ISEC Labs #9

Seguridad en Sistemas SCADA e Infraestructuras Críticas

Javier Moreno y Daniel Fernández
jmoreno<arroba>isecauditors.com
dfernandez<arroba>isecauditors.com

1. Resumen

En este nuevo ISecLab se pretende comentar el problema de la seguridad en los sistemas SCADA que actualmente están gestionando infraestructuras críticas. Se hace un repaso de las principales características de estos sistemas, mayoritariamente industriales, así como de su arquitectura. Posteriormente se introduce el concepto de infraestructura crítica y se describe el tratamiento que a estos activos están dando tanto la Unión Europea como la administración pública española. Se hace especial hincapié en el hecho de que los sistemas SCADA están manejando gran parte de las infraestructuras críticas nacionales. Finalmente, se desglosan las principales vulnerabilidades que afectan a estos sistemas y, por ende, a la gestión de las infraestructuras críticas que cuentan con este tipo de componentes de control.

2. ¿Qué son los Sistemas SCADA?

2.1 Definición

Un sistema SCADA (Supervisory Control and Data Acquisition) es un sistema de control de procesos industriales. Los procesos que son controlados por sistemas SCADA pueden ser de tres tipos:

- Industriales: Fabricación, producción, generación de energía....
- Basados en Infraestructuras: Tratamiento de aguas, transporte de gas,...
- Basados en Instalaciones: Aeropuertos, barcos, trenes, edificios,...

De esta forma, actualmente existen multitud de sistemas SCADA que controlan y monitorizan procesos de vital importancia para el desarrollo cotidiano de la vida de las personas: sistemas SCADA controlan las aperturas de las presas, sistemas SCADA controlan centrales nucleares, sistemas SCADA controlan la producción y distribución de la electricidad y el gas, sistemas SCADA controlan aviones y trenes, etc. Es decir, son de uso tan masivo como en este mismo párrafo.

Los sistemas SCADA monitorizan el estado de las infraestructuras para controlar que sus parámetros de funcionamiento están dentro de los límites aceptables y, de no ser así, envían señales para modificar la configuración de los mismos y corregir su funcionamiento.

2.2 Arquitectura de los sistemas SCADA

La arquitectura básica de un sistema SCADA se basa en los siguientes elementos:

- **Human Machine Interface (HMI)**: es el sistema encargado de presentar la información procesada al operador humano. Este operador es el que controla y monitoriza los procesos.
- **Master Terminal Unit (MTI):** es el sistema encargado de adquirir la información de los procesos industriales que controla el sistema SCADA así como de enviar comandos de control a esos mismos procesos. Tratamiento de aguas, transporte de gas,...
- **Infraestructura de Comunicaciones**: encargada de conectar la MTU con los controladores remotos. La comunicación puede producirse a través de multitud de medios: Internet, teléfono, radio, cable, wifi, etc.
- **Remote Terminal Unit (MTI):** envían las señales de control a los dispositivos controlados por el sistema SCADA y adquieren los datos de estos dispositivos para transferirlos a la MTU. En algunos sistemas, en vez de RTU, se usan PLC (Programmable Logic Controllers).

En la Figura 1 se muestra un ejemplo de arquitectura de un sistema SCADA controlando y monitorizando tres elementos:

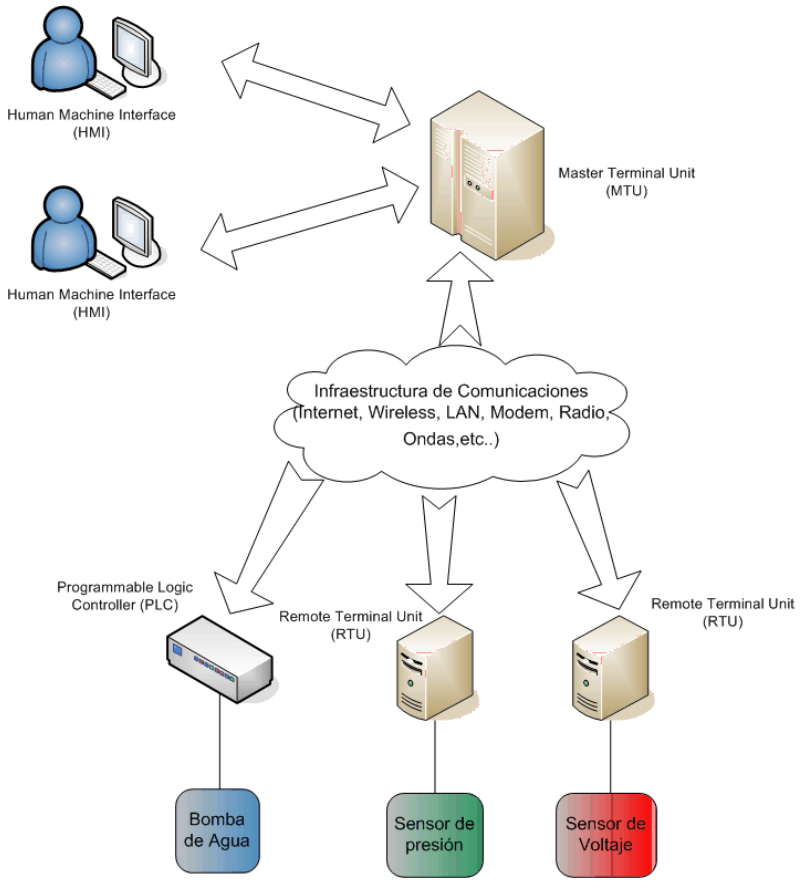

Figura 1 – Arquitectura de un Sistema SCADA

2.3 Evolución de los Sistemas SCADA

Cuando los sistemas SCADA aparecieron el entorno tecnológico era mucho más limitado que el que existe hoy en día sin embargo, actualmente, se está produciendo una convergencia entre los sistemas clásicos de control industrial y las nuevas tecnologías de información. Esta convergencia tiene por objetivo mejorar la eficiencia, el mantenimiento y la capacidad de procesamiento de los sistemas de control industriales.

En resumen, se puede afirmar que se están mezclando dos culturas:

- Tecnologías de la Información
- Control de sistemas industriales

En la Figura 2 se muestra un resumen de las principales diferencias entre los sistemas SCADA en el pasado y en la actualidad:

	Pasado	*Actual*
Sistema Operativo	Propietarios	Abiertos
Comunicaciones	Protocolos propietarios	Protocolos estándar
Flujo de información	Segmentados	Integrados
Soluciones HW/SW	Monolíticos	Modulares
Arquitecturas	Cerradas	Abiertas

Figura 2 – Evolución de los sistemas SCADA

Esto supone que, por ejemplo, los sistemas de control industriales implementan o soportan protocolos como TCP/IP en vez de por protocolos propietarios o que también se estén incorporando en redes WiFi o redes cableadas LAN en sustitución de las redes de comunicación dedicadas que se utilizaban anteriormente. Del mismo modo, ordenadores de propósito general empiezan a gestionar los elementos clásicos de control industrial (HMI, MTU, RTU, PLC,...) que cohabitan en las redes con infraestructuras tecnológicas abiertas como bases de datos, servidores de correo, servidores web, o hasta sistemas de escritorio basados en Windows y Linux.

3. ¿Qué una Infraestructura Crítica?

Para entender la relación entre los sistemas SCADA y lo que se incluye dentro del concepto de Infraestructura Crítica, a la que tanta importancia parece que se le ha dado, es necesario entender cuál es el marco legislativo que define, primero, cuándo una infraestructura es crítica y, segundo, que implica esa clasificación.

Esto se pretende llevar a cabo mediante la regulación legislativa y mediante la creación de organismos, en su mayoría gubernamentales, que monitoricen o hasta aseguren, el cumplimiento de dicha legislación.

3.1 Legislación y definición

Desde el año 2004 la Unión Europea ha venido trabajando en distintas resoluciones y comunicaciones relativas a la protección de infraestructuras críticas. Este esfuerzo ha dado como resultado la creación y aprobación del Programa Europeo para la Protección de Infraestructuras Críticas [1]

La primera conclusión de este programa es la unificación de la definición de infraestructura crítica:

"*Infraestructura crítica: instalaciones, equipos físicos y de tecnología de la información, redes, servicios y activos cuya interrupción o destrucción pueden tener grandes repercusiones en la salud, la seguridad o el bienestar económico de los ciudadanos o en el funcionamiento de los gobiernos de los Estados miembros*"

La otra gran conclusión de ese programa es que desde la Unión Europea se insta a los estados miembros a abordar, de forma nacional, la protección de las Infraestructuras Críticas.

A raíz de esta petición del Unión Europea, el gobierno español, en mayo de 2007, aprobó el Plan Nacional de Protección de Infraestructuras Críticas. Una vez aprobado dicho plan, en noviembre de 2007 se crea el Centro Nacional de Protección de Infraestructuras Críticas (en adelante CNPIC, [2]).

