

Cybersituational Awareness - Appunti

Francesco Lorenzoni

Febrero 2025

Contents

I 20 Conceptos	5
1 20 conceptos más relevantes	7
1.1 Fundamentos de la Ciberconciencia Situacional	7
1.2 Componentes estructurales de la CS	8
1.3 Colaboración y visualización en CS	8
1.4 Análisis y gestión de riesgos	9
1.5 Herramientas y tecnologías para la CS	9
1.6 Dominios físicos y cibernéticos	10
1.7 Ciberinteligencia para mejorar la CS	10
II Introducción to CS	13
2 Ciberconciencia Situacional	17
2.1 Introducción	17
2.2 Conciencia Situacional	17
2.2.1 Situation Understanding	18
2.2.2 Situational Awareness in Cyberspace	18
2.3 Ciberconciencia situacional	19
2.3.1 Vulnerabilidades	19
2.3.2 Amenazas - Threats	19
3 Cyber Intelligence Visualization	23
3.1 Visualization Charts	23
3.1.1 Georeferenced visualizations and IP-Port mapping	23
4 Sources of Intelligence	27
4.1 Herramientas de Ciberconciencia Situacional	27
4.1.1 Objetivos principales	27
4.1.2 Diferenciación con otras herramientas	27
4.1.3 Capacidades clave	27
4.1.4 Requisitos operacionales	27
4.2 Connection of Cyber Sensors	28
4.3 SIEM	29
4.4 Incident Response Systems	29
5 Hybrid Situational Awareness	31
5.1 Introducción	31
III Sistemas Ciberfísicos	33
6 Cyber-Physical Systems	37
6.1 Introducción	37
6.2 Componenentes de CPSs	37
6.2.0.1 Industrial Control Systems	37
6.3 Vulnerabilidades	38
6.3.1 Vulnerabilidades más comunes	39
6.4 Vulnerabilities Assessment	39
6.4.1 Intrusion detection	40
6.4.2 Exploits mitigación	40

7 ICS Cyberdefense	41
7.1 ICS Security Architecture	41
7.1.1 Defense-in-depth	41
7.1.2 Network Segmentation and segregation	42
7.1.3 Firewalling	43
7.2 ICT Risk Assessment and Analysis	43
7.3 Security Control Implementation	44
7.3.1 Identificación y Autenticación	44

Part I

20 Conceptos

Chapter 1

20 conceptos más relevantes

1.1 Fundamentos de la Ciberconciencia Situacional

1. Ciberconciencia Situacional (CS)

La conciencia situacional en el ciberespacio es el concepto fundamental definido como “*la capacidad de saber lo que está sucediendo en el ciberespacio*”. Es esencial porque constituye la base para comprender y reaccionar a las amenazas ciberneticas de manera oportuna y eficaz. Además, la CS no solo es relevante para la detección de amenazas, sino también para la optimización de recursos de seguridad, permitiendo priorizar esfuerzos donde realmente se necesitan y evitar la fatiga de alertas que afecta a muchos equipos de seguridad.

Definition 1.1 (Situational Awareness) *Situational awareness is the perception of the elements of the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future*

2. Ciclo cognitivo de la CS

El ciclo de la CS se compone de adquisición de datos, procesamiento, análisis, distribución y acción. Este ciclo continuo es fundamental porque representa el flujo completo de información desde su captación inicial hasta la toma de decisiones basada en ella, garantizando que la CS sea un proceso dinámico y no un estado estático. La efectividad de cada fase impacta directamente en la calidad general de la conciencia situacional, donde fallos en cualquier punto pueden crear puntos ciegos críticos para la seguridad organizacional.

i. Fase de percepción

Primera etapa del modelo de Endsley donde se capturan los datos relevantes del entorno cibernetico. Esta fase es crucial porque establece la base informativa sobre la cual se construirá toda interpretación posterior. Una percepción incompleta o distorsionada inevitablemente conducirá a una CS defectuosa independientemente de la sofisticación del análisis posterior. La percepción requiere tanto amplitud como profundidad de visibilidad en el entorno digital para capturar patrones y anomalías significativas.

ii. Fase de comprensión

Segunda etapa donde se sintetizan y contextualizan los datos percibidos para crear información significativa. Su importancia radica en transformar datos aislados en un panorama coherente que revela relaciones, patrones y desviaciones significativas. Este proceso integra el conocimiento previo con los datos actuales para determinar la relevancia y el significado de los eventos observados, distinguiendo entre actividades normales y potenciales indicadores de amenaza.

iii. Fase de proyección

Tercera etapa que permite anticipar estados futuros basados en la comprensión actual de la situación. Es vital porque transforma la CS de una herramienta puramente descriptiva a una predictiva, permitiendo a las organizaciones pasar de posiciones reactivas a proactivas. La capacidad de proyectar escenarios futuros probables permite anticipar movimientos de atacantes, priorizar vulnerabilidades según la probabilidad de explotación, y asignar recursos defensivos antes de que ocurran los incidentes.

3. Situation Understanding

El entendimiento situacional va más allá de la simple conciencia situacional, y se refiere a, dada una situación, comprender las posibles consecuencias y predecir eventos futuros. Es relevante porque permite anticipar las amenazas antes de que se materialicen completamente. Mientras que la conciencia situacional responde a la pregunta “*¿qué está sucediendo?*”, el *entendimiento situacional* busca responder “*¿por qué está sucediendo y qué podría ocurrir después?*”. Esta profundidad adicional de análisis es fundamental en el complejo entorno cibernetico, donde las relaciones causa-efecto no siempre son evidentes y donde un solo indicador puede ser parte de un ataque multifacético más amplio.

4. Sensemaking

Incluye las actividades cognitivas necesarias para desarrollar conciencia, comprensión y traducirlas en acciones. Es fundamental porque conecta la conciencia con la acción concreta en el dominio cibernetico. El proceso de

sensemaking representa el puente crítico entre la observación pasiva y la respuesta activa, transformando el conocimiento abstracto en decisiones operativas tangibles. Este proceso involucra la contextualización de la información dentro de marcos mentales preexistentes, la resolución de ambigüedades y contradicciones, y la creación de narrativas coherentes que expliquen los eventos observados.

1.2 Componentes estructurales de la CS

5. Network Awareness

Componente fundamental que proporciona conocimiento completo sobre los sistemas, redes y activos digitales propios. Es esencial porque establece la línea base para detectar anomalías y determinar el estado normal de operación.

Además, un apropiado particionamiento de la red y una segmentación adecuada son una de las primeras líneas de defensa contra las amenazas, y son cruciales para limitar el alcance de un ataque y contener su propagación.

6. Threat Awareness

Conocimiento sobre las amenazas actuales, emergentes y potenciales que podrían afectar a la organización. Su importancia radica en proporcionar contexto sobre los actores maliciosos, sus capacidades, motivaciones y tácticas, permitiendo una defensa orientada específicamente a las amenazas más probables y peligrosas para cada entorno particular.

Además, conocer las amenazas permite también de mejorar el Situation Understanding, y por tanto también la capacidad de predecir las consecuencias de una determinada situación.

7. Mission Awareness

Comprensión de cómo los activos y procesos ciberneticos se relacionan con los objetivos organizacionales críticos. Es crucial porque alinea las actividades de ciberseguridad con el valor empresarial, permitiendo priorizar la protección de los sistemas y datos que realmente importan para la continuidad y éxito de la misión organizacional. Sin esta perspectiva, las organizaciones pueden desperdiciar recursos protegiendo activos de bajo valor mientras dejan vulnerables componentes críticos para la misión.

1.3 Colaboración y visualización en CS

8. Common Operational Picture (COP)

“A single identical display of relevant (operational) information (e.g. position of own troops and enemy troops, position and status of important infrastructure such as bridges, roads, etc.) shared by more than one Command.” — wikipedia

Es fundamental porque proporciona una base común para la conciencia situacional a todos los niveles de mando. La COP trasciende la mera representación visual para convertirse en un marco referencial compartido que asegura que todos los actores involucrados en la ciberseguridad interpreten la situación desde una misma perspectiva informativa.

La COP se aplica tipicamente en el contexto militar, pero su concepto se ha extendido a la ciberseguridad, donde la necesidad de una visión unificada y coherente de la situación es igualmente crítica.

9. Visualización de ciberinteligencia

Las técnicas de visualización son fundamentales para representar eficazmente el ciberespacio, compuesto por grandes cantidades de datos complejos y multidimensionales, ayudando a analistas y decisores a identificar rápidamente patrones y anomalías. En el contexto de la ciberdefensa, donde los conjuntos de datos pueden incluir millones de eventos por segundo, las representaciones visuales adecuadas transforman masas amorfas de datos en estructuras comprensibles. Hemos visto muchas técnicas de visualización, que no son equivalentes, y es importante también elegir la más adecuada para cada contexto, de lo contrario, los datos podrían seguir siendo incomprendibles o de poca utilidad..

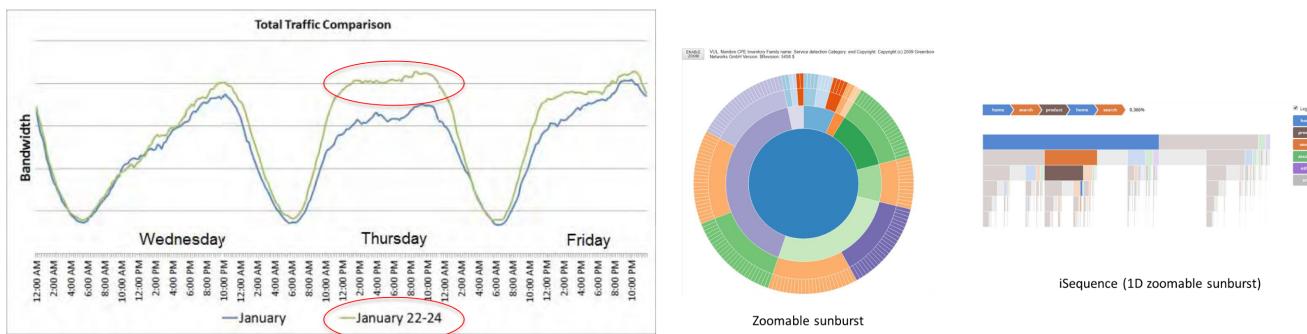


Figure 1.1: Ejemplos de visualización de datos

10. Gestión de la sobrecarga informativa

Esto se refiere a la importancia de estrategias y técnicas para filtrar, priorizar y presentar solo la información relevante para cada contexto y rol.

