Defining Services Using the Warfighter's Language

Michael S. Russell
General Dynamics Information Technology

Warfighters establish relationships with other warfighters to exchange information and accomplish their mission. Net-centricity and other information service concepts provide a means, but to a warfighter these are just technical solutions to the operator's need. The missing piece in the push towards service oriented approaches is an understanding of what warfighters expect from a service and a means to capture these expectations as part of the Joint Capabilities Integration and Development System (JCIDS).

Service-Oriented Architectures (SOA), and services in general, are a troublesome subject for many warfighters. Warfighters understand what information they need to execute a mission, and they are comfortable defining information requirements through JCIDS documents and supporting architectures. However, when this information is provided by a service, especially when depicted as a cloud labeled *Global Information Grid (GIG)*, this comfort level goes down.

Defining a service from a technical perspective is not hard. According to the World Wide Web Consortium [1], a service is a software system designed to support interoperable machine-to-machine interaction over a network. Services are standards-based and may contain the business logic needed to turn raw data into information.

This definition is fine for the engineers, but really does nothing to help warfighters specify what information they need from the service, when they need it, and how they can trust that the service – which they do not control – will provide them accurate and timely information. Additionally, the warfighter may not have visibility into, or control over, the business rules used to derive this information from raw data.

The issue with services is fundamentally one of perception. The average person typically goes to a Web site known to be trustworthy, one that provides timely and accurate information. Warfighters do the same thing; they get information from a trustworthy source, normally a higher echelon that they know provides authoritative, timely, and accurate information. The services paradigm can break this approach by obscuring the source of information (and how that information was derived) from the warfighter.

When services are implemented in a way that mimics traditional lines of communication, nothing changes from the warfighter's perspective. They are still receiving the same information from the same sources. However, this approach limits the benefits of a true services-oriented approach since it just replaces one communications technology for another without changing how information is discovered and delivered.

"An optimal services implementation allows the warfighter to specify the needed information, when it is needed, the quality of the information, and an objective way to determine the trustworthiness of the information."

An optimal services implementation allows the warfighter to specify the needed information, when it is needed, the quality of the information, and an objective way to determine the trustworthiness of the information. This allows the system supporting the warfighter to search the GIG and other networks for an available information source that provides that information, to establish a connection, and to start providing information. This optimal implementation will also enable the warfighter to specify, or at least have insight into, the business rules used to generate the information.

However, this implementation often requires the warfighter to accept that formalized information flow between command echelons, such as the flow of logistics information from superior to subordinate, may no longer exist. Telling a warfighter that his subordinates will receive information directly from a service outside of the chain of command may fit reality, but it may not fit doctrine or a warfighter's perception about how information should flow.

Defining Services for the Warfighter

Warfighters tend to think very directly: *I need to know tomorrow's weather forecast. The weather service provides forecasts, so I will call it and get tomorrow's forecast.* The warfighter could describe this need architecturally, as shown in Figure 1. In the example, the unit's commander knows that the same weather service is habitually attached to his unit and knows it will provide accurate and timely information. He will also have visibility into the business rules used to derive the information he needs from raw data.

Figure 1: *How the Warfighter Describes a Need*

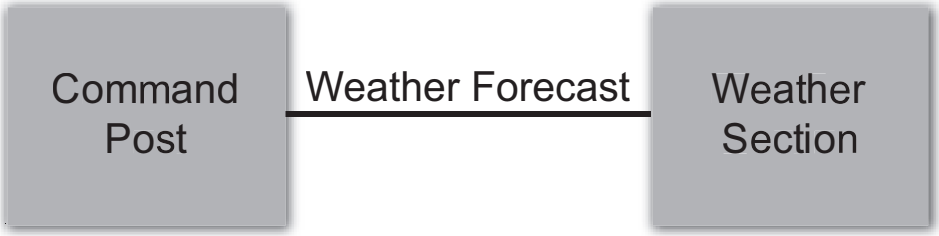


Figure 2 shows a non-services implementation of this requirement. The network device could be a local area network, a radio, or another communications device.

A services approach could be used to implement the same technical requirement. In Figure 3, the technical solution

has implemented a services approach but from the warfighter's perspective, nothing has changed. The same information is flowing from the same source. This approach is similar to how selected services, such as address books, are currently provided.

