Pruebas de Seguridad y Fiabilidad en Sistemas de Multilateración CNS/ATM basados en Riesgos Operacionales.

Availability and Reliability Test on Multilateration CNS/ATM System based on Operational Risk.

Guillermo Brito Acuña

Empresa Cubana de Navegación Aérea (ECNA). La Habana. Cuba.

Resumen

Este artículo presenta los resultados obtenidos de la aplicación del módulo "Pruebas de Sistemas" sección de la tesis "Marco de Trabajo para la Gestión de Riesgos en Infraestructuras Críticas"; aplicado durante la etapa de verificación y validación en sistemas de multilateración en varios aeródromos. Estos sistemas son considerados críticos para la gestión del tráfico aéreo dado que permiten determinar la posición exacta de las aeronaves en tiempo real con alta precisión. El artículo identifica limitantes en los marcos de trabajo para la protección de infraestructuras críticas y métodos para aumentar seguridad, fiabilidad y calidad en estos sistemas. Explica la concepción del método utilizado para garantizar la disminución de los riesgos y documenta los resultados obtenidos de la aplicación del módulo "Pruebas de Sistemas" en sistemas de multilateración en su fase de prueba y certificación, lo cual aumenta la seguridad y la fiabilidad en la infraestructura crítica que lo implementa.

Palabras clave: Gestión de Riesgos Preventivos, Seguridad en Infraestructuras Críticas, Gestión de Riesgos en el Desarrollo de Sistemas, Pruebas de Multilateración, Pruebas basadas en riesgos.

Abstract

This article presents the results from the application of the module "Systems Tests", a section of the master´s thesis "Risk Management Framework on Critical Infrastructure", which was applied during the verification and validation phases in multilateration systems in several aerodromes. These systems are critical for Air Traffic Management because they allow determining the exact real time position of aircrafts with high precision. This article also identifies the frameworks limits for the protection of critical infrastructures and methods for security, safety and quality enhancement in these systems. Furthermore it explains the concept of the method used to guarantee risk reduction and document the results of the application of the module "Systems Tests" in multilateration systems during test and certification phases. This raises safety and security in the critical infrastructure that use this module.

Keywords: Preventive Risk Management, Assurance in Critical Infrastructure, Risk Management by Systems Development, Multilateration Test, Risk based Tests.

Introducción

Las infraestructuras críticas son aquellas instalaciones, redes y tecnologías, cuya interrupción puede tener una repercusión importante en la salud, la economía o el eficaz funcionamiento de los gobiernos (Moteff, Copeland, & Fischer, 2003). Estas soportan servicios vitales en infraestructuras consideradas de alta fiabilidad y seguridad (McGregor & Silva, 2017). En ellos se evidencia que las amenazas informáticas no sólo comprometen el mundo digital, sino que también son un riesgo mayor para el mundo físico (Clark & Hakim, 2017). Estas infraestructuras críticas se encuentran en sectores como el energético, el nuclear, el aeroespacial y la aeronavegación (Moteff, et al., 2003). Para garantizar su seguridad se utilizan principalmente la auditoría de la red para eliminar posibles brechas de seguridad, el aislamiento de la red o el bloqueo de intrusión por medio de cortafuegos; y fortalecer la seguridad de los terminales desconectando servicios innecesarios del sistema operativo, el análisis y resolución de errores de los sistemas operativos y el uso de antivirus (Stergiopoulos, 2016).

Estos métodos no siempre incluyen gestión de interrupciones en las infraestructuras, aun cuando es evidente el impacto que tiene en la seguridad de la misma. En el artículo "Consideraciones sobre el desarrollo en infraestructuras críticas, software de seguridad o sistemas críticos" (Guillermo Brito Acuña, 2016a).

