Systems Engineering for the Global Information Grid: An Approach at the Enterprise Level

Patrick M. Kern
Deputy to the Assistant Secretary of Defense, Networks and Information Integration/ Department of Defense Chief Information Officer

Because the numerous United States Department of Defense (DoD) and Intelligence Community (IC) networks were originally built to serve many different constituencies, making the Global Information Grid (GIG) a reality requires solving interoperability and performance issues at the enterprise level. This will be accomplished through the use of systems engineering – a discipline whose techniques manage the complexity of systems from abstraction to decomposition. The GIG Technical Foundation (GTF) addresses a number of systems engineering challenges involving focus, evolution, coverage, and applicability.

As you are probably aware, the GIG is a complex, ongoing effort intended to integrate all information systems, services, and applications within the DoD and the IC into a seamless, reliable, and secure network that will support horizontal information flow and net-centric warfare.

The GIG represents a different way of thinking about delivering capabilities, a way of thinking that can cope with the uncertainties we face in the world today. In the past, missions focused on narrow objectives against known adversaries and were organized with tightly managed organizational responsibilities across the DoD and IC constituencies. Today, adversaries are shadowy and shifting, objectives are far-reaching, and new responsibilities link our organizations at all levels. The DoD and IC networks built in the past evolved into stovepipes, tied to missions and organizations that now are forced to adapt to a more fluid world. The GIG confronts uncertainty, inherent in today's world, with the agility that comes from interconnected, interoperable solutions that can be tailored to today's missions and objectives. Making the GIG a reality requires breaking out of stovepipes and solving interoperability and performance issues at the enterprise level. We have approached the problem of building, populating, operating, and protecting the GIG by applying systems engineering discipline to the complex set of communications systems, information systems, services, and applications that make up the GIG. Systems engineering as a discipline provides us with the techniques to manage the complexity of systems.

Enterprise-Wide Systems Engineering (EWSE), as applying systems engineering to the GIG at this level is known, can only succeed by properly focusing the effort. EWSE utilizes interoperability and end-to-end performance as the criteria to determine what is within scope. Enterprise decisions for these requirements are then documented and enforced in the design of GIG component systems, laying the groundwork for the GTF. The GTF is the configuration-managed, synchronized set of all authoritative technical guidance required for planning, developing, acquiring, and implementing an interoperable and secure GIG.

Background

With origins in a wide range of component systems procured to support autonomous agencies and services, the GIG is more accurately an organizing construct than an actual system. Its legacy components vary in terms of performance, storage, and process, and they must continue to support their existing user communities even as they become part of the GIG. While many individual component systems are unknown at the enterprise level, the GIG's component set – as well as the components themselves – will evolve to reflect participant groups' capabilities and financial priorities. The challenge is to establish a process that brings these disparate components together into a single entity that meets the needs of all users.

As GIG component systems are designed, built, and funded by member organizations, it is necessary to deductively establish the functions, protocols, and data models required for their interoperability and performance. Such an investment will benefit all GIG users.

Scope of the Effort

The Assistant Secretary of Defense, Networks and Information Integration (OASD[NII]/DoD Chief Information Officer) tasked the Defense Information Systems Agency to lead an Enterprise Documentation Framework Working Group that would apply systems engineering practices to create the GTF. The GTF provides structure and traceability for all GIG documentation in a manner similar to that of a document tree. The GTF is based on and traceable to operational needs derived from national and DoD strategic guidance and direction. It includes enterprise-level GIG documentation (GIG capabilities; activities; technical requirements, including standards and specifications; and the GIG Architecture) and other GIG-related technical documentation[1].

Applying systems engineering at the enterprise level to support development of the GTF must start with the GIG's vision as outlined in the Net-Centric Operations Environment Joint Capability Document[2]. Once top-level requirements are defined to identify the necessary functionality, this functionality can be decomposed into system segments and sub-segments.

Top-level requirements have been decomposed into three areas – general, enterprise management, and Information Assurance – and flow down to requirements at the segment level. These segments include transport, services, applications, computing infrastructure, and enterprise operations.

