Encuentro Internacional de Educación en Ingeniería ACOFI
2º Congreso Latinoamericano de Ingeniería
2019 10 al 13 de septiembre - Cartagena de Indias, Colombia
RETOS EN LA FORMACIÓN DE INGENIEROS EN LA ERA DIGITAL

PROCEDIMIENTO DE DISEÑO DE SISTEMAS CIBERFÍSICOS DE TIEMPO REAL TOLERANTES A ATAQUES CIBERNÉTICOS

Carlos Mario Paredes Valencia

Universidad Autónoma de Occidente
Santiago de Cali, Colombia

Resumen

En los últimos años, el mundo se ha expuesto al crecimiento en el desarrollo de varios tipos de sistemas ciberfísicos, los cuales han tenido un gran impacto desde el sector energético, automovilístico, industrial, así como en el sector médico. Estos, consisten en una combinación de dispositivos móviles, sistemas integrados y computadoras que se usan para monitorear, detectar y actuar sobre elementos físicos del mundo real para cumplir una tarea específica. Las partes informáticas que conforman este tipo de sistemas suelen interconectarse, normalmente por medios inalámbricos, para compartir información y datos que interactúan entre ellos, y en ocasiones con servicios de computación en la nube. Tener en cuenta que la gran mayoría de estos sistemas trabajan como sistemas de control distribuido, en donde el controlador, sensores y actuadores se comunican a través de redes de comunicaciones. Esto permite tener mayor flexibilidad en estos sistemas, en donde se tolera la integración de nuevos nodos a través de redes de comunicación como Internet, que ha contribuido al aumento en la capacidad de cómputo, la cobertura y adaptabilidad de las aplicaciones. Sin embargo, al mismo tiempo plantea nuevos desafíos que se relacionan con la seguridad y la confiabilidad de las aplicaciones derivada de la vulnerabilidad que presentan frente a ciberataques, los cuales pueden causar daños como afectaciones en la infraestructura física, el medio ambiente y los costos de producción, alterar la calidad de los productos involucrados en los procesos, incluso hasta atentar contra la vida humana, entre otros.

De este modo el propósito de esta investigación se centra en poder determinar nuevas estrategias y procedimientos que teniendo en cuenta puntos de vista desde la teoría de control y de la protección de información, se garanticen niveles de seguridad y confianza en aplicaciones de control soportadas en sistemas ciberfísicos, en relación a ciberataques que afecten la integridad de las mediciones y acciones de control, o el cumplimiento de plazos de tiempo real.

Palabras clave: ciberataques; sistemas de control distribuido; sistemas ciberfísicos

Abstract

Lately, the cyber-physical systems, has allowed the development of applications in different sectors such as energy, automotive, industrial and medical. These systems consist of a combination of mobile devices, integrated systems and computers that are used to monitor, detect and act on physical elements of the real world, fulfilling a specific task. The computer parts that make up these types of systems are interconnected, usually by wireless means, to share information and data that interact with each other and sometimes with cloud computing services as well. Take into account that the vast majority of these systems perform as distributed control systems, where the controller, sensors and actuators communicate through communication networks. This allows greater flexibility in these systems, which includes the integration of new nodes through communication networks such as the Internet. This has contributed to the increase in computing capacity, coverage and adaptability of applications. However, at the same time, this suppose new challenges related to the security and reliability of the applications, which may alter the quality of the products involved in the processes, even up to threatening human life, among others.

In this way the purpose of this research focuses on establishing strategies and procedures that take into account the views from the theory of control and protection of information, guaranteeing the levels of security and confidence in the control applications supported in cyber-physical systems, regarding to cyber-attacks that may affect both, the compliance with the real time periods, and the, integrity of measurements and control actions.

