



SMART Grid
SMART City
SMART People
SMART Strategy
en la Defensa de un País...

Claudio B. Caracciolo

Centro de Ciberseguridad Industrial (CCI)

Coordinador en Argentina

“Ciberseguridad Industrial es el conjunto de prácticas, procesos y tecnologías, diseñadas para gestionar el riesgo del ciberespacio derivado del uso, procesamiento, almacenamiento y transmisión de información utilizada en las organizaciones e infraestructuras industriales, utilizando las perspectivas de personas, procesos y tecnologías”



Personas inteligentes





Personas con malas intenciones



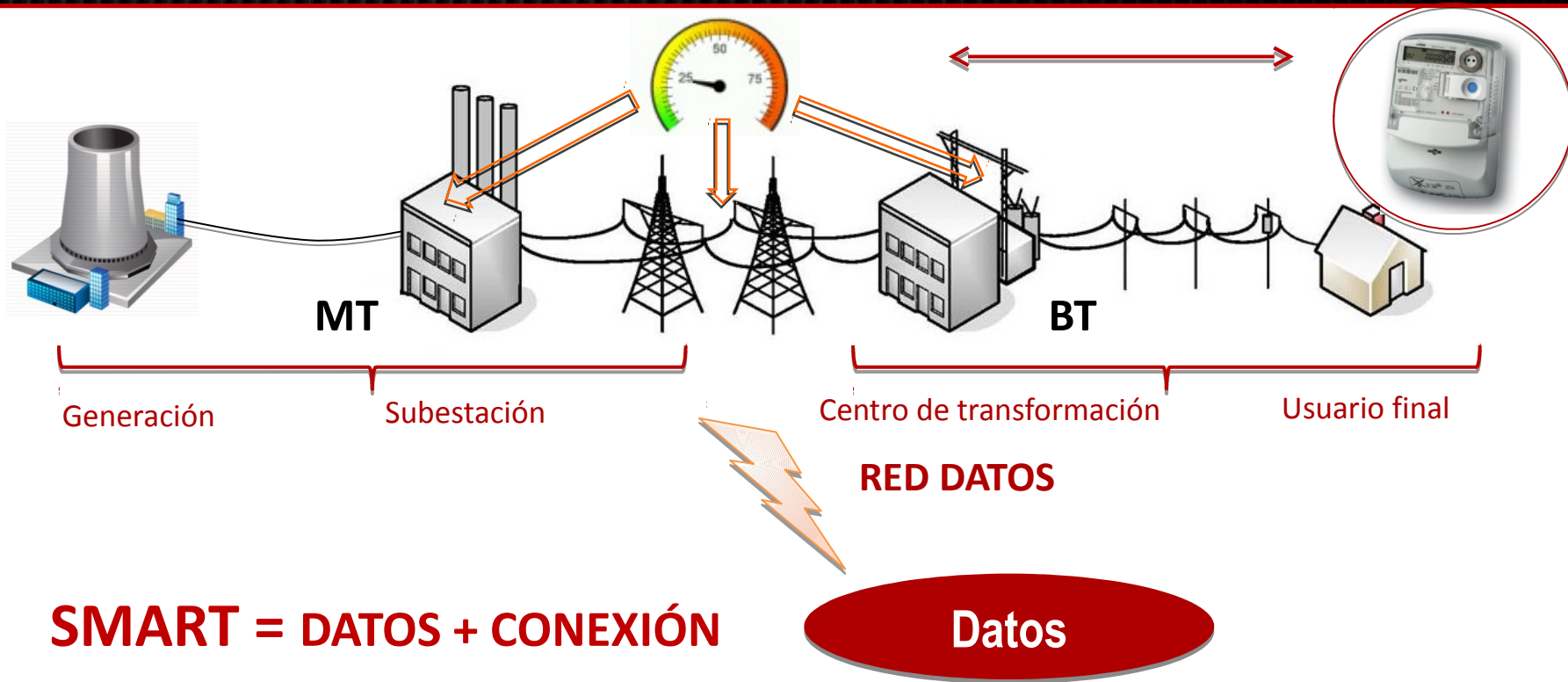


Conocer, medir, decidir...





