2008-06

A Service Oriented Approach (SOA) to the IT-based Protection of Critical Infrastructures--A First Approach to Integrate SOA into a Complex Operational Analysis within Risk Assessment and Risk Management Processes

Rughooputh, Razvan

A Service Oriented Approach (SOA) to the IT-based Protection of Critical Infrastructures- A First Approach to Integrate SOA into a Complex Operational Analysis within Risk Assessment and Risk Management Processes

Razvan Bugheanu, Marius Dumitrascu
Goran Mihelcic, Stefan Pickl

Department of Computer Science
Chair for Operations Research
University of the Federal Armed Forces Munich

http://www.unibw.de/stefan.pickl
Stefan.Pickl@unibw.de

Germany-85577 Neubiberg-München

ABSTRACT

The design and optimization of comfortable decision support systems becomes more and more important. One disadvantage of many complex systems is that they often consist of a large amount of heterogeneous single applications that are inefficiently integrated into the overall process. This happens as such processes tend to grow over time, caused by an increase of complexity and supplementary demands by users for further functionalities, which leads to demands of new applications that are added to the system and need not always be compatible to the legacy applications. This results in process inefficiencies such as breakings in the media chain, high coordination effort, redundancy and an inefficient handling of information as the processing time increases. In case of threat on a critical infrastructure element, a fast and flexible acquisition, processing, and allocation of information are crucial. Flexibility, fast adaptability, and high process efficiency are central characteristics of a Service Oriented Architecture (SOA) which qualifies it to be used in the context of OR analysis in order to protect optimally the critical infrastructure.
This contribution gives an introduction in SOA as well as an overview of an integration of SOA-elements within the analysis of complex critical infrastructures. We combine an approach from an operational point of view together within a service-orientated framework within such a complex decision support process of an OR/MS-analyst.

1. Introduction
Critical Infrastructures as Complex Systems within an Uncertain Environment

Critical infrastructures are vital elements on which our daily live and society are based on, wherefore it is of great importance to pay a special attention to the protection of these elements.
The following sectors can be identified as being critical infrastructure elements[1]: Banking and Finance; Chemical Industry; Commercial Facilities; Commercial Nuclear Reactors, Materials, and Waste; Dams; Defence Industrial Base; Drinking Water and Wastewater Treatment Systems; Emergency Services; Energy; Food and Agriculture; Government Facilities; Information Technology; National Monuments and Icons; Postal and Shipping; Public Health and Healthcare; Telecommunications; and Transportation Systems. Break-downs or disturbances of such critical systems as a result of e.g. war, disaster, civil unrest, vandalism, or sabotage, may cause severe damage in the supply of a wide part of users linked to these systems and can have severe consequences to vital functions of the society.

[1] George Mason University, "What is CIP", School of Law, December 2006, http://cipp.gmu.edu/cip/, accessed 30 March 2008

A definition is given in the "Patriot Act 2001 of the U.S.A" that describes critical infrastructures as[2]:

> *"systems and assets, whether physical or virtual, so vital […] that the incapacity or destruction of such systems and assets would have a debilitation impact on security, national economic security, national public health or safety, or any combination of those matters."*

Further definitions emphasize the interrelationship of the critical infrastructure elements[3]:

> *"Critical infrastructures are the complex and highly interdependent systems, networks, and assets that provide the services essential in our daily life."*

Thus, certain sections of critical infrastructure elements depend on each other and threats or risks that concern the one can influence the other. It is obvious that classical approaches from Operational Analysis should be combined in the future with such service-orientated approaches. They might help to identify processes as well as to support a comfortable risk management.

2. Identification Processes and Risk Management – Vulnerability Analysis

Hence, methods and processes for early-warning- or precautionary-, emergency planning-, information-exchange/distribution-, and recovery systems have to be developed to increase the robustness of such infrastructures. The protection of critical infrastructure elements requires the capability to identify and monitor these elements in a first step. During the monitoring phase there should be established the ability to analyse whether these elements of critical infrastructure are under attack or in danger caused to natural influences.