Los sistemas efectivos de CS implementan mecanismos de filtrado contextual, agregación inteligente y destacado adaptativo de anomalías para garantizar que cada nivel decisional reciba exactamente la información necesaria en el momento oportuno. Claro que esto incluye también técnicas de visualización, pero no se limita a eso. La *Mission Awareness*, puede ayudar a determinar qué información es relevante para cada contexto y, por tanto, también a filtrar la información con mayor eficacia.

1.4 Análisis y gestión de riesgos

11. Factores de riesgo

Amenazas, vulnerabilidades, impacto, probabilidad, y condición predisponente son elementos clave para cuantificar y priorizar los riesgos en el ciberespacio. Estos cinco componentes interrelacionados forman el marco fundamental para una evaluación del riesgo cibernético, permitiendo transformar conceptos abstractos en métricas comparables y accionables. Cada uno de estos se puede descomponer en subcomponentes más específicos, proporcionando un nivel de detalle que permite una evaluación más precisa y granular de los riesgos. Por ejemplo, las amenazas pueden dividirse en fuentes de amenaza y eventos de amenaza, mientras que las vulnerabilidades pueden clasificarse según su naturaleza (técnica, humana, organizativa) o su ubicación (sistemas, procesos, infraestructura).

El riesgo es una función de la probabilidad de que se produzca una amenaza y del impacto potencial que sufrirá un activo si se produce el suceso. El riesgo suele representarse como un valor único, normalmente decimal, o como un vector en el que se evalúan aisladamente distintos tipos de impactos.

$$risk(e) = probability(e) \times impact(e)$$

El impacto también puede medirse utilizando la degradación, es decir, el porcentaje % del activo afectado que se pierde

$$impact(e) = value(asset) \times degradation(asset)$$

12. Análisis de consecuencias

Las técnicas para evaluar el impacto de los ataques cibernéticos son cruciales para comprender las potenciales repercusiones operativas y estratégicas de las amenazas. Por ejemplo, hemos mencionado grafos de ataque que representan las relaciones entre vulnerabilidades y cómo los ataques pueden propagarse a través de múltiples sistemas. Estos gráficos permiten visualizar la complejidad de los ataques y sus posibles consecuencias en cascada, facilitando la identificación de puntos críticos.

En el video sobre los sistemas idraulicos de una tarea, se menciona una herramienta para simular el estado físico de un sistema, permitiendo de determinar diferencias entre el estado expectado y el real, y así detectar problemas.

1.5 Herramientas y tecnologías para la CS

13. Sensores cibernéticos

Estos son las fuentes de datos que alimentan los sistemas CS son cruciales porque determinan la calidad y la integridad de la información disponible para el análisis.

Estos sensores constituyen la primera fuente de ciber inteligencia de la organización, abarcando desde sistemas de detección de intrusiones de red y host, monitores de tráfico encriptado, analizadores de comportamiento de usuarios y entidades (UEBA), hasta honeypots y sistemas señuelo diseñados para atraer y estudiar actividades maliciosas.

14. Posicionamiento de sensores

El posicionamiento estratégico de sensores es esencial para maximizar la cobertura y minimizar los puntos ciegos en la red.

El diseño de la arquitectura de sensores debe considerar factores como la topología de la red, los flujos de tráfico, y las áreas críticas que requieren monitoreo intensivo.

Un posicionamiento inadecuado puede resultar en una falta de visibilidad en áreas críticas, permitiendo que los atacantes de hacer daños graves.

15. SIEM (Security Information and Event Management)

Estos sistemas centralizados son fundamentales para la recopilación, correlación y análisis de eventos de seguridad procedentes de diferentes fuentes en la red. Los SIEM actúan como el centro neurálgico de las operaciones de seguridad, proporcionando una plataforma unificada donde convergen datos estructurados y no estructurados de múltiples sistemas para crear un contexto coherente. Su capacidad para normalizar datos heterogéneos facilita la detección de patrones y anomalías que serían imposibles de percibir examinando cada fuente aisladamente.

Hemos visto que los SIEM son herramientas potentes, pero no son la solución definitiva para la CS. Aunque proporcionan una base sólida para la recopilación y análisis de datos, su eficacia depende de la calidad de los datos que reciben y de la capacidad de los analistas para interpretar correctamente los resultados.

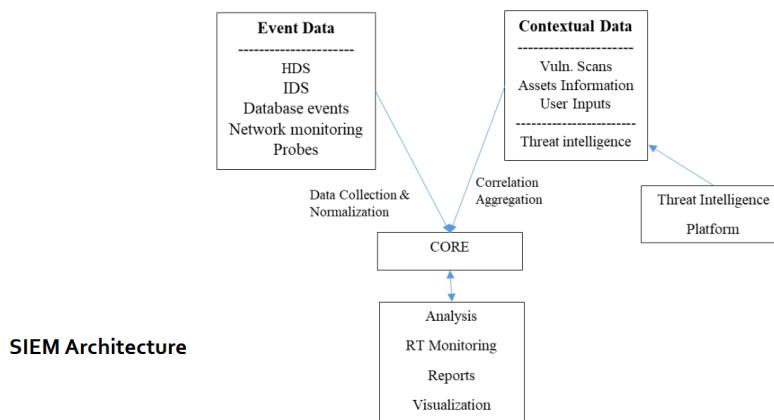


Figure 1.2: SIEM esquema

1.6 Dominios físicos y cibernéticos

16. Cyber Hybrid Situational Awareness

La integración de la conciencia situacional física y cibernética es esencial porque reconoce que los eventos en un dominio influyen en el otro, proporcionando una visión más completa de las amenazas modernas. Este enfoque híbrido responde a la creciente convergencia entre los mundos físico y digital, donde las fronteras tradicionales se difuminan con la proliferación de dispositivos IoT, sistemas de control industrial conectados y tecnologías operativas digitalizadas. La visión integrada permite detectar amenazas compuestas que utilizan vectores tanto físicos como digitales.

17. Georreferenciación de activos

La vinculación de activos cibernéticos con elementos físicos es esencial para la situational awareness híbrida, permitiendo visualizar las interdependencias entre el mundo físico y digital. Esta capacidad de localizar precisamente los recursos digitales en el espacio físico proporciona un contexto crucial para interpretar eventos de seguridad, especialmente en organizaciones con presencia geográficamente distribuida o infraestructuras complejas. La georreferenciación permite correlacionar incidentes cibernéticos con eventos físicos próximos.

1.7 Ciberinteligencia para mejorar la CS

18. Estándares para caracterización e intercambio de información

Los marcos estandarizados como STIX, TAXII, OpenIOC y MITRE ATT&CK son esenciales para garantizar la interoperabilidad y consistencia en la comunicación de información sobre amenazas entre diferentes organizaciones y herramientas. Estos estándares proporcionan un lenguaje común y estructuras de datos unificadas que permiten la automatización en el procesamiento e incorporación de inteligencia externa, eliminando la necesidad de conversiones manuales propensas a errores y reduciendo significativamente el tiempo entre la *identificación de una amenaza* y la *implementación de defensas correspondientes*.

19. Fuentes de Ciberinteligencia

La recopilación eficaz de información para la CS se basa en cuatro fuentes fundamentales de inteligencia: HUMINT (inteligencia humana), OSINT (inteligencia de fuentes abiertas), SIGINT (inteligencia de señales) y TECHINT (inteligencia técnica). Esta diversificación de fuentes es crucial porque cada una aporta una perspectiva única y complementaria sobre el panorama de amenazas. La HUMINT proporciona información valiosa sobre intenciones, motivaciones y capacidades de actores maliciosos a través de contactos personales y redes de informantes. La OSINT aprovecha la abundancia de información disponible públicamente para identificar tendencias emergentes, vulnerabilidades recién descubiertas y campañas de ataque en curso. La SIGINT permite detectar patrones anómalos en las comunicaciones y el tráfico de red que pueden indicar actividades maliciosas. Finalmente, la TECHINT analiza los artefactos técnicos de ataques (malware, exploits, infraestructura) para comprender las capacidades técnicas de los adversarios y desarrollar contramedidas efectivas.

20. Sistemas de Respuesta a Incidentes

Los sistemas de respuesta a incidentes son plataformas especializadas que permiten la inserción, almacenamiento y gestión centralizada de incidentes de seguridad, facilitando la coordinación de respuestas efectivas. Son fundamentales porque proporcionan un marco estructurado para el seguimiento completo del ciclo de vida de los



Figure 1.3: Ciberinteligencia

incidentes, desde su detección inicial hasta su resolución y el análisis posterior. Estos sistemas están diseñados para integrarse con TIPs (Plataformas de Inteligencia de Amenazas) y SIEMs, creando un ecosistema cohesivo de herramientas de seguridad. Ayudan a los miembros del *Computer Incident Response Team* (CIRT) a gestionar adecuadamente los incidentes, proporcionando gestión de flujos de trabajo y registros detallados sobre qué ocurrió, cuándo y cómo, tanto respecto al incidente como a la respuesta implementada. La documentación meticulosa que facilitan estos sistemas es invaluable para el aprendizaje organizacional, permitiendo refinar continuamente los procedimientos de respuesta basándose en experiencias previas y adaptarse a tácticas de ataque en evolución.