Segment and sub-segment requirements are specified as needed for interoperability and performance according to the top-level requirements, which can be traced from GIG capabilities and requirements to segment and sub-segment requirements. Sub-segment requirements, needed to achieve interoperability and end-to-end performance, are often the specification of protocols or mechanisms.

Figure 1 illustrates the relationship between top-level requirements, segment-level requirements, and sub-segment requirements for a transport segment example.

Systems Engineering Challenges

In addition to scope, the GTF addresses a number of systems engineering challenges involving the following:

- **Focus.** All requirements for achieving the GIG capabilities – including what is currently feasible and what requires further development – must be specified by the GTF to ensure that programs understand the needed transitions. Programs, services, and agencies responsible for existing GIG component systems are then responsible for developing transition plans that reflect the requirements of the GTF.

- **Evolution.** Many aspects of the GIG's long-term vision, including pervasive mobility, ad-hoc network connection, efficient resource use, and dynamic resource allocation/management are not achievable through use of current technologies. Long-term GIG design must not be limited to requirements dependent on current technology, but include provisions for emerging and future technologies as well.
- **Coverage.** As mentioned earlier, the GIG is made up of a wide variety of components, many of which are unknown at the enterprise level. Components will be added and removed as organizational needs evolve, and the components themselves will also evolve. As a result, requirements for the GIG must be specified in terms of component type rather than for specific components. Requirements must also be defined for the set of systems needed to meet GIG capabilities rather than for those appropriate only for existing/planned systems.
- **Applicability.** Since GIG users will operate in a variety of environments, requirements need not apply to all environments or modes. Specific domains of applicability must be defined which work in concert to provide overall enterprise capabilities. For example, fixed users are well connected and can reliably reach centralized data centers. The fixed users are not severely constrained in power, memory, storage, and processing. Examples of fixed user modes are camps, posts, stations, and bases served by the Defense Information System Network. Advantaged tactical users operate in a slowly changing environment subject to high latency and limitations on bandwidth that may constrain reach-back to centralized data centers. The advantaged tactical users are not severely constrained in power, memory, storage, and processing. Examples of advantaged tactical user modes are tactical operations centers and Navy ships. Disadvantaged tactical users operate in a highly dynamic topology, with limited and sometimes no fixed infrastructure, subject to disruption in communications and with severe constraints on one or more of power, memory, storage, and processing. An example of disadvantaged tactical user mode is a Mobile Ad-Hoc Network formed by vehicles and dismounted soldiers.

Assembling the GTF

The GTF is intended to address all requirements relating to the GIG's long-term vision, even those not achievable through the use of currently available technologies, protocols, and mechanisms. Sub-segment requirements are divided into two categories – current requirements, which are achievable using current technology, and maturing requirements, which rely on emerging and future technologies.

