Emerging complex technologies made up of connected subsystems require standards that advance interoperability and security in the marketplace.

It is not always remembered that the international system of units, commonly known as the metric system, got its biggest boost from the French Revolution and the political determination of that time to place commerce and human affairs in general on a more rational foundation.

Today, standards — and systems of standards — are again at the center of efforts to master many of the great challenges facing the world. Standards are front and center as building blocks for solving problems, problems that now come in larger and larger packages as technologies become complex structures in which smaller structures are embedded.
ENABLE INTEGRATED SYSTEMS

Standards for Today’s Complex Technologies

Part 5 of a Series

BY ALAN R. EARLS
Steven E. Waldren, M.D., director of the Center for Health Information Technology at the American Academy of Family Physicians, gives the example of how standards are proving to be crucial to healthcare delivery and healthcare reform. Waldren, a medical informaticist and member of ASTM International Committee E31 on Healthcare Informatics, cites ASTM E2369, Specification for Continuity of Care Record (CCR), published in 2005, which defines a core data set of the most relevant administrative, demographic and clinical information facts about a patient’s healthcare. That standard references many other ASTM standards and allows practitioners to easily share and exchange information electronically.

“I think the main role of standards is to change the way people compete in the marketplace. Standards can be driven by the federal government or other concerned entities that want to help drive a marketplace. It works when a group of stakeholders says ‘we need to standardize something,’” Waldren says.

Waldren says that has been the process with CCR. “We needed to start getting more interoperability of core clinical data so we wouldn't have to reinvent the wheel all the time,” he says. “Then, vendors and organizations can build additional functionality on top of that.” Now, with the work of the federal government in both the Bush and Obama administrations, there is a push for standards to get data moving more smoothly within healthcare, potentially saving costs. Although the CCR standard is not tied directly to the Health Insurance Portability and Accountability Act of 1996, it does support that law’s privacy and security requirements using yet other standards — for XML coding, encryption and digital signatures — provided by the World Wide Web Consortium.

Waldren says the ASTM standard brought together representatives from his organization as well as the American Academy of Pediatrics, representatives of the long-term care nursing field and vendors, and provided an effective forum for raising important issues and working out crucial compromises. “Any time you have standardization, you have competing perspectives from different stakeholder groups and you must really strike a balance to get everyone to feel like it is something they can get behind and support,” Waldren says. “You must balance the ideal solutions with the pragmatic solution.”

Importantly, he notes, ASTM standard E2369 wasn’t created in a vacuum. “The standard we developed was based on other standards developed within the computer industry,” he explains. In healthcare, Waldren says, “We have had to try to determine what would really work today in our effort to ‘move the needle.’ That meant that CCR was able to represent a lot of different types of data, including free text that the computer itself can't really process or analyze as well as the highly structured structures in which smaller structures are embedded.
codes that are more useful for a computer," he explains.

Of course, ASTM is only one of many organizations working to formulate standards and move them into practice. Jason Wisdom, an information technology consultant, says standards are critical to IT operations, the internet and even individual computing devices. "Without them, wheels need to be reinvented again and again — it’s terrible for productivity," he says.

Wisdom says industry standards and protocols span multiple companies, for an industry (such as healthcare) or a kind of technology (such as Web browsers).

In the past, healthcare IT has been "notoriously weak" when it comes to standards, he says. "Health insurance is a good example: different carriers track different information, have different codes for specialties and have different levels of detail for the information they do track," he says. Thus, Wisdom says, some insurance companies have different formats for storing a patient's medical history. This creates an administrative nightmare for hospitals and other organizations who accept multiple insurance plans. Different formats of data need to be reconciled, and there are a lot of errors, including misspellings of patient names. "Standards would fix all of these problems," he says.

SECURITY STANDARDS IN INFORMATION TECHNOLOGY

Likewise, in information technology, security standards are extremely important because, without standards, some security systems will end up being weaker than others. "And your entire defense is only as good as your weakest link — once a hacker penetrates any one layer, the hacker is into the system, and has that much easier access to everything else," says Wisdom.

"Without standards, you never know what your weakest link is. With standards, you have a uniform defense with no weak links," he adds.

Indeed, Niall Browne, chief information security officer at LiveOps and chairman of the BITS Financial Security Committee, a not-for-profit industry consortium, says, "Standards are the key to creating security." For instance, he explains, enhancing credit card security required development of the Payment Card Industry Data Security Standard, an information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, automated teller machine and point-of-sale cards. The standard was the result of major credit card organizations pooling their efforts to increase controls around cardholder data and reduce credit card fraud.

Similar efforts have enhanced the security of other aspects of information technology, Browne says. For protecting consumer data, there is the Gramm-Leach-Bliley Act, also known as the Financial Services Modernization Act of 1999, which requires much stronger protection of personal information.

Making an analogy to the construction of a home, Browne compares security standards to building codes — a critical ingredient in making a structure that is safe and durable. In a similar way, he says, security standards provide the groundwork for tailoring security to the needs of a given entity or for developing more complex security tools.

In his own work with BITS, Browne says the goal has been to create industry standards for thousands of financial organizations and related entities. "This year we are focusing on how to build controls for the cloud," he explains, referring to the server-based digital network on which it is expected most entities and many individuals will eventually store their digital assets.
Although much of the effort to develop computer security standards has been led by the private sector, the U.S. government has also played a role. William Barker, from the National Institute of Standards and Technology’s Computer Security Division, says that his organization’s activities are rooted in the National Bureau of Standards Act and extend into information technology, most recently through the Federal Information Security Management Act of 2002.

