IMPORTANCIA DEL ESTUDIO DEL CONTROL PARA LOS SISTEMAS CYBER-FÍSICOS

IMPORTANCE OF CONTROL STUDY FOR CYBER-PHYSICAL SYSTEMS

Carlos Pillajo
Universidad Politécnica Salesiana - Ecuador
cpillajo@ups.edu.ec
Javier E. Sierra
Universidad Pontificia Bolivariana – Colombia
javier.sierra@upb.edu.co

RESUMEN

Los Sistemas Ciber-Físicos (CPS) tienen la capacidad de integrar funciones de cómputo y de comunicación con el seguimiento y control de las entidades del mundo físico. Estos sistemas se componen generalmente por un conjunto de dispositivos en red, tales como: sensores, actuadores, unidades de procesamiento de control y dispositivos de comunicación. Debido a la heterogeneidad del hardware un CPS puede abarcar múltiples dispositivos con diferentes arquitecturas, protocolos e interfaces, los CPS tienden a ser sistemas híbridos y distribuidos.

En este trabajo, proporcionamos enfoque para el análisis de requisitos y principios de modelado de CPS que se ilustran a través de un sistema de control de un manipulador, Revisaremos cómo los objetivos de seguridad tradicionales de integridad, disponibilidad y confidencialidad pueden ser interpretados por CPS, además revisaremos el estado de los sistemas de control en los CPS y el trabajo por realizar en este campo.

Palabras Claves: Sistemas Cyber Fisicos, Modelos CPS, Arquitectura CPS, Control de CPS

INTRODUCCION

Las tecnologías, las ciencias e ingenierías siguen redefiniendo las capacidades del mundo físico, actualmente los seres humanos podemos comunicarnos desde dos puntos totalmente diferentes y alejados como sea posible a través de internet, la cual también nos permite interactuar con los objetos a distancia, personas y lugares. En este milenio las necesidades de nuestra sociedad exigen cada vez más capacidades innovadoras en el tiempo y el espacio. Los enfoques actuales para el diseño de sistemas, desarrollo y operación no son suficientes [1], por lo tanto, surgen los Sistemas Ciber-Físicos (Cyber-Phisical-System CPS) que son integraciones de cómputo con los procesos físicos. Ordenadores y redes incrustadas para supervisar y controlar los procesos físicos, por lo general con los lazos de retroalimentación donde los procesos físicos afectan a los cálculos y viceversa [2]. Sin embargo la convergencia entre la cibernética y el mundo físico está abriendo nuevas líneas de investigación para los investigadores de la computación ubicua, de hecho en un mundo convergen acciones e información producida en el mundo físico que pueden afectar y modificar los contextos personales y sociales, por lo que también puede afectar la información y los servicios que se manejan en el mundo cibernético [3]. Figura N1