3.2 ¿Qué es y qué hace el CNPIC?

El CNPIC es el organismo responsable de la dirección, coordinación y supervisión de la protección de infraestructuras críticas nacionales. Este organismo depende de la Secretaría de Estado de Seguridad dentro del Ministerio del Interior.

El CNPIC tiene entre algunos de sus principales cometidos la custodia, el mantenimiento y la actualización del Plan de Seguridad de las Infraestructuras Críticas nacionales pero otros cometidos del CNPIC son los siguientes:

- Valoración de la amenaza y análisis de riesgos sobre instalaciones estratégicas.
- Establecimiento de mecanismos de información, comunicación y alerta.
- Punto Nacional de Contacto, en el marco de la Protección de Infraestructuras Críticas de la Unión Europea.
- Supervisar y coordinar los planes sectoriales de protección de infraestructuras.
- Elaborar protocolos de Colaboración entre organismos públicos y privados.

3.3 Catálogo de Infraestructuras Críticas

La Unión Europea, mediante la directiva 2008/114 [3] del 8 de Diciembre de 2008, establece que la responsabilidad de la identificación y designación de Infraestructuras Críticas corresponde a cada uno de los estados miembros.

Por este motivo el CNPIC ha recopilado, en el Catalogo de Infraestructuras Estratégicas [4], las principales infraestructuras estratégicas de España. Esta información se encuentra clasificada y está custodiada por el CNPIC.

El Plan Nacional de Infraestructuras Críticas contempla la inclusión de las infraestructuras críticas en doce sectores:

- Administración
- Alimentación
- Energía
- Espacio
- Sistema Financiero y Tributario
- Agua
- Industria Nuclear
- Industria Química
- Instalaciones de Investigación
- Salud
- Tecnologías de Transporte
- Transporte

3.4 Borrador del Real Decreto

También a raíz de la directiva europea 2008/114 el gobierno está preparando un Real Decreto que establezca las normas para la protección de las Infraestructuras Críticas nacionales.

Actualmente existe un borrador de este futuro Real Decreto (publicado el 31 de marzo de 2010) [5] al que hasta hace pocos días se podían hacer observaciones y comentarios.

El objetivo del Real Decreto es doble:

- Dirigir y coordinar las actuaciones de los distintos órganos de las Administraciones Públicas en materia de protección de infraestructuras críticas.
- Regular las obligaciones que deben asumir los operadores de las Infraestructuras Críticas ya sean estos públicos o privados.

El Real Decreto define como operador crítico a toda aquella entidad (pública o privada) que gestiona alguna infraestructura que haya sido clasificada como crítica. Los operadores deberán colaborar con el CNPIC en la protección de las Infraestructuras Críticas cuya gestión sea de su responsabilidad para lo cual deben:

- Elaborar un Plan de Seguridad de Operador
- Elaborar un Plan de Protección Específico para cada una de las infraestructuras críticas que gestionen.
- Seleccionar un enlace entre el CNPIC y el operador crítico.

El gobierno se ha dado cuenta de que la mayoría de las Infraestructuras Críticas nacionales están en manos de empresas privadas y por esa razón este Real Decreto viene a formalizar la colaboración que debe existir entre la Administración y las entidades privadas de cara a proteger Infraestructuras Críticas a nivel nacional.

4. Vulnerabilidades de los Sistemas SCADA

En el diseño inicial de los sistemas SCADA, el objetivo era crear un sistema de control y monitorización que tuviera muy alto rendimiento y fuera sencillo de manejar; la seguridad no era un requisito esencial.

En los últimos años, los sistemas SCADA han evolucionado desde el uso de software y hardware propietario y un diseño aislado, en la década de los 70, a sistemas que incluyen ordenadores de propósito general, comunicaciones basadas en protocolos abiertos y acceso desde Internet. Esto ha hecho que las amenazas y vulnerabilidades de estos sistemas se hayan incrementado además por su integración en las redes corporativas.

Los dos puntos anteriores unidos al hecho de que las principales infraestructuras críticas del país están controladas por sistemas de este tipo hacen que sea esencial analizar y evaluar su seguridad y, por ende, la de las infraestructuras críticas donde están siendo utilizados, con un punto de vista muy similar al que se trata habitualmente la Seguridad en Tecnologías de Información.