Keywords*: cyber-attacks; distributed control systems; cyber-physical systems*

1. Introducción

La evolución de los sistemas embebidos, inicialmente hacia las redes de sensores y recientemente a los sistemas ciberfísicos, ha posibilitado el desarrollo de nuevas aplicaciones en las que diversos nodos autónomos se distribuyen geográficamente y cooperan a través de redes de comunicación tanto alambradas como inalámbricas. Ejemplos de estas aplicaciones se encuentran hoy día en diferentes sectores, entre los cuales podemos mencionar las Smart Grid en el sector eléctrico, los Vehículos Autónomos en escenarios de movilidad, las Body Sensor Networks en temas de salud, y las Smart Factory en las industrias, entre otros, (Fawzi, Tabuada, and Diggavi 2012; Shoukry et al. 2016) - (Cárdenas, Amin, and Lin 2011).

Varias de estas aplicaciones son etiquetadas como de seguridad critica en relación el cumplimiento de plazos estrictos de tiempo real, asociados a la generación de acciones a partir de la interacción entre los sistemas computacionales y los sistemas físicos relacionados con la aplicación, debido a que el no cumplimiento de estos requisitos puede causar un daño irreparable al sistema físico que se controla, así como a las personas que dependen de ello (Ge et al. 2017). Adicionalmente, las mediciones y acciones de control pueden ser alteradas mientras se transmiten a través de las redes

de comunicaciones, de esta manera se requieren nuevos algoritmos de control que en presencia de situaciones adversas puedan llevar al sistema a estados seguros y estables (Jin and Haddad 2018), (Bezzaoucha Rebai, Voos, and Darouach 2017). Este tipo de situaciones ha generado gran interés en la comunidad científica en los últimos años, en busca de alternativas en los diseños de los sistemas automáticos que tengan en consideración requisitos asociados al intercambio de información a través de redes de comunicaciones (Orojloo and Azgomi 2017), (Chapman, Ofner, and Pauksztelo 2016).

Con base en lo anterior, el propósito de esta investigación se centra en poder determinar nuevas estrategias o procedimientos de diseño que garanticen niveles de seguridad y confianza en aplicaciones de control soportadas en sistemas ciberfísicos, en relación a ciberataques que afecten la integridad de las mediciones y acciones de control, o el cumplimiento de plazos de tiempo real.

2. Arquitectura de un sistema ciberfísico

Desde el punto de vista de los sistemas dinámicos, el estado actual de un sistema ciberfísico integra las variables medidas asociadas al conjunto de sensores que tenga el sistema y las variables de control (Krotofil and Cárdenas 2013). El valor normal de un cierto parámetro de proceso se conoce como el punto de ajuste, y la diferencia entre los valores de las variables de proceso y los puntos de ajuste referenciados son calculados por los controladores para posteriormente generar acciones que compensen esta diferencia con base en una estrategia de control.

En los sistemas ciberfísicos es muy importante que los operadores conozcan el estado actual de las variables, por lo tanto, comúnmente se utilizan interfaces gráficas de usuario (GUI), llamadas interfaz hombre-máquina (HMI). La arquitectura general de estos sistemas, normalmente se componen de dos capas principales:

1. Capa cibernética: consiste en una red corporativa, una red de control y una zona desmilitarizada (DMZ).
2. Capa física: consisten en un conjunto de sensores, actuadores y dispositivos físicos.

En la capa cibernética, la red corporativa es la que contiene las estaciones de trabajo y el servidor de aplicaciones y está a cargo de la administración comercial e interacción con el cliente, mientras que la red de control está compuesta por controladores tales como PLCs, servidores de control y HMI, y tiene como finalidad monitorear y controlar el sistema. Por último, la DMZ es una red segmentada aparte que se conecta directamente con los firewalls. Los servidores que contienen datos históricos y los servidores web que contienen los datos del sistema a los que se debe acceder desde las redes corporativas, se colocan en este segmento separado para mejorar la seguridad (Stouffer et al. 2015). La capa cibernética a menudo usa protocolos industriales para comunicar los dispositivos de la capa física, como por ejemplo Modbus. La comunicación entre los sensores y los controladores en un sistema ciberfísico puede ser divida en tres categorías:

- Comunicación sensor a sensor que conecta los datos sensados.

- Comunicación sensor a controlador, para elaborar el estado del sistema con base en lo cual se generan las acciones de compensación a aplicar sobre el sistema físico.
- Comunicación controlador a controlador, para coordinar acciones que lleven el sistema a puntos óptimos de funcionamiento con base en un criterio definido.