21. Gráficos de escenarios de ataque

Los *attack scenario graphs* son una herramienta avanzada de visualización que representa las relaciones entre las vulnerabilidades de un sistema y muestra cómo pueden desarrollarse ataques multi-etapa. Son fundamentales para la CS porque permiten anticipar posibles rutas de compromiso antes de que sean explotadas por atacantes. Estos gráficos pueden vincularse con *software dependency graphs* para visualizar cómo un paso de ataque a un componente puede afectar a otros componentes dependientes, creando un modelo completo de la superficie de ataque. La representación visual de estas relaciones facilita la identificación de puntos críticos donde una sola vulnerabilidad podría desencadenar efectos en cascada a través de múltiples sistemas. Esta perspectiva estructurada supera las limitaciones de los enfoques tradicionales que solo consideran vulnerabilidades individuales, permitiendo priorizar defensas basadas no solo en la gravedad de vulnerabilidades aisladas, sino también en su posición estratégica dentro de posibles cadenas de ataque.

22. Niveles de mando CS: Táctico, Operativo y Estratégico

La subdivisión de la conciencia situacional en los niveles táctico, operativo y estratégico es crucial porque permite adaptar la información a las necesidades específicas de los diferentes niveles decisionales. El nivel *táctico* (a veces llamado *técnico*) se enfoca en visualizar y gestionar eventos relacionados con activos específicos, requiriendo información detallada y técnica para la detección y respuesta inmediata a incidentes. El nivel *operativo* busca sintetizar los detalles del nivel táctico y contextualizarlos en términos de su impacto en la misión organizacional, facilitando la coordinación de múltiples acciones tácticas dentro de un marco temporal más amplio. El nivel *estratégico* requiere información abstracta y contextualizada sobre el panorama general de amenazas y su posible impacto en los objetivos organizacionales a largo plazo, permitiendo la planificación defensiva, la asignación de recursos y el alineamiento con requisitos regulatorios. Esta estructura jerárquica asegura que cada nivel reciba la información con el grado apropiado de detalle y abstracción.

Part II

Introducción to CS

2 Ciberconciencia Situacional	17
2.1 Introducción	17
2.2 Conciencia Situacional	17
2.2.1 Situation Understanding	18
2.2.2 Situational Awareness in Cyberspace	18
2.3 Ciberconciencia situacional	19
2.3.1 Vulnerabilidades	19
2.3.2 Amenazas - Threats	19
3 Cyber Intelligence Visualization	23
3.1 Visualization Charts	23
3.1.1 Georeferenced visualizations and IP-Port mapping	23
4 Sources of Intelligence	27
4.1 Herramientas de Ciberconciencia Situacional	27
4.1.1 Objetivos principales	27
4.1.2 Diferenciación con otras herramientas	27
4.1.3 Capacidades clave	27
4.1.4 Requisitos operacionales	27
4.2 Connection of Cyber Sensors	28
4.3 SIEM	29
4.4 Incident Response Systems	29
5 Hybrid Situational Awareness	31
5.1 Introducción	31

Chapter 2

Ciberconciencia Situacional

There are tasks (tareas) each monday. Each monday the lectures are asynchronous, and a task if given which lasts one or two weeks. The tarea may be commited by email if the deadline expires but it is preferable to finish in time.

2.1 Introducción

1. Conciencia Situacional
 - i. Situational Awareness
 - ii. Situational Awareness in Physical World
 - iii. Situational Awareness in Cyberspace
2. Visualización
 - i. Cyberintelligence Visualization
 - ii. Visualization Charts
3. Herramientas de ciberconciencia situacional
 - i. Cybersituational Awareness Tools
 - ii. Sources on Intelligence
 - iii. Risk and Consequences Analysis
4. Conciencia situacional híbrida
 - i. Hybrid situational awareness
 - ii. Cyber-Hybrid Situational Awareness Tools
5. Seguridad de sistemas ciberfísicos y protección de infraestructuras críticas
 - i. Cyber-Physical Systems (CPS)
Un CPS es un sistema que tiene una parte cibernética y otra física. Así de sencillo, según el prof. Esteve.
 - ii. CPS Vulnerabilities
 - iii. Industrial Control Systems Cyberdefense
 - iv. Critical Infrastructure Protection

“Ciberconciencia situacional significa Saber lo que está pasando en el ciberspacio” — Manuel Esteve

Un punto fundamental para saber lo que está pasando en el ciberspacio es la **visualización**. La visualización es una herramienta fundamental para la ciberconciencia situacional. En otras palabras, es necesario cabir lo que es importante que se visualice sobre el monitor pantalla (“videowall”) y lo que no.

2.2 Conciencia Situacional

Definition 2.1 (Situational Awareness) *Situational awareness is the perception of the elements of the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future*

Está también otra definición de conciencia situacional, que se encuentra en el *United States Army Field manual*:

Definition 2.2 (Situational Awareness - II) *Knowledge and understanding of the current situation which promotes timely, relevant and accurate assessment of friendly, competitive and other operations within the battlespace in order to facilitate decision making. An informational perspective and skill that fosters an ability to determine quickly the context and relevance of events that are unfolding*

Ambas definiciones pueden adaptarse al contexto cyber de Internet. De aquí se deriva la definición de *Cyber Situational Awareness* dada anteriormente “saber lo que está pasando en el ciberspacio”. Hay otras definiciones también:

Definition 2.3 (Cyber Situational Awareness) Comprehensive cyber situation awareness involves three key areas: computing and network components, threat information, and mission dependencies

MITRE

Definition 2.4 (Cyber Situational Awareness) Gathering real-time information about an organization's computer networks in order to provide an effective response to an attack

Computer Language Dictionary

2.2.1 Situation Understanding

Definition 2.5 (Situation Understanding) Understanding involves having a sufficient level of knowledge to be able to draw inferences about the possible consequences of the situation, as well as sufficient awareness of the situation to predict future patterns

Note that the following concepts related with situational awareness and are “similar” but they are not the same:

- ◊ Data
- ◊ Information
- ◊ Perceptions
- ◊ Intelligence
- ◊ Knowledge

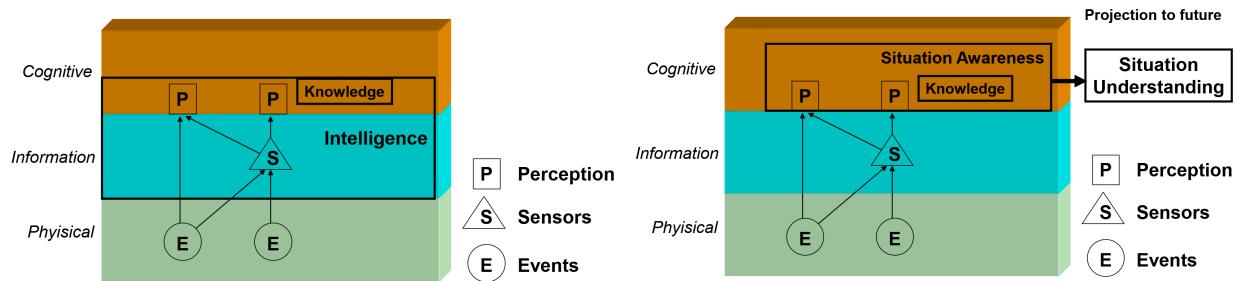


Figure 2.1: Producing Cyber Situational Awareness

2.2.2 Situational Awareness in Cyberspace

Cyber situational awareness involves three areas:

1. Networks and systems - *Network Awareness*
2. Threats and incidents (including APT and any other kind of attacks) - *Threat Awareness*
3. Fulfillment of the mission - *Mission Awareness*

- ◊ Network awareness:
 - Assets and configuration management
 - Vulnerabilities auditing
 - Patch management
 - Sharing of incident awareness
- ◊ Threat awareness
 - Internal incidents and suspicious behavior tracking
 - Knowledge of external threats, by mean of intelligence activities
 - HUMINT, OSINT, SIGINT
 - Share threat intelligence with government organizations (CERTs) or industry associations
- ◊ Mission awareness:
 - Develop a Common Operational Picture to understand all dependences and components to operate/develop missions in cyberspace
 - Select the best response decisions during incident management
 - Risk assessment before any response task execution
 - Find out mission impact during forensic analysis, after incident
 - Elaborate defense planning for future incidents management

Situational awareness can be generated at three traditional military command and control levels:

1. Tactical

The main goal at this level is to visualize and take care of events and situations related with assets. Sometimes this is called also *Technical level*

2. Operational

Main goal at this level is to summarize tactical level details and putting them in context of impact to organization misión.

3. Strategical

Es fundamental cabir que la ciberconciencia situacional se puede costruir a partir desde cuatro fuentes de información de cyber intelligence techniques:



Figure 2.2: Cyber intelligence techniques

- ◊ Cyber HUMINT - Human Intelligence, una fuente de información, por ejemplo, son *usuarios*, que proporcionan información sobre los seres humanos
- ◊ Cyber OSINT - Open Source Intelligence
- ◊ Cyber SIGINT - Signal Intelligence
- ◊ Cyber TECHINT - Technical Intelligence

2.3 Ciberconciencia situacional

Aparte del conocimiento de la situación en general, ahora podemos centrarnos en lo que ocurre en el *ciberespacio*. Esto se llama *Cyber Situational Awareness*.