La literatura especializada en el tema recomienda varias formas de tratar estas situaciones que pueden atentar contra la seguridad de las infraestructuras. Estas se pueden resumir como normas para la gestión de riesgo (ISO, 2015a), modelos para el desarrollo de sistemas en estas infraestructuras (Guillermo Brito Acuña, 2016b), normas para los sistemas de gestión de la seguridad informática o de la información (ISO, 2015b), y marcos de trabajo para la seguridad en las infraestructuras (Guillermo Brito Acuña, 2017; Technology, 2014). Estas fueron analizadas y de ellas se utilizaron las medidas y buenas prácticas para el dominio en cuestión, que fueron aplicados en el desarrollo de esta investigación. Luego se documentan los principios básicos a emplear para disminuir las afectaciones de seguridad o disponibilidad en cualquier infraestructura. Además, se describió el cuasi experimento realizado sobre la infraestructura crítica CNS/ATM cubana y las mediciones y mejoras obtenidas a partir de su implementación.

Materiales y métodos

Las infraestructuras críticas CNS/ATM (Communication Navigation Surveillance / Air Traffic Management, Comunicación, Navegación, Vigilancia / Gestión del Tráfico Aéreo) conocidas también como de aeronavegación son sistemas críticos para la aeronavegación, entre cuyas funciones se encuentran: garantizar las comunicaciones, mensajería y gestión del espacio aéreo. Estas emplean tecnologías digitales, incluyendo sistemas de satélites y radares c (J. T. FORCE & INITIATIVE, 2010; J. T. I. FORCE, TRANSFORMATION, 2013; ISO, 2015b; Stouffer, Falco, & Scarfone, 2011) con diversos niveles de automatización, aplicados como apoyo de un sistema imperceptible de gestión del tráfico aéreo global(OACI, 2013). Para garantizar esto la OACI reconoce en (Anexo, 2010) como crítico: a) Servicio de gestión y monitoreo a equipamiento aeronáutico y de comunicaciones, b) Servicio de hora centralizada para las aplicaciones aeronáuticas, c) Servicio de información de vuelo, d) Servicio de transmisión de información Radar, e) Soporte de comunicaciones de la Red de Radares del país. Todas estas son soluciones adoptadas por países y líneas aéreas con el fin de garantizar los servicios que soportan la aeronavegación de forma eficiente y segura.

Vinculada con todos estos sistemas está la multilateración, conocida como posicionamiento hiperbólico o método diferencial telemétrico, es el proceso de localizar un objeto con precisión, realizando la medición de la diferencia de tiempo de arribo de una señal emitida desde un objeto a tres o más receptores(OACI, 2007). Esto, mediante múltiples interrogadores o receptores, es útil para el control de superficie en los aeropuertos y para el control de área amplia en los diferentes espacios aéreos. Brinda además potencialidades respecto al intercambio de información tierra aire (MORENO QUINTANA, 2017).

Estas prestaciones potencian la seguridad operacional, permitiendo obtener información meteorológica o de aeródromo al necesitarlo. Esta tecnología está vinculada a la exactitud y la cobertura que se logre con los elementos de dichos sistemas, pero trae consigo una serie de riesgos tecnológicos, relacionados con mantener estos indicadores de calidad ante fallos técnicos de los receptores u otros equipamientos o canales de datos. Los métodos conocidos para garantizar la seguridad en estas infraestructuras (J. T. FORCE & INITIATIVE, 2010; J. T. I. FORCE, TRANSFORMATION, 2013; ISO, 2015b) no incluyen la protección en sistemas específicos o la gestión de riesgo en el desarrollo de software.

Para ello los diferentes organismos y organizaciones internacionales han incorporado indicaciones específicas, tal es el caso de Hardware (Eurocae, 2000), equipamientos específicos como la multilateración (Eurocae, 2003), en sistemas (RTCA, 2012) o en software (Eurocae, 2012b), que a su vez pueden subdividirse en suplemento de los mismos (Eurocae, 2012a). Esto demuestra una gran sectorización e implica gran complejidad para validar adecuación funcional y seguridad en campos interrelacionados. Estos sistemas están cada vez más difundidos en proyectos desarrollados para infraestructuras críticas.

Resultados y discusión

Como parte de la investigación Marco de trabajo para la gestión de riesgos en infraestructuras críticas, se previó un módulo dedicado específicamente a la especificación de pruebas en software y sistemas. Mediante este se pretende compatibilizar los nuevos sistemas desarrollados con el ecosistema existente.