Figure 4 depicts a common technical implementation that allocates the weather information requirement to a GIG service, as opposed to a habitually associated weather section. Several different weather information providers could conceivably meet the warfighter's information need. This depiction, even if technically correct, does not tell the warfighter who will be providing the information, only that someone will provide it.

Figure 4 highlights the issue many warfighters have with services. While the services themselves are invisible to the warfighter, the information provided by them is not. The issue from the warfighter's perspective is not about the services themselves, but rather the concept of who owns the information, how that information flows, and what rules were used to derive that information. This issue readily becomes apparent when a services approach is implemented in such a way as to break traditional command and unit relationships.

This approach has operational benefits: a deploying unit may no longer need an associated weather section, weather information can be pulled from a wider variety of weather sources, and constant weather information can be sent to all units within a geographic region. There are, however, downsides including quality of service, the loss of connection to a local information source, the need to quantify information trustworthiness, and the rules used to derive the data.

To mitigate these downsides, warfighters should have more control over the requirements process that specifies how services will be implemented. This includes being able to specify an organization that provides trusted information and the business rules that organizations use to generate the warfighter's mission critical data.

Requirements Development

Warfighters are responsible for defining information requirements by specifying who exchanges what information, with whom it is exchanged, why the information is necessary, how the information is derived, and how the information exchange must occur [2]. Typically, these information requirements revolve around the following:

- Describing the required information.
- Identifying the information producer and consumer.
- Describing operational performance, security, and information assurance attributes.
- Detailing the business process, including operational activities and/or triggers that initiate information transfer.

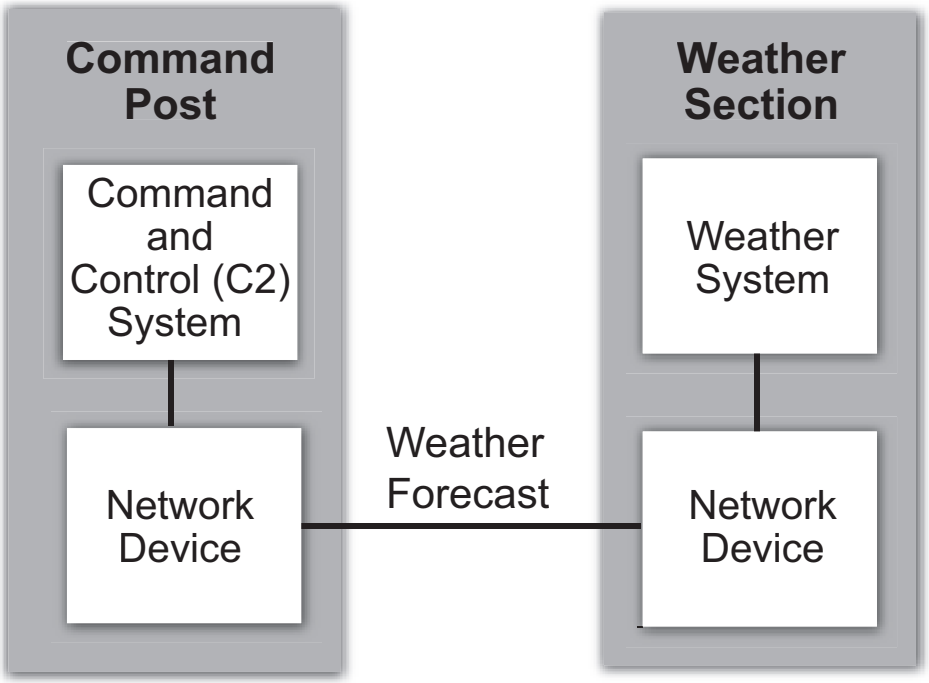


Figure 2: *Technical Implementation*

Describing how one operational unit sends information to another operational unit is straightforward. Using the weather forecast example, the weather section exchanges weather information with the command post upon request, the information is needed for mission planning, and the information is unclassified but must be securely and accurately delivered.

