NOMBRE DE LA REVISTA: International Journal of Critical Infrastructure Protección

Título del Artículo: Obtaining high preventive and resilience capacities in critical infrastructure by industrial automation cells

Autores: Santiago González González, Sebastián Dormido Canto, José Sánchez Moreno

Fecha de Publicación: 03/07/2020

Volumen: 29 **Página inicial:** 100355-1 **Página final:** 100355-16

Factor de impacto de la revista: 2.865

Rango de la revista en su categoría: Q2 (35/91)

Enlace al artículo: https://doi.org/10.1016/j.ijcip.2020.100355

International Journal of Critical Infrastructure Protection 29 (2020) 100355

Contents lists available at ScienceDirect

International Journal of Critical Infrastructure Protection

journal homepage: www.elsevier.com/locate/ijcip

Obtaining high preventive and resilience capacities in critical infrastructure by industrial automation cells

Santiago G. González[a,*], S. Dormido Canto[b], José Sánchez Moreno[b]

[a] National Centre for the Protection of Infrastructures and Cybersecurity, Secretary of State for Security, Ministry of Interior Spain, CETSE, El Pardo, Madrid, 28048, Spain

[b] Department of Computer Science and Automatic Control, Universidad Nacional Educación a Distancia (UNED), Madrid, 28040, Spain

ARTICLE INFO

Article history:
Received 19 July 2019
Revised 7 March 2020
Accepted 29 March 2020
Available online 3 July 2020

Keywords:
Cybersecurity
Industrial control system
Critical infrastructure
National Security
Cyber Resilience

ABSTRACT

The advances in Information Technologies (ITs) are providing Industrial Control Systems (ICS) with a great capacity for interconnection and adaptability. However, the use of communication networks makes ICS highly vulnerable. Consequently, it is essential to develop methodologies for the identification and subsequent classification of the ICS that intervene in critical infrastructure assets with any level of complexity, scalability and heterogeneity. The System and Infrastructure of Knowledge for Real Experimentation by means of Cells of Industrial Automation (SIKRECIA), described in this work, provides new capabilities for research, development, simulation and testing of the functioning of these systems, and the ability to foresee the behavior of a specific system in industrial production. The scenarios recreated through SIKRECIA have the ability to anticipate new threats that affect the ICS of critical infrastructures. Using SIKRECIA, a specific vulnerability of a PLC has been verified through the engineering programmed for the management of a traffic light control system. The results obtained demonstrate the high dependence between IT and OT (Operation Technologies) systems and therefore the importance of being able to recreate those environments before entering into operation. As SIKRECIA is an open system, it can use components from different industrial manufacturers to cover the existing architectures in the process industry.

1. Introduction

The research presented in this contribution is the result of the work developed in the area of cybersecurity in ICS environments [1–3]. To obtain a real result adapted to the specific needs of the so called "evaluation of prior risks" in an industrial production system, it is necessary to use real scenarios. At the same time, it provides the ability to perform forensic analyses of non-allowed interventions and analyses of behavior patterns through different tools present in the SIEM (Security Information and Event Management).

Academic institutions must take the initiative in the provision of scenarios for simulation testing and tests of real components of the industry, as well as the architectures deployed for this purpose. The importance of virtualized environments should be relegated to the background, since industrial systems require real contexts with complete operational readiness. These actions are intended to generate confidence in the world of operation technologies (OT).

One of the main issues that motivated the work presented here was the analysis of what was proposed in the technical report "Introduction to the Framework Certification of Cybersecurity Components (ICCF)" [4], published by the Joint Research center (JRC), the science and knowledge service of the European Commission, which pursues a scientific dispensation provision for the European policy-making process. This report aims to propose an initial set of common and comprehensive European requirements to promote IACS cybersecurity certification in Europe, to the point where suppliers are stimulating new demands by responding with innovation in its products to devise the cybersecurity certification of IACS components and play a key role in protecting critical infrastructures, and as a result of improving the resilience of systems and, therefore, both, a greater sense of security for citizens.

The IACS Components Cybersecurity Certification Framework (ICCF) aims to provide sufficient help to make certification in cybersecurity fluid and easy, always at a controlled cost and with recognition within and outside European borders. In this way, the possible inclusion of the SIKRECIA system as one more architecture collaborating in IACS is feasible, having a place by its very nature within the role of ICCF identified as laboratory, and complying with consistent evaluation pathways in evaluation, assessment, testing

* Corresponding author.
E-mail addresses: Santiago.gonzalez@invi.uned.es, sgg@interior.es (S. G. González), sebas@dia.uned.es (S. Dormido Canto), jsanchez@dia.uned.es (J. Sánchez Moreno).

https://doi.org/10.1016/j.ijcip.2020.100355
1874-5482/