this domain (e.g. satellite control, onboard navigation systems). CCISs are currently the most common and therefore preferred domain. However, it is expected that the COE concept will over time be extended into non-CCIS areas. One example is the Domain Specific Software Architectures (DSSA) project of ARPA, which attempts to standardize real-time avionics architectures through an Avionics Domain Application Generation Environment (ADAGE) (ADAGE, 1999).

Throughout this paper the following terms will be used:

- **Common applications, modules or subsystems** provide functionality, which is available and needed by effectively all users, independent of their specific task in the organization. Examples are e-mail or word-processing.
- **Functional Area Sub-Systems (FASS)** and associated applications provide functionality, which is required only by a limited group of users specifically for their tasks. Examples are logistics or human-resource management.

An integrative approach is needed, which could provide guidance to project managers, engineers and budget authorities on how to

- derive generic technical requirements from existing operational requirements, i.e. by mapping of existing building blocks of technical solutions (e.g. an e-mail system) against a common class of operational needs (e.g. communicate tasks effectively with remote subordinates),
- select state-of-the-art standards, which support the desired functionality, and are implemented in commercially available and market-proven products to avoid bespoke developments,
- aggregate standards and the associated products into building blocks with well-known and tested characteristics, which can be assembled to operational systems with minimal development effort, and
- to reduce system development risks, and to ensure the system’s ability to evolve in order to benefit from information technology advances.

In addition, this approach had to be harmonized with ongoing standardization activities, both on policy level (interoperability policies) and technical level (STANAG development). To allow smooth cooperation with the member nation’s systems, the resulting NATO COE should also be harmonized and compatible with existing national COEs.

**BACKGROUND - WHAT IS A COE?**

The COE concept is an approach that is much broader in scope than just software reuse or standard compliance. The COE concept encompasses both, but its principles are far more reaching, as it comprises

- from a structural viewpoint
  - an architecture and approach for building interoperable and open systems,
Related Content

The Challenge of Establishing a Recognized Interdisciplinary Journal: A Citation Analysis of the International Journal of IT Standards and Standardization Research
www.igi-global.com/article/the-challenge-of-establishing-a-recognized-interdisciplinary-journal/83544?camid=4v1a

Adopter-Centric Checklist Application: Product Life Cycle Support Adoption and Diffusion in the UK MoD
Josephine Wapakabulo Thomas (2010). *Data-Exchange Standards and International Organizations: Adoption and Diffusion* (pp. 221-256).
www.igi-global.com/chapter/adopter-centric-checklist-application/38122?camid=4v1a
Understanding the Technology Development Process at the Early Standardization Stage: The Case of Cognitive Radio
www.igi-global.com/article/understanding-the-technology-development-process-at-the-early-standardization-stage/121702?camid=4v1a

Framework Design and Case Study for Privacy-Preserving Medical Data Publishing
www.igi-global.com/chapter/framework-design-and-case-study-for-privacy-preserving-medical-data-publishing/125338?camid=4v1a