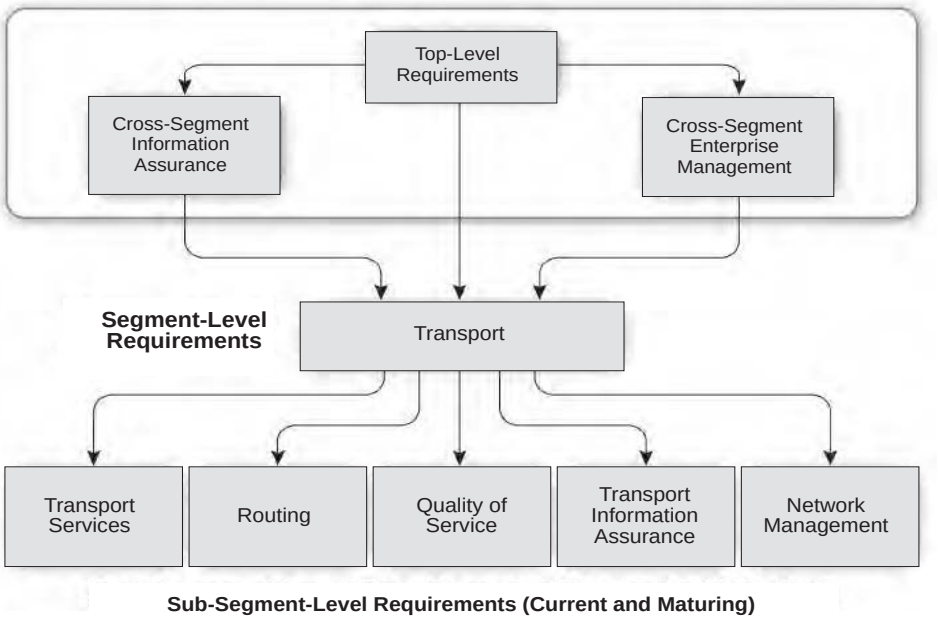
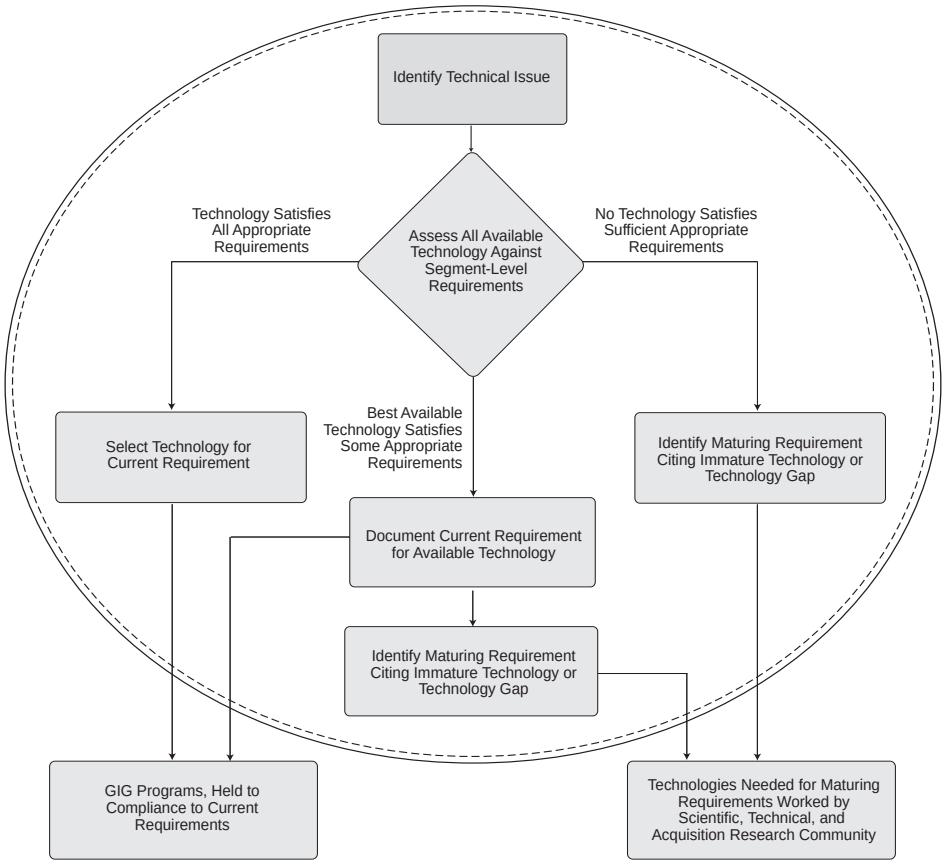


Figure 1: *Transport Segment Example Illustrating the Relationship Between Requirements*

Current requirements are testable and will be enforced in the design of GIG component systems. By contrast, maturing requirements are used to document technologies needed to achieve GIG capabilities, verify the feasibility of achieving GIG capabilities and provide insight on research needed to meet the GIG vision.

Occasionally, use of a technology, mechanism, or protocol that does not satisfy GIG requirements is sanctioned if no other resource is available. In these instances, a current requirement is defined for the existing technology, and a maturing requirement is

Figure 2: *Process for Assessing Technologies for Inclusion in the GTF*



defined for the needed technology. For example, inter-domain routing today would use border gateway protocol version 4 as a current requirement. A new protocol to support pervasive mobility is defined as a maturing requirement.