The identification process should be linked to a risk management process, to determine e.g. the vulnerability of certain infrastructure elements and to develop special protection plans. The Department of Defence (DoD) of the U.S.A, which is the responsible authority in the protection of the national sectors: Financial Services; Transportation; Public Works; Global Information Grid Command Control; Intelligence Surveillance, and Reconnaissance; Health Affairs; Personnel; Space; Logistics; and Defence Industrial Base, has developed a "Critical Infrastructure Protection Lifecycle" (CIP) that details the above statements and consists of the following six phases[4]:

- Analysis and Assessment;
- Remediation;
- Indications and Warnings;
- Mitigation;
- Incident Response; and
- Reconstitution.

---

[2] "USA PATRIOT ACT OF 2001", October 2001, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107.pdf, accessed 30 March 2008

[3] George Mason University, "What is CIP", School of Law, December 2006, http://cipp.gmu.edu/cip/, accessed 30 March 2008

[4] Department of Defense, "The Department of Defense Critical Infrastructure Protection (CIP) Plan", November 1998, http://www.fas.org/irp/offdocs/pdd/DOD-CIP-Plan.htm, accessed 30 March 2008

The Analysis and Assessment phase is the crucial part of the CIP life cycle. The identification of the vulnerability and the characteristics of critical elements such as their interrelationship to other elements are derived in this phase. During the Remediation phase, precautionary actions are taken on the base of the Analysis phase in order to fix identified vulnerabilities of the regarded element. The task of the Indications and Warnings phase focuses on the monitoring of the critical infrastructure element in order to reveal possible threats or hazards (identification) and to inform the owners or authorities linked to the element about the potential danger (warning). The Mitigation phase manages the actions that are taken in response to the analysed indications and warnings of the previous phase in order to minimize the overall threat or damage of the critical infrastructure. The Incident Response phase takes place after the occurrence of an infrastructural event that threatens the functionality of a critical infrastructure, and tries to eliminate the cause or source of this event. The final Reconstitution phase comes into action when an infrastructural event had damaged the functionality and capability of a critical infrastructure and comprises actions to recover it.

3. Integration of IT-based Systems (Metrics, Methods and Tools)

The usage of IT-based Systems in order to accommodate the demand on information that is needed to achieve a sufficient situational awareness –within an Operational Analytic Approach- at the particular phases is advised. One disadvantage of many systems that are in use to support the CIP lifecycle is that they often consist of a large amount of heterogeneous single applications that are inefficiently integrated into the overall process. This happens as such processes tend to grow over time, caused by an increase of complexity and supplementary demands by users for further functionalities, which leads to demands of new applications that are added to the system and need not always be compatible to the legacy applications. This results in process inefficiencies such as breakings in the media chain, high coordination effort, redundancy and an inefficient handling of information as the processing time increases. In case of threat on a critical infrastructure element, a fast and flexible acquisition, processing, and allocation of information are crucial. Flexibility, fast adaptability, and high process efficiency are central characteristics of a Service Oriented Architecture (SOA) which qualifies it to be used in the context of the protection of critical infrastructure. Although it is difficult to define the history of Service Oriented Architecture in terms of when it was created and who founded it, SOA's history can be defined in terms of the impact it has had on industry practices and thinking. In the early days of functional programming, data and functionality were strictly separated.

The next step was merging data and functionality into encapsulated, reusable object implementations (object orientation). This worked particularly well for large, monolithic applications, such as complex graphical user interfaces.

4. SOA (Service Orientated Architecture)

In the middle of the 1990s, people started to apply the concepts of object orientation to distributed systems. CORBA and a number of other standards for distributed object computing emerged. The limitations of this approach became clear when applying distributed object technology in large-scale projects. As a result, Service Oriented Architectures emerged, with supporting technology platforms such as XML Web services. Service Oriented Architectures evolved of past platforms, preserving successful characteristics of traditional architectures, and bringing with it distinct principles that foster service-orientation in support of a service-oriented enterprise. The roots of service-orientation can be found in three different areas.