Entendiendo la importancia de SG

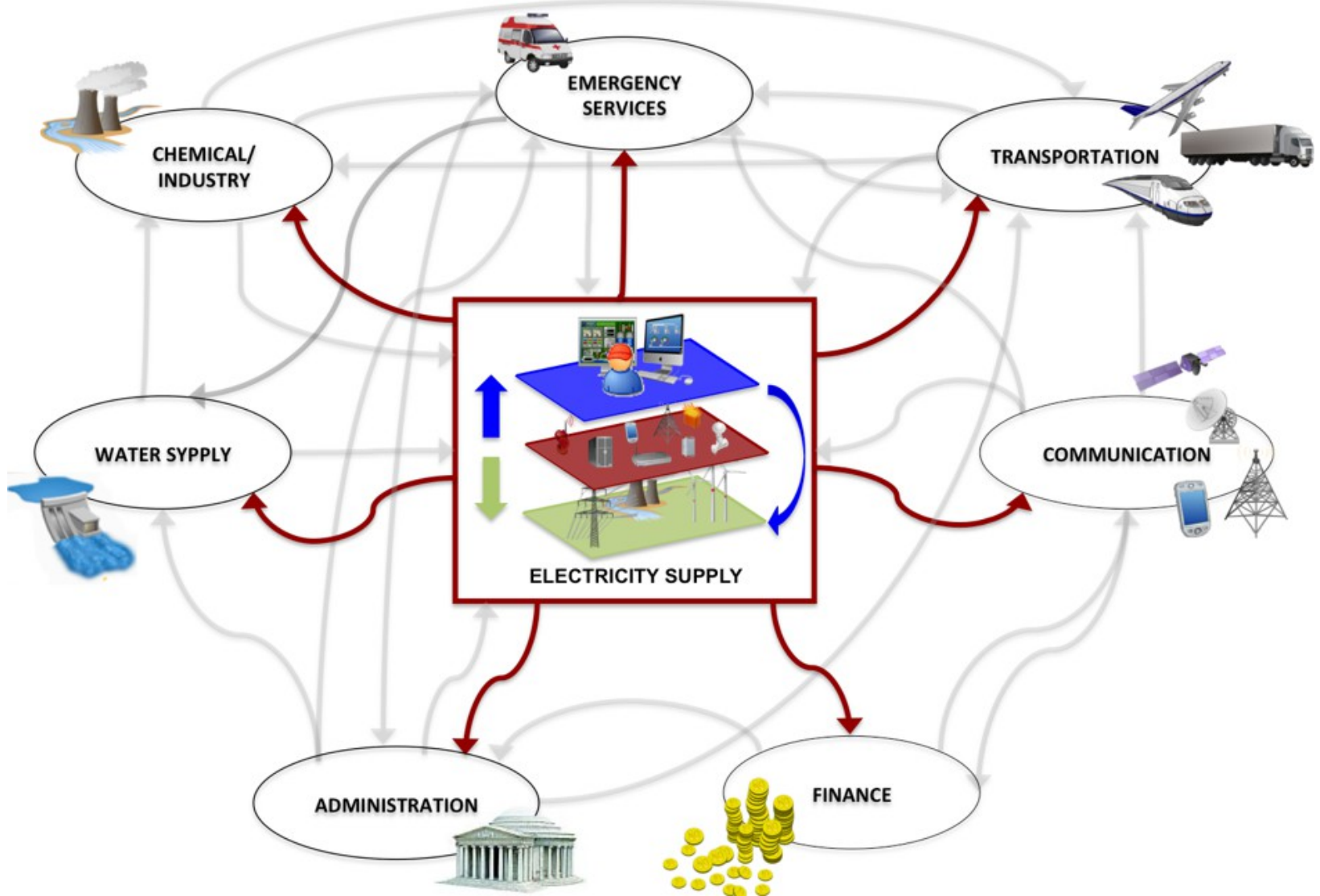


"Una red eléctrica renovada, a la que se ha añadido comunicación de dos sentidos, una de los sistemas de monitorización (del proveedor) y otra (la medición inteligente) del consumidor"

"Las redes eléctricas que puedan integrar de manera eficiente el comportamiento y las acciones de todos los usuarios conectados a ella - generadores, consumidores y aquellos que hacen ambas cosas - con el fin de garantizar un sistema de energía sostenible económicamente, eficiente con bajas pérdidas, de alta calidad y seguridad en el suministro."



INTERDEPENDENCIA EN INFRAESTRUCTURAS





Visión del Riesgo de CiberSeguridad en SG

Project Basecamp

ZDNet
20th Anniversary

US Edition

News & Blogs | Reviews | Downloads | Small Business

Companies | Hardware | Software | Mobile | Security

Shodan search exposes insecure SCADA systems

By Ryan Naraine | November 2, 2010, 7:44am PDT

Summary: Hackers are using the Shodan computer search engine to find Internet-facing SC systems using potentially insecure mechanisms for authentication and authorization.