Associated information with assets:

- ◊ Alarms
- ◊ Events
- ◊ Software
- ◊ Services
- ◊ Plugins
- ◊ Properties
- ◊ Netflow (this is fundamental for the ciberconciencia situacional)
- ◊ Groups

2.3.1 Vulnerabilidades

Definition 2.6 (Vulnerabilities) *Security gaps that can be used by potential attackers*

Vulnerabilidades son asociadas con los *assets*, propios o ajenos. Intrínsecamente todos los assets son propensos a haber vulnerabilidades, ahora o en el futuro, cuando algunas condiciones cambian.

Vulns son codificadas y clasificadas en varios modos:

- ◊ Attack vectors
- ◊ Assets affected by X
- ◊ Exploitation easiness of effort tradeoff
- ◊ Criticality
- ◊ Damage assessment if exploited

En general, así como si pueden caracterizar las vulnerabilidades:

- ◊ Vuln ID
- ◊ Asset
- ◊ Scan time
- ◊ Service
- ◊ Severity

2.3.2 Amenazas - Threats

Definition 2.7 (Threats) *Elements that can harm our protected system parts or as a whole. Pueden ser internal o external.*

Tenemos que caracterizar amenazas como:

- ◊ Kind
- ◊ Impact
- ◊ Probability
- ◊ Origin

MITRE es la más conocida organización que se dedica a la ciberconciencia situacional, y que ha desarrollado un framework para la ciberconciencia situacional. La MITRE attack matrix es una herramienta que permite visualizar las amenazas y los ataques que se pueden producir en un sistema.

Una amenazas no es sinónimo de *incidente*, que tiene una definición dedicada.

Definition 2.8 (Incident) *Un incidente es un evento que supera cierto umbral de peligro*

Tarea 1 - Conceptos complementarios de Ciberconciencia Situacional

1. [youtube.com/watch?v=cVaX07btaiU](https://www.youtube.com/watch?v=cVaX07btaiU)

Este vídeo aborda el tema de la conciencia cibersituacional en la producción de OT. Entre los conceptos más relevantes mencionados se encuentran:

- i. El Monitoring si divide en **Event Monitoring** y **Network Monitoring**, el primero basado en una tecnología de event collection (SW) que se instala en los dispositivos que los generan, y el segundo basado en la heurística sobre el tráfico de red. El video señala cómo la heurística puede conducir a veces a falsos positivos y entonces sea necesaria interpretación humana.
- ii. La importancia de definir ambos los escenarios de ataque y los de defensa: más precisamente, agregando raw event data se pueden identificar escenarios (secuencia de eventos) en una lista de use-cases, y a partir de uno use-case, un técnico humano puede buscar en un runbook lo que tiene que hacer para mitigar lo use-case de ataque.

2. [youtube.com/watch?v=Sn6c5s3WFWw](https://www.youtube.com/watch?v=Sn6c5s3WFWw)

- i. Este vídeo subraya la importancia de la ciberconciencia situacional especialmente para hacer frente a “unknown threats”, que no coinciden con ninguna regla o pattern específico ya conocido (algo como Zero-Day Vulnerabilities).

3. [youtube.com/watch?v=4geDznrTdbQ](https://www.youtube.com/watch?v=4geDznrTdbQ)

- i. Este video introduce el tema de la **priorización**: en las organizaciones medianas y grandes, es habitual tener enormes cantidades de posibles amenazas, y es necesario priorizarlas para poder actuar de manera eficiente. La conciencia situacional puede ser de grande ayuda en este sentido.
- ii. **Common Operating Picture**, parece referirse a evitar mantener la información divisa en “silos”, y a entender cómo y qué datos **agregar**, para obtener una visión más completa de la situación. Esta agregación de datos puede variar según la “Mission” de la organización.

4. [youtube.com/watch?v=T9bmqccjfkg](https://www.youtube.com/watch?v=T9bmqccjfkg)

- i. **Attack scenario graphs** son una herramienta para visualizar las relaciones entre las vulnerabilidades de un sistema, y entonces cómo multi-step ataques pueden ser realizados. Estos grafos pueden ser relacionados con *software dependency graphs*, para visualizar como uno step de ataque a un componente puede afectar otros componentes que dependen de él.
- ii. El video destaca el aspecto de “attack cascade” también al hablar de la **superficie de ataque**, cuya definición típica carece del concepto de daño de una brecha en la superficie al igual que los posibles pasos de ataque posteriores, limitándose a una visión más simple que sólo considera los entry points.
- iii. Otro aspecto mencionado es la importancia y la dificultad de **agregar datos** de diferentes fuentes, que ponen un desafío a la ciberconciencia situacional, así como la limitación de los modelos de scoring de las vulnerabilidades, que además de estar limitados por ellos mismos, necesitan ser relacionados con el contexto de la organización.

Chapter 3

Cyber Intelligence Visualization

Objetivo principal: producir para analistas y responsables de la toma de decisiones mecanismos útiles para comprender, de un vistazo, la información relevante y las tendencias dentro de las enormes cantidades de datos en bruto que les proporcionamos actualmente en las herramientas ciberneticas.

Las herramientas de ciber inteligencia generan una gran cantidad de datos, en gran parte testuale, y es necesario que los analistas sean capaces de procesarlos y entenderlos de manera rápida y eficiente.

The needs for the cyber intelligence domain are pretty specific:

- ◊ Breakdown the overwhelming amount of data into manageable pieces to find the data we are actually interested in.
- ◊ Topological representations to show the relationships among the elements.
- ◊ Adapt the representation to the timing and pace of the cyberspace.
- ◊ Coupling cyber space domain data with physical domain data.

Es frequentemente necesario representar multi-dimensional data en un espacio 2D o 3D, y utilizar visualizaciones interactivas para permitir a los analistas analizar empezando por la información clave más relevante y siguiendo con datos más finos.

Los puntos clave de la visualización de la inteligencia cibernetica son:

- ◊ Dimensionality reduction and complexity reduction.
- ◊ Assuming inherent non-linearities and couplings
- ◊ Tools and visualization techniques are need to help in the iterative process:

3.1 Visualization Charts

Area	Bar	BoxPlot	Bubble	Column
Doughnut	ErrorBar	FastLine	Funnel	Kagi
Line	Pie	Point	Polar	Radar
Range	Spline	StackedArea	StackedBar	StepLine

Table 3.1: Basic tecnicas for Cyber Intelligence Visualization

Los investigadores y profesionales descubrieron que las técnicas de visualización existentes no satisfacen las necesidades de representación del ciberespacio, mientras que la *graph-based* visualización gráficos proporciona medios para mostrar datos interrelacionados multidimensionales en un gráfico de pocas dimensiones.

Una tecnica eficiente para reducir las dimensiones de los datos es utilizar el color.

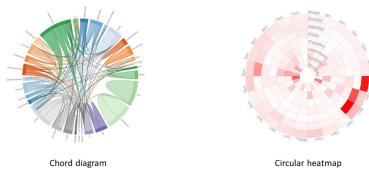


Figure 3.1: Relational color-based dimension reduction

3.1.1 Georeferenced visualizations and IP-Port mapping

Hoy en día, mucha información del ciberespacio se acopla a magnitudes físicas del mundo real. Por ejemplo, si conocemos la localización de una dirección IP, podemos determinar de donde proviene el ataque. También es posible colorear un mapa según la distribución geográfica de los ataques.