The first area is concerned with Programming Paradigms: functional decomposition (COBOL, PASCAL), modularization and component programming (ADA, Visual Basic, Prolog), object-oriented programming (SIMULA, C++, Java) and service oriented computing. The second aspect involves Distribution Technology: mainframe computing, Remote Procedure Call (RPC), Distributed Component Object Model (DCOM), Common Object Request Broker Architecture (CORBA), Enterprise Java Beans (EJB). Another important area is represented by Business Computing : SAP (Systems, Applications and Products in Data Processing) introduced R/2(1981), the first business-computing platform that enabled enterprise-wide real time processing of financial data and resource planning information. Complex enterprise applications emerged in the past years: Enterprise Resources Planning (ERP), Supply Chain Management (SCM), Customer Relationship Management (CRM).[5]

> Service-Oriented Architecture is both: a design concept and architecture. The design concept in SOA is about designing applications/systems that have well defined self-describing access interfaces, having services composed into business processes. The architecture is about having simple mechanisms to use these access-interfaces for integration purposes.[6]

A formal definition of Service Oriented Architecture is given by Thomas Erl in his book "Service-Oriented Architecture: Concepts, Technology, and Design", stating that:

> *"A contemporary SOA represents an open, agile, extensible, federated, composable architecture comprised of autonomous, QoS-capable, vendor diverse, interoperable, discoverable, and potentially reusable services, implemented as Web services."*[7]

Although Service Oriented Architecture solutions are technology independent, the broad acceptance of the web service design model made the web-based implementation of an SOA to a standard solution. Among technologies like web services, XML (Extended Markup Language) is used to send and receive data in a standardized format, and HTTP (Hypertext Transfer Protocol) is used as communication protocol. Furthermore, supplementary technologies have become de facto standards. The most important are briefly described in the following. Primarily a communication protocol, Simple Object Access Protocol (SOAP) which is platform and language independent, allows the communication between processes. Based on XML, it is used for describing and sending messages. The Web Services Description Language (WSDL) describes the interface to the web service using XML. It indicates where the service is located and what operations are provided for use. The Universal Description, Discovery and Integration (UDDI) directory serves as a place where the registration and search for web services are managed. Many software solutions that support SOA implementations have been developed and a large amount is available as open source (J2EE, Fuse, WebSphere).

The main motivation for creating a SOA is the desire to increase agility of IT systems. In addition, SOAs offer benefits at several levels, ranging from a reduction of technology dependence to a simplification of the development process to an increase in flexibility and reusability of the system's infrastructure.

---

[5] Dirk Krafzig, Karl Banke, *Enterprise SOA: Service-Oriented Architecture Best Practices*(Prentice Hall PTR, 2004), Ch 2.2-2.4

[6] Juric, Loganathan, Sarang, Jennings, *SOA Approach to Integration*(Birmingham: Packt Publishing, 2007), 57

[7] Thomas Erl, *Service-Oriented Architecture: Concepts, Technology, and Design*(Prentice Hall PTR, 2005), Ch 3.2.11

The ultimate goal of the additional reusability and flexibility provided by a SOA is the agile system platform, in which all processes and services are completely flexible and can be rapidly created, configured, and rearranged as required by experts without the need for technical staff. This facilitates a superior reaction time. Another motivating factor is the potential of efficiency, balancing the complexity that threatens a certain element of critical infrastructure on different levels. Identifying the following elements of complexity: technology, processes, functionality, integration, maintenance, the simplicity is achieved through: decomposition, appropriate granularity, decoupling from technology, reuse and documentation. Cost Savings can be obtained through reduced project costs, reduced maintenance costs, and the development of future proof solutions. Further benefit is contributed through the reuse of existing code that significantly reduces the risk of failure in following projects. The service itself can be used in different technological contexts that guarantee a protection of investment. [8]