MADE IN

Stuxnet

U.S.A.

Project Robus: Master Serial Killer

- Objetivo: Análisis de la Implementación de Protocolos Industriales (el primero: DNP3)
- DNP3: 17 advisories, 28 tickets reportados
- Técnicas de Fuzzing
- Todos los dispositivos analizados son vulnerables: solo 2 ok!

Firmware	!	X	!	!	!
Ladder Logic	!	!	X	!	X
Backdoors	!	X	X	✓	✓
	X	X	X	!	!
	!	X	N/A	N/A	X
	!	!	X	!	!
	✓	✓	X	✓	✓
Undoc Features	!	X	X	!	!



Pero qué han hecho otros??



The Department of Energy plays a key role in protecting the critical energy infrastructure of the nation as specified in the **National Strategy for Homeland Security**.

In fulfilling this responsibility, the Secretary of Energy's Office of Independent Oversight and Performance Assurance has conducted a number of assessments of organizations **with SCADA networks to develop an in-depth understanding of SCADA networks and steps necessary to secure these networks**.

www.ea.doe.gov/pdfs/21stepsbooklet.pdf



Pero qué han hecho otros??



Homeland Security Presidential Directive 7 establishes a national policy for Federal departments and agencies to identify and prioritize critical infrastructure and to protect them from terrorist attacks. The directive defines relevant terms and delivers 31 policy statements. These policy statements define what the directive covers and the roles various federal, state, and local agencies will play in carrying it out.

www.dhs.gov/critical-infrastructure-sectors



Pero qué han hecho otros??

**Cyber Security
Procurement
for Control
Version 1.5
Draft**

November 2006

Cyber Assessment Methods for SCADA Security

May Robin Permann
Staff
Information & Communications Systems
Idaho National Laboratory
Idaho Falls, ID 83415

Kenneth R
Computer
Cyber Sec
Idaho Nat
Idaho Fal

KEYWORDS

Supervisory Control and Data Acquisition, SCADA, Cyber S

ABSTRACT

The terrorist attacks of September 11, 2001 brought to light the vulnerabilities of critical infrastructure in the United States. In response, the U.S. Government is directing the development of programs to implement the National Infrastructure Protection Plan. One part of this effort involves assessing Supervisory Control and Data Acquisition (SCADA) systems. These systems are essential to the control of critical elements of the nation's infrastructure, such as electric power, oil, and gas production and distribution. Such systems are also essential to the defense and economic security of the United States. One of the objectives of this program is to identify vulnerabilities and weaknesses in SCADA systems and work together to design secure control systems that resolve these vulnerabilities.

This paper describes vulnerability assessment methodology and activities designed to identify and resolve vulnerabilities in SCADA systems of critical infrastructure.

INTRODUCTION

The National SCADA Test Bed (NSTB) program is sponsored by the Department of Energy (DOE) and the Department of Electricity and Energy Assurance (DOE-OE) to improve the security of the electric power sector. The Idaho National Laboratory (INL) SCADA Test Bed is conducting various SCADA system configurations. NSTB work includes vulnerability assessment and mitigation, standards development, and new security assessment tools. Information obtained from this program will be used by and/or industry in order to enhance security by helping them protect their own systems against external and internal cyber threats.

Copyright 2005 by ISA - The Instrumentation and Control Society
Presented at 15th Annual Joint ISA POWTECH Conference
<http://www.isa.org>

INL/EXT-05-00993

Common Control System Vulnerability

November 2005

Prepared by Idaho National Laboratory

INL
Idaho National Laboratory

Homeland Security

Control Systems Security Center



Cíber-resiliencia es
Anticipar, resistir,
recuperar y evolucionar

Miguel Rego
Director de @INTECO
En #securmatica



Por donde empezar en infraestructuras críticas:

- ✓ *Definir una estrategia de defensa conjunta*
- ✓ *Definir una estrategia de respuesta conjunta.*
- ✓ *Definir herramientas, controles y métricas regionales*
- ✓ *Definir una estrategia de comunicación alternativa ante un incidente.*
- ✓ *Estudiar, analizar y crear protocolos de comunicación y herramientas de gestión.*



Qué hacer?

Ser Práctico



Qué hacer? → No perder tiempo en lo obvio





Qué hacer? → Diseñar solidamente





Qué hacer? → Mantener el ritmo





Muchas Gracias.

Claudio B. Caracciolo

*CSA en Eleven Paths
Coordinador del CCI en Argentina
Presidente de ISSA Argentina*

*Claudio.caracciolo@ar.cci-es.org
@holesec
www.cci-es.org*