Under that act and subsequent guidance from the U.S. Office of Management and Budget, standards and guidelines are provided that are mandatory for federal agencies and often referenced voluntarily by other levels of government and the private sector. “NIST is supposed to and does primarily work with consensus-based standard development organizations because, if we can achieve the end using the consensus standards, that is our default approach,” says Barker. However, he notes, in some cases, such as with FISMA, if requirements are exclusive to the federal government, NIST will develop standards on its own. “In the last decade we have only published federal information processing standards in response to specific legislation,” he adds.

**SMART GRID STANDARDS**

Standards also apply to challenges beyond the “cyber” domain. Indeed, these days, the impact of standards and systems of standards on whole industries has probably never been greater. Here again, NIST is involved. For example, Dean Prochaska, national coordinator for smart grid conformance at NIST, says his work with standards has been rooted in federal policy efforts to modernize the grid, specifically the Energy Independence and Security Act of 2007. “EISA directed NIST to take primary responsibility to coordinate the development of a framework including protocols and standards for the information management to achieve interoperability of Smart Grid devices and systems,” he says.

According to Prochaska, the U.S. Congress directed that NIST create a framework that was flexible, uniform and technically neutral. The American Recovery and Reinvestment Act of 2009 supplied funding to accelerate the NIST work and also to jump start smart grid deployment and support demonstration projects.

When the effort started, Prochaska said the initial focus was on “picking the low-hanging fruit,” an information-gathering exercise conducted through three workshops that attracted some 1,500 people. The result was the release of NIST Special Publication 1108 – NIST Framework and Roadmap for Smart Grid Interoperability, Release 1.0. That framework constituted the smart grid vision and included a reference model “so that people could start talking about the Smart Grid in a common manner and know how things tied together,” he says. Crucially, the effort also involved identifying some 75 existing standards that could be leveraged to accelerate the deployment of the smart grid.

“Of the existing standards, not all of them were ready for prime time,” says Prochaska. So, the team identified 16 initial priority action plans that would fill critical gaps in the existing standards.

Today, the NIST smart grid work continues to evolve. “The second phase of our work was to create a public-private partnership called the Smart...
Since its establishment in December 2009, the Smart Grid Interoperability Panel has grown to more than 660 member organizations and more than 1,700 individual participants. The SGIP does not create the standards for smart grid, but works with various standards development organizations to accomplish its goals.

Grid Interoperability Panel (SGIP). We needed to establish a more permanent organization that could guide the development and evolution of the standards into the future,” he says. Since its establishment in December 2009, SGIP has grown to more than 660 member organizations and more than 1,700 individual participants. Prochaska says the SGIP does not create the standards for the smart grid, but works with various standards development organizations to accomplish its goals.

**THE THRESHER TEST AND BEYOND**

On a more tactical level within the energy field, it is a private sector effort that is creating a badly needed set of standards for an emerging field. According to Roger H. French, Ph.D., a professor of engineering and director of the Solar-Durability and Lifetime Extension Center at Case Western Reserve University, in Cleveland, Ohio, the viability of the solar photovoltaics industry is in part dependent on a current industry effort to develop a lifetime performance qualification test. Called the Thresher test, it was recently presented at an NREL Photovoltaic Module Reliability Workshop held in Colorado.

According to French, the standard is focused on crystalline silicon (c-Si) modules and is being developed by an informal industry group involving module manufacturers and others.

“The goal here is to develop an accelerated test of c-Si modules, in which the testing is done sequentially, separated by evaluations (measurements) done after each step in the testing,” French explains. According to French, the goal is that the c-Si modules be exposed to a number of different stressors, and that these results can be correlated to field performance. “This type of data would be very useful to developers who are rolling out new PV power plants, and making decisions on modules,” he says. And that, ultimately, can make PV technology more economically viable as part of the smart grid or independently.

According to David M. Burns, a senior specialist at the 3M Weathering Resourece Center in St. Paul, Minn., a reliable standardized approach to assessing the durability of PV module designs is important for the long-term viability of the solar industry. Current PV standards are based on initial qualification (fitness for use) testing. “As the industry grows, there are increasing calls for information on the expected life of these systems to allow users to compare technologies and assess their long-term economics,” Burns says. Work to create Highly Accelerated Life Testing (HALT) protocols for predicting PV module service life is ongoing on a number of fronts — private manufacturers, private and public research institutions, industry consortiums, etc. ASTM International Committee E44 on Solar, Geothermal and Other Alternative Energy Sources provides a venue for all the parties to come together to develop the core industrial solar energy standards to support and grow the PV industry.

Back to the larger picture of integrating technologies: NIST expects to continue to focus on smart grid, cloud computing, healthcare IT and identity management standards, implementing the National Strategy for Trusted Identities in Cyberspace, an Obama administration proposal for the creation of online secure identities for Americans in cyberspace. “These efforts have varying degrees of private sector leadership, but when we look at the identity issue, I think we will see the maximum cooperation between government and private sector,” Barker says.

“To the extent we can serve as a catalyst that is the best role for us,” Barker says. And, thinking strategically, “we are giving a lot of thought to what we need to be doing next, not solving today’s problems but looking out 5 to 10 years to come up with solutions that will be relevant then,” he adds.

And, of course, the consensus-based process — involving all stakeholders — will remain a crucial element of that effort. Indeed, as Waldren notes, it is at the heart of effective standards development. “There is an expression; standards aren’t made, they are adopted,” he says. “If you make a standard but nobody implements it, it isn’t really much of a standard.”

 **ALAN R. EARLS** is a writer and author who covers business and technology topics for newspapers, magazines and websites. He is based near Boston, Mass.

See the November/December 2009, March/April 2010, May/June 2010 and July/August SN issues for the earlier articles in the “Standards Enable” series.