Sobre la base de recomendaciones de muchos de los estándares, al comenzar se realiza una evaluación de la seguridad del sistema. El efecto de un fallo sobre el funcionamiento total del mismo se evalúa, se estudia y se analiza, clasificándolo en niveles de criticidad. Las categorías de evaluación son: a) Catastrófico, cuando el impacto de este riesgo implica muerte, múltiples lesiones graves, pérdida económica y de prestigio muy elevada. b) Severo, cuando existen daños estructurales y pocas lesiones graves. c) Mayores, pérdida de eficiencia o lesiones menores. d) Menores, reducción de los índices de seguridad dentro de las capacidades del personal y e) Sin Implicaciones.

Para el caso del sistema de multilateración se identificaron como datos críticos, la cobertura y la precisión del sistema. Se consideró de nivel de criticidad Mayor, producto que la pérdida de este, podría producir una afectación en los índices de seguridad operacional al poner aeronaves bajo los mínimos de distancia permitidos.

Luego se identifican los estándares y buenas prácticas que definen estos sistemas y sus componentes. En el caso que se documenta en este artículo intervienen resoluciones de la OACI y del país en cuanto a seguridad tecnológica y de telecomunicaciones. Intervienen también las asociadas a equipamiento de protección contra descargas eléctricas y aterramientos, calidad del equipamiento hardware, niveles de certificación de los software y estándares propios del tema a verificar: como los ED-117(Eurocae, 2003) para multilateración y control de superficie, y ED 142 para la multilateración en área amplia WAM (Eurocae, 2010).

Luego se identifican los requerimientos primarios de cada uno de los componentes de la arquitectura o sus estándares y si alguno de ellos responde a otro estándar. En el caso que se presenta, se identificaron precisiones sobre el modo ADS-B y sus requerimientos. Los requerimientos serán rastreables desde el diseño hasta las pruebas que se realizarán para demostrar adecuación multidisciplinaria. Para el diseño de las pruebas el autor considera útil las pruebas basadas en historias de usuario, para validar múltiples requerimientos funcionales y pruebas basadas en casos de prueba para detectar las vulnerabilidades.

Estas últimas deben realizarse con mayor o menor profundidad atendiendo al grado de criticidad que tenga el sistema. En el cuasi experimento realizado en los sistemas de multilateración de muestra utilizados, se determinaron pruebas asociadas a distintos frentes, tal es el caso de pruebas de adecuación a la legalidad y a los procesos de certificación de los sistemas que lo componen, hasta las órdenes de trabajo, calidad de los requerimientos, análisis de riesgo, plan de despliegue y políticas de mantenimiento.

Las pruebas operacionales y de seguridad se realizaron en una red paralela independiente a la utilizada para las operaciones realizadas, interpretándose esta sectorización por vlan como un entorno controlado de pruebas. Se analizan los requisitos y requerimientos establecidos por el fabricante o diseñador de los productos para garantizar que el equipamiento o concepción del sistema no incumpla con ellos, comprometiendo así la garantía y las prestaciones del mismo.

Para las pruebas de seguridad, se interpretó la cobertura como parte de la disponibilidad del sistema, ya que esta última es dependiente de la cantidad de repetidores activos que capten la señal ADS-B o MLAT de las aeronaves. En el experimento también se verificó la fiabilidad mediante la comprobación de la tolerancia a fallo del sistema, el tratamiento de errores y que la disponibilidad del mismo se comportara de forma adecuada según el requerimiento de lograr 100 % de cobertura incluso cuando fallen 2 repeti-

dores en cualquier parte del aeródromo o de la WAM. Para ello se desplegó una serie de respondedores en diferentes puntos del área geográfica y se apagaron los diferentes respondedores e interrogadores, lo cual permitió establecer el área donde se mantiene la disponibilidad cuando los respondedores están de baja. Otro experimento con respecto a la disponibilidad se realizó estableciendo un área donde, al mover los respondedores, no se viera afectada la cobertura, por cada respondedor y se estableció una gráfica determinando los límites de movilidad ante el fallo de varios repetidores.

La fiabilidad se vinculó con la precisión, mediante su característica de madurez, o sea, capacidad del sistema para satisfacer las necesidades para desempeñar las funciones especificadas, cuando se usa bajo unas condiciones y periodo de tiempo determinados. Como variante del experimento anteriormente descrito se comprobó también la variación de la precisión ante las mismas condiciones. Las mediciones de acuerdo a las métricas establecidas en ED-117(Eurocae, 2003) y ED 142 (Eurocae, 2010) obteniendo una exactitud con una falla menor de 7.5 metros.