Continued on Page 18

Figure 3: *Service-Enabled Technical Implementation*

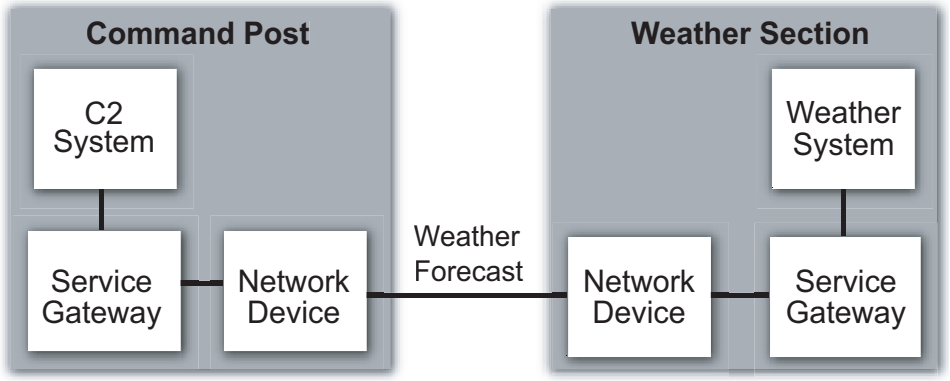
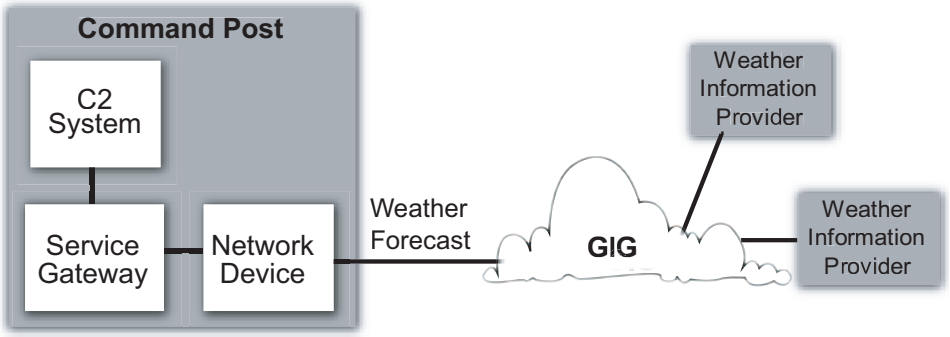


Figure 4: *Net-Centric Technical Implementation*



Continued From Page 15

However, when this same scenario is detailed using the services implementation in Figure 4, the information producer cannot always be defined. The information producer could be one of many weather information producers located in the deployed theater, at a stateside-based location, or any point in between. Instead of describing the expected point-to-point information exchange, the warfighter now sees a request sent to a service. This can leave the warfighter feeling he has lost control of where he receives his information and with doubts of the trustworthiness of the information.

Mitigating these concerns requires changes to the way operationally related architecture data is documented. First, change the way architectural diagrams are designed, highlighting the fact that an information service is provided by an organization, not a computer. Warfighters build trust with other warfighters, not the technology which provides information. Fundamentally, services are just the way an organization – no matter where in the world it is located – can provide information to the warfighter.

Second, requirements developers should add additional information to the warfighter's information exchange matrix (information concerning quality, trustworthiness, etc.) and to the warfighter's list of Information Exchange Requirements. For example, trusted operational sources for information could be added as well as the warfighter's expectations for graceful information degradation on limited bandwidth networks.

Third, the warfighter is concerned about how raw data is captured, validated, and used to develop information. In today's rapid-paced environment, the warfighter does not have time to study raw data to derive the information needed to make effective decisions. However, making decisions based on information derived to support someone else's business process may lead to a bad decision. So the warfighter must be able to help specify the processes used to develop the information, or at least be able to have some visibility into the process.

Capturing the Warfighter's Service-Related Requirements

From the warfighter's perspective, information is being exchanged from one organization to another. From this perspective, services are the technical implementation – not the operational requirement. A diagram such as Figure 5, while it still includes the GIG, clearly identifies to the warfighter where he can get his weather forecast and, to some extent, an expectation about the quality of data that will be received; more importantly, it informs the warfighter who to call if the information does not meet his mission needs.