5. Risk Assessment and Management: SOA and CRISYS (Critical Infrastructure and System Analysis) - Complex Scenarios

It is possible to create a new service simply by choreographing existing building blocks. SOA allows for a more efficient development process and a high degree of modularity, which in turn makes it possible to decouple the development process. The overhead of project management is significantly reduced. Using SOA facilitates independence from technology; choosing the best of breed products and combining them as required by the particular application field, helps to shift the attention from technological issues to questions of service functionality and service design. SOA might be an excellent technique to be integrated in a complex system analytic process to protect critical infrastructures.

In the following, the focus will be put on a special scenario and the description of a system that is extremely valuable in the protection of critical infrastructures. The advantages of a SOA-based development of the system will become obvious. Imagining the potential threat of a terrorist vehicle carrying a hazardous load possibly heading towards an identified element of critical infrastructure, demands for a system that reports the current position of this vehicle to the authorities capable of escalating this potential threat. A system that accommodates this demand is referred to as a tracking and monitoring system. This system is vital for several phases mentioned in the first part of this paper: Indications and Warning phase that implies monitoring of the critical infrastructure elements to reveal possible threats and to inform authorities about the potential danger:

- The Mitigation phase in which the tracking system can help to minimize the overall threat on the critical infrastructure.

Even more, the Incident Response phase which tries to eliminate the cause or source of the event (which in this case is the terrorist vehicle) could not be carried out without a tracking and monitoring system. A vehicle tracking system is an electronic device installed in a vehicle in order to enable the owner or a third party to track the vehicle's location. Most modern vehicle tracking systems use Global Positioning System (GPS) modules for an accurate location of the vehicle. Many systems also combine a communications component such as cellular or satellite transmitters to communicate the vehicle’s location to a remote user. Vehicle information can be viewed on electronic maps via the Internet or specialized software. Current vehicle tracking systems have their roots in the shipping industry.

---

[8] Dirk Krafzig, Karl Banke, *Enterprise SOA: Service-Oriented Architecture Best Practices*(Prentice Hall PTR, 2004), Ch 11.1

Corporations with large fleets required some sort of system to determine where each vehicle or vessel is at any given time. There exist several types of vehicle tracking devices. Typically they are classified as passive and active. Passive devices store GPS location, speed, heading and sometimes a trigger event such as key on/off, door open/closed. Once the vehicle returns to a predetermined point, the device is removed and the data downloaded to a computer for evaluation. Passive systems include an auto download type that transfer data via wireless download. Active devices also collect the same information but usually transmit the data in real-time via cellular or satellite networks to a computer or data center for evaluation. In the following, the focus will be put on active systems[9]. A vehicle tracking system can efficiently monitor and, equipped with the relevant devices, even control vehicles. Technologies used in this process linked with means of wireless communication are essential to the system determining the vehicle location. It is required to have a technique to handle the huge amount of spatial data entailed in a digital road map in order to trace the accurate position within a reasonable time. The GIS (Geographic Information System) and GPS (Global Positioning System) technology have brought some breakthrough in the area of transportation monitoring.

One of the most useful applications[10] is a vehicle tracking and monitoring system to determine and trace the position of the mobile object (automobile, vessel, aircraft, etc.). Especially, the land vehicle tracking system locates vehicles using GPS satellites, GPS receivers and auxiliary equipments, and displays the geographical coordinate of the vehicle position on a digital road map of the monitoring system. GPS is a navigation support system developed originally for military purpose. Recently, GPS technology is widely spread and used in many applications, since its C/A (Coarse Acquisition) code is freely available to civilians. According to the near live report of the 2d Space Operations Squadron (2 SOPS) at Schriever AFB, CO who operates the GPS system, there are currently 28 satellites in activity. At least four of them are observable from any place in the globe. Unlike one might think GPS satellites are not geostationary (except the SBAS satellites) as they orbit at about 20,000 kms of altitude.

