

CROSSTALK would like to thank NAVAIR for sponsoring this issue.



In the beginning, there was DoD Standard 2167A for the development of software for weapon systems, and DoD standard 7935A for the development of Automated Information Systems. East was east and west was west, and never the twain would meet – or so we thought. Would we ever need the extreme rigor for requirements management, design,

documentation, configuration management, technical reviews, testing, security and safety that were used for military systems for administrative systems?

Someone thought so. In 1994, east and west not only met but became one. Military Standard 498 merged 2167A and 7935A to define a set of activities and documentation suitable for the development of both types of software development. Shortly afterward, it was cancelled as part of acquisition reform, and superseded by commercial standards such as IEEE 12207. But its legacy of fusing tactical and non-tactical systems (also known as IT – Information Technology and IS – Information Systems) remains. The world has changed much in the past 20 years, and it is clear that we do need to adjust even more to the blurring lines of what were at one times two distinctly different types of software.

The proliferation of mobile technology continues to expand through the commercial and Federal IT service marketplace. Naval Air Systems Command (NAVAIRSYSCOM) is exploring the value of transitioning “traditional” IT products into highly tactical

environments. The Electronic Kneeboard (EKB) program seeks to place cutting edge mobile technology directly in the warfighter’s hands. EKB will deliver tablet technology for use in every USN and USMC aircraft in the fleet, providing real-time access to digital flight information products, imagery, and other tactical information sources. Program success is dependent upon productizing traditional Enterprise IT services, like Mobile Device Management, for bandwidth-constrained tactical scenarios.

EKB is just one of an increasing trend of modern-day tablets and laptops being used to make up for functionality and ease-of-use limitations of legacy systems. As long as modern information systems and legacy embedded systems remain independent of one another, the latter are not subject to conventional cyber attacks. However, if these systems are interconnected and interoperate, previously-avoided cybersecurity risks may be introduced. The article “Cybersecurity and Modern Tactical Systems” by Warren Axelrod in this issue looks at how these risks might be mitigated.

Another critical area that we need to manage as we fuse IT and real-time tactical systems is software safety. Military standard 882E addresses the levels of control yielded to software, and prescribes the levels of rigor that need to be applied. It is possible, and even probable, that devices that were developed for the commercial world for average consumers will also be integrated into our military systems – not just for off-line use. We need to be mindful of not only the benefits but also to apply the appropriate rigor of the new world we are in.

Al Kaniss
Software Engineering Branch Head
NAVAIR