Las principales vulnerabilidades de los sistemas SCADA serán las siguientes se pueden agrupar en los siguientes tipos:

4.1 Deficiencias en la Arquitectura de Red

Estas vulnerabilidades tienen su origen en el hecho de que los sistemas SCADA fueron inicialmente diseñados como sistemas aislados. Ahora esto ha cambiado y los sistemas industriales están interconectados con redes corporativas e incluso con Internet. Los factores más importantes que afectan a la seguridad son [6] [7] [8] [9]:

1. Interconexiones

   Cuantas más interconexiones tengan el sistema más expuesto está y, por tanto, más vulnerable es. Las redes corporativas y las industriales están cada día más interconectadas lo que hace que, por ejemplo, un vulnerabilidad en un servidor de base de datos o un servidor web en la misma red pueda ser explotado permitiendo un escalado a una RTU que controla la apertura de una presa o al panel de control de un sistema de una central eléctrica.

2. Protocolos abiertos

   La seguridad de los sistemas SCADA ha estado durante muchos años basada en la ocultación que el uso de protocolos propietarios proporciona según la premisa de security by obscurity. Sin embargo, el uso de protocolos abiertos en los sistemas de control conlleva asumir una serie de riesgos que deben ser mitigados con medidas correctivas aplicadas a todos los niveles y dado que los SCADA no han sufrido esa adaptación a los riesgos de estos protocolos a medida que se implementaban en sus comunicaciones, el resultado es que existen multitud de sistemas de control industrial que están utilizando protocolos abiertos sin la securización adecuada.

3. Accesos remotos

   Habitualmente los sistemas industriales se encuentran en localizaciones remotas. Sirva como ejemplo un centro de control ferroviario que controla los cambios de vía y cruces de los trenes. El HMI y la MTU normalmente están ubicados en el centro de proceso de datos de la estación, mientras que las RTUs (o PLCs) y los sensores correspondientes se pueden encontrar a kilómetros de distancia realizándose el control de los dispositivos de forma remota. Esta cultura del acceso remoto en sistemas SCADA ha hecho que al adaptar los sistemas industriales a los sistemas tecnológicos actuales estos incluyan multitud de accesos remotos antes inexistentes añadiendo nuevas formas de acceso al propio sistema de control.

4. Redes inalámbricas

   Íntimamente relacionado con el punto anterior está el problema de las redes inalámbricas que se despliegan en entornos industriales. Estas redes solucionan de una forma barata y eficiente el problema de movilidad y despliegue de infraestructuras que suele existir en eso entornos, como por ejemplo en naves industriales de almacenamiento donde se colocan decenas de APs para que los operarios a través de dispositivos portátiles puedan realizar las búsquedas de los pedidos de forma rápida. Estas redes WiFi pueden incluso carecer de autenticación o de cifrado de datos entre cliente y punto de acceso o implementar tecnologías vulnerables lo que hace añade un gran factor de riesgo para la seguridad.

5. Uso de sistemas de seguridad

La adopción de tecnologías de información de usos común (sistemas Windows, Ethernet, Internet, etc...) está sucediendo a todo velocidad en el mundo de los sistemas SCADA. Sin embargo esta convergencia no está siendo tan rápida en lo que a sistemas de seguridad se trata. Muchas redes industriales se conectan a redes corporativas usando firewalls de forma muy permisiva como no separando zonas de red o no controlando correctamente el tráfico entre ellas. En muchos casos el uso de IDS/IPS se reserva exclusivamente a las redes de servidores y no se emplean en las redes de sistemas industriales (por dispersión, complejidad u otras razones). La gestión de logs que permitiría entre otras cosas analizar las causas en caso de incidentes de seguridad, no se incorporan a las redes industriales debido a la imposibilidad de trabajar con protocolos propietarios o al coste del desarrollo agentes o, incluso, a la imposibilidad de capturar registros de estos sistemas sea o no de forma normalizada.

4.2 Vulnerabilidades a nivel de Software y Hardware

Las vulnerabilidades a nivel de sistema base aparecen por la adopción de sistemas de propósito general (aplicaciones y sistemas operativos) por parte de los sistemas SCADA.