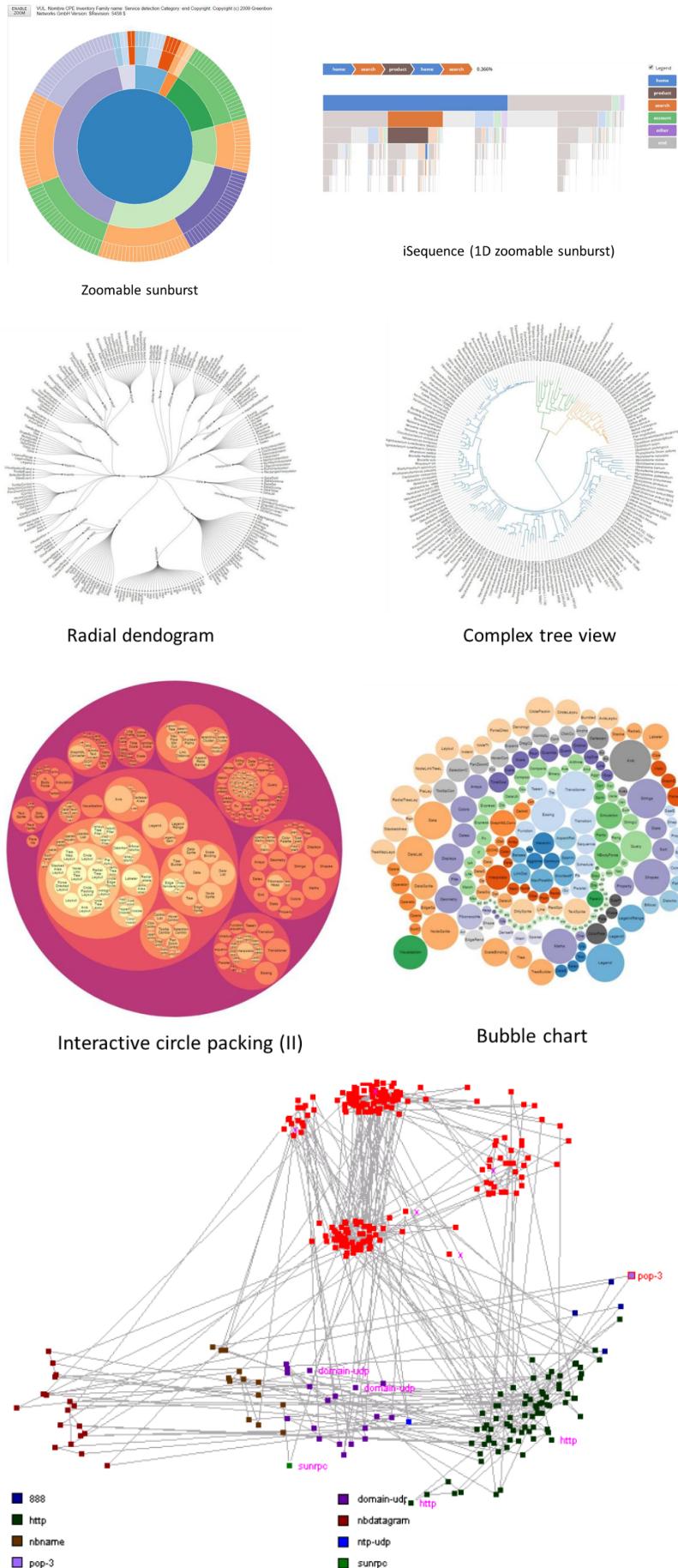


Figure 3.1: Graph-based visualización techniques

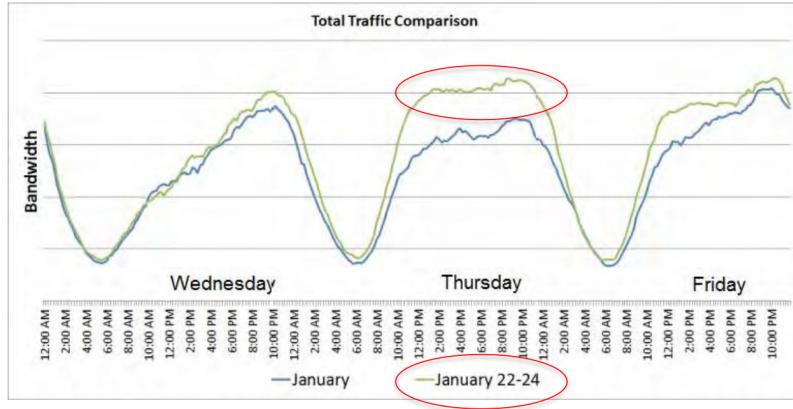


Figure 3.2: Según el profesor, este gráfico es muy importante porque muestra que para identificar lo que es *anormal*, es necesario saber lo que es *normal*.

Gráficos que muestran las conexiones abiertas a los puertos de un nodo de red, o entre nodos de red, pueden mostrar fácilmente la actividad de exploración.

Chapter 4

Sources of Intelligence

4.1 Herramientas de Ciberconciencia Situacional

Las herramientas de ciberconciencia situacional (CSA) son necesarias porque los sistemas de monitorización de ciberseguridad y las herramientas de ciberinteligencia generan enormes cantidades de información que resultaría imposible analizar manualmente. Este análisis manual sería laborioso y propenso a errores. Además, un problema crítico es que los analistas pueden "ahogarse en un mar de detalles" y perder la visión global de la situación.

4.1.1 Objetivos principales

Las herramientas de CSA deben mejorar el rendimiento, la cognición y la comprensión tanto para analistas como para responsables de toma de decisiones. Específicamente, ayudan a responder preguntas fundamentales como:

- ◊ ¿Hay algún ataque en curso? Si es así, ¿dónde está el atacante? ¿Cómo evoluciona la situación?
- ◊ ¿Cómo está afectando el ataque a la empresa o misión? ¿Cómo podemos evaluar el daño?
- ◊ ¿Cómo se espera que se comporten los atacantes? ¿Cuáles son sus estrategias?
- ◊ ¿Podemos predecir futuros plausibles de la situación actual?
- ◊ ¿Cómo creó el atacante la situación actual? ¿Qué intentaba conseguir?

4.1.2 Diferenciación con otras herramientas

Estas preguntas no pueden ser respondidas por otras herramientas de ciberseguridad o ciberinteligencia convencionales:

- ◊ Un IDS no proporciona percepción situacional, pues ésta va más allá de la simple detección de eventos
- ◊ Un SIEM puede correlacionar eventos, pero no proporciona un Common Operational Picture (COP) como paso previo para generar sensemaking
- ◊ Un sistema de detección de vulnerabilidades (VDS) produce una vista estática de vulnerabilidades, pero no la correlaciona con información de incidentes en tiempo real
- ◊ Las diferentes herramientas de inteligencia (HUMINT, OSINT, SIGINT, TECHINT) generan su propio tipo de conocimiento que debe ser correlacionado

4.1.3 Capacidades clave

Según la OTAN (Multinational Cyber Defence Capability Development), las herramientas de CSA deben incluir capacidades como:

- ◊ Visualizar listas de riesgos actuales, ordenados por impacto y con localización geográfica
- ◊ Generación de informes con diferentes niveles de detalle (drill down/roll up)
- ◊ Vistas jerárquicas personalizadas
- ◊ Seguridad de datos basada en unidad y localización
- ◊ Visualización de dependencias entre activos
- ◊ Agregación de incidentes por región geográfica o por red, con vistas enlazadas
- ◊ Generación y selección de cursos de acción posibles
- ◊ Fusión de datos de múltiples fuentes
- ◊ Gestión de vistas y paneles de control
- ◊ Capacidades avanzadas de visualización y simulación

4.1.4 Requisitos operacionales

El proyecto PANOPTESEC estableció requisitos fundamentales para estas herramientas, que incluyen:

- ◊ **Para fuentes y recolección de datos:** Interfaces estándar y no estándar para la recolección de datos de múltiples fuentes, capacidad de almacenar datos en bruto, recolección de información de configuración de sistemas, información sobre dispositivos, sistemas operativos, aplicaciones, topología de red, etc.
- ◊ **Para correlación de datos:** Motor de correlación de información que traduzca datos de múltiples fuentes a una representación común, identificación de elementos comunes, resolución de conflictos entre elementos informativos, creación de una vista unificada del sistema monitorizado y un modelo de impacto en la misión.
- ◊ **Para visualización:** Sistema que muestre la conciencia situacional de ciberdefensa en tiempo real, representando niveles de riesgo en estado estable y dinámico, impacto anticipado en la misión, detalles sobre sistemas críticos, información sobre topología de red, vulnerabilidades, rutas de ataque, y eventos de seguridad en tiempo real, así como acciones de mitigación propuestas.

4.2 Connection of Cyber Sensors

If we are to connect two systems to exchange data about assets (the same applies to threats, vulnerabilities, etc.) we have to agree on:

- ◊ What is an asset and what features and properties does it have
 - From a format perspective
 - Syntactically
 - Semantically
- ◊ How to exchange that data in an automatic and standard way between any given systems

This leads to the definition of standards for elements characterization and exchange, such as:

- ◊ SCAP - Security Content Automation Protocol
- ◊ Assets
 - ARF - Asset Reporting Format
 - AI - Asset Identification
 - CPE - Common Platform Enumeration
- ◊ Vulnerabilities
 - CVE - Common Vulnerabilities Enumeration
 - CVSS - Common Vulnerability Scoring System
 - CWE - Common Weakness Enumeration
 - OSVDB - Open Source Vulnerability Database
 - CVRF - Common Vulnerability Reporting Framework
- ◊ Threats
 - STIX - Structured Threat Information eXpression
 - TAXII - Trusted Automated eXchange of Indicator Information
 - MAEC - Malware Attribute Enumeration and Characterization
 - CAPEC - Common Attack Pattern Enumeration and Classification
 - CybOX - Cyber Observable eXpression
- ◊ etc...

Tipicamente, la comunicación entre sensores y sistemas se hace con XML (sorprendentemente predominante) o JSON, pero hay también enfoques basados en REST o proprietary APIs. El workflow planea de obtener informaciones de varios tipos de distintas fuentes, integrar las informaciones, correrlas, y finalmente generar ciberconciencia situacional.

1. Comunicación directa entre sistemas a través de uno exchange standard, como ARF o STIX
2. Federation/Middleware: un sistema centralizado que recibe datos de los sensores y los distribuye a otros sistemas
3. Subscription: hay un cloud de servidores para enviar datos a través de mecanismos propios.
Por la mayor parte, estos sistemas son de pago y no open source.
4. Common Collaborative Repository: Se uploadan datos a un repositorio común confiable y autorizado, como algunos SIEMs, CVE, ...

4.3 SIEM

SIEM stands for Security Information and Event Management. It is a system that collects and aggregates log data from many different sources, normalizes the data, correlates it, and then alerts based on rules and heuristics. Tipicamente es un elemento centralizado que gestiona una subred, o parte de una.

- ◊ Splunk
- ◊ QRadar
- ◊ OSSIM
- ◊ AlienVault USM (old)

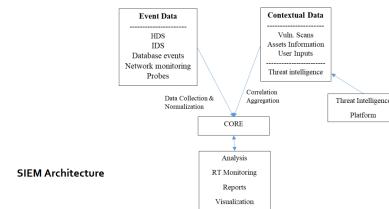


Figure 4.2: SIEM Architecture

4.4 Incident Response Systems

Based on existing ticketing systems, they allow insertion, storing and management of incidents on a central point, aiming at providing response coordination and proper management among interested parties.

They are designed to be integrated with TIPs (Threat Management Platform?) and SIEMs, and to help *Computer Incident Response Team* (CIRT) members carry out incident handling properly, providing workflow management and logs of what happened, when and how about the incident and the response.

Chapter 5

Hybrid Situational Awareness

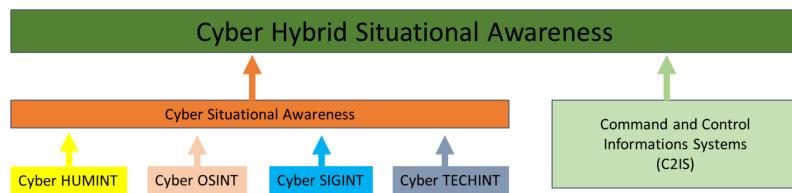


Figure 5.1: Cyber Hybrid Situational Awareness

5.1 Introducción

The cybersecurity decision makers will be able to jointly perceive the situation of physical world and cyber space domains as a unique decision making domain, as any decision taken in one domain affects the other three.

