

Knowledge-Based Support for Security Risk Analysis of Microgrid

Introduction

- Like any other networked system, a Microgrid system can be a prime target of cyber security attacks need to be taken into that consideration during the design and operations of a Microgrid.
- There is a lack of realisation of the potential risk of cyber attacks and lack of knowledge for analysing and addressing the risks that can exploited to launch cyber be attacks, which can result in a huge social and financial damages.

Research Problem

- Microgrid systems are a new breed whose systems design, development, and operations may not be driven by security sensitive considerations.
- Key stakeholders (e.g., designers, developers, managers, and operators) may not have the required cyber security knowledge to analyse the threat landscape and the potential solutions.





Project Objectives

- Determine the types of cyber security threats to and solutions for Microgrid systems for coalescing the available information in a readily usable form.
- Develop a knowledge-based approach that can support cyber security risk analysis of Microgrid.
- Leverage a semantic and extensible Wiki platform that can support our approach to capturing and sharing cyber security knowledge for analysing threats and devising solutions of Microgrid.

Gang Yang, Puzhi Yao, (gang.yang, puzhi.yao)@student.Adelaide.edu.au, Master of Software Engineering Supervised By Prof. M. Ali Babar, (ali.babar@Adelaide.edu.au) School of Computer Science

Key Milestones

- Reviewed a large amount of literature on cyber secu to Smart Grid and Microgrid for identifying and categorial reported cyber security threats, vulnerabilities, challe potential impacts and proposed solutions for systems.
- Built and evaluated an Ontological model to chai knowledge system which captures cyber security the solutions of Microgrid.
- Designed and Implemented a semantic Wiki (i.e., based system for implementing the cyber security model for easy of capture and management of cyb knowledge.

Section in Navigation Section in Navigation secture implementation Secting Rev Major Strategy applies to a High-Level Data Endrarge Accord Cortrol System Navion Coronal Cortion System Navion Beterove Architecture a Ucorgit Cortol System Navion Security Rev Major Strategy Coronal System Navion Security Rev Major Strategy Coronal System Navion Design Approach Design Approach Figure 2 : Implemented Semantic Wiki Prage View Type Security Cover System Navion - Knowledge Attributes descrite: - latency bathwith, and quality of service (QKS) for intra-notice communications - figure 2 : Implemented Semantic Wiki Prage View Part Cover Security see Structure [2]	Sub-Class	User Extras Help Debu]		Search for Resourc	es
Sourty Risk I High-Level Data Exchanges exture Implementation I High-Level Data Exchanges applies to I High-Level Data Exchanges Design Approach I Cyter Acors Enclaves I High-Level Data Exchanges I High-Level Data Exchanges I Knowledge attributes Secure Vinteour I Enclaves Type I Design Approach Knowledge content Intercoreal donation and quelty of server (Qis) for intre-enclave communications Hypes of hebroix Halloto expect Intercoreal donation and quelty of server (Qis) for intre-enclave communications Hypes of hebroix Halloto expect Intercoreal donation and quelty of server (Qis) for intre-enclave communications Hypes of hebroix Halloto expect Intercoreal donation and quelty of server (Qis) for intre-enclave communications Hypes of	Inter-related	Edit View Sort Type		History Community Source		
Figure 2: Implemented Semantic Wiki Page View • which enclaves need to communicate • types of network traffic that will be communicated between enclaves • iatency, bandwidth, and QoS for inter-enclave communications • latency, bandwidth, and QoS for inter-enclave communications • iatency, bandwidth, and QoS for inter-enclave communications rid Cyber Security Label Data Exchange Ref Veitch, C. K., Henry, J. M., Richardson, B. T., & Hart, D. H. (2013). Microgrid cyber security reference architecture. Sandia Nat. Lab.(Hierarch. SNL-NM), Albuquerque, NM, USA, Tech. Page SAND2012 E472	applies to Design Approact	Security Risk Reference Architecture Implementation Security Risk Mitigation Strategy Security Criterion Asset	Type Comment	 Microgrid Control System Network Cyber Actors Enclaves Functional Domains Design Approach Data exchange defines communication domains. Within an enclave, data exch Iatency, bandwidth, and quality of ser types of network traffic to expect necessary level of enclave cyber second 	Knowledge Menti n between actors within enclaves and functional nange attributes describe: rvice (QoS) for intra-enclave communications	Enter your Comment tes There are no discussions yet. One of in other links Instances linking here Related approach ⁻¹ Integrated security framework with 3 Iayers * Cyber Actors * Enclaves *
Ref Veitch, C. K., Henry, J. M., Richardson, B. T., & Hart, D. H. (2013). Microgrid cyber security reference architecture. Sandia Nat. Lab. (Hierarch. SNL-NM), Albuquerque, NM, USA, Tech.	Ser	nantic Wiki Page		 types of network traffic that will be co latency, bandwidth, and QoS for inter 	mmunicated between enclaves r-enclave communications	SCADA Control and Communication Network with ACT •
Kep. SAND2013-5472. Knowledge reference source	-			Veitch, C. K., Henry, J. M., Richardson	b.(Hierarch. SNL-NM), Albuquerque, NM, USA, Tech.	

		Future Work
urity threats gorising the enges, their Microgrid	**	Carry out extensive evaluation of the developed approach and system with the real users of Microgrid systems. Refine and enhance the approach
aracterise a threats and		and the implemented systems for Microgrid cyber security decision making.
, OntoWiki) knowledge ber security	*	Deploy the system in real-life setting for assessing it robustness and value.

Key References
 Wenye Wang and Zhuo Lu. Cyber security in the smart grid: Survey and challenges. Computer Networks, 57(5):1344–1371, 2013. Dubois, É., Heymans, P., Mayer, N., & Matulevičius, R. (2010). A systematic approach to define the domain ISSRM. In Intentional Perspectives on Information Systems Engineering (pp. 289-306). Springer Berlin Heidelberg. Veitch, C. K., Henry, J. M., Richardson, B. T., & Hart, D. H. (2013). Microgrid cyber security reference architecture. Sandia Nat. Lab.(Hierarch. SNL-NM), Albuquerque, NM, USA, Tech. Rep. SAND2013-5472.
CRICOS Provider Number 00123M
seek LIGHT