1. Vulnerabilidad en Sistemas Operativos y Aplicaciones

La adopción por parte de los sistemas SCADA de Sistemas Operativos de propósito general o aplicaciones comerciales comunes implica heredar las vulnerabilidades de este software. Periódicamente aparecen diferentes vulnerabilidades sobre software que en los sistemas operativos o servicios de red, muchas veces, son muy fáciles de solventar: simplemente se ha de descargar el parche correspondiente de la web del fabricante e instalarlo en el servidor pertinente. El problema aparece por que en los sistemas industriales puede no ser tan sencilla esta corrección por las implicaciones que tiene realizar paradas, reinicios, o cambios en el sistema que podrán afectar a los sistemas que tienen en el tiempo real una componente crítica. Otro punto de vital importancia es que un fallo en la actualización de un sistema SCADA o un reinicio no previsto puede poner en peligro incluso vidas humanas algo de lo que normalmente los sistemas de propósito general no son responsables.

2. Parcheado defectuoso y securización complicada

En línea con el punto anterior, el parcheado de los equipos SCADA es una tarea ardua ya que históricamente estos equipos no han tenido una política de actualización rígida por lo que en algunos casos pueden llevar años sin actualizarse. La securización de sistemas SCADA también es complicada ya que en la mayoría de los casos requiere la colaboración de los fabricantes que no suelen estar dispuestos que sus equipos pierdan ciclos de procesamiento en virtud de una mayor seguridad. Los sistemas industriales son muy estrictos en la gestión de ventanas de mantenimiento: una parada para actualizar o para securizar un sistema puede provocar daños irreparables en infraestructuras críticas o perdidas monetarias importantes debido a solo unas horas de parada de control o de la producción.

3. Cifrado

Los sistemas SCADA, debido al falso sentido de invulnerabilidad que les ha perseguido siempre, han apartado de sus procesos mecanismos básicos de seguridad que en otros entornos serían elementales: si los sistemas estaban completamente aislados y nadie del exterior podía acceder a ellos, ¿qué necesidad había de cifrar la información? Esa premisa se ha ido heredando hasta los tiempos actuales donde los sistemas SCADA están conectados a redes corporativas y a Internet dónde la información se transmite por canales abiertos y es necesario protegerla, tanto por su sensibilidad en caso de captura como, más importante, por la posibilidad de que fuera alterada implicando, por ejemplo un cambio erróneo en un proceso industrial.

4. Dificultad en la realización de análisis de vulnerabilidades

La realización de análisis de vulnerabilidades se convierte en una tarea complicada o casi imposible en en entornos SCADA, tanto estas acciones como los test de intrusión deben ser realizadas con sumo cuidado sobre estos sistemas, ya que, se podría provocar un fallo de funcionamiento o incluso una denegación de servicio que podría ser catastrófica dependiendo de la infraestructura que ese sistemas SCADA este gestionando o monitorizando.

4.3 Seguridad Física

Como se ha comentado en puntos anteriores, los sistemas SCADA suelen encontrarse distribuidos a través de grandes distancias la mayoría de las veces, en localizaciones físicamente inseguras.

La seguridad física tradicional se vuelve de vital importancia a la hora de asegurar entornos o sistemas industriales debido a que muchas de sus instalaciones pueden estar situadas en sitios remotos y aislados donde un robo o intrusión podría realizarse sin despertar la sospecha de nadie o, incluso generando alertar cuya atención in-situ podría implicar un largo espacio de tiempo. Instalar controles de acceso disuasorios (señales y carteles), preventivos (cerrojos, candados y tornos de acceso) y detectores (CCTV o sensores de presencia) es fundamental en este tipo de instalaciones, y garantizar un pronta respuesta en caso necesario, es fundamental.

Los fallos en infraestructuras críticas a menudo implican peligros que se traducen en pérdidas de vidas humanas. Para evitar estas pérdidas, se deben diseñas los planes de evacuación necesarios para cada tipo de infraestructura.

Por último hay que reducir al máximo las vulnerabilidades producidas por amenazas a la seguridad física de las instalaciones donde se encuentran los sistemas SCADA. De este modo se debe estar protegido ante incendios, inundaciones, temperaturas extremas o toxinas así como ante cortes eléctricos o fallos estructurales. Históricamente este tipo de amenazas sí que se han tenido en cuenta en los sistemas SCADA por lo que se suelen requerir grandes implantaciones.

4.4 Cultura de seguridad y formación

Las vulnerabilidades encuadradas en este apartado están relacionadas con el hecho de que las personas que habitualmente tienen la responsabilidad de gestión y/o uso de los sistemas SCADA no están acostumbradas a trabajar en un entorno de TIC de propósito general y mucho menos en un entorno bajo una cultura de Seguridad TIC. Los conflictos entre los departamentos de ingeniería (o de producción) y los departamentos informáticos (o de sistemas) son más habituales de lo que debieran detectándose dos puntos de fricción habitual.