The main ideas to generate hybrid situational awareness are:

- ◊ Events in cyberspace (incidents, attacks...) produce effects in real-kinetic world, tan could affect to course of operations and mission development
- ◊ Events in physical world could produce effects in cyberspace, for instance a physical attack to a command post or to a electric grid infraestructure
- ◊ Cyberspace operations and kinetic operations are dependent
- ◊ Hybrid situational awareness is a fusion of cyber and physical situational awareness

Cada componente fisico tiene un componente ciber, y entonces lo que pasa en el mundo fisico afecta al mundo ciber y viceversa. La Conciencia Situacional híbrida es la fusión de la CS física y la CS ciber.

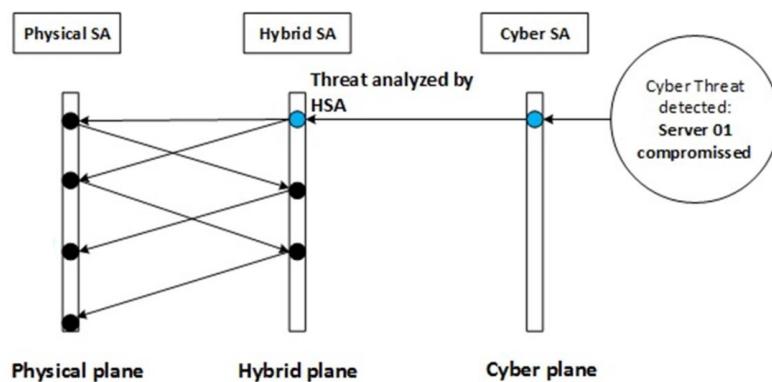


Figure 5.2: Example of Cyber event which produces an effect in the physical world

Part III

Sistemas Ciberfísicos

6	Cyber-Physical Systems	37
6.1	Introducción	37
6.2	Componenetes de CPSs	37
6.3	Vulnerabilidades	38
6.3.1	Vulnerabilidades más comunes	39
6.4	Vulnerabilities Assessment	39
6.4.1	Intrusion detection	40
6.4.2	Exploits mitigación	40
7	ICS Cyberdefense	41
7.1	ICS Security Architecture	41
7.1.1	Defense-in-depth	41
7.1.2	Network Segmentation and segregation	42
7.1.3	Firewalling	43
7.2	ICT Risk Assessment and Analysis	43
7.3	Security Control Implementation	44
7.3.1	Identificación y Autenticación	44

Chapter 6

Cyber-Physical Systems

6.1 Introducción

Definition 6.1 (CPS) *A cyber-physical system is a system of collaborating computational elements controlling physical entities*

Cyber-Physical System (CPS) is a generic term for a variety of control systems, such as SCADA (Supervisory Control and Data Acquisition) systems, ICSs (Industrial Control Systems), BCSs (Building Control Systems), and the global electrical smart grid

Definition 6.2 (CPS - 2) *A Cyber Physical System (CPS) is a network of interacting and collaborating computational elements controlling physical entities, including sensors, actuators, control processing units, and communication devices*

Definition 6.3 (CPS - 3) *CPS are systems used to monitor and control the physical world*

Definition 6.4 (CPS - 4) *CPS are IT systems that are integrated into physical world application*

Events out of temperatures

Consideremos un escenario en el que se mide la temperatura con un sensor. Para saber si la temperatura es alta o baja, se necesita un umbral, lo que se llama un **valor de referencia**. Esto permite de comparar la temperatura medida con el valor de referencia y tomar una decisión, como por ejemplo generar una alarma si la temperatura es demasiado alta.

6.2 Componenetes de CPSs

CPS tienen vulnerabilidades específicas, porque hay:

- ◊ Isolation assumption
- ◊ Increased connectivity
- ◊ Heterogeneity
- ◊ Long life cycle of components
Hay softwares que todavía necesitan Windows XP

6.2.0.1 Industrial Control Systems

Sometimes are called SCADA (Supervisory Control and Data Acquisition) systems or DCS (Distributed Control Systems).

El ejemplo más común de ICS son las redes de PLC, por wired o wireless. Tradicionalmente, los PLCs se comunican con un SCADA a través ambos de un protocolo OT (Operational Technologies) de comunicación propietario y de los protocolos IT standard.

Tradicionalmente, la isolación era la mejor defensa para estos sistemas. Patching y updates son un problema, porque los sistemas no pueden ser apagados, y entonces no pueden ser parcheados.

SCADA systems se componen de 4 niveles:

1. Sensors and actuators
2. Distributed controllers, which include programmable logic controllers (PLCs), intelligent electronic devices (IEDs), and other forms of programmable automation controllers (PACs)

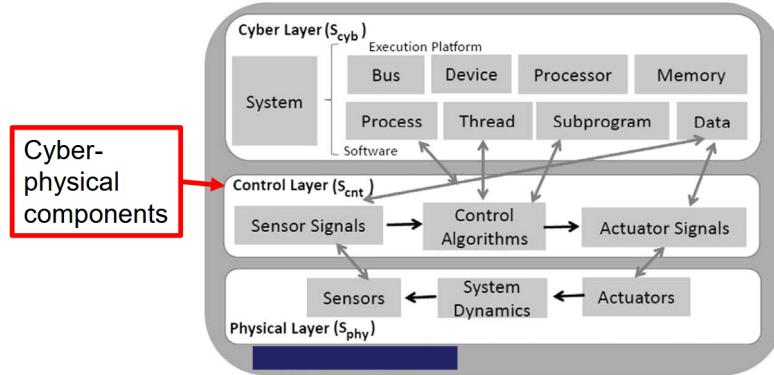


Figure 6.1: Cyberphysical Components

3. Supervisory and control systems, which encompasses systems that store process data, and implements control schemes to manage the lower levels
4. Human machine interfaces (HMIs), which enable the human operators to manage the physical process

Diferencias entre ICS y sistemas IT:

- ◊ Logic execution has a big impact on the physical environment
- ◊ Edge devices are, at least, so relevant as hosts servers
- ◊ Computation resources of edge devices are usually very limited
- ◊ Safety is the most relevant design constrain
- ◊ Continuous availability and time-critically constrains
- ◊ Hard-Real time vs Soft-Real time vs Best-Effort systems

SCADA network components:

- ◊ Servers and workstations that are used by operators to interact with the field devices segment
- ◊ HMI software-based graphical user interface
- ◊ Monitoring of field devices
- ◊ Field devices data updating
- ◊ Historian systems
- ◊ Back up systems (similar to IT systems)

Field devices components:

- ◊ Programmable Logic Controllers (PLCs)
- ◊ Remote Terminal Units (RTUs)
- ◊ Intelligent Electronic Devices (IEDs)
- ◊ IEDs are microprocessor based devices as sensors, motors (actuators), brakes, lights, etc
- ◊ IEDs are controlled by RTUs and PLCs by mean of field buses protocols (as PROFIBUS DP)
- ◊ RTUs monitor IEDs and transmit data to PLCs using ModBUS RTU and DNP3
- ◊ Sometimes, directed to the SCADA network using ModBUS TCP
- ◊ PLCs are control computers, with many types of I/O interfaces

Usual incidents in ICSs:

- ◊ Blocked or delayed flow of information through ICS networks, which could disrupt ICS operation
- ◊ Unauthorized changes to instructions, commands, or alarm thresholds, which could damage, disable, or shut down equipment, create environmental impacts, and/or endanger human life
- ◊ Inaccurate information sent to system operators, either to disguise unauthorized changes, or to cause the operators to initiate inappropriate actions, which could have various negative effects
- ◊ ICS software or configuration settings modified, or ICS software infected with malware, which could have various negative effects
- ◊ Interference with the operation of equipment protection systems, which could endanger costly and difficult-to-replace equipment
- ◊ Interference with the operation of safety systems, which could endanger human life

6.3 Vulnerabilidades

1. Vulnerabilities inherent in the CPS product, or platform vulnerabilities
2. Vulnerabilities because of poor network design or configuration, or network equipment vulnerabilities

3. Vulnerabilities caused during the installation, configuration, and maintenance of the CPS, or management vulnerabilities

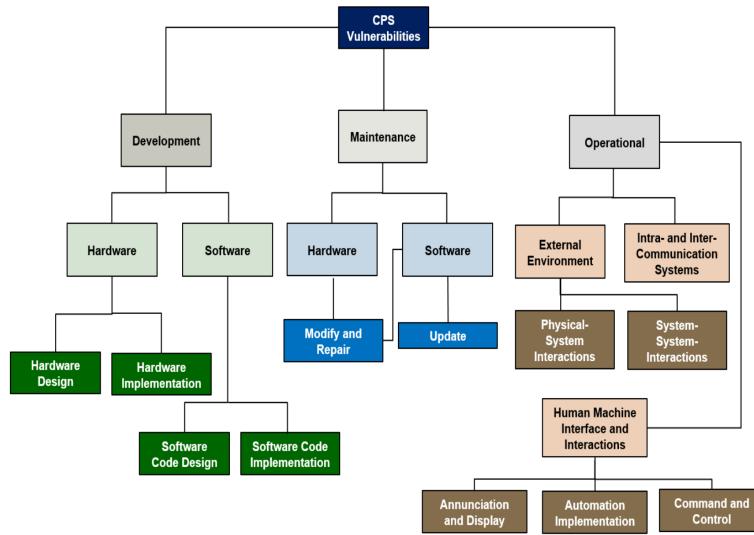


Figure 6.2: CPS Vulnerabilities taxonomía

A la izquierda de la figura 6.2 hay una lista de vulnerabilidades son vulnerabilidades de plataforma, al centro hay vulnerabilidades de la gestión, y a la derecha vulnerabilidades operacionales.