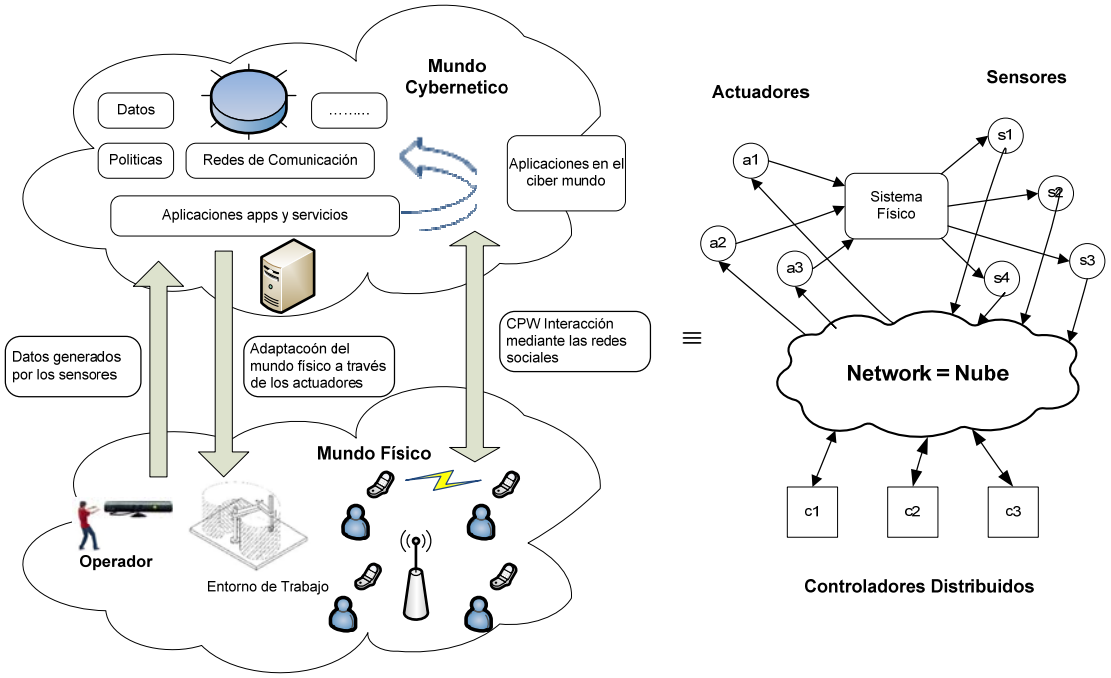

Figura N1. Interacción de sistemas CPS

Los Sistemas Ciber-Físicos tienen la capacidad de integrar funciones de cómputo y de comunicación con el seguimiento y control de las entidades del mundo físico. Estos sistemas se componen generalmente por un conjunto de agentes en red, incluyendo: sensores, actuadores, unidades de procesamiento de control, y dispositivos de comunicación [4]. En los CPS, el tiempo que se necesita para realizar una tarea puede ser crítico para corregir funcionamiento del sistema, los procesos físicos son composiciones de muchas cosas que ocurren al mismo tiempo, a diferencia de los procesos de software, que están profundamente arraigadas en los pasos secuenciales [5], Con el seguimiento del software y controlar el proceso físico, tales sistemas se consideran para hacer las aplicaciones tradicionales tales como el transporte y la red eléctrica más segura y más eficiente, las aplicaciones típicas de los CPS tienden a ser sistemas híbridos y distribuidos. Por lo general están compuestas por los dominios de computación en red y también los dominios físicos distribuidos. En tales sistemas, tenemos que tener en cuenta no sólo la forma de diseñar el mundo discreto (es decir, los dominios de software) y el mundo continuo (es decir, los dominios físicos), sino también considerar cómo combinarlos juntos sin problemas. [6]. Considerablemente, menos atención se ha dado a principios del análisis de requerimientos y modelado de CPS, es decir, además de desarrollar el modelo formal, también necesitamos saber cómo determinar qué dominios se incluyen por CPS. Estas tareas son los requisitos previos para el análisis formal. Ayudan a construir una comprensión clara sobre CPS, y allanar el camino para construir un modelo formal preciso y detallado. Sin embargo, son escasos los trabajos que han tenido estas tareas en cuanto a los sistemas de control para CPS, por otro lado, la teoría de control tienen fuertes resultados en algoritmos robustos y tolerantes a fallos en contra de las dudas o fallas bien definidas, por lo tanto, en este artículo esbozamos algunos desafíos en los algoritmos del sistema de control para CPS [4].

TRABAJOS RELACIONADOS

Como una nueva generación de sistema de ingeniería, Los CPS ha atraído a muchas atenciones en los últimos años. Viendo el CPS como la integración del proceso de computación con el proceso físico, Lee et al. en [8] ha argumentado que tenemos una distancia de los factores físicos abstractos del proceso de computación en el futuro a la luz de los diferentes principios que hemos seguido en el mundo de la informática y el mundo físico. Además, Marco Conti en [3] han detallado los retos de la investigación para CPS, como la abstracción en tiempo real y la solidez, las cuestiones de seguridad.

En otra dirección, los problemas de seguridad y desafíos a la CPS se han discutido en [9]. Y cuando se centra en la fiabilidad de la CPS, Lin et al. en su propuesta de investigación doctoral [10] ha propuesto tomar el modelado basado en agentes para el análisis cuantitativo de fiabilidad en CPS

Huang et al. Argumentó que la arquitectura orientada al servicio ya existente puede ofrecer una solución parcial para el modelado de CPS [11]. Y así, han extendido el modelo de servicio existente para especificar los servicios prestados por personas físicas, y también proporcionó un algoritmo de composición de servicios de dos niveles. A la luz de las propiedades de los CPS, Fritzson, P. en [12] afirma que la Modélica es una herramienta adecuada para el modelado y simulación de CPS.

Con la proliferación de dispositivos, las alternativas de conectividad, aplicaciones y servicios, un desafío clave es cómo orquestar horizontalmente para permitir la interoperabilidad sin fisuras de todos ellos para el beneficio de los usuarios finales. Por lo general se conoce como el Internet de las Cosas (IoT), una abundancia de inteligencia informática direccionable, con capacidades de detección y, de accionamiento, incrustados en procesos físicos (por lo tanto, ciber-físicos) objetos para interactuar con su entorno físico [3].

