CONCEPTUAL SOS MODEL AND SIMULATION SYSTEMS FOR A NEXT GENERATION NATIONAL HEALTHCARE INFORMATION NETWORK (NHIN-2): CREATING A NET-CENTRIC, EXTENSIBLE, CONTEXT AWARE, DYNAMIC DISCOVERY FRAMEWORK FOR ROBUST, SECURE, FLEXIBLE, SAFE, AND RELIABLE HEALTHCARE

**Elliot Sloane, Thomas Way,
Vijay Gehlot, and Robert Beck
Villanova University
800 Lancaster Avenue
Villanova, PA 19085
610-519-6432
{elliot.sloane, thomas.way,
vijay.gehlot, robert.beck}@villanova.edu**

Abstract – This paper describes the emerging US National Healthcare Information Network (NHIN). Scheduled to be completed for the US Department of Health and Human Services (DHSS) by 2014, the NHIN will be a complex System of Systems information network built up from consumer, physician, hospital, and Regional Healthcare Information Organizations (RHIOs). The advantages and disadvantages of NHIN's RHIOs are discussed, and a proposed Service Oriented Architecture (SOA) version we have preliminarily named NHIN-2 is described. This paper explains the advantages of the proposed SOA-enhanced NHIN-2, and how it could be modeled and simulated using tools and techniques currently being developed in the ARCES project for the US Department of Defense (DoD). The paper discusses the potential "dual use" or "peacetime dividends" the DoD work could provide in developing the NHIN-2.

INTRODUCTION

The US National Information Healthcare Network (NHIN)

In 2006, the US Department of Health and Human Services (DHHS) initiated the design and development of a first generation National Healthcare Information Network (NHIN) [1]. The overarching goals of NHIN are to create a technical framework to allow sharing of medical data between care providers, referred to as interoperability, and to create an Electronic Health Record (EHR) for all US citizens by 2014. NHIN by nature is a complex System of Systems (SoS) challenge because contemporary healthcare depends on multiple disparate clinical specialists (e.g., radiologist, cardiologist, or rheumatologist) and care-delivery-providers (e.g., hospital, physician office, or home care), each using specialized computer systems for optimal clinical data and practice management. In addition, telemedicine tools are enabling an ever-expanding diversity of points-of-care, creating a growing number of smaller healthcare subsystems that extend to personal, consumer-based health care technologies [2].

The NHIN project development process employs an iterative, one-year analysis-design-prototype cycle. Each year groups of clinicians, providers, and researchers are organized into teams known as the American Healthcare Information Community (AHIC) [3]. These teams have the task of specifying annual clinical and operational goals and requirements for the NHIN [3]. Once AHIC has specified the coming year's NHIN goals, a DHHS-funded technology team known as the Healthcare Information Technology Standards Panel (HITSP) identifies, evaluates, and recommends the most appropriate technical frameworks and standards that DHHS should

specify in order to meet the interoperability and EHR goals specified by AHIC [4]. The first year's design was finalized in late October, 2006, and was accepted by the Secretary of Health in January of 2007 [5].

During 2007, four teams of vendors and providers have been funded by DHHS build and test demonstration pilot projects of Regional Healthcare Information Organizations (RHIOs) based on the 2006 HITSP recommendations. In addition, AHIC has specified a new set of clinical goals for 2007, and HITSP projects are underway to identify, review, and recommend the technical framework and standards DHHS should employ to achieve the new AHIC goals.

This paper is organized in the following sections: An explanation of the advantages and limitations of the NHIN's RHIO architecture, a description of a robust Service Oriented Architecture (SOA) alternative version we are presently calling NHIN-2, and a discussion of how SOA modeling and simulation tools being developed for Department of Defense (DoD) applications could be used to design the proposed NHIN-2. The paper concludes with a discussion about potential next steps for this proposed design.