6. Monitoring and Tracking – Role of Metrics, Methods and Tools (Operations Research/Management Science)

This means that depending on your position, at certain times, the "sky" will be unfavourable (poor alignment and elevation of satellites) and it will be difficult for a GPS receiver to have a good communication with the satellites. GPS satellites transmit two low power radio signals, designated L1 and L2. Civilian GPS uses the L1 frequency of 1575.42 MHz in the UHF band[11]. The signals travel by line of sight, meaning they will pass through clouds, glass and plastic but will not go through most solid objects such as buildings and mountains. A GPS signal contains three different bits of information — a pseudorandom code, ephemeris data and almanac data. The pseudorandom code is simply an I.D. code that identifies which satellite is transmitting information[12].

---

[9] Parkinson, B.W. ,*Global Positioning System: Theory and Applications* (1996) ch 1

[10] Satellite Navigation & Positioning Laboratory (SNAP Lab) , „Principles and Practice of GPS Surveying“, http://www.gmat.unsw.edu.au/snap/gps/gps_survey/chap12/1233.htm , accessed 30 March 2008

[11] Satellite Navigation & Positioning Laboratory (SNAP Lab) , „Principles and Practice of GPS Surveying“, http://www.gmat.unsw.edu.au/snap/gps/gps_survey/chap3/311.htm , accessed 30 March 2008

[12] Satellite Navigation & Positioning Laboratory (SNAP Lab) , „Principles and Practice of GPS Surveying“, http://www.gmat.unsw.edu.au/snap/gps/gps_survey/chap3/312.htm , accessed 30 March 2008

Ephemeris data tells the GPS receiver where each GPS satellite should be at any time throughout the day. Each satellite transmits ephemeris data showing the orbital information for that satellite and for every other satellite in the system. Almanac data, which is constantly transmitted by each satellite, contains important information about the status of the satellite (healthy or unhealthy), current date and time. This part of the signal is essential for determining a position. A GPS receiver accepts the signals involving the satellite's clock and orbit information of each one of the seen satellites and calculates the difference between the receiver clock at the signal's reception time and the satellite clock at its transmission time. The time difference derives a distance (usually called pseudo range) from the receiver to each one of the satellites and then the location of each satellite can be elicited from its orbit information. Finally, the location of the receiver is computed by the triangular measurement using the resulting positions of those satellites[13].

The vehicle tracking system needs to be channelized by a wireless communication link from the receiver of the vehicle to the monitoring station. Beyond this kind of immediate demand, the advent of wireless era accelerates the nationwide construction of various wireless networks. Currently, a conventional private network, a TRS (Trunked Radio System) network, a cellular network, a satellite network and a data packet network may be a candidate for the application:

- All concepts explained above could be bound together within an Operational Analysis in order to obtain a perspective view of the entire monitoring system.

Recalling the previous example of the potential threat through a terrorist vehicle carrying a hazardous load (e.g. chemicals, explosives, radioactive substances, etc.), possibly heading towards an identified element of critical infrastructure, and the hereby arising demand for a system that is able to track its position, the described tracking and monitoring system is advised. Implementing the needed devices at the target vehicle (tagging) – possibly during a stop at a gas station or any other scenario – or making use of already implemented sensors (like e.g. already installed GPS-modules in rental cars) makes it possible to apply a tracking and monitoring system.

A very important part of the entire system consists in a collection of software programs able to ensure an efficient communication between a GPS receiver and a processing unit. All information received should be analyzed by experts in different domains: communications, radioactive materials, national security, situational awareness, chemical weapons, etc. One or more teams placed in different locations across the entire area (or all over the world) are needed.

