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

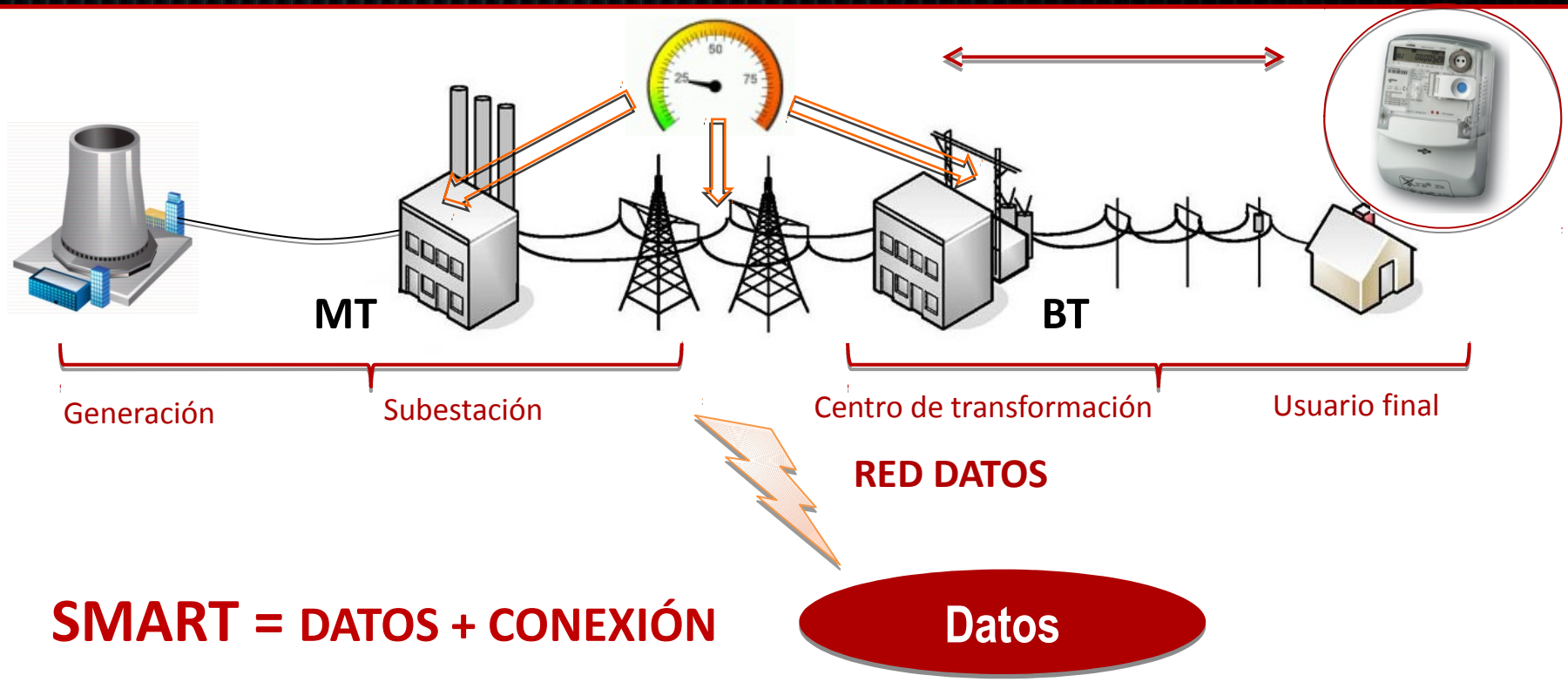
"Ciberseguridad Industrial es el conjunto de prácticas, procesos y tecnologías, diseñadas para gestionar el riesgo del ciberespacio derivado del uso, procesamiento, almacenamiento y transmisión de información utilizada en las organizaciones e infraestructuras industriales, utilizando las perspectivas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