Advantages of the NHIN's Regional Healthcare Information Organization (RHIOs) Architecture

The RHIOs are a very important architectural component of NHIN. Instead of creating a single national medical data warehouse for all citizens' data, DHHS chose to rely on a network architecture of independent RHIOs whose job is to pass patient data from one RHIO to another when and as needed. For example, if a patient from Philadelphia was injured during a skiing vacation in Utah, a RHIO in Utah would locate all available medical data for that patient through a RHIO near Philadelphia and share it with the physicians and nurses in Utah. The RHIO's job is not specifically to maintain all of the data in a region, but rather to serve as a central registry and data relay system for all of the patient data that is held by the clinical care providers within its membership area. The HITSP frameworks and standards, therefore, could essentially govern the transfer of data between the RHIOs, leaving the RHIOs and their members some latitude in deciding their own internal systems, software, and standards.

This RHIO architecture has many advantages, including the following:

- Most patient data is kept in the hospital, specialty departments, and physician offices the patient visits most frequently, ensuring rapid availability for the most likely clinical users, the patients, and their families.
- Each RHIO may be flexibly designed to support a finite variety of local legacy healthcare information systems instead of having to simultaneously support all potential legacy systems across the country;
- Any single RHIO or telecommunication failure should be a local event that is unlikely to disrupt patient care in other regions;
- Confidential, life-critical patient data is not aggregated in any single repository where it could be vulnerable to privacy breaches, tampering, or loss;
- The emerging HITSP standards that have been accepted by the Secretary of Health are based on commonly-accepted XML data formats, which help ensure ready data identification and interpretation; and
- The NHIN's RHIO architecture is based on a PULL data model, whereby RHIOs responses can be limited to patient inquiries it receives.

Potential Challenges and Risks of the NHIN's Regional Healthcare Information Organization (RHIOs) Architecture

The RHIO architecture currently moving into pilot and demonstration phases can be visualized as a national network of proprietary regional star networks that are designed to facilitate relatively 'static' data transfers between local and regional providers. This RHIO architecture has several fundamental risks, including:

- Though a single point RHIO failure may not affect other regions, it could cause major expensive or life-threatening disruptions within its own region, which is actually the most likely region where most patient may need medical care;
- If one or more RHIOs introduces significant information completeness or capacity constraints into the national RHIO network because of financial or technical difficulties, that could have expensive or life-threatening regional/national consequences for patients and providers;

- Lack of RHIO standardization could lead to extensive continuous, expensive, and error-prone maintenance of each proprietary RHIO to match expanding clinical and technical requirements;
- Reactive data and software management among RHIOs is likely, unless each RHIO aggressively monitors and incorporates the inherently dynamic volume and type of medical information it must handle;
- Patients who live near two or more RHIO fringe areas are likely to constantly have clinical records spread among two, three, or more RHIOs;
- Physicians and hospitals that change outsource providers for laboratory, imaging, or other services may similarly select outsource resources that span multiple RHIOS;
- The NHIN's present PULL design will not necessarily forward critical emergent information from a RHIO that arrives after it has forwarded the clinical data which was requested (e.g., if a positive pregnancy test arrived in Philadelphia for the injured skier, that information might not be forwarded to Utah; and
- Remote or mobile data, from consumer healthcare products or ambulances for example, may not be incorporated into the RHIO's data transfer if those systems are not "online" at the time of the request.

SOA ENHANCEMENTS FOR MILITARY APPLICATIONS

Based on recent work for the Air Force and DoD (see Acknowledgements in the last section below), this paper discusses an enhanced Service-Oriented Architecture (SOA) that has uniquely robust and secure features. At the end of this section, we will explain how these SOA enhancements system could offer a promising direction for a next generation NHIN, which we have called NHIN-2.

As shown in Figure 1, SOA is a distributed network architecture design approach that partitions service providers (or provision) from service consumers (or consumption), using service brokers to manage the process.
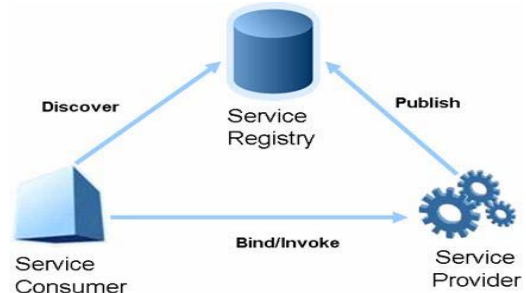

Figure 1. Traditional SOA model.