1. Autenticación

   Es muy común en sistemas SCADA usar contraseñas compartidas o incluso emplear un único usuario compartido entre todos los operadores. Este hecho que facilita la operatividad del día a día a los usuarios elimina un correcto procedimiento de autenticación y la capacidad de auditoría sobre las acciones de los usuarios asociadas a personas de forma nominal. Tampoco se suelen contemplar políticas de expiración de contraseñas ni de longitud mínima con lo que la problemática empeora. En entornos industriales implantar un doble factor de autenticación basado en biometría está limitado por las condiciones de trabajo como por ejemplo el uso de gafas de seguridad que impide los escáneres de retina y de iris o la suciedad en las manos que inhabilita el uso de lectores de huellas dactilares.

2. Experiencia y formación de la plantilla

   Los entornos industriales controlados por sistemas SCADA han evolucionado a una velocidad muchas veces mayor que la formación de los responsables de estos sistemas que pueden tener la sensación que son invulnerables, que a nadie le interesa la información que manejan y que la seguridad es únicamente una ralentización del proceso de producción industrial.

5. Conclusiones

Los sistemas SCADA, sistemas de control y monitorización de procesos industriales, fueron diseñados en su momento partiendo de protocolos propietarios y para funcionar en entorno aislados. La convergencia de los departamentos de TIC y de producción y la rápida evolución de las tecnologías de información han hecho que los sistemas SCADA adopten como suyas tecnologías de uso corriente como Internet, TCP/IP o Sistemas Operativos de propósito general. Además de asumir sus ventajas (procesamiento, facilidad de uso, reducción de costes, etc.) han asumido también sus vulnerabilidades y amenazas.

Las vulnerabilidades de las que adolecen los sistemas SCADA que gestionan infraestructuras críticas son debidas, en algunos casos, al diseño de seguridad empleado en su concepción o a que estos no fueron pensados para utilizarse en conjunción de tecnologías de propósito general.

La sociedad actual no sería tal y como hoy en día la conocemos sino fuera por el correcto funcionamiento de ciertas infraestructuras denominadas críticas: plantas eléctricas, medios de transportes, presas, telecomunicaciones y hospitales - entre otros - hacen que los ciudadanos de nuestro país disfruten de un bienestar confía en el correcto funcionamiento de sistemas automatizados de incalculable importancia y criticidad.

Las autoridades europeas y nacionales le han dado más importancia al riesgo que supondría un ataque sobre estas infraestructuras críticas y han hecho un esfuerzo en la regulación armonizada de su protección. Los gobiernos son los responsables de gestionar las obligaciones de los operadores de las infraestructuras críticas, ya sean estos públicos o privados, mediante la legislación que garantice la realización planes de protección y securización de las infraestructuras que estos gestionan y ser más conscientes de las responsabilidades (ya conocidas) que estos tienen.

Sin duda, los esfuerzos que están realizando los gobiernos, como el español, mediante la creación y potenciación de organismos como el CNPIC demuestra que las infraestructuras críticas han pasado a ser formalmente consideradas como tal y regularse formalmente bajo este criterio y los gestores de éstas tendrán que realizar mayores esfuerzos para alcanzar los niveles de seguridad regulatorios.

6. Referencias

[1] http://europa.eu/legislation_summaries/justice_freedom_security/fight_ag...

[2] Centro Nacional de Protección de Infraestructuras Críticas http://www.cnpic-es.es/

[3] Directiva 2008/114/CE del Consejo Europeo. Accesible en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075...

[4] Definición del Catálogo de Infraestructuras Críticas por el CNPIC. Accesible en: http://www.cnpic-es.es/cnpic/index.php?option=com_content&view=article&i...

[5] Borrador del Real Decreto para la protección de Infraestructuras Críticas. Accesible en: http://www.cnpic-es.es/cnpic/images/realdecreto/proyecto%20rdpic.pdf

[6] "21 Steps to Improve Cyber Security of SCADA Networks", Department of Energy of United States of América. Accesible en: http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf

[7] Wikipedia: http://en.wikipedia.org/wiki/SCADA

[8] "Securing SCADA Systems", Ronald L. Krutz, PhD, WILEY 2006.

[9] "Security for Critical Infrastructure SCADA Systems" SANS Institute. Accesible en: http://www.sans.org/reading_room/whitepapers/warfare/security-critical-i...

[10] "Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control", National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce (2002)