Cómo hemos dicho antes, típicamente es difícil actualizar el software para CPSs, esto es el motivo por el cual hay muchas vulnerabilidades relacionadas a la mantenimiento del software.

Las vulnerabilidades más comunes son:

- ◊ Improper Input Validation / Validación incorrecta de las entradas
- ◊ Permissions, Privileges and Access Control / Permisos, privilegios y control de acceso
- ◊ Improper Authentication / Autenticación incorrecta
- ◊ Insufficient Verification of Data Authenticity / Verificación insuficiente de la autenticidad de los datos
- ◊ Poor Code Quality / Código de baja calidad
- ◊ Security Configuration and Maintenance / Configuración y mantenimiento de la seguridad
- ◊ Credentials Management / Gestión de credenciales

6.3.1 Vulnerabilidades más comunes

La más explotada vulnerabilidad en CPSs es **Buffer Overflow**, que es típicamente permitida por la falta de validación de las entradas: los programadores suelen tener en cuenta lo que debería ocurrir y lo que podría ocurrir por error, pero no todas las posibilidades maliciosas.

Malas prácticas de código permiten a los atacantes suministrar datos inesperados y modificar así la ejecución del programa. Esta vulnerabilidad se llama **Lack of Bounds Checking**.

Cross-Site scripting vulnerabilidades pueden ser explotadas para muchos tipos de ataques, como el **Cross-Site Request Forgery** (CSRF), que permite a un atacante ejecutar comandos en el contexto de un usuario autenticado. En general, el Cross-Site Scripting permite **Code Injection**.

6.4 Vulnerabilities Assessment

Para los CPS, los objetivos de seguridad están en orden inverso de prioridad, siendo la disponibilidad considerada la más importante, en lugar de la confidencialidad. El personal de la industria a menudo usa el término "seguridad" para referirse a la disponibilidad y fiabilidad del sistema.

Nada debe hacerse en una red CPS activa que pueda interferir o interrumpir las operaciones críticas del sistema. En el entorno CPS, los objetivos de seguridad del mundo IT son reemplazados por la salud y seguridad humana, la disponibilidad del sistema, y la puntualidad e integridad de los datos. Esta es la principal diferencia entre las evaluaciones de seguridad de CPS y de IT.

Esta diferencia también se aplica a las estrategias de mitigación. Ninguna solución de ciberseguridad puede implementarse en la red CPS si interfiere con la respuesta del sistema. El equipo de evaluación cibernética debe trabajar

con el personal de la industria y los proveedores para realizar una evaluación efectiva sin comprometer la seguridad, disponibilidad o integridad del CPS.

CPS Vulnerabilities Assessment Execution Phases:

1. **Reconnaissance** - The first part of a cyber security assessment is to identify a target to attack.
2. **Exploration** - Once a target has been identified, the assessment team attacks the system
3. **Exploit development** - Once a problem has been identified, the assessment team may optionally develop an exploit for the vulnerability.

All these phases have specific aspects in CPS vulnerabilities assessment

6.4.1 Intrusion detection

HIDS no se utilizan mucho en ICSs, porque —tipicamente— no se puede instalar software sobre CPS componentes. Entonces, se utilizan **Network IDS** basados sobre **anomalías**. La detección por firmas (signature-based) tiene buena precisión para IT sistemas, pero no lo es para ICSs, porque ...// TODO

La detección por firmas (signature-based) tiene buena precisión para IT sistemas, pero no lo es para ICSs, porque tiene que depender de firmas conocidas y actualizadas, mientras que los protocolos y comportamientos en entornos ICS son muy específicos y a menudo propietarios.

Lateral Movements son muy comunes en ICSs, porque los atacantes pueden moverse lateralmente a través de la red para obtener acceso a otros sistemas, y entonces, **honeypots** son una defensa muy eficaz para detectar y monitorear estos movimientos. Los honeypots simulan componentes legítimos del sistema, atrayendo a los atacantes y permitiendo analizar sus técnicas sin comprometer los sistemas reales.

La segmentación de la red, junto con controles de acceso estrictos entre zonas, también es fundamental para limitar la capacidad de los atacantes de moverse lateralmente una vez que han comprometido un punto de entrada inicial en la red ICS.

6.4.2 Exploits mitigación

En general es muy difícil mitigar los exploits en CPSs, porque no se pueden aplicar parches a los sistemas.

Chapter 7

ICS Cyberdefense

A single security product, technology or solution cannot adequately protect an ICS by itself. A multiple layer strategy involving two (or more) different overlapping security mechanisms —defense-in-depth— is desired so that the impact of a failure in any of the mechanisms involved is minimized.

Lo más importante es separar la red corporativa de la red industrial.

Providing logical separation between the corporate and ICS networks (e.g., stateful inspection firewall(s) between the networks, unidirectional gateways)

- . Employing a DMZ network architecture (i.e., prevent direct traffic between the corporate and ICS networks), exploiting, for example, a firewall between the two networks.

7.1 ICS Security Architecture

ICS possible attack vectors:

- ◊ Backdoors and holes in network perimeter
- ◊ Vulnerabilities in common protocols
- ◊ Attacks on field devices
- ◊ Database attacks
- ◊ Communications hijacking and ‘man-in-the-middle’ attacks
- ◊ Spoofing attacks
- ◊ Attacks on privileged and/or shared accounts

Major security objectives for an ICS security architecture implementation should include the following:

- ◊ Restricting logical access to the ICS network and network activity
- ◊ Restricting physical access to the ICS network and devices
- ◊ Protecting individual ICS components from exploitation
- ◊ Restricting unauthorized modification of data
- ◊ Detecting security events and incidents
- ◊ Maintaining functionality during adverse conditions
- ◊ Restoring the system after an incident

7.1.1 Defense-in-depth

A single security product, technology or solution cannot adequately protect an ICS by itself. A multiple layer strategy involving two (or more) different overlapping security mechanisms, a technique also known as defense-in-depth, is desired so that the impact of a failure in any one mechanism is minimized:

- ◊ Firewalls
- ◊ DMZs
- ◊ IDS
- ◊ Incident response mechanisms
- ◊ Physical security and access control
- ◊ Staff education and training

Para garantizar una protección adecuada de los sistemas ICS, es fundamental desarrollar políticas de seguridad, procedimientos y materiales formativos y educativos específicamente diseñados para estos entornos. Estas políticas deben formularse considerando los diferentes niveles de amenaza a los que puede estar expuesto el ICS. Un enfoque eficaz requiere que la seguridad se aborde durante todo el ciclo de vida del sistema: desde la fase inicial de diseño de la arquitectura, pasando por el aprovisionamiento, la instalación y el mantenimiento, hasta el desmantelamiento final. Un elemento crucial de esta estrategia consiste en implementar una topología de red estratificada, donde las comunicaciones más críticas ocurren en el nivel más seguro y fiable, reduciendo así el riesgo de comprometer los procesos esenciales.

- ◊ Providing logical separation between the corporate and ICS networks
e.g., stateful inspection firewall(s) between the networks, unidirectional gateways
- ◊ Employing a DMZ network architecture
(i.e., prevent direct traffic between the corporate and ICS networks)
- ◊ Ensuring that critical components are redundant and are on redundant networks
- ◊ Designing critical systems for graceful degradation (fault tolerant) to prevent catastrophic cascading events
- ◊ Disabling unused ports and services on ICS devices after testing to assure this will not impact ICS operation
- ◊ Restricting physical access to the ICS network and devices
- ◊ Restricting ICS user privileges to only those that are required to perform each person's job (i.e., establishing role-based access control and configuring each role based on the principle of least privilege)
- ◊ Using separate authentication mechanisms and credentials for users of the ICS network and the corporate network (i.e., ICS network accounts do not use corporate network user accounts)
- ◊ Using modern technology, such as smart cards for Personal Identity Verification (PIV)
Regularizar acceso físico es fundamental
- ◊ Implementing security controls such as intrusion detection software, antivirus software and file integrity checking software
- ◊ Applying security techniques such as encryption and/or cryptographic hashes to ICS data storage and communications where determined appropriate
- ◊ Expediently deploying security patches after testing all patches under field conditions on a test system if possible, before installation on the ICS
- ◊ Tracking and monitoring audit trails on critical areas of the ICS
- ◊ Employing reliable and secure network protocols and services where feasible

7.1.2 Network Segmentation and segregation

1. Corporate and ICS must be separated, at least, by a firewall and a DMZ
2. Connections between corporate and ICS network must be minimized
3. Servers containing the data from the ICS that needs to be accessed from the corporate network must be put on DMZ segment
4. Minimum access should be permitted through the firewall, including opening only the ports required for specific communication

DMZ (demilitarized zone) is a network segment that is isolated from the corporate network and the ICS network, but is accessible from both. The DMZ is used to provide a buffer between the corporate network and the ICS network. The DMZ is typically used to host servers that need to be accessed from both the corporate network and the ICS network, such as web servers, email servers, and DNS servers. The DMZ is also used to host servers that need to be accessed from the Internet, such as web servers and email servers. Some considerations:

- ◊ The DMZ should be connected to the firewall such that specific
- ◊ (restricted) communication may occur between only the corporate network and the DMZ, and the ICS network and the DMZ
- ◊ The corporate network and the ICS network should not communicate directly with each other
- ◊ Creating a DMZ requires that the firewall offer three or more interfaces, rather than the typical public and private interfaces