Self-contained services communicate with each other when required, yet they do not depend on the state of other services, creating a loosely coupled architecture that is easily reconfigurable. The SOA approach is attractive for complex System of Systems (SoS) designs because of its flexibility and reusability, and its isolation of functionality from the details of implementation. The general roles commonly described in SOA are service provider (SP), service consumer (SC) and service broker (SB). The SP produces services, making them available by publishing service interfaces in a service registry (SR). The SC uses SP services based on rules in the published service interfaces. A SB component of SOA manages the SR for both providers and consumers, and may assist in the "bind/invoke" tasks shown in Figure 1.

In the "traditional" SOA model as applied in many industrial settings, the available SP services are static. For example, a single-hospital SOA could use the hospital's Admission/Discharge/Transfer (ADT) system as the main Patient Registry SP, which the SB and all SC users might query for patient names, addresses, and other demographic and billing data. The elegance of the SOA architecture is that any new SC user, such as a new homecare business unit created by the hospital could plug into SOA's SB and SP immediately to help manage its homecare activities. All new hospital SC users only have to create a single interface to the whole system, as long as they carefully follow the correct common SOA communication and data protocols established by the hospital.

The flexibility and 'plug-and-play' interoperability of SOA led to its adoption by DoD for enterprise services deployments. The DoD and Defense Information Systems Agency (DISA) have defined a core set of services for defense-related SOA systems in its Net-Centric Enterprise Solutions for Interoperability (NESI) initiative [6]. These Net-

Centric Enterprise Services (NCES) defined by NESI include services, nodes and utilities for use in DoD domain, and mission-related enterprise information systems, and have led to significant, ongoing development efforts.

The SOA requirements for DoD use must include the following:

Table 1. Unique SOA requirements for SOA

• Service guarantees	• Security
• Fault tolerance	• Dynamic service discovery
• Load balancing	
• Interoperable multiple connection types	• Availability awareness (a.k.a. "presence management")

The requirements listed in Table 1 are similar to many other industry applications, but the three in the right hand column, Security, Dynamic service discovery, and Availability awareness, are particularly difficult to assure for DoD due to severe environmental demands.
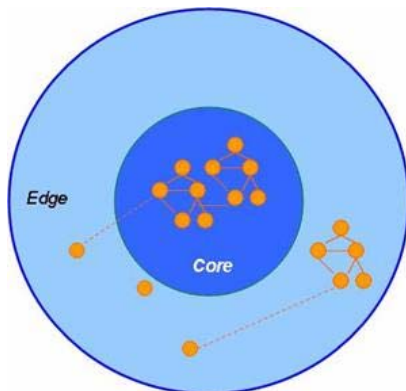

Figure 2. SOA Core and Edge diagram for DoD applications.

A simplified Core and Edge diagram (Figure 2) can help to illustrate DoD's severe environmental demands. SOA resources, such as general personnel records, can exist at the Pentagon in Arlington, VA. Those records can be provided by a permanent SP, and would be considered part of the Core SOA resources. Officers on the ground could be using PDA's with wireless digital cameras that link to other troops via an AWACS or satellite capture and relay system. That airborne system serves as an in-theatre SP that can relay crucial pictures for all participating military teams, perhaps saving many civilian or military lives. Since both the PDAs and the relay stations are mobile, however, the wireless links occasionally are overloaded or fail completely. Such intermittent mobile resources would be

shown in the Edge area of Figure 2. Wireless link failures, battery failures, PDA damage, thunderstorms, are all examples of the severe environmental considerations that Edge SOA operations must overcome for safe and reliable deployment.

These three use case examples of Edge-region challenges and solutions for DoD's SOA deployment can help illustrate the situation:

1. **Security:** An officer's PDA may allow her to pull up combat-related maps and even send IM feedback to her subordinates. That officer may have extensive access to high-security-clearance data and personnel, but if the PDA falls into a civilian's hands, the access to sensitive data at potentially hundreds of military SPs within the DoD's SOA fabric must be abruptly and effectively cut off. A very robust and dynamic Security Manager (SM) is necessary for DoD SOA deployments.

2. **Dynamic service discovery:** If a new GIS-based Improvised Explosive Device (IED) database were suddenly created, all service personnel's PDAs would certainly benefit from access to that data immediately. In the "classical" SOA context, all the SC module in all PDA's, and the main SB itself, may need to be updated with software patches to allow access to the new IED SP. For DoD applications, a robust and dynamic Service Discovery (SD) module could work with the SB to automatically handle these demands seamlessly.

