International Gas Union Research Conference
IGRC COPENHAGEN 2014
September 17-19
Gas Innovations Inspiring Clean Energy

Title: Semantic Cyber Security for Semantic Intelligent (SCADA/DCS): Application in modern gas industry

Authors: Sahli Nabil[1], BenMohammed Mohamed[2], El-Bay Bourennane[3]

[1]GRTG Factory SONELGAZ Group, LIRE Laboratory Constantine 2 University
AIG Association Algeria, n.sahli@sonelgaz.dz
[2]LIRE Laboratory Constantine 2 University, Computational Department Algeria,
ben_moh123@yahoo.com

[3]Le2i Laboratory Burgundy University, BP 47870 21078 Dijon cedex France, ebourenn@u-bourgogne.fr

Keywords:

Semantic intelligent (SCADA/DCS); Security Protocol; Semantic Cyber Security; Semantic vulnerabilities; (SNMP) Intelligent Monitoring ; Modern gas industry.

I-INTRODUCTION:

For several years, (**DCS** - Distributed Control Systems) have played a key role in the design of modern power applications such as modern gas industry, particularly in the automatic management of real time gas platforms, using (**SCADA** - Supervisory Control and Data Acquisition) systems [1]. A telemetry system is complex, with a number of assets and locations to monitor and control, wide platforms in large area. From a communications perspective, it can be a multi-layered system using a variety of communications media such as radio, cellular, and fiber to interconnect sites. Then, a top-end graphical (SCADA/DCS) [2] system is required to display all field data in a manner that can be easily understood.

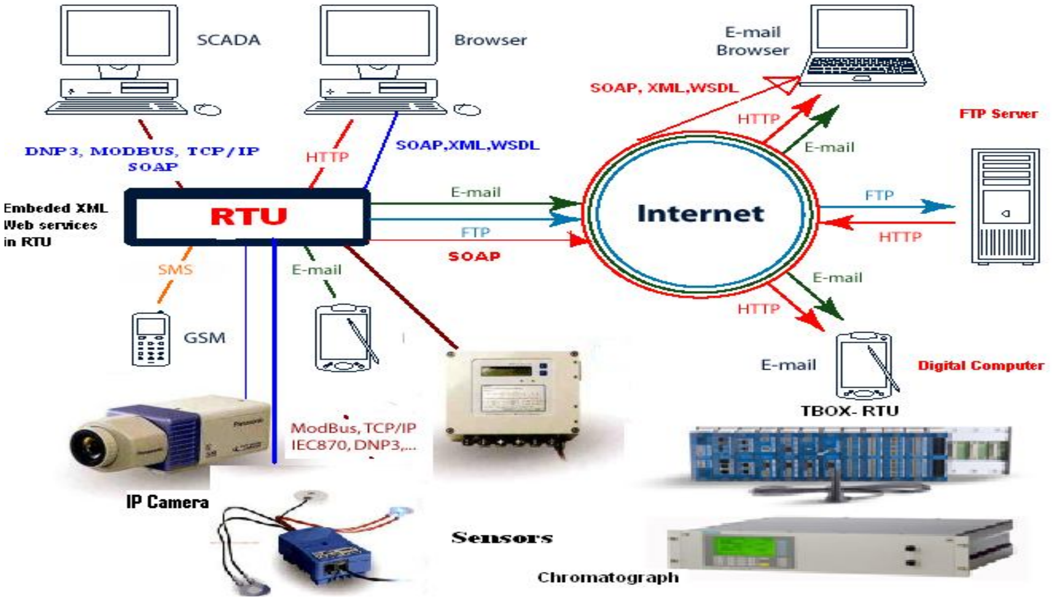
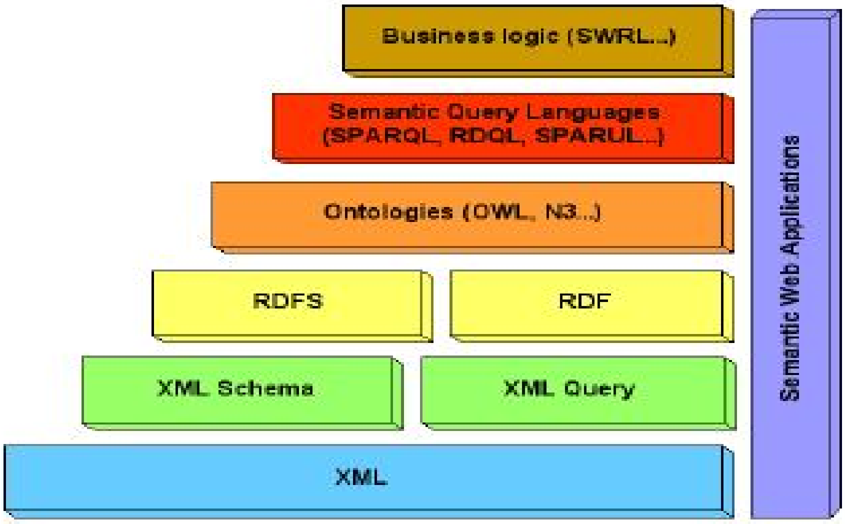


Figure 1. Modern (SCADA/DCS) systems platform

The use of semantic intelligent application embedded in (SCADA/DCS) intelligent devices creates new generation of vulnerabilities and problems in these systems as presented in the figure 1.

II-THE SEMANTIC CYBER SECURITY

In this work, we present a semantic cyber security system and we study the semantic intelligent (SCADA/DCS) systems vulnerabilities [11, 12], focusing on the semantic attacks.



.

Figure 2 . Multiple layers in the semantic application embedded in modern semantic (SCADA/DCS) [3]

For resolving semantic problems we propose a security global solution for the new generation of (SCADA/DCS) systems, which are typically employed in wireless communication support systems, embedded intelligent devices, embedded web services, embedded semantic and intelligent applications. The proposed solution atoms at protecting critical semantic (SCADA/DCS) processes from the effects of major failures of information systems, network disruptions or damage, and we focus our attention on the newest generation (OS- Operating System), such systems named semantic intelligent (SCADA/DCS). We used a security block in the global network access point composed by ((Firewall), (IDS – Intrusion Detection System) and network antivirus), security protocols deployed in different network (OSI) model levels. We applied our security global solution to modern gas industrial platforms in Algerian university laboratory and university laboratory in France. We used our mixed coordinates (ECC – Elliptic Curve Cryptography) solution [5], this is an encryption and key management protocol developed specifically for low latency embedded applications, it supports low speed links, short messages, (request/response), polled messages. We integrated security mechanisms in specific (SCADA/DCS) protocol (**DNP3** - Distributed Network Protocol version 3). We present in the figure 2, an example of semantic attack scenario in modern (SCADA/DCS) systems.

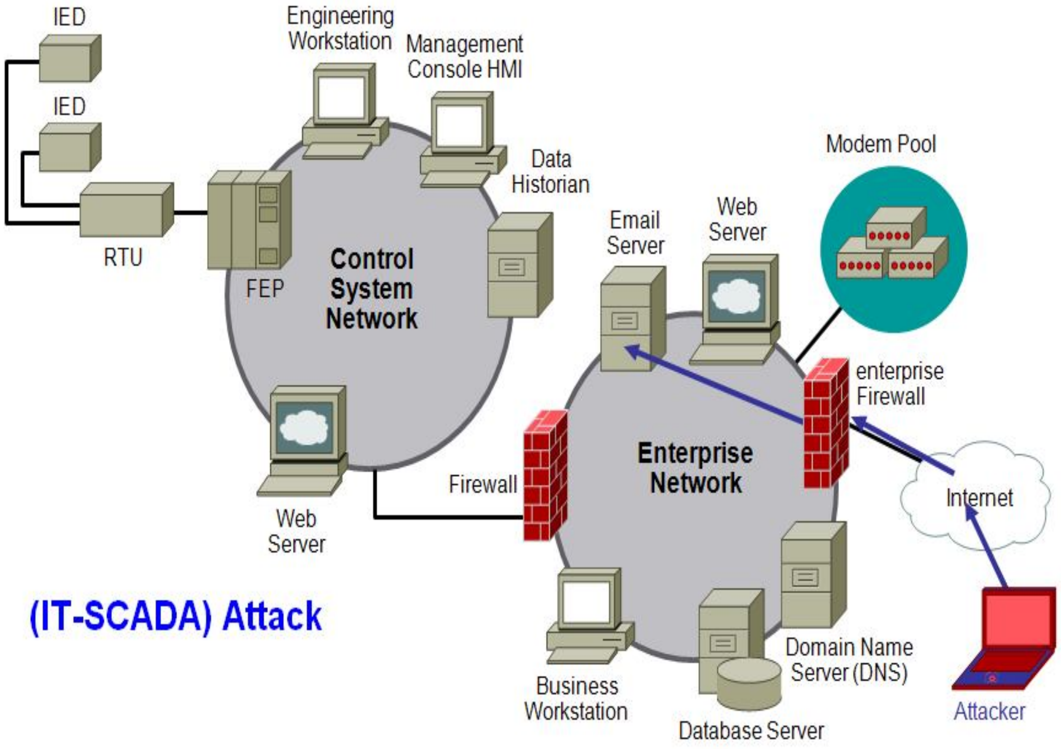


Figure 3. Semantic attack scenario in modern (SCADA/DCS) systems

III-OUR SEMANTIC SECURITY SOLUTION

Moreover, we made use of the (WS-Security) framework and we crypt and signed all the improved security protocols frames with mixed coordinates (ECC) and a hash function. Where encryption implementation between (SCADA/DCS) embedded intelligent devices and (**RTU** – Remote Terminal Unit/**PLC** Programmable Logic Controller) should not degrade the functional or performance capability of the operational function in these semantic intelligent systems [9], with the use of adapted semantic security global solution.

Advantages of the (DNP3) communications protocol in industrial and utility telemetry systems, the key features of the (DNP3) protocol and the benefits to industrial and utility telemetry systems. The DNP3 protocol has a number of features and advantages. However, the following features are particularly useful for industrial and utility applications , Open protocol , Classification of field data ,Report by exception ,Time-stamped data , Support for time synchronization , Secure authentication , Diagnostic information for each (I/O) point ,Communication to multiple masters. Advanced communications factures for (DNP3-Based) telemetry systems (Peer-to-peer communications, (DNP3) message pass-through [6], Data Concentration). (DNP3) is an exceptional protocol, it is modern, robust, intelligent, and a truly open protocol. It is still an evolving protocol. This is illustrated by the addition of secure authentication. In our work we proposed a new semantic (DNP) version obtained by the combination of (DNP) protocol with (**SOAP** – Simple Object Access Protocol) and (**SNMP** – Simple Network Management Protocol) [7] for semantic communication and intelligent (IT-SCADA) platform monitoring, where (IT-SCADA) obtained by the inter-conexion between (IT) network and (SCADA/DCS) network.

We resumed in the table 1 below, our results in our global semantic security solution, obtained by the use of the new security (DNP) protocol combined with other (**IT** - Information Technology) protocols as (SOAP), (**SSL** - Secure Socket Layer /**VPN** - Virtual Private Network), (SNMP) protocol and the use of (ECC) cryptography solution combined with a hash function for securing the communications in the modern (SCADA/DCS). We resumed our security (IT-SCADA) interconnected platform in the figure 3 below, where we used (SSL/VPN) optimized with (**ECC**- Elliptic Curve Cryptography) mixed coordinates for creating virtual partition (VPN1) for (IT) application named enterprise zone, (VPN2) for (SCADA/DCS) named control zone and (**DMZ**- Demilitarized Zone) between the too virtual partitions as presented in the figure 3 below.

We introduced the use of semantic security ontologies for resolving semantic vulnerabilities in modern semantic (SCADA/DCS) systems, we presented the security ontologies classification in the figure 3. The security ontologies composed by:

-Beginning security ontologies.
-Security taxonomies.
-General security ontologies.
-Specific security ontologies.
-Web oriented security ontologies.
-Risk based security ontologies.
-Security ontologies requirements.
-Modeling security ontologies.

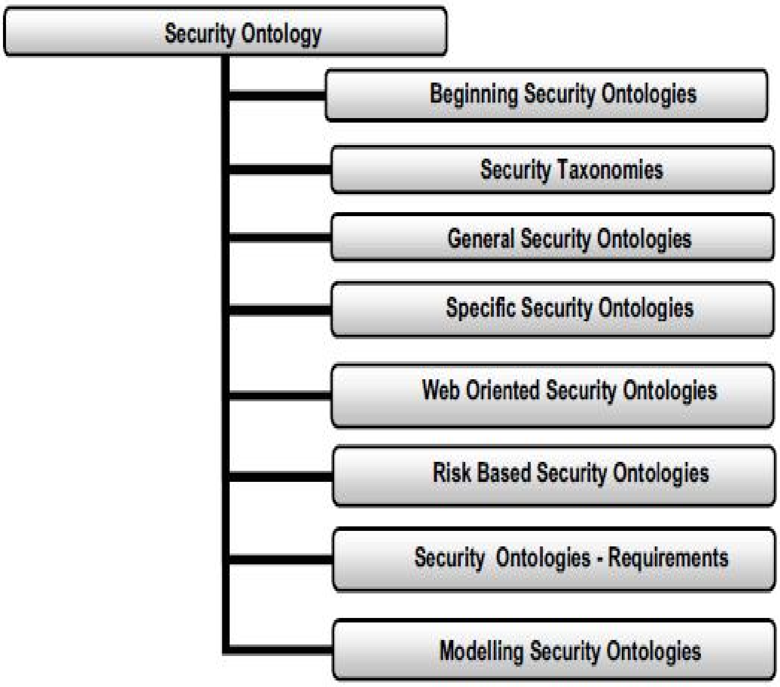

Security Ontology
Beginning Security Ontologies
Security Taxonomies
General Security Ontologies
Specific Security Ontologies
Web Oriented Security Ontologies
Risk Based Security Ontologies
Security Ontologies - Requirements
Modelling Security Ontologies

Figure 4. Classification of security ontologies [4,10]

We proposed the integration of security ontologies in the semantic security block, composed by semantic firewall, semantic (IDS- Intrusion Detection System) and network anti virus [5] as embedded software's in security devices. Implemented with (OWL-S) standard [10].

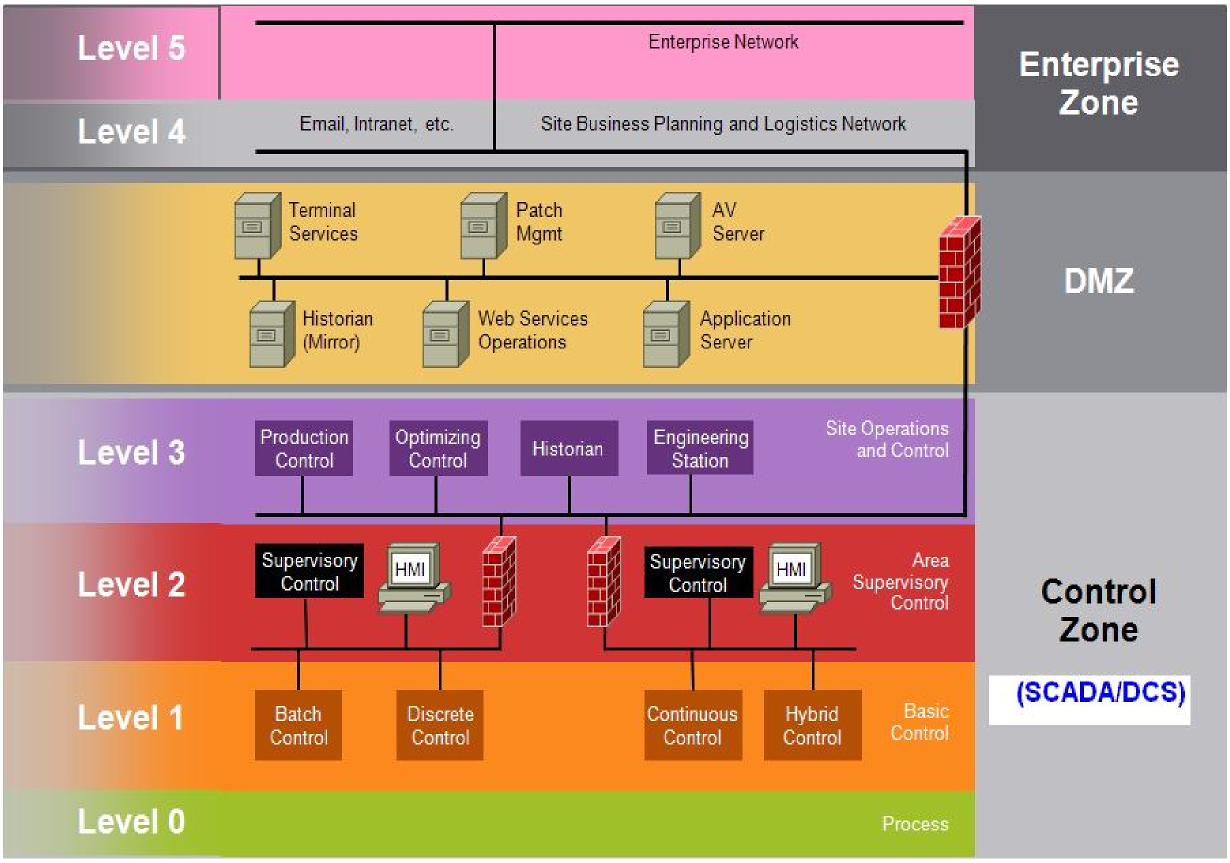


Figure 5. Our proposed solution topology for modern (IT-SCADA)

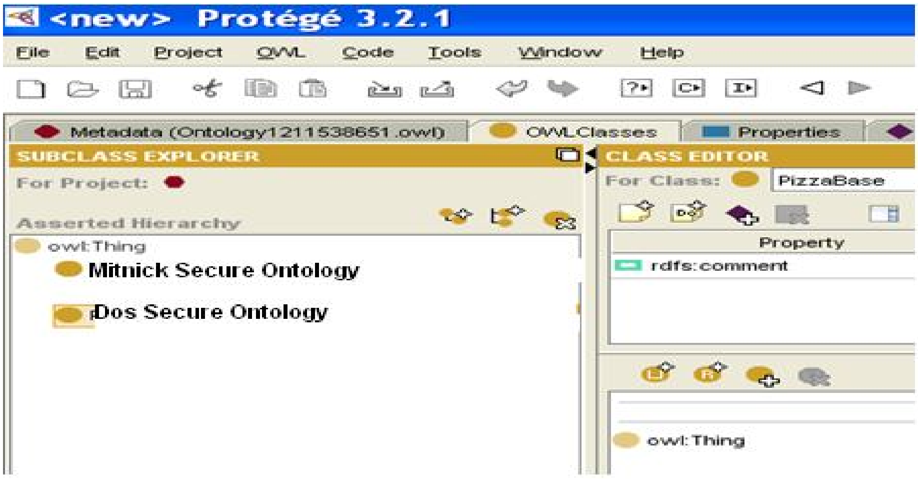


Figure 6 . Our Secure ontologies implemented with "Protégé 3.2.1" Editor

We resumed our global security solution in the table 1. We applied our global security solution in modern gas industry in Algerian and European laboratory.

Table 1. Security level proposed in our global solution

Security Level	Proposed solution
Message	(DNP/SOAP/Security) Protocol
Application	(SSL/VPN) Protocol
Application	(DNP/SOAP/SNMP/Security) Protocol
Cryptography and Signature	Mixed coordinates ECC combined with hash Function XML Signature [8]
Access point	Security semantic Block (Firewall, IDS, Network Antivirus)

IV-CONCLUSION

We conclude that in our work we proposed a new secured (DNP) protocol version combined with optimized (VPN/SSL) protocol, optimized (SNMP) protocol combined with internet messaging (SOAP) protocol and with the use of security block. We proposed the integration of security ontologies in the security devices composed the security block and (ECC) mixed coordinates solution combined with a hash function in all cryptography and signature operations.

REFERENCES

[1] B.Brian, F.Broyles, “Is there anything new under the SCADA sun”, December, 2003.

[2] Riptech, Inc. “Understanding SCADA System Security Vulnerabilities”, iwar.org.uk/rerources/utilities/SCADAWhitepaperfinal1.pdf, January ,2001.

[3] Devendra Kumar Sloni, V.K.Sharma, Safe semantic web and security aspect implication for social networking, International journal of computer applications in engineering sciences , vol ISSN: 2231-4946, I, Issue II, june, 2011, pp 141-149.

[4] Amina souag, Camile salenzi, Izabelle Watiou, Ontolgy for security recurments: a letterature survey and classification, 19 juin, 2012.

[5] N.Sahli, M.Benmohammed, “Security solution for semantic SCADA optimized by ECC cryptography mixed coordinates“, IEEE ICITES 2 end international conferences Sousse Tunisia, ISBN: 978-2-4673-1167-0, 2012, pp 230-235.

[6]S.Patel and J.Graham, "Security Considerations in DNP3 SCADA systems", 17 th International conferences on computer applications in Industry and engineering. November 17-19, 2004.

[7] http://www.commentcamarche.net/contents/internet /snmp.php3 , 2013.

[8]B.Laurence, M.David, "XML Signature Extensibility Using Custom Transforms", 5th International Conference on Web Information Systems Engineering, Brisbane, Australia, Web Information Systems –WISE , November 22-24, 2004, pp 102-112.

[9]G.Bush, "National Policy to Security Cyberspace", The White House, Washington, February, 2003.

[10]G. Denker, S.Nguyen, and A.Ton, "OWL-S Semantics of Security Web Services: a Case Study", SRI International, Menlo Park, California, USA, 2004.

[11] P.Lindstrom, "Attacking and Defending Web Services", a Spire Research Repport, January, 2004.

[12] S.Faut, "SOAP Web Services Attacks: Are you web applications vulnerable", SPI Dynamics, 2003.