Se realizaron pruebas de eficacia en el desempeño y estrés de dispositivos con más carga de acuerdo a la estrategia de prueba/criticidad diseñada. Estos múltiples cuasi experimentos fueron validando, a su vez, la adecuación funcional del sistema y su usabilidad. Con el objetivo de compatibilizar con otros sistemas del ecosistema y la protección de los mismos, se realizaron verificaciones, pruebas de compatibilidad y calidad del hardware, el software y los medios de intercambio y almacenamiento de la información. Para la valoración de la posición de los repetidores y respondedores se tuvieron en cuenta las características físicas en el terreno, aterramiento, dispersores, ventilación, existencia de los canales de datos, coaxiales o inalámbricos, y la posibilidad de amenazas de ataque sobre ellos.

Se analizó la política e implementación de los servidores y sus trazas. Se comprobó la integración de los mismos con el ecosistema de representación radar de vigilancia al que complementa, demostrándose el aumento de cobertura en algunas regiones. Se analizaron también los riesgos introducidos por comunicarse con otras aplicaciones que permiten utilizar su señal para otras prestaciones. Tal es el caso de la gestión del tráfico dentro del aeródromo y como apoyo a la atención de riesgos e incidentes en tiempo real. Se realizó una comparación de los datos procesados del radar con los datos procesados en los servidores de multilateración en cuanto a cobertura y precisión de esta información. Para ello se analizaron datos de un mes completo, obteniéndose como resultado una mejora de la cobertura sobre áreas que, por su situación geográfica o ángulo respecto a los radares, no tenían la cobertura apropiada. Los análisis de exactitud tuvieron un nivel de equivalencia con el previsto superior al 99 % en cada prueba.

Conclusiones

A partir del análisis de los resultados de las pruebas realizadas se mitigó una serie de riesgos que fueron detectados. Se previeron problemáticas con la integración del ecosistema, la seguridad recomendada en los enlaces de datos inalámbricos, y se identificaron riesgos operacionales y tecnológicos en cuestiones de aterramientos.

Mediante la aplicación del módulo de pruebas de sistemas, se logró un método multidisciplinario y colaborativo que conduce a la gestión de riesgos a la infraestructura de forma preventiva, predictiva

y correctiva. Demuestra la posibilidad de detectar problemáticas en campos diametralmente opuestos mediante la implementación de pruebas con historias comunes. Demostró también la aplicabilidad del módulo de pruebas de sistemas a componentes y equipamiento no dependientes del software, sino del hardware. Esta metodología para pruebas potencia la disminución de recursos y personal especializado para la certificación propia de proyectos en infraestructuras críticas.

Referencias

Acuña, G. B. (2016a). Consideraciones sobre el desarrollo en infraestructuras críticas y software de seguridad. Serie Científica de la Universidad de las Ciencias Informáticas, 9(5), 33-42.

Acuña, G. B. (2016b). MODELO W, APLICACIÓN PARA EL DESARROLLO Y CERTIFICACIÓN DE SOFTWARE CRÍTICOS CNS/ATM SEGÚN ESTÁNDAR DO-178. RCCI.

Acuña, G. B. (2017). Marco de Trabajo para la Gestión de Riesgos en Infraestructuras Críticas. www.informaticahabana.cu/node/4213 retrieved from

Anexo, O. (2010). 10-Telecomunicaciones Aeronáuticas. Canadá, 2010. Vol. 1.565 pp: ISBN 92-9194-778.

Clark, R. M., & Hakim, S. (2017). Protecting Critical Infrastructure at the State, Provincial, and Local Level: Issues in Cyber-Physical Security Cyber-Physical Security (pp. 1-17): Springer.

Eurocae. (2000). ED 80 /RTCA 254, Design Assurance Guidance for Airborne Electronic Hardware.

ED 117, MINIMUM OPERATIONAL PERFORMANCE SPECIFICATION FOR MODE S MULTILATERATION SYSTEMS FOR USE IN ADVANCED SURFACE