3. Seguridad en sistemas ciberfísicos

La principal diferencia entre los planes de seguridad en un dominio cibernético y los sistemas ciberfísicos, es que el objetivo de seguridad en el primer caso es asegurar y proteger los datos almacenados y transmitidos, así como garantizar la disponibilidad del servicio, mientras que en el segundo caso el objetivo principal es proteger la operación normal del proceso. El conocimiento requerido para llevar a cabo un ataque exitoso contra estos sistemas es elevado, dado que el atacante necesita adquirir el conocimiento suficiente sobre el comportamiento del proceso además de las condiciones de falla, los principios de control, así como el procesamiento de señales que se lleva a cabo dentro del sistema. Sin esto, un adversario no puede llevar el sistema a un estado inseguro.

Desde el punto de vista de control existen normalmente dos flujos de datos principales. El primero está relacionado con la medida de los sensores que se envía a los controladores, y el segundo con los comandos de control que se envían a los respectivos actuadores. Estos dos flujos de datos son relevantes dado que son los principales objetivos de ataques en el dominio ciberfísico. El envío de datos errados al controlador o a los actuadores ocasiona la generación de acciones incorrectas en relación a los objetivos de control, lo que puede generar la evolución del sistema a un estado inseguro. La teoría de control convencional se enfoca en el estudio de los sistemas dinámicos en donde cada componente es conectado a través de "canales ideales", si se considera la inserción de las redes de comunicación el funcionamiento de los sistemas de control resulta en un control a través de "canales no ideales". Fenómenos tales como retardos en la comunicación, datos corruptos, paquetes en desorden, errores de cuantización y congestiones en la red, pueden degradar el desempeño del sistema e incluso llevarlo a un estado inestable (Zhang et al. 2017).

El propósito de evaluar y clasificar las consecuencias de estos ataques contra este tipo de sistemas es de gran interés, de esta manera a continuación se presentan algunas consideraciones y modelamiento de algunos de los ataques que pueden llegar a ser involucrados en los procesos que gobiernan estos sistemas.

4. Tipos de ataques

El diseño y análisis de estos sistemas de control se dificulta debido a que se deben tener en cuenta requisitos extra funcionales, tales como tiempos de cómputo, acceso a la memoria y el uso de la energía, para garantizar el cumplimiento de plazos de tiempo real, la autonomía de la aplicación y la robustez de la misma(Sifakis 2010).

Los desafíos de seguridad en los sistemas embebidos, pueden llegar a incluir heterogeneidad, complejidad, adaptabilidad, control descentralizado, presiones de tiempo del mercado, rendimiento, eficiencia energética y costos de seguridad (Mirjalili and Lenstra 2008), (Sharma 2013).

En la figura 1 se observan los componentes de seguridad en los sistemas embebidos

Figura 1. Componentes de seguridad en sistemas embebidos (Sharma 2013)

•**Disponibilidad:** es la capacidad de un sistema embebido para poder funcionar como se diseñó en principio, aún en presencia de acciones no deseadas o intentos deliberados de comprometer el funcionamiento. Es decir, el sistema debe resistir la ruptura del sistema ante cualquier evento o intento de piratería o hackeo.
•**Confidencialidad:** Garantía de que cualquier información sensible recibida o procesada por el sistema esté protegida contra divulgaciones accidentales, agentes/dispositivos no autorizados o destinatarios no deseados.
•**Integridad:** los datos almacenados deben ser protegidos contra la corrupción o cambios ilegítimos. Permite mantener la información importante contra las modificaciones no autorizadas. En otras palabras, busca mantener la exactitud de la información sin ser manipulada por agentes ajenos al proceso.
•**Confiabilidad:** capacidad de funcionamiento garantizando cierto nivel de prestaciones, durante largos periodos de tiempo, aún en presencia de errores y fallos considerados en el diseño. Esta característica combina las siguientes características: detección de fallos, tolerancia a fallos, y previsión y pronóstico de fallas.