ARQUITECTURA

La visión es diseñar un sistema como una colección de servicios y abstracciones de aplicación específica, que sean estructurados y desarrollados automáticamente en una plataforma destino de acuerdo con las limitaciones en términos de: a) las capacidades del hardware, y b) los requisitos de aplicación [7]. En los sistemas actuales, las aplicaciones solicitan servicios al núcleo de confianza a través de una interfaz bien definida por ejemplo, mediante llamadas al sistema. Estas interfaces o APIs, generalmente se definen en un nivel que satisfaga las necesidades comunes de un amplio espectro de aplicaciones, lo que hace que sea incómodo para las aplicaciones es especificar exactamente qué comportamiento necesitan del sistema inferior.

Los puntos de vista antes mencionados sugieren un sistema que debe estar estructurado como un colección de servicios de componentes, que pueden ser aislados utilizando técnicas de hardware y/o de software o combinados en un sólo espacio de dirección de acuerdo con requisitos bien definidos. Este aislamiento incurre en demoras entre los distintos servicios de comunicación, por lo que el sistema automáticamente debe arreglarlo con los canales de comunicación creados dinámicamente para satisfacer el equilibrio entre los requisitos de retardo y el aislamiento.

Debido a la heterogeneidad del hardware, un sistema cibernético-físico puede abarcar múltiples dispositivos con diferentes arquitecturas, protocolos e interfaces. Tradicionalmente, la invocación de servicios ha involucrado complejos procedimientos de cálculo de referencias para el intercambio de datos entre plataformas de manera independiente de la arquitectura. Teniendo presente además, que para los servicios distribuidos es deseable un sistema unificado de estándares ISA independiente del hardware. Cuando un servicio es implementado sobre una plataforma destino es recompilado y posiblemente vinculado con la verificación, la comunicación, la protección y otro código de contenido para un conjunto de instrucciones de hardware específico.

MODELOS

En este trabajo, proporcionamos un enfoque para el análisis de requisitos y principios de modelado de CPS. En este enfoque proponemos la construcción de la estructura del modelo para capturar la arquitectura del sistema, y el modelo objetivo para capturar las relaciones de refinamiento de las necesidades del usuario y los requisitos de los dominios en CPS [6]. Estos modelos ayudan a construir una clara comprensión acerca de CPS entre los usuarios y los diseñadores, allanando el camino para definir el modelo preciso y formal. Que son estos modelos y como se construyen se ilustran a través de un sistema de control de un manipulador. El modelo estructura es la captura del dominio físico y el dominio del software los cuales son incluidos por los CPS, y que fenómenos comparten entre ellos. Al mismo tiempo, el modelo meta es la captura de las relaciones entre los requerimientos del usuario y los requerimientos de esos dominios, estos modelos se complementan uno a otro. Mientras el modelo estructura muestra la arquitectura del CPS, el modelo meta muestra las relaciones del modelo estructura. El enfoque propuesto tiene para las siguientes contribuciones:

1) Ayuda a determinar los límites del sistema a través de la definición del modelo de estructura, y determinar el límite entre los dominios físicos y la dominios de software a través de la definición del modelo meta.

2) Se prepara el terreno para construir el modelo formal preciso y detallado del CPS. Los supuestos, requisitos dominios derivados proporcionan buenos materiales para la definición del modelo formal.

3) Ayuda a construir un entendimiento claro entre los usuarios y los diseñadores, ya que los modelos de estructura y metas son más fáciles de ser entendidos por los usuarios y el diseñador de los modelos formales.

MODELO ESTRUCTURA

Nosotros detallamos el modelo estructura e ilustramos mediante un ejemplo aplicado al control de manipuladores.

Control de manipuladores.- el sistema de control de brazos manipuladores son buenos ejemplos de sistemas cyberfisicos. Un control de manipulador consiste de varios controles discretos, el control de cada uno de las articulaciones. Los requerimientos del sistema de control son usualmente mantener la velocidad de una manera segura de los brazos. Para reunir los requerimientos el sistema de control del manipulador necesitamos setear los

sensores que monitorean el entorno y setear los controladores de los actuadores. En general el sistema de control de manipulador es complejo pero aquí nosotros tomamos una idea para ilustrarla.

El modelo estructura del CPS.- Un modelo estructura se compone de dominios y sus fenómenos compartidos como se ilustra en la figura N2. Los dominios son los diferentes componentes que constituyen el CPS. Estos dominios son dominios de software y dominios físicos, estos dominios tienen una estructura jerárquica, en el modelo estructura los diferentes dominios se relacionan a través de los fenómenos compartidos. El modelo estructura del control de un manipulador se muestra en la figura N3. El cual está compuesto por los siguientes dominios: manipulador bajo control, sistema de control, monitoreo de sensor, los dominios representados por el rectángulo son dominios físicos y los dominios representados por el rectángulo con doble línea vertical son dominios de software.