3. **Availability awareness:** If the IED SP is maintained in an on-position AWACs airplane, communications with multiple officers' PDAs can be expected to drop offline periodically. In "traditional" SOA, the general expectation is that fairly robust continuous network and/or Internet access remains in an "always-on" state. For DoD applications, a Presence Management (PM) module could work with the SM and SD modules to ensure that when any PDA comes back online, it is a) authenticated for access to secure data and personnel, b), provided immediate status updates from the SPs it had been using, and c) notified of any new SP resources that had been added.

There may be multiple ways to achieve the kinds of SOA robustness and flexibility that DoD

requires. One that is under development for Wright Patterson Air Force Base is called the Multi-Channel Service Oriented Architecture (MCSOA) [7].

A key enhancement goal of MCSOA is the Dynamic Service Discovery Agent (DSDA) shown in Figure 3. Depending on configuration, the DSDA can handle any or all of the enhanced tasks listed in Table 1. In fact, the DSDA's must also exhibit sufficient redundancy that full or partial failure of any single Agent can be overcome by one or more available Agents. The MCSOA simulation, modeling, and development process includes the SM, SD, and PM tasks described in the example above.
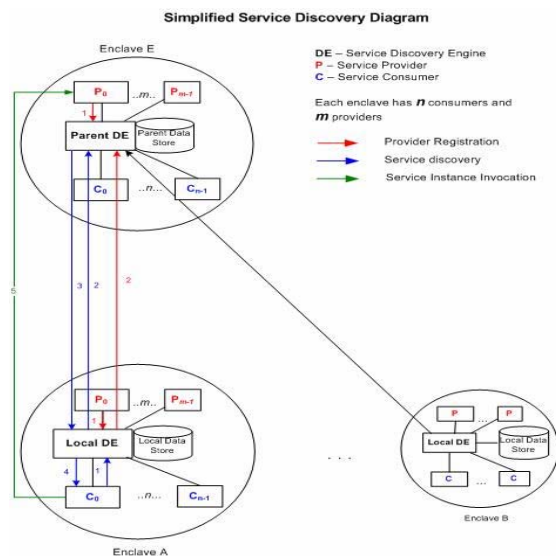

Figure 3. MCSOA Dynamic Service Discovery Agent

The simulation and modeling project under way at Villanova University focuses on discovering operational boundaries of alternative system design and telecommunication optimization strategies. The project uses a freely available "formal methods" simulation tool known as the Colored Petri Net (CPN), and a second, hybrid proprietary discrete simulation tool known as MESA/Extend to do whitebox and blackbox simulations and modeling. For further details about the technical facets of the simulation, modeling, and design of MCSOA's SOA enhancements, the reader may wish to refer to a different paper in this conference [8], as they will not be repeated here.

In this paper, the MCSOA development, modeling, and simulation systems are being used to illustrate our NHIN-2 design proposal. The

authors recognize that many other technical and/or commercial SOA tools might be use to achieve similar results, but we do not have access to those resources and therefore cannot discuss them.

PROPOSED ENHANCED-SOA NHIN-2

We will now use the above three DOD SOA use cases to illustrate how to create an acceptable enhanced-SOA NHIN-2. The following three NHIN-2 use cases parallel the DoD examples:

1. **Security:** In the healthcare world, the security needs are quite demanding due to the rigorous and often divergent Federal and State HIPAA requirements. For example, Massachusetts has specific HIPAA disclosure data restrictions for HIV tests and drugs that may differ from other states [9]. The Massachusetts law must be obeyed for data that in or out of any system in that state. To meet state-specific HIPAA laws using MCSOA a central "HIPAA SP" can be created that maintains all of the State and Federal HIPAA privacy laws and exceptions. The DSDA can locate and transfer those rules to any SB that needs them. Another "Provider SP" could contain all authenticated physicians and nurses, which wither the DSDA or a separate "HIPAA Security SP" could handle. Although these functions might seem like they could be Core functions other Edge applications will be described shortly.