Collaboration between different teams is usually ensured by different software tools. Also a secure infrastructure is needed to prevent unauthorized access. Virtual Private Networks are used and particular communication protocols are implemented in order to ensure privacy. All software tools involved should communicate with each other, and the integration of new functionalities must be achieved in a simple, flexible and efficient way. Agility, modularity, ease of integration, technology independence and reusability should be the main characteristics of the entire system's architecture.

SOA natively supports these characteristics and much more, allowing a system in which processes and services are completely flexible and can be rapidly created, configured,

[13] Aidala, V. J and Hammel, S. E , "Observability Requirements for Three-Dimensional Tracking Via Angle Measurements," *IEEE Transactions on Aerospace and Electronic Systems, AES-21*, 2 (Mar. 1985): 200-207.

rearranged, and exchanged as required. These features of a SOA accommodate the demands for an efficient information handling and reaction time in situations general OR/MS applications as well as the threat on critical infrastructure elements.

7. Summary

This contribution combines a traditional operational approach within the analysis of critical infrastructures with a Service Oriented Architecture (SOA)-framework. An introduction into SOA and its characteristics is presented. Advantages of flexibility, fast adaptability, and high process efficiency are central characteristics of a Service Oriented Architecture which qualifies it to be used in the context of the analysis and protection of critical infrastructures. As critical infrastructure security will be an important task in the future there might be a need to combine pure analytic approaches with software-engineering capabilities. The integration of SOA into Operations Management and Operational Analysis will become more and more important in the near future. First possible applications and results within such an OR/MS-process to support intelligent decision support systems are illustrated.

8. Acknowledgement

The authors want to thank Alex Bordetsky for stimulating discussions and all his help to be integrated in the Maritime Interdiction Operation (MIO)-experiments series.

REFERENCES

Aidala, V. J and Hammel, S. E , ”Observability Requirements for Three-Dimensional Tracking Via Angle Measurements,” *IEEE Transactions on Aerospace and Electronic Systems, AES-21*, 2 (Mar. 1985): 200-207.

Dirk Krafzig, Karl Banke, *Enterprise SOA: Service-Oriented Architecture Best Practices* (Prentice Hall PTR, 2004), Ch 2.2-2.4

Dirk Krafzig, Karl Banke, *Enterprise SOA: Service-Oriented Architecture Best Practices* (Prentice Hall PTR, 2004), Ch 11.1

Juric, Loganathan, Sarang, Jennings, *SOA Approach to Integration* (Birmingham: Packt Publishing, 2007), 57

Parkinson, B.W. ,*Global Positioning System: Theory and Applications* (1996) ch 1

Thomas Erl, *Service-Oriented Architecture: Concepts, Technology, and Design* (Prentice Hall PTR, 2005), Ch 3.2.11

Department of Defense, “The Department of Defense Critical Infrastructure Protection (CIP) Plan”, November 1998, http://www.fas.org/irp/offdocs/pdd/DOD-CIP-Plan.htm, accessed 30 March 2008

George Mason University, “What is CIP”, School of Law, December 2006, http://cipp.gmu.edu/cip/, accessed 30 March 2008

Satellite Navigation & Positioning Laboratory (SNAP Lab), „Principles and Practice of GPS Surveying“, http://www.gmat.unsw.edu.au/snap/gps/gps_survey/chap12/1233.htm , accessed 30 March 2008

Satellite Navigation & Positioning Laboratory (SNAP Lab), „Principles and Practice of GPS Surveying“, http://www.gmat.unsw.edu.au/snap/gps/gps_survey/chap3/311.htm , accessed 30 March 2008

Satellite Navigation & Positioning Laboratory (SNAP Lab), „Principles and Practice of GPS Surveying“, http://www.gmat.unsw.edu.au/snap/gps/gps_survey/chap3/312.htm , accessed 30 March 2008

“USA PATRIOT ACT OF 2001”, October 2001, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107.pdf, accessed 30 March 2008