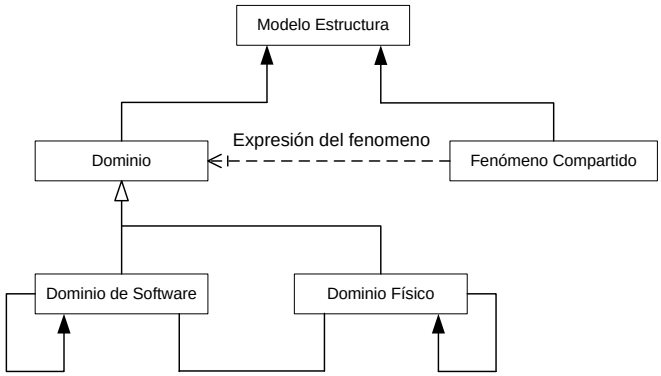

Figura N2. Modelo estructura del CPS

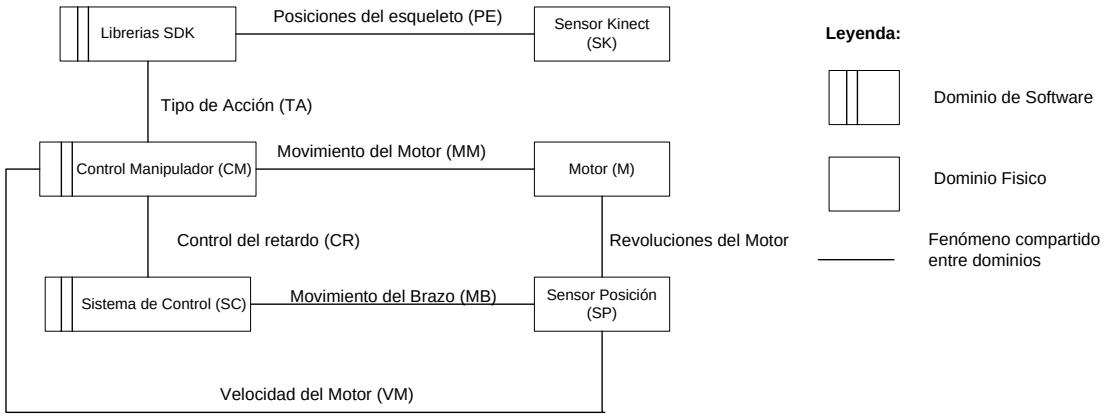

Figura N3. Modelo estructura de un sistema de control de un Manipulador

Dado que las aplicaciones de CPS son a menudo fiabilidad crítica y el mundo físico está lleno de incertidumbres, el CPS debe satisfacer esos requisitos estrictos de confiabilidad tales como los requisitos de seguridad, los requisitos de tiempo y los requisitos de adaptación

El trabajo relacionado en el control automático

Los algoritmos de estimación y control utilizados en CPS deben estar diseñados para satisfacer ciertos objetivos operacionales, tales como, la estabilidad en lazo cerrado, la seguridad, la vida de la conexión, o la optimización de una función de rendimiento [4].

Vamos a revisar cómo los objetivos de seguridad tradicionales de integridad, disponibilidad y confidencialidad pueden ser interpretados por CPS.

La integridad .- se refiere a la fiabilidad de los datos o recursos, la integridad en CPS se puede ver como la capacidad de mantener los objetivos operacionales de la prevención, detección, o sobrevivir a los ataques de engaño en la información enviada y recibida por los sensores, los controladores, y los actuadores.

La disponibilidad .- se refiere a la capacidad de un sistema de ser accesible y utilizable en la demanda. La falta de resultados sobre la disponibilidad de denegación de servicio (DoS). Si bien en la mayoría de los sistemas informáticos de un ataque DoS temporal no puede comprometer sus servicios, las fuertes restricciones de tiempo real de muchos sistemas ciber-físicos introducen nuevos desafíos. Por ejemplo, si un proceso físico fundamental es inestable en lazo abierto, un DoS en las mediciones del sensor puede hacer que el controlador incapaz de evitar daños irreparables en el sistema y entidades alrededor de ella.

La confidencialidad .-se refiere a la capacidad de mantener información secreta de usuarios no autorizados. A falta de confidencialidad resulta en la divulgación, una circunstancia o evento mediante el cual una entidad obtiene acceso a los datos para los que no está autorizado.

Una abstracción general de CPS puede verse en la figura N4. Sea ***y*** representan las mediciones de los sensores, y ***u*** las órdenes de control enviadas a los actuadores. Un controlador por lo general se puede dividir en dos componentes: un algoritmo de estimación para seguir el estado del sistema físico dado **y**, y el algoritmo de control que selecciona un comando de control ***u*** dada la estimación actual.