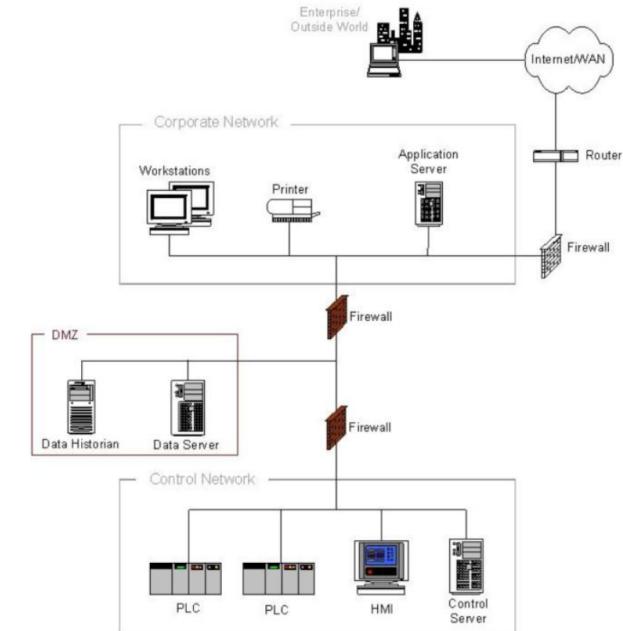


Figure 7.3: Segmentation and segregation example

Segmentation alternatives:

- ◊ Physical network separation to completely prevent any interconnectivity of traffic between domains
- ◊ Logical network separation enforced by encryption or network device-enforced partitioning
 - VLANs
 - VPNs
 - Unidirectional gateways (diodes)

- ◊ Network traffic filtering
 - IP and route information
 - Port and/or protocol level filtering
 - State-based filtering
 - Application filtering

Final recommendations to implement a defense-in depth by mean of segmentation and segregation:

1. Apply it at more than just the network layer
2. If a system doesn't need to communicate with another system, it should not be allowed to. In such case, there should no possible *physical* path for the communication to occur.
3. If a system needs to talk only to another system on a specific port or protocol and nothing else, it should be restricted as such.
Whitelisting over blacklisting
4. The most critical components require more strict isolation from other components
5. Implement whitelisting instead of blacklisting
6. Denying communications traffic by default and allowing communications traffic by exception
7. Extending the DMZ concept to other separate subnetworks

7.1.3 Firewalling

There are three types of firewalls: *Packet filtering*, *stateful inspection*, and *application-proxy* firewalls.

Primarily, firewalls are used to protect Internet connections; however, firewalls have applicability also in ICS network environments that do *not* include or require Internet connectivity:

- ◊ To restrict connectivity to and from internal ICS networks servicing more sensitive or criticality functions
- ◊ To restrict ICS inter-subnetwork communications between functional security subnets and devices

In an ICS environment, firewalls are most often deployed between the ICS network and the corporate network, to:

1. Block all communications with the exception of specifically enabled communications between devices on the unprotected LAN and protected ICS network
2. Enforce secure authentication of all users seeking to gain access to the ICS network
3. Enforce destination authorization: Users can be restricted and allowed to reach only the nodes on the control network necessary for their job function
4. Record information flow for traffic monitoring, analysis, and intrusion detection

Special considerations about firewalls use in ICS environments:

1. The possible addition of **delay** to control system communications
2. Using firewalls on an individual device basis can create significant management **overhead**, not permissible in control networks
3. Firewalls should be configured so they do not permit either incoming or outgoing traffic by default
4. By safety, real-time monitoring of firewalls and other security sensors is required to rapidly detect and initiate response to cyber incident

7.2 ICT Risk Assessment and Analysis

The impact of a cyber incident in an ICS may include both digital and physical effects. **Risk assessments** in ICS need to incorporate those potential effects, while **safety** is the major consideration that directly affects decisions on how ICS are engineered and operated.

Definition 7.1 (Safety) *Safety can be defined as “freedom from conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.”*

Another major concern for ICS operators is the availability of services provided by the ICS. The ICS may be part of critical infrastructure (for example, water or power systems), where there is a significant need for continuous and reliable operations. These two concerns must be kept in mind to implement a risk assessment framework in ICS.

“ICS may have strict requirements for availability or for recovery” — Manuel

Most of ICS engineers and decision makers will consider that safety and availability are more relevant for ICS than cybersecurity...it could be a big mistake...and also quite dangerous.

It is important to incorporate the effect of a ICS incident impact on the physical process/system, on dependent systems/processes and, on the physical environment among other possibilities, especially when ICS is part of a critical infrastructure.

The nature of ICS means that there are additional considerations that do not exist when doing a risk assessment of a traditional IT system:

- ◊ Impacts on safety
- ◊ Physical impact of a cyber incident on an ICS, including the larger physical environment; effect on the process controlled, and the physical effect on the ICS itself
- ◊ Physical disruption of an ICS process
- ◊ The consequences for risk assessments of non-digital control components within an ICS.

Impact of physical disruption of an ICS process:

- ◊ An incident that impacts the ICS and disrupts the dependent process may cause cascading impacts into other related ICS processes
- ◊ Impact to related ICS processes could include both systems and processes within the organization or systems and processes external to the organization
- ◊ Damage to the ICS or physical plant may cause either short or long term outages depending on the degree of the incident

An example of a cyber incident impacting the ICS is the Stuxnet malware, which caused physical damage to the centrifuges as well as disrupting dependent processes

Final considerations:

- ◊ Safety systems may also reduce the impact of a cyber incident to the ICS
- ◊ Safety systems are often deployed to perform specific monitoring and control functions to ensure the safety of people, the environment, process, and ICS
- ◊ These safety system could mitigate a ICS cybersecurity incident impact
- ◊ Evaluating the impact of an incident must also incorporate how the impact from the ICS could propagate to a connected ICS or physical system
- ◊ Impact propagation could occur due to both physical and logical dependencies
- ◊ This situation is known as “Cascade Effect”, and it is very dangerous in the case of ICS incidents in critical infrastructure

7.3 Security Control Implementation

- ◊ Access control technologies are filter and blocking technologies designed to direct and regulate the flow of information between devices or systems once authorization has been determined
- ◊ Role-based Access Control (RBAC) should be used to restrict ICS user privileges to only those that are required to perform each person's job (i.e., configuring each role based on the principle of least privilege)
- ◊ Legacy ICS systems or specialized ICS equipment may require development of specialized interface software for access control due to they use a number of proprietary operating systems or customized operating system implementations and interface
- ◊ VLANs are effectively deployed in ICS networks, with each automation cell assigned to a single VLAN to limit unnecessary traffic flooding and allow network devices on the same VLAN to span multiple switches
- ◊ The general recommendation is to use a one-to-one relationship between subnets and VLANs
- ◊ Switches have been susceptible to attacks such as MAC spoofing, table overflows, and attacks against the spanning tree protocols, depending on the device and its configuration

// TODO

7.3.1 Identificación y Autenticación

- ◊ Computer systems in ICS environments typically rely on traditional passwords for authentication
- ◊ Control system suppliers often supply systems with default passwords
- ◊ These passwords are factory set and are often easy to guess or are changed infrequently, which creates additional security risks
- ◊ Protocols currently used in ICS environments generally have inadequate or no network service authentication
- ◊ Challenge/response authentication may not be feasible for control system due to the possible latency that may be introduced
- ◊ There are now several forms of authentication available in addition to traditional password techniques being used with ICS
 - Traditional physical lock and keys
 - Security cards (e.g., magnetic, smart chip, optical coding)
 - Radio frequency devices in the form of cards, key fobs, or mounted tags
 - Dongles with secure encryption keys that attach to the USB, serial, or parallel ports of computers
 - One-time authentication code generators (e.g., key fobs).

- Smart Card Authentication
- Biometric Authentication

Disaster Recovery Planning:

1. Required response to events or conditions of varying duration and severity that would activate the recovery plan.
2. Procedures for operating the ICS in manual mode with all external electronic connections severed until secure conditions can be restored.
3. Roles and responsibilities of responders.
4. Processes and procedures for the backup and secure storage of information.
5. Complete and up-to-date logical network diagram.
6. The security plan should define a comprehensive backup and restore policy

Audit and Accountability:

1. It is necessary to determine that the system is performing as intended
2. Traditionally, the primary basis for audit in IT systems has been recordkeeping
3. Many of the process control devices that are integrated into the ICS have been installed for many years and do not have the capability to provide the audit records
4. The critical tasks in managing a network in an ICS environment are ensuring reliability and availability to support safe and efficient operation
5. Monitoring of sensors, logs, Intrusion Detection Systems (IDS), antivirus, patch management, policy management software, and other security mechanisms should be done on a real-time basis where feasible

Intrusion Detection and Prevention:

- ◊ By mean of IDS, as HIDS an NIDS
- ◊ In a ICS, NIDS are useful to detect attacks at corporate network and DMZ segment
- ◊ Less useful inside control network due to less knowledge about SCADA attacks network patterns
- ◊ HIDS are more useful in regular OS computers and servers at corporate an DMZ networks, due to control devices use (usually) legacy OS, with bit limitationn in CPU and memory

The best way to detect intrusions inside control network is a good characterization of “normal” traffic to detect suspicious changes in it, denoting attacks. This is especially true for ICS environments, because the traffic is generated by automated applications with little human interaction, making it very predictable.

- ◊ A patch may remove a vulnerability, but it can also introduce a greater risk from a production or safety perspective
- ◊ Patching the vulnerability may also change the way the OS or application works with control applications, causing the control application to lose some of its functionality
- ◊ Another issue is that many ICS utilize older versions of operating systems that are no longer supported by the vendor, then available patches may not be applicable
- ◊ Patching should be scheduled to occur during planned ICS outages, and previously tested in a similar system out of production mode