With this diagram, the warfighter has a definite knowledge about who will be providing the information required to execute the mission (in this case a U.S. Navy [USN] stateside-based weather service and a U.S. Air Force [USAF] theater-based service). There is no need to capture every possible information provider, just the most likely ones. Figure 6 provides one possible technical implementation of the same operational need.

Approaching the architectural diagrams in this manner enables the warfighter to be more specific about what information is expected to be provided. This specificity should also be captured in the information exchange matrix. The Department of Defense (DoD) Architecture Framework v1.5 provides a recommended information exchange matrix format. The matrix emphasizes the operational characteristics of the information and is not intended to be an exhaustive listing of all operational details. Rather, this product is intended to capture the most important aspects of selected information exchanges [2].

Starting with this matrix and adding the following data elements will help capture the warfighter's expectations for service-provided information. These elements address the warfighter's need to control how service-derived information is sourced, stored, and acted upon.

- **Information owner.** The sending operational node is not necessarily the owner or producer of the information; sometimes it acts as a *pass-through* or *operate off* of derived information. This is the operational entity actually producing the information that the warfighter requires to execute his mission.
- **Information storage.** Does the warfighter require his system to locally store the information? Information such as operations orders may need to be stored, but individual common operational picture elements may not. Warfighters have mission critical information that must be present regardless of network or service operational status, and only being able to access this information when the *network is up* is not an option.
- **Information perishability.** How long does the information received from a service need to stay operationally relevant to meet the warfighter's mission requirements? If

Figure 5: *Operationally Focused SOA Diagram*

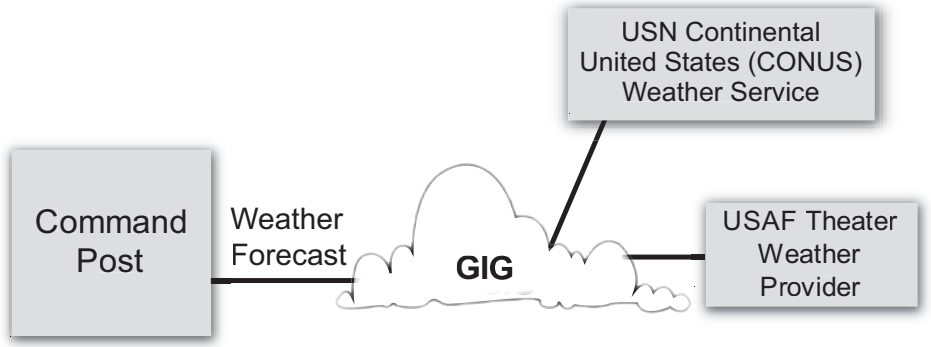
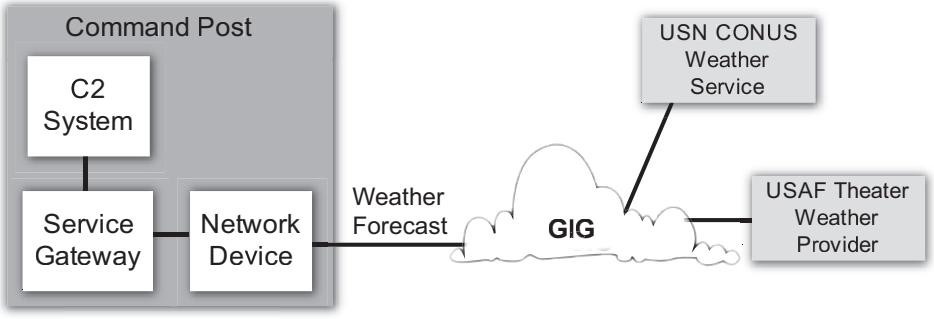


Figure 6: *Implementation Oriented SOA Diagram*



the network only allows a 30 minute information update, but the information is only valid for 15 minutes, the warfighter's needs will not be met.

- **Quality.** This is a subjective or objective measure that defines *how good* the information should be regardless of its source. Operationally, the information must meet this threshold; the system must be able to cycle among available, trusted information sources to provide the best information.
- **Trustworthiness:** This provides a subjective or objective measure that ranks the information owner, enabling the warfighter to give precedence to one information owner over another based on operational considerations. The warfighter should also be able to explicitly exclude information providers if desired.
- **Information derivation:** This includes the business rules the warfighter expects to be implemented to change raw data into useful information. There are many possible and correct ways to derive information. As the warfighter will be making decisions based on the information, not raw data, the warfighter needs to be assured that the way information will be generated meets its requirements.

The following data elements should be added to the matrix to capture how the warfighter's expectations about information produced by its system could be made available through a service. Though similar to some information assurance-related elements, they serve a different operational purpose.

- **Service discoverability.** Should the information be discoverable by all users (public), users fitting a certain profile (restricted), or only upon invitation (private)?
- **Subscriber roles.** Should information exchange be restricted to other users within a defined chain of command (role based) or not (non-role based)?
- **Subscriber availability.** Will the information be available to external subscribers continually (continuous) or in accordance with the situation and doctrine (limited)? This enables other warfighters to determine how much they can depend on this information source.
- **Subscriber storage.** Should the information be storable by the subscriber? In some instances, there is an operational requirement to disable a subscriber's ability to store service-provided information.

Current Implementation

Weather information, a subset of what is known within the DoD as Meteorology and Oceanography (METOC) information was chosen to showcase a net-centric service currently available to warfighters called the Joint METOC Data Services Framework (JMDSF) [3] provided by the Naval Oceanographic Office or NAVOCEANO. The JMDSF is designed to be a tool kit for deploying data-oriented services to securely deliver geospatial information and is the vehicle used by DoD to establish a single access point for all METOC data.

Using JMDSF, NAVOCENO can collate METOC data from numerous government and commercial providers, normalize this data, and publish it for all DoD METOC information users. JMDSF is responsible to the warfighter for recording where authoritative data resides, thereby easing the warfighter's concern for authenticating data [3]. To make this service even more useful, a Web-based front end and file transfer protocol push capability has been developed to enable the warfighter's system to retrieve METOC information in a variety of ways over networks of differing capacity.

No matter how useful, JMDSF is still a technical implementation of a net-centric service, not the operational activity providing the information. That organization will still be NAVOCENO, the Air Force Weather Agency, or some other operational entity. No matter how good JMDSF is at delivering METOC data on behalf of NAVOCENO, it is still only the current technical solution. The operational need to retrieve and act on METOC information does not change. By describing this need in terms of the operational requirement via the technical service solution, the warfighter can clearly define his requirements and be assured the technical solution will implement it.

Conclusion

Net-centric services provide warfighters with improved access to the information they need to make decisions, but only when these services are implemented in a way that reflects the warfighter's requirements. The services themselves are invisible to the warfighters, but the information the services provide is not.

Warfighters must be assured that their information needs will be met regardless of the technology that implements their requirements; especially since these services will be eclipsed by newer technologies over time. So identifying netcentric service requirements should be accomplished early in the JCIDS cycle and validated at each step. Regardless of the technology that provides information, the warfighter's requirement to ensure all information is timely, accurate, relevant, and trustworthy will not change.◆

References

1. "Web Services Glossary." W3C <www.w3.org/TR/ws-gloss/#webservice>.
2. DoD Architecture Framework Working Group. "DoD Architecture Framework, v1." Washington: Assistant Secretary of Defense for Networks and Information Integration, 2004.
3. Washburn, P., and T. Morris. "NAVOCEANO Web Services: Online Data and Functionality for the Warfighter." CHIPS Jan.-Mar., 2005: 37-39.

About the Author

Michael S. Russell is a senior technical director for General Dynamics Information Technology. He has served as lead systems engineer or systems architect on numerous federal, DoD, and industry development efforts, and currently manages programs for the U.S. Marine Corp's Systems Command. Prior to this, Russell served in the U.S. Army. He is a faculty member with the Federal Enterprise Architecture Certification Institute and is a member of International Council on Systems Engineering. Russell holds a master's degree in software engineering from George Mason University and has taught systems engineering courses for the past eight years.

General Dynamics Information Technology
16 Center ST
STE 109
Stafford, VA 22556
Phone: (540) 657-5393
E-mail: mike.russell@gdit.com