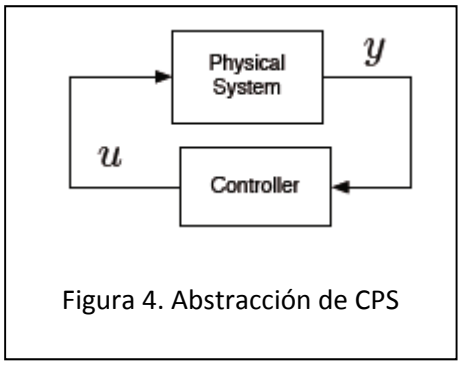

Figura 4. Abstracción de CPS

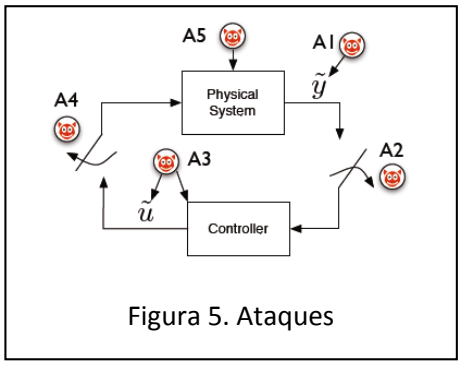

Figura 5. Ataques

Ataques a CPS (Fig. 5) se pueden resumir como sigue: A1 y A3 representan ataques de engaño, donde el adversario envía información falsa $\tilde{y} \neq y$ ó $\tilde{u} \neq u$ a partir de (uno o más) sensores o controladores. La falsa información puede incluir: una medición incorrecta, la hora incorrecta cuando se observó la medición, o el ID del remitente incorrecto. El adversario puede

lanzar estos ataques mediante la obtención de la clave secreta o por comprometer algunos sensores (A1) o controladores (A3).

A2 y A4 representan ataques DoS, donde el adversario evita que el controlador de recepción de las mediciones del sensor. Para lanzar un ataque DoS adversario puede atascar las vías de comunicación, dispositivos de compromiso y evitar que el envío de datos, atacar a los protocolos de enrutamiento, etc

A5 representa un ataque directo contra los actuadores o un ataque físico externo de la planta. Desde el punto de vista algorítmico no podemos dar soluciones a estos ataques (excepto detectarlos). Por lo tanto, importantes esfuerzos se deben colocar en la disuasión y la prevención del compromiso de actuadores y otros ataques directos contra el sistema físico, por ejemplo, la seguridad del sistema físico, cámaras de vigilancia, etc

La arquitectura de CPS en la figura. 1 indica un sistema distribuido espacialmente en el que el sistema, sensores, actuadores y controladores coordinan su funcionamiento a través de una red de comunicación para lograr algún objetivo de rendimiento. Un problema típico en la teoría de control es diseñar una política de control para asegurar que bajo el bucle de realimentación, un sistema inestable en lazo abierto se mantiene estable. La naturaleza de tales sistemas impone varias restricciones en el diseño de algoritmos de control. En primer lugar, las limitaciones impuestas por las redes de comunicación tales como la capacidad limitada, retardo aleatorio, pérdida de paquetes y la conectividad de red intermitente pueden causar denegación de servicio. Bajo Denegación de Servicio (DoS) el actuador puede dejar de recibir ciertos paquetes del controlador que son críticas para estabilizar un sistema inestable en lazo abierto. Como resultado, el sistema puede entrar en un estado del que podría ser imposible para estabilizarlo. Si el contenido de la información de los paquetes de medición y / o de control se ve comprometida, puede dar lugar a la aplicación de políticas de control incorrectos. Estos factores indican claramente la necesidad de incorporar características de la red en el diseño de algoritmos de control. Tales problemas se estudian en los sistemas de control en red robustos [13]. En segundo lugar, los sensores y actuadores son vulnerables al azar de fracasos. Para permitir el funcionamiento deseado en los modos de falla, tenemos que introducir redundancias apropiadas en la etapa de diseño.

sistemas de control de red robustos

Comenzamos considerando un escenario en el que el sistema y estimador remoto se comunican a través de una red de comunicación. El objetivo del estimador es generar estimaciones estatales recursivas basadas en mediciones enviadas por el sensor. Bajo perfecta comunicación no hay pérdida de datos y los paquetes llegan al estimador instantáneamente.

Bajo la integridad perfecta, los datos de medición no se vea comprometida. Para este caso ideal, el filtro de Kalman es el estimador óptimo. Recordemos el filtro de Kalman básico en la teoría de sistemas de tiempo discreto lineal

$$x_{k+1} = Ax_k + w_k \ , \quad y_k = Cx_k + v_k \qquad (1)$$

donde, $k \epsilon \mathbb{N}, x_{k,} w_k \in \mathbb{R}^n$ denotar el vector de estado y el ruido del estado, respectivamente, $y_k , v_k \in \mathbb{R}^p$ denotan el vector de salida y ruido de medición, respectivamente.