Estos requisitos han guiado distintas soluciones de implementación en estos sistemas a nivel de hardware, software, y combinaciones de estos. Los ataques en los sistemas embebidos pueden ser clasificados en tres grandes categorías: ataques físicos, ataques de software y ataques de canal lateral (Al-Wosabi, Shukur, and Ibrahim 2015).

Los ataques físicos se pueden clasificar en las siguientes categorías:

- Ataques invasivos. Tienen como objetivo alterar físicamente la correcta operación en un integrado. Este tipo de ataques requieren de personas con gran experticia.
- Ataques semi-invasivos. Este tipo de ataques tratan de observar el comportamiento del chip del sistema integrado después de que un atacante haya disparado un evento. Un ejemplo de ello pueden ser los denominados ataques de falla, los cuales inducen una falla en el flujo de cómputo del procesador durante una operación de criptografía y observan el resultado criptográfico a medida que la falla se propaga.
- Ataques no invasivos. Usan la explotación de las características del integrado, tales como la disipación de potencia, tiempo de cálculo, entre otras, para poder extraer información sobre los datos procesados.

Los ataques de canal lateral están basados en observar ciertas propiedades de los sistemas embebidos. Los estudios han podido determinar que realizando un profundo análisis sobre el tiempo de cómputo, en donde se determinan patrones y secuencias, para determinar claves secretas. Algunas de las actuales soluciones a estos ataques están siendo desarrolladas agregando ruido aleatorio a la información. En el campo de los ataques de software las principales contribuciones se soportan en hardware seguro, coprocesadores seguros, protección de memorias y registros (Sharma 2013).

Otros tipos de ataques cibernéticos son los ataques de Denegación de Servicio (DoS), ataques de repetición y ataques de engaño, cuyos modelos matemáticos se presentan en la tabla 1; donde y_k es la medición del sensor, mientras que $\overline{y_k}$ representa la señal recibida por el controlador con ataques.

Tabla 1. Modelos matemáticos de ciberataques (Wang et al. 2016)

Tipos	**Modelo matemático**
Ataques tipo DoS	$\overline{y_k} = \propto y_k$, donde $\propto$ es una variable de decisión que puede tomar el valor de 1 o 0, es seteada por el atacante
Ataques de repetición	$\overline{y_k} \in Y_k$, donde Y_k es el set de medidas aceptadas por los atacantes antes del tiempo k
Ataques de engaño	$\overline{y_k} = y_k + {y_k}^a$, donde ${y_k}^a$ es un vector inyectado por los atacantes.

• Ataques tipo DoS. También conocidos como ataques Jamming, son estrategias que a menudo son usadas por los atacantes para afectar la transmisión de las medidas o señales de control, al ocupar el recurso de la red de manera que el rendimiento del sistema puede deteriorarse tanto como sea posible.
• Ataques de repetición. Son ataques muy comunes y naturales por los atacantes que desconocen la dinámica de los sistemas. Consiste en registrar lecturas de los sensores y actuadores comprometidos por una cierta cantidad de tiempo para repetir este set de información en posteriores intervalos.
• Ataques de engaño o integridad. También conocidos como ataques de inyección de falsos datos, son los ataques más generales y son considerados como los más peligrosos en este tipo de sistemas,

porque los atacantes pueden ingresar datos maliciosos que degradan el rendimiento general de los sistemas.

De este modo, en estos sistemas hay dos tipos de señales que son críticas para la operación estable y normal del sistema. Las señales sensadas desde el sensor hacia los sistemas de control y las señales de control desde los módulos de control hacia el sistema físico. La manipulación o perdida de una o ambas señales puede resultar en la operación inestable del sistema. Un ciberataque que resulta de la manipulación de los datos es referido como un ataque de integridad y un ataques que resulta en una perdida prolongada de estas señales es llamado como un ataque tipos Dos (Deniel of Service-Denegación de Servicio) (Sridhar and Manimaran 2010).