At all phases of the process of assembling the GTF, stakeholders and subject matter experts participate in working groups to assess technologies and determine the appropriate match for current and maturing requirements. Figure 2 (see page 11) illustrates the process used to assess technologies for inclusion in the GTF.

Community Role in GTF Development

Before the establishment of the GTF, different organizations attempted to define the GIG in separately developed technical, policy, and guidance documents. This resulted in more than 7,000 pages of documentation, which, although well written, contained gaps, overlaps, and inconsistencies that reflected the GIG's fragmented origins in component systems originally intended to function independently. Once it was realized that the emerging GIG documentation did not have the technical maturity to meet end-to-end interoperability and performance compliance standards, members of the GIG user community began to develop baselines against which its individual components could be measured.

Today's GTF is a set of source documents drawn across the GIG community, along with governing statements for GIG development, providing portfolio and program managers with clear guidance on how to implement net-centricity and end-to-end interoperability throughout the acquisition life cycle. It includes authoritative source documents that define the strategic guidance, operational context, operational capabilities, GIG capabilities, GIG activities, and technical direction needed to take the GIG through the following timeframes: near (0-2 years), mid (3-7 years), and far (8+ years).

The GTF also contains governing statements extracted from these source documents that more concisely describe the GIG and are traceable throughout the GIG's Enterprise Document Framework. All content is stored and managed in a DOORS[3] requirements database to facilitate requirements management and configuration control.

Compliance

By developing this integrated approach to compliance assessment that aligns current processes and provides an entry point to the Net-Ready Key Performance Parameter evolution, the GTF does the following:

- Allows program managers to self-assess individual programs.
- Applies consistently to all programs at all levels of oversight.
- Ensures high confidence in end-to-end interoperability and performance compliance at the enterprise level.

Policy has also been revised to direct all compliance to the GTF.

Conclusion

The GIG is an ambitious undertaking that is fundamental to net-centric warfare. We have established an enterprise process to apply systems engineering discipline to the decisions that need to be made to make the GIG a reality. The product of the enterprise approach is a GTF, a new approach to GIG policies and a set of processes for compliance to the GTF.

While the GTF is still an evolving effort, the requirements in the GTF have been flowed into program requirements documents, ensuring more robust interoperability and performance as those programs come online as part of the GIG. The approach we are putting in place will allow us to build, populate, operate and protect the GIG to meet the challenges of today's world.◆

Acknowledgements

The author would like to recognize the contributions and significant input to this article by Ms. Julie Tarr, Senior Systems Engineer, and Mr. Tony Dessimone, Senior Scientist.

Notes

1. Some portions of the GTF are not publicly released.
2. <www.jcs.mil/j6/netcentric.html>.
3. DOORS is an acronym for Dynamic Object-Oriented Requirements System (a Quality Systems and Software, Inc., Quality Systems and Software database management system).

About the Author

Patrick M. Kern is the NII Net-Centric Systems Engineer leading the integration of transformational programs for OASD/NII. He is responsible for end-to-end system engineering for the GIG. Kern has a bachelor's degree in aerospace engineering from the University of Michigan and a master of business administration in engineering management from the University of Colorado.

OASD/NII
3D174 Pentagon
Phone: (703) 697-4704
E-mail: patrick.kern@osd.mil

WEB SITES

Air Force Center for Systems Engineering Reference Library

www.afit.edu/cse/

The Reference Library provides links to key systems engineering policies, guides, industry standards, important historical systems engineering documents, and other related documents.

The United States Army Information Systems Engineering Command

www.hqisec.army.mil/

The United States Army Information Systems Engineering Command has the primary mission of system engineering and integration of information systems for the U.S. Army. Their mission includes the design, engineering, integration, development, sustainment, installation, testing, and acceptance of information systems. It provides matrix support to the program executive officer and program manager structure for systems engineering and integration of assigned information systems.

Systems and Software Engineering Organization Systems Engineering Plan

www.acq.osd.mil/se/as/sep.htm

The Software Engineering Plan is a *living* document that captures a program's current and evolving systems engineering strategy and its relationship with the overall program management effort. Its purpose is to guide all technical aspects of a program, and provides a comprehensive, integrated technical plan to achieve its objectives.