Cuantificación de robustez .- De una calidad de servicio (QoS) de punto de vista, cada yk medición cruda enviada a través de la red de comunicación puede no llegar al estimador de distancia. En particular, los paquetes pueden ser dejados cuando la red está congestionada. Aunque esta situación no es necesariamente contradictoria, su efecto es similar a un ataque DoS. Esto ha motivado a los investigadores a diseñar filtros de Kalman que tengan en cuenta la historia de pérdidas de paquetes. Dos modelos de pérdida de paquetes ampliamente utilizados son: el modelo de Bernoulli y el modelo de Gilbert-Elliot. El modelo de Bernoulli describe el proceso de pérdida de paquetes por variables aleatorias Bernoulli independientes y idénticamente distribuidas. El Modelo de Gilbert-Elliot considera que el estado de la red evoluciona de acuerdo a una cadena de Markov. Este modelo puede representar pérdidas de paquetes en ráfagas.

El aumento de robustez .- Un enfoque prometedor para diseñar algoritmos que son robustos al parámetro variaciones es el enfoque minimax o estimación robusta. Minimax se acerca para diseñar estimadores pueden ser vistos como un juego en el que el rendimiento del estimador depende de los elementos de un conjunto de estimadores y un conjunto incertidumbre que incluye el conjunto de posibles valores de los parámetros desconocidos pueden asumir. Ahora discutimos brevemente la idea principal detrás de minimax o estimación robusta.

Los componentes de CPS son vulnerables a fallos aleatorios y la degradación del servicio. En el área de control automático, detección de fallos y diagnóstico métodos (FDD) así como el control tolerante a fallos (FTC) diseños se han desarrollado con el fin de aumentar la fiabilidad y facilidad de mantenimiento de los sistemas propensos a fallas. El objetivo principal de un sistema de FTC es mantener la estabilidad y asegurar un nivel de rendimiento aceptable en condiciones normales de funcionamiento, así como en el mal funcionamiento de los componentes mediante el empleo de los despidos físicas y / o analíticos apropiados.

Enfoques del FTC se pueden clasificar en dos categorías: pasivos y activos. En el enfoque pasivo del FTC, un número limitado de configuraciones defectuosas se tienen en cuenta durante el diseño del controlador. Una vez diseñado, el controlador pasivo puede compensar las configuraciones previstas sin ningún esquema FDD o diseño de control reconfigurable. Así, en efecto, el enfoque pasivo FTC se puede ver como el diseño de control robusto para un número limitado de fallos.

Un sistema en enfoque activo de FTC, tiene cuatro componentes [5]: unidad FDD, mecanismo de reconfiguración, controlador reconfigurable y gobernador de referencia. La unidad FDD estima los parámetros de estado y de fallo del sistema en base a los datos de medición y control.

Los principales problemas en el diseño de los sistemas de la FTC activos son: (1) Diseño de RC, (2) esquemas FDD que son sensibles a los fallos y robusto para modelar las incertidumbres y las variaciones de las condiciones de funcionamiento, (3) mecanismo de reconfiguración de recuperar adecuadamente el desempeño normal de funcionamiento

Control para CPS: ¿Qué falta?

El campo de control automático es más maduro en comparación con la seguridad de la información; Sin embargo, a pesar de los grandes logros en el campo de la teoría de no linealidad, sistemas híbridos, control robusto, de teoría de juegos y el control tolerante a fallos, aún queda mucho por hacer para el diseño de algoritmos de control de seguridad para asegurarnos la supervivencia de CPS.

Tenemos que diseñar algoritmos de control y estimación robustas novedosos que se consideran modelos de ataque más realistas desde el punto de vista de la seguridad, estos modelos de ataque deben modelar el engaño y los ataques de denegación de servicio. Bajo la influencia de este tipo de ataques, estos algoritmos deben optimizar el rendimiento del peor caso. Además del estado del sistema a controlar, el estado de la red de comunicación debe ser estimado de forma conjunta. Enfoques para estimar los indicadores de calidad de servicio y la integridad de la red de comunicación basada en los datos disponibles de la red deben ser desarrollados. El estado estimado de la red se debe utilizar para el diseño de políticas de transmisión de los sensores e interruptores, así como las políticas de programación para los controladores para optimizar el rendimiento.