5. Referencias

- Al-Wosabi, Abdo Ali Abdullah, Zarina Shukur, and Muhammad Azwan Ibrahim. 2015. "Framework for Software Tampering Detection in Embedded Systems." *Proceedings - 5th International Conference on Electrical Engineering and Informatics: Bridging the Knowledge between Academic, Industry, and Community, ICEEI 2015*: 259–64.
- Bezzaoucha Rebai, Souad, Holger Voos, and Mohamed Darouach. 2017. "A Contribution to Cyber-Security of Networked Control Systems: An Event-Based Control Approach." *2017 3rd International Conference on Event-Based Control, Communication and Signal Processing, EBCCSP 2017 - Proceedings*.
- Cárdenas, Alvaro A, Saurabh Amin, and Zong-syun Lin. 2011. "Attacks against Process Control Systems : Risk Assessment, Detection, and Response." *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*: 355–66.
- Chapman, Jonathan P., Simon Ofner, and Piotr Pauksztelo. 2016. "Key Factors in Industrial Control System Security." *2016 IEEE 41st Conference on Local Computer Networks (LCN)*: 551–54. http://ieeexplore.ieee.org/document/7796838/.
- Fawzi, Hamza, Paulo Tabuada, and Suhas Diggavi. 2012. "Security for Control Systems under Sensor and Actuator Attacks." *Decision and Control (CDC), 2012 IEEE 51st Annual Conference on*: 3412–17.
- Ge, Hui et al. 2017. "Analysis of Cyber Physical Systems Security via Networked Attacks." *Chinese Control Conference, CCC*: 4266–72.
- Jin, Xu, and Wassim M. Haddad. 2018. "An Adaptive Control Architecture for Leader–follower Multiagent Systems with Stochastic Disturbances and Sensor and Actuator Attacks." *International Journal of Control* (Cdc): 1–10. https://www.tandfonline.com/doi/full/10.1080/00207179.2018.1450524.
- Krotofil, Marina, and Alvaro A. Cárdenas. 2013. "Resilience of Process Control Systems to Cyber-Physical Attacks." *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 8208 LNCS: 166–82.
- Mirjalili, S Hasan, and Arjen K Lenstra. 2008. "Security Observance throughout the Life-Cycle of Embedded Systems." *Proceeding of 2008 International Conference on Embedded Systems and Applications (ESA'08)*: 186–92. http://infoscience.epfl.ch/record/149724/.
- Orojloo, Hamed, and Mohammad Abdollahi Azgomi. 2017. "A Method for Evaluating the Consequence Propagation of Security Attacks in Cyber–physical Systems." *Future*

Generation Computer Systems 67: 57–71. http://dx.doi.org/10.1016/j.future.2016.07.016.

- Sharma, S. 2013. "Embedded Systems – A Security Paradigm for Pervasive Computing." *2013 International Conference on Communication Systems and Network Technologies*: 472–77. http://ieeexplore.ieee.org/document/6524441/.
- Shoukry, Yasser et al. 2016. "SMT-Based Observer Design for Cyber-Physical Systems under Sensor Attacks." *2016 ACM/IEEE 7th International Conference on Cyber-Physical Systems, ICCPS 2016 - Proceedings*.
- Sifakis, Joseph. "Embedded Systems Design – Scientific Challenges and Work Directions." : 2010.
- Sridhar, Siddharth, and G. Manimaran. 2010. "Data Integrity Attacks and Their Impacts on SCADA Control System." *IEEE PES General Meeting, PES 2010*: 0–5.
- Stouffer, Keith et al. 2015. "NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security." http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf.
- Wang, Dong et al. 2016. "Recent Advances on Filtering and Control for Cyber-Physical Systems under Security and Resource Constraints." *Journal of the Franklin Institute* 353(11): 2451–66. http://dx.doi.org/10.1016/j.jfranklin.2016.04.011.
- Zhang, Dan, Peng Shi, Qing Guo Wang, and Li Yu. 2017. "Analysis and Synthesis of Networked Control Systems: A Survey of Recent Advances and Challenges." *ISA Transactions* 66: 376–92.

Sobre los autores

- **Carlos Mario Paredes Valencia**: Ingeniero Mecatrónico. Profesor e investigador. cmparedes@uao.edu.co

---