

## Q&A WITH DAWN MEYERRIECKS STANDARDS AND CERTIFICATION ARE CRITICAL



Dawn Meyerriecks  
Principal Director for GIG Enterprise Services  
DISA, US DoD

Dawn Meyerriecks, Principal Director for GIG Enterprise Services, Defense Information Systems Agency (DISA), US Department of Defense, spoke with The Open Group's Eva Kostelkova about challenges presented by the transition of defense systems to COTS (Commercial Off-The-Shelf systems).

Meyerriecks addressed DISA's needs, emphasized the need for standards, certification of conformance, and validation of business processes, and discussed a list of DISA's challenges to the industry.

**Q: Moving defense systems to COTS means that the government will have to deal with the fast-changing commercial markets and the impact of events like mergers, acquisitions, and closing of suppliers. What role do you see for standards and certification to play in this transition?**

**A:** We want to have standards applied to all important interfaces. Then, if a vendor for a particular product goes away, it will have less of an impact. So we won't care as much who supplies the software, as long as they are using the standards interfaces that we have defined. By abstracting through a standard who is doing the implementation behind the standard, we are less dependent on a particular vendor and we can minimize the impact of any corporate changes.

We learned that lesson with COE, but it can be applied to POSIX, Linux, and a lot of other examples. We don't want to commoditize to the extent that people aren't able to succeed commercially, but being vendor-independent, vendor-neutral helps us protect our equity.

**We want to have standards applied to all important interfaces ... being vendor-independent, vendor-neutral helps us protect our equity.**

**Q: How do you ensure vendors are conformant?**

**A:** We think certification is incredibly important. There are lots of examples when you write a specification but do not do a reference implementation and do not have a test suite to go with it – and you don't get an interoperable product. If we have a common test harness against which people can test, we can validate that they meet the specification.

There are some interesting things in POSIX; for example: you guys did a lot of work. A lot of people who thought they were POSIX-compliant, when we forced them to go through the certification process, discovered that they had problems. It was everybody, not just the margin players; it was big players too. And a lot of them incorporated your test suites into their internal processes. As a result we got a better product.

**A lot of people who thought they were POSIX-compliant, when we forced them to go through the certification process, discovered that they had problems. It was everybody, not just the margin players; it was big players too.**

**Q: How do you see the relationship between certification and testing in your environment?**

**A:** We currently use multiple types of certification to mitigate risk and various classes of tests, including operational and validation tests, but we'd like to push certification testing to provide interoperability and security. Both are key.

**We'd like to push certification testing to provide interoperability and security. Both are key.**

We'd like to see a formal specification language, then a certification suite that validates all components, and then have the providers of business processes validate the whole process. We should build layers, end-to-end, that can dynamically compose business processes.

So for certification and testing, we'd like it to converge! It's a long way from now. Suppliers view the time-to-market as a trade-off with respect to certification and testing, so it is challenging to motivate the market. But we need to look at the big picture, consider more long-term investments, and not just next quarter profit and loss statements.

**We should build layers, end-to-end, that can dynamically compose business processes.**

**Q: Dynamically allocated and composed systems, including Grid, seem to play a large role in the defense systems. How do you see meeting the challenges of certifying such systems?**

**A:** You had a great speaker at the San Diego conference, Dr. Susan Zevin from NIST. I think she is right. There are a couple things we need to fundamentally rethink and approach in a different way.

When we think about software in the dynamically composable environment, we need to characterize not only what the interfaces are from the standards perspective, but also when it is safe to invoke the service or the source, under

what circumstances. You have to know what your envelope is. We have always enumerated every possible way it could be used and exhaustively tested every possible path. The problem is that we can't imagine how it is going to be used. Even if the path is perfect but it is invoked in the wrong environment, it might execute perfectly but still get the wrong answer. One of the examples is a correlator; even if the correlator is perfect, when it is fed bad data it will give bad results. We have to fundamentally rethink how we characterize the limits to which software can be applied – and that is a different way of looking at the problem.

**In the dynamically composable environment, we need to characterize not only what the interfaces are from the standards perspective, but also when it is safe to invoke the service.**

Susan Zevin said that we have to get better at formal specification. Part of that formal specification has to do with the environment in which you can invoke the component. We have never tried to describe that. We need a vocabulary, from an architectural standpoint, that will allow us to describe the environment and that we will all agree to. Collectively, we have not done this – not because we don't know it needs to be done; we haven't done it because it's really hard. And so there are quite a few steps that have to be taken. The Open Group is doing some good work with architecture that starts getting at this. We won't get it right immediately, but it's a start.

**We have to fundamentally rethink how we characterize the limits to which software can be applied.**

**Q: Defense systems need to be tested both by the vendor and the defense customers of those systems. But, extensive testing by both parties is expensive and takes time. How can the government and industry work best together to decrease the time-to-field?**

**A:** There are lots of things we could do. The government could demand better quality

products from commercial vendors, for example; we could insist that certain qualifications be met before we buy something. But it can be slow, and if there is no commercial demand and we are the only ones requesting it, vendors don't see return on investment to go through this. So to accomplish that and influence vendors, the government has to show leadership and team up with commercial consumers.

**We are thinking about a model that moves some responsibility for outputs of the services to the service provider.**

The other approach we are thinking about is a model that moves some responsibility for outputs of the services to the service provider. For example, if we have a correlator provider, we'd like to hold the correlator provider responsible for the output of their correlator. This would motivate them to validate data feeds, which give us value-added output as opposed to bad output. So it is about validating business process *versus* validating each piece separately. This is where we need to evolve with the standards communities: this is different. Parts need to be validated, but at the end of the day, you need the value proposition of the whole business process.