EL FUTURO CPS

En el CPS convergen dos realidades los sistemas cibernéticos y los sistemas físicos, el mundo está ante una amplia variedad de dispositivos inteligentes, como las etiquetas RFID, sensores y actuadores inteligentes, mucha nuevas tecnologías están dando lugar a la aparición de una infraestructura integrada y muy densa para el seguimiento del mundo físico, y por lo tanto, la recolección de información relacionada con los comportamientos de los usuarios, sus necesidades y la dinámica.

La gestión de una infraestructura tan compleja requiere el desarrollo de políticas eficaces y escalables para el manejo de la cooperación entre estos dispositivos y adaptar su comportamiento a los rápidos cambios físicos así como a los cambios debidos a la actividad actual social y mutua interacción, estos contextos son los que invocan los servicios digitales de acceso a la información y a las comunicaciones personales. El desarrollo de arquitecturas y políticas que sean capaces de adaptarse de forma autónoma los componentes en el mundo cibernético es un área importante de investigación [3].

Reconociendo la complejidad sin precedentes, desafíos críticos, y la importancia del impacto económico, técnico, social de los CPS, las revistas técnicas internacionales como la IEEE tendrán un capítulo especial en el futuro, en donde traerá diferentes sectores, incluyendo la aviación, automóvil, energía, medicina y fabricación, para poner de relieve los retos específicos de cada sector, en común, y las direcciones de investigación de CPS. El papel de las disciplinas académicas clave, incluyendo sensores, redes, comunicaciones, control, seguridad en los CPS, métodos, herramientas y las aplicaciones serán exploradas [1].

Debido a que el personal técnico de alta calidad deben ser capaces de trabajar en un ámbito multidisciplinar, los marcos actuales de educación y formación de la fuerza laboral no son suficientes para satisfacer estas necesidades, ya que los CPS unen múltiples disciplinas

académicas y exige por tanto la oferta de cursos que combinan, por ejemplo, la teoría del control y la informática de sistemas embebidos, ciencias de la computación con la ingeniería y la física.

Sistemas físicos cibernéticos no estará operando en un ambiente controlado, y deben ser robustos para condiciones inesperadas y adaptables. La cuestión, no es si el diseño del sistemas es robustos, sino más bien en qué nivel de construir en robustez. El principio de que tenemos que seguir es simple, componentes de cualquier nivel de abstracción se deben hacer predecible y fiable si esto es tecnológicamente factible, si no es tecnológicamente factible, entonces el siguiente nivel de abstracción por encima de estos componentes debe compensar con robustez [2].

Software predecible y fiable no elimina la necesidad de diseñar sistemas robustos, pero cambia dramáticamente la naturaleza del desafío, los sistemas operativos, lenguajes de programación, interfaces de usuario, y la creación de redes se han elaborado más y cada vez son mas amigables. Todos se han construido sobre una abstracción de software, donde el tiempo es irrelevante.

La próxima generación de sistemas ciber-físicos, plantea grandes desafíos en el diseño de software. No se trata sólo de diseñar un sistema en torno a los plazos de ejecución, lo más importante es maximizar la utilización de recursos. En este trabajo proponemos un sistema base para la arquitectura de software en el que los servicios, algoritmos controladores se puedan diseñar e implementar y componer fácilmente de acuerdo con la demanda, mediante aplicaciones individuales, de manera que satisfagan requisitos específicos de confianza, seguridad, eficiencia, confiabilidad y previsibilidad, mientras que permanecen dentro de la límites de las capacidades del hardware determinado [7].

CONCLUSIONES

Debido a la heterogeneidad del hardware, un sistema cibernético-físico puede abarcar múltiples dispositivos con diferentes arquitecturas. Tradicionalmente, la invocación de servicios ha involucrado complejos procedimientos de cálculo de referencias para el intercambio de datos entre plataformas de manera independiente de la arquitectura. Teniendo presente además, que para los servicios distribuidos es deseable un sistema unificado independiente del hardware.

Diseñar nuevos algoritmo de control seguros, proactivos y arquitecturas que son robustas frente a un modelo determinado que proporcionen límites de rendimiento demostrables, para entender los límites de la capacidad de recuperación de los algoritmos.

En el diseño de estos nuevos algoritmos tenemos que estudiar cómo los ataques afectan al rendimiento de los algoritmos de estimación y control y en última instancia, la forma en que afectan la incorporación de los modelos dinámicos de los sistemas que están monitoreados y controlados.

Bibliografía

[1] R. Poovendran, «Cyber 2013;Physical Systems: Close Encounters Between Two Parallel Worlds [Point of View],» *Proceedings of the IEEE,* vol. 98, nº 8, pp. 1363-1366, Aug 2010.

[2] E. Lee, «Cyber Physical Systems: Design Challenges,» de *Object Oriented Real-Time Distributed Computing (ISORC), 2008 11th IEEE International Symposium on*, 2008.