2. **Dynamic service discovery:** Medication errors have allegedly caused tens of thousands of annual deaths in the US [10]. Manufacturers periodically recall drugs, or identify new dangerous drug interactions, or both. If new dangerous drug information becomes available, MCSOA's DSDA could broadcast that information all the way to home-based automated drug dispensing systems,, which would be acting in personal SC roles in the NHIN-2 SOA fabric.

3. **Availability awareness:** The two above use cases can be generalized to illustrate the role MCSOA's Presence Manager (PM) fills. An Edge example for the first use case would occur if a "first responder" such as a EMT was attempting to revive a non-responsive traffic accident victim in an ambulance. The wireless link to the ambulance might be quite

erratic, especially if tunnels, mountains, or thunderstorms are encountered. If data about the victim's medications or diabetes status comes available during a periodic communications lapse, the PM would store and forward that critical data as an enhanced service to the SC and SP.

CONCLUSIONS

We have proposed leveraging emerging DoD research and development as a valuable "dual use" or "peacetime dividend" for national healthcare applications. For example, the MCSOA system under developed for DoD includes Security Management (SM), Service Discovery (SD), and Presence Management (PM) capabilities using Dynamic Service Discovery Agents. These features could be used to improve individual and aggregate static data exchange between RHIOs in many ways. For example, the SM, SD, and PM features can be used together by the DSDA to help guarantee automatic updates to all bona fide healthcare providers to protect and improve a patient's care. The SD mechanism, integrated with PM presence, ensures up-to-date data by observing updates as part of its registration/presence information.

Using the DoD modeling presence and discovery modeling as described in our other paper [8], the proposed NHIN-2 could can also improve context-awareness and fault-tolerance, such as managing a telemedicine application's bandwidth constraints by automatically compressing data, or applying dynamic load-balance in a heavily loaded system to reduce system faults.

Building systems based on the conceptual NHIN-2 model, even as prototypes can be prohibitively expensive. By leveraging the CPN and MESA/Extend MCSOA modeling techniques we are developing for DoD, our models can be used to confirm that any NHIN-2 system design or configuration has the expected and desirable properties, and to also gain new insights into the workings of the system. This approach can help limit wasted programming or deployment resources by detecting and fixing robustness, security, flexibility, safety, or reliability faults early in the design and configuration process.

ACKNOWLEDGEMENTS

REFERENCES

[1] Health Information Technology web site, U.S. Department of Health & Human Services. Accessed at: www.HHS.gov/healthit.

[2] Continua Health Alliance web site. Accessed at: www.continuaalliance.org.

[3] AHIC Workgroups web site at U.S. Department of Health & Human Services, Health Information Technology. Accessed at: www.hhs.gov/healthit/ahic/workgroups.html.

[4] Healthcare Information Technology Standards Panel web site, American National Standards Institute (ANSI). Accessed at: www.ansi.org/hitsp.

[5] Secretary of Health Acceptance and Planned Recognition of Certain Healthcare Information Technology Standards Panel (HITSP), Interoperability Specifications for Health Information Technology. US Federal Register, March 1, 2007. 72(40) p. 9339.

[6] Netcentric Enterprise Solutions for Interoperability (NESI) public web site, U.S. Navy. Accessed at: http://nesipublic.spawar.navy.mil.

[7] Service-Deployment Frameworks and Routing Fabrics: the elements of a Multi-Channel Service Oriented Architecture (MCSOA). Whitepaper, available at: http://www.gestalt-llc.com/resources/d_mcsoa.pdf

[8] Sloane, E.B., Way, T., Gehlot, V., Beck, R., Solderitch, J., Dziembowski, E. A hybrid approach to modeling SOA Systems of Systems using CPN and MESA/Extend, Proceedings of the 1st Annual IEEE Systems Conference, Honolulu, HI, April 9-12, 2007.

[9] Massachusetts Bureau of Communicable Disease Control: Frequently Asked Questions Regarding Reporting of Communicable Disease under HIPAA web site. Accessed at: http://www.mass.gov/dph/comm/hipaa/faq_cdc.htm

[10] Institute of Medicine. To Err is Human: Building a Safer Health System. National Academy Press, 2000. Washington, D.C. Available at: http://www.nap.edu/