Personas inteligentes

Personas con malas intenciones

Conocer, medir, decidir…

Entendiendo la importancia de SG

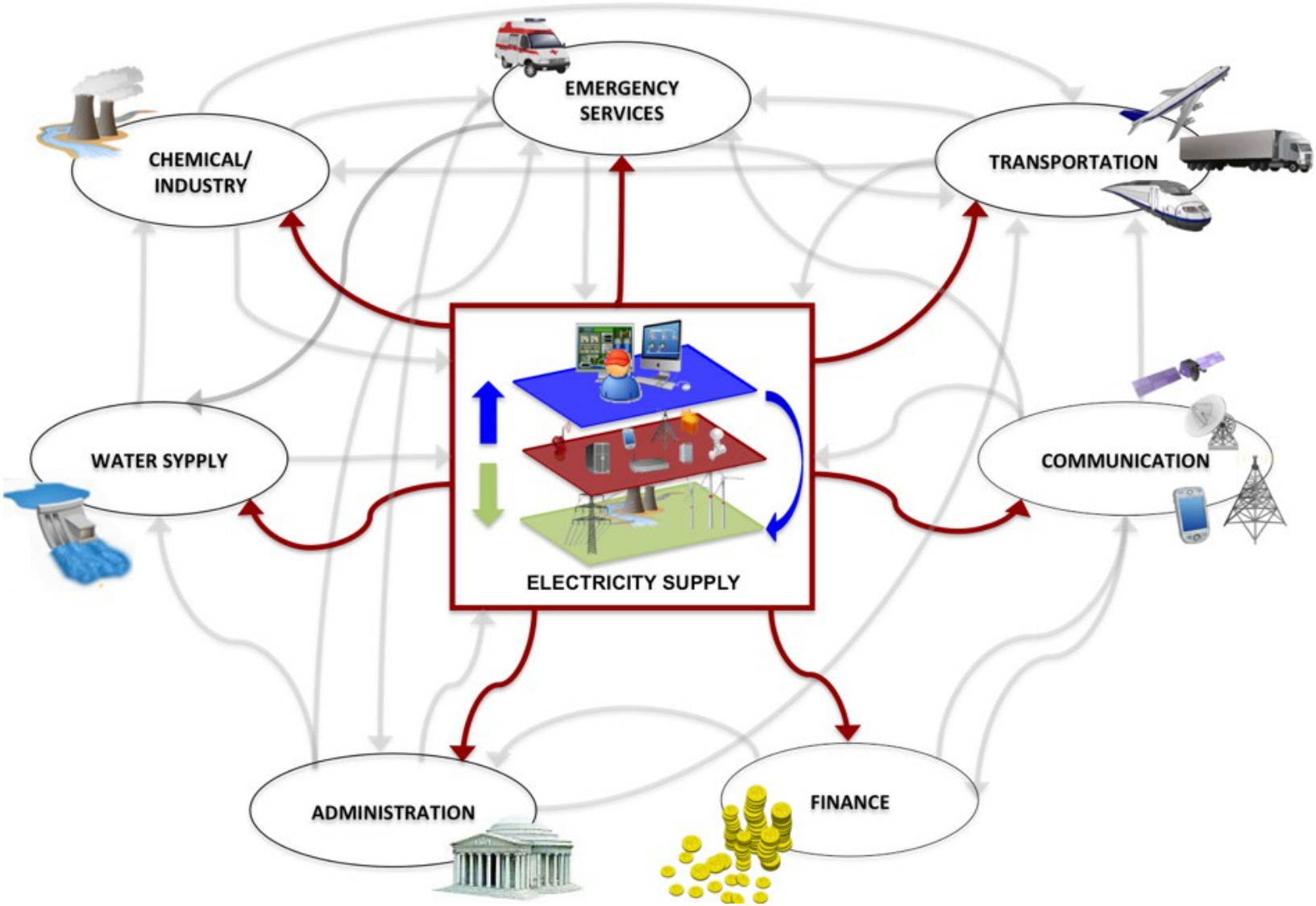


SMART = DATOS + CONEXIÓN

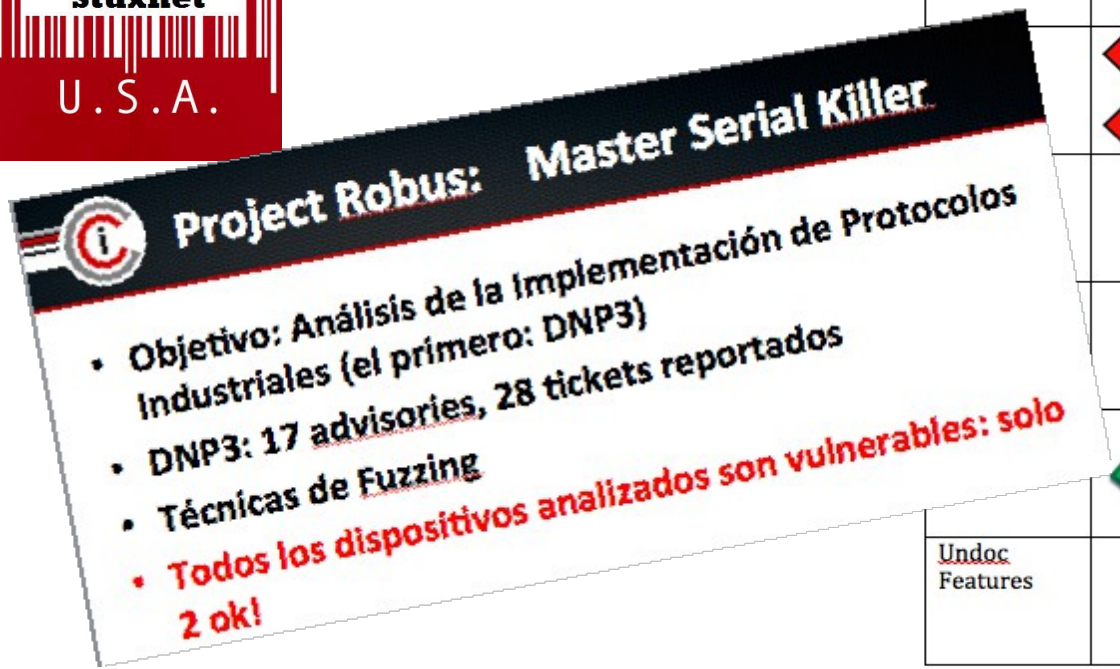
"Una red eléctrica renovada, a la que se ha añadido comunicación de dos sentidos, una de los sistemas de monitorización (del proveedor) y otra (la medición inteligente) del consumidor"

“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

	A-B QUALITY	Schneider Electric	GE	SEL	Koyo
Firmware	!	✗	!	!	!
Ladder Logic	!	!	✗	!	✗
Backdoors	!	✗	✗	✓	✓
	✗	✗	✗	!	!
	!	✗	N/A	N/A	✗
	!	!	✗	!	!
	✓	✓	✗	✓	✓
Undoc Features	!	✗	✗	!	!

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 Secur
Procuremer
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
United States. In response, the U.S. Government is directin
infrastructure by creating programs to implement the Natio
part of this effort involves assessing Supervisory Control a
These systems are essential to the control of critical eleme
electric power, oil, and gas production and distribution. S
have a debilitating impact on the defense or economic sec
objectives of this program is to identify vulnerabilities an
work together to design secure control systems that resol

This paper describes vulnerability assessment methodolo
activities designed to identify and resolve vulnerabilities
critical infrastructure.

INTRODUCTION

The National SCADA Test Bed (NSTB) program is sp
of Electricity and Energy Assurance (DOE-OE) to in
sector. The Idaho National Laboratory (INL) SCADA
various SCADA system configurations. NSTB work
vulnerability assessment and mitigation, standards d
new security assessment tools. Information obtaine
and/or industry in order to enhance security by help
their own systems against external and internal cyb

Presented at 15th Annual Joint ISA POWI
http://

Resiliencia

Ciber-resiliencia es
Anticipar, resistir,
recuperar y evolucionar

Miguel Rego
Director de @INTECO
En #securmatica

Herramientas técnico – legales

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.

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