[3] M. Conti, S. K. Das, C. Bisdikian, M. Kumar, L. M. Ni, A. Passarella, G. Roussos, G. TrÃ¶ster, G. Tsudik y F. Zambonelli, «Looking ahead in pervasive computing: Challenges and opportunities in the era of cyberâ€“physical convergence,» *Pervasive and Mobile Computing ,* vol. 8, nº 1, pp. 2-21, 2012.

[4] C. Liu, W. Zhang, H. Zhao y Z. Jin, «Analyzing Early Requirements of Cyber-physical Systems through Structure and Goal Modeling,» de *Software Engineering Conference (APSEC, 2013 20th Asia-Pacific*, 2013.

[5] M. Szczodrak, Y. Yang, D. Cavalcanti y L. Carloni, «An open framework to deploy heterogeneous wireless testbeds for Cyber-Physical Systems,» de *Industrial Embedded Systems (SIES), 2013 8th IEEE International Symposium on*, 2013.

[6] G. Magureanu, M. Gavrilescu, D. Pescaru y I. Jian, «UML profile for Cyber-Physical System wireless communication specification,» de *Applied Computational Intelligence and Informatics (SACI), 2012 7th IEEE International Symposium on*, 2012.

[7] M. Gavrilescu, G. Magureanu, D. Pescaru y I. Jian, «Towards UML software models for Cyber Physical System applications,» de *Telecommunications Forum (TELFOR), 2012 20th*, 2012.

[8] P. Derler, E. Lee y A.-S. Vincentelli, «Modeling Cyber 2013;Physical Systems,» *Proceedings of the IEEE,* vol. 100, nº 1, pp. 13-28, Jan 2012.

[9] P. Fritzson, «Modelica 2014; A cyber-physical modeling language and the OpenModelica environment,» de *Wireless Communications and Mobile Computing Conference (IWCMC), 2011 7th International*, 2011.

[10] G. Magureanu, M. Gavrilescu, I. Tal, A. Toma, D. Pescaru y I. Jian, «Generating OMNeT++ specifications from UML models for PSoC distributed applications,» de *Applied Computational Intelligence and Informatics (SACI), 2011 6th IEEE International Symposium on*, 2011.

[11] J. S. Ting, «ARQUITECTURA DE SOFTWARE PARA LOS ACTUALES SISTEMAS CIBER-FÍSICOS,» 2011.

[12] E. Wang, Y. Ye, X. Xu, S. Yiu, L. C. K. Hui y K. Chow, «Security Issues and Challenges for Cyber Physical System,» de *Green Computing and Communications (GreenCom), 2010 IEEE/ACM Int'l Conference on Int'l Conference on Cyber, Physical and Social Computing (CPSCom)*, 2010.

[13] A. A. C. S. A. S. Sastry, «Secure Control: Towards Survivable Cyber-Physical Systems,» 2010.

[14] Y. Tan, M. C. Vuran y S. Goddard, «Spatio-Temporal Event Model for Cyber-Physical Systems,» de *Distributed Computing Systems Workshops, 2009. ICDCS Workshops '09. 29th IEEE International Conference on*, 2009.

[15] J. Huang, F. Bastani, I.-L. Yen, J. Dong, W. Zhang, F. J. Wang y H. J. Hsu, «Extending service model to build an effective service composition framework for cyber-physical systems,» de *Service-Oriented Computing and Applications (SOCA), 2009 IEEE International Conference on*, 2009.

[16] J. Lin, S. Sedigh y A. Miller, «A General Framework for Quantitative Modeling of Dependability in Cyber-Physical Systems: A Proposal for Doctoral Research,» de *Computer Software and Applications Conference, 2009. COMPSAC '09. 33rd Annual IEEE International*, 2009.

[17] L. Schenato, B. Sinopoli, M. Franceschetti, K. Poolla y S. Sastry, «Foundations of Control and Estimation Over Lossy Networks,» *Proceedings of the IEEE,* vol. 95, nº 1, pp. 163-187, Jan 2007.

[18] E. A. Lee, «Computing Foundations and Practice for Cyber-Physical Systems: A Preliminary Report,» 2007.

[19] J. Hespanha, P. Naghshtabrizi y Y. Xu, «A Survey of Recent Results in Networked Control Systems,» *Proceedings of the IEEE,* vol. 95, nº 1, pp. 138-162, Jan 2007.

[20] J. Eker, J. Janneck, E. Lee, J. Liu, X. Liu, J. Ludvig, S. Neuendorffer, S. Sachs y Y. Xiong, «Taming heterogeneity - the Ptolemy approach,» *Proceedings of the IEEE,* vol. 91, nº 1, pp. 127-144, Jan 2003.