**Q: When we think about performance, predictability, and fault tolerance, commercial systems traditionally approached it based on "best effort" or over-provisioning. Defense systems often have more stringent mission requirements. How do you see this difference between COTS and defense needs being addressed?**

**A:** The current approach is over-provisioning. For example, although we are committed to IP convergence, in some cases, the over-provisioning may look like not converging on the IP. We have systems like the Defense Red Switch for command and control; it is classified, always manned and answered, and it is on unique proprietary infrastructure because of the availability, reliability, and other requirements.

**It is about validating business process versus validating each piece separately.**

We are also looking at grid computing, but in a non-classical sense. We are committed to positive government control of all critical IT resources, so we cannot depend on the public infrastructure or a vendor to fall back on if we didn't have enough CPU power. Ultimately, it is a government person who makes calls about what

**When we have to decide which processes live and which die based on missions they are supporting, we want to be able to analyze what the implications are in real time, so we can make good decisions.**

the priorities are and what missions are going to go on. So the answer there is: we'll have to provision carefully so we have enough capacity, x times over the amount we need, and then start deciding, based on SLA, class of service, quality of service, etc., who doesn't get cycles in situations of deprivation and starvation. Then you go down the Maslow hierarchy, based on what's really important to get done.

**Q: Would you consider simulation and modeling useful tools to increase predictability?**

**A:** Yes. In order to make dynamic composability work, and get the availability and reliability, we are trying to build a detailed component model – at the same time we are actually building components. When we have to decide which processes live and which die based on missions they are supporting, we want to be able to analyze what the implications are in real time, so we can make good decisions. That includes who gets resources in a resource starved environment, that includes analysis of the mission and which missions we can abandon with the least amount of harm, and so on.

**Enterprise management is a huge deal to us.**

The major power problems we experienced not so long ago are a good example of a situation when people do exactly what their conops and training tell them to do, but their efforts result in actually propagating the problem rather than

stopping it. We realized that we'll need to think differently.

We started doing work with Eric Bonabeau and University of New Mexico, and Stewart Brand. They have done a lot of modeling of genetic systems and social systems, looked at the psychology behind it, and tried to figure out how these networks interact. But nobody has ever done any work with that from an IT perspective. And this gets back to safety and what are the limits – because we hope, as we build our components, that these modelers can run massively parallel simulations to see how you might be able to string the components together, and identify when there might be effects that you don't want – mutations as opposed to healthy life forms. That will allow us to go back and look at the definition of the components that we put together, and either modify it or characterize it so that it doesn't get invoked in that particular way.

We think there is a whole different area or discipline in computer science. It is an interesting problem set to me and I believe that there will be benefits at the global level as well, as they start thinking about it, see how these problems interrelate, and what the implications are for us as a society. And we've got some really good minds working on it. I think there are lots of lessons to learn, and I look forward to what comes out of it.

This is all really new. We just put a contract in place a few weeks ago. It takes time as they are not a classical government contractor, but we are doing a lot of things like that now, and where appropriate, we go directly to people who build products or think differently.

**Q: What do you see as the biggest gaps in using COTS technologies for DoD net-centric services? Where do the commercial vendors need to “do better”?**

**A:** One of the things that is eating our lunch is identity management and camps that have sprung up around that. Liberty and Passport are two obvious ones. We have to live with both communities but they haven't converged from the standards perspective, so we have to custom code to try to bridge them. Of course, there is security relevance, so it gets even trickier. At the end of the day, if we mediate those two implementations and those two models, it is an

imperfect match, a lossy match. You lose information one way or the other because it doesn't map exactly. These sorts of things are big concern for us. We are tied to a specific implementation. In some cases we have to do both. So that's one of the areas – great example of where standards work needs to be done.

Enterprise management is a huge deal to us. SNMP is great for what it was designed to do but it is really inadequate for managing complex enterprises and for what we are asking it to do today. Another area that's a huge deal to us is the immaturity of web services from the security perspective. Also work flow immaturity, event orchestration, support to hard real time ... we have a list of areas where we would like to see standards convergence in products. Not just on paper, but we want somebody that actually does the implementation. Another example is IPv6: DoD is going to have to define its own profile, which part of IPv6 we will standardize to because the industry has not been able to sort that out.

**We have a list of areas where we would like to see standards convergence in products. Not just on paper, but we want somebody that actually does the implementation.**

There are a lot of good reasons why standardization doesn't always happen right away but for those of us who implement IT, it is a big deal. Because then we have to try to pick sides or land in the middle, and end up with custom code, which is not what we are after.

**Q: What is your dream for an industry response to DISA's needs? What can The Open Group's members do to make a difference?**

**A:** I gave you the 9-18 months list; I would like the standards bodies, and The Open Group, to address the list. Sometimes the process is not always efficient but it is effective. It takes a while where there has to be a buy-in, but we'll all win if we can end up collectively with better solutions.

And since the key difference is people, I want great minds to think like this: get great minds.

## DISA's Challenges to the Industry

### Technical Challenges

- ❑ How does one document the architecture of the Internet, and what does system architecture mean in a net-centric environment?
- ❑ Identity management and access controls
- ❑ Evolving standards and “hard” integration points, heterogeneity, and interoperability implications
- ❑ Coalition and HLS information sharing, “need to share” *versus* “need to know”
- ❑ Risk management, operational testing, certification, accreditation (of what and how)

### Cultural Challenges

- ❑ Market-driven model *versus* policy mandates
- ❑ Leverage community intellectual property
- ❑ Common approaches and methods
- ❑ Common vocabulary
- ❑ Command implications: “Command and coordinate” *versus* “Command and control”

### What You Can Do

- ❑ Emphasize secure interoperability and integration with sponsors and partners (including flexibility and balanced evolution with industrial technology base)
- ❑ Define standard processes and detailed evaluation criteria for common products (including accreditation process overhaul/streamlining)