Accepted Manuscript

Title: A review of cyber security risk assessment methods for SCADA systems

Author: Yulia Cherdantseva, Pete Burnap, Andrew Blyth, Peter Eden, Kevin Jones, Hugh Soulsby, Kristan Stoddart

PII: S0167-4048(15)00138-8
DOI: http://dx.doi.org/doi: 10.1016/j.cose.2015.09.009
Reference: COSE 946

To appear in: *Computers & Security*

Received date: 19-5-2015
Revised date: 18-9-2015
Accepted date: 29-9-2015

Please cite this article as: Yulia Cherdantseva, Pete Burnap, Andrew Blyth, Peter Eden, Kevin Jones, Hugh Soulsby, Kristan Stoddart, A review of cyber security risk assessment methods for SCADA systems, *Computers & Security* (2015), http://dx.doi.org/doi: 10.1016/j.cose.2015.09.009.

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

ACCEPTED MANUSCRIPT

A Review of Cyber Security Risk Assessment Methods for SCADA Systems

Yulia Cherdantseva[1], Pete Burnap
School of Computer Science and Informatics, Cardiff University, UK; email: y.v.cherdantseva, burnapp@cs.cardiff.ac.uk
Andrew Blyth, Peter Eden
Faculty of Computing, Engineering and Science, University of South Wales, UK; email: andrew.blyth, peter.eden@southwales.ac.uk
Kevin Jones, Hugh Soulsby
Cyber Operations, Airbus Group Innovations, UK; email: kevin.jones, hugh.soulsby@eads.com
Kristan Stoddart
Department of International Politics, Aberystwyth University, UK; email: kds@aber.ac.uk

Abstract

This paper reviews the state of the art in cyber security risk assessment of Supervisory Control and Data Acquisition (SCADA) systems. We select and in-detail examine twenty-four risk assessment methods developed for or applied in the context of a SCADA system. We describe the essence of the methods and then analyse them in terms of aim; application domain; the stages of risk management addressed; key risk management concepts covered; impact measurement; sources of probabilistic data; evaluation and tool support. Based on the analysis, we suggest an intuitive scheme for the categorisation of cyber security risk assessment methods for SCADA systems. We also outline five research challenges facing the domain and point out the approaches that might be taken.

Keywords: SCADA, cyber security, risk assessment, risk analysis

1. Introduction

A Supervisory Control and Data Acquisition (SCADA) system is a type of Industrial Control System (ICS). An ICS controls processes in the industrial sector and in the sectors which form a Critical National Infrastructure (CNI) **Error! Reference source not found.**. The list of sectors forming CNI varies from country to country. In the UK, CNI is defined as *"Those infrastructure assets (physical or electronic) that are vital to the continued delivery and integrity of the essential services upon which the UK relies, the loss or compromise of which would lead to severe economic or social consequences or to loss of life"* and is formed by nine sectors: energy, food, water, transportation, communications, emergency services, health care, financial services and government **Error! Reference source not found.**.

SCADA systems stand out among other ICSs as systems that (1) monitor and control assets distributed over large geographical areas, and (2) use specific control equipment such as a Master Terminal Unit (MTU) and Remote Terminal Unit (RTU), which we further discuss in Section 2. Initially, SCADA systems were used in power transmission, gas pipeline and water distribution control systems. Nowadays, SCADA systems are widely used in steel making, chemistry, telecommunications, experimental and manufacturing facilities [2, 4, 6].

The smooth and reliable operation of SCADA systems is vital for such sectors of

[1]Corresponding author

Download English Version:

https://daneshyari.com/en/article/6884209

Download Persian Version:

https://daneshyari.com/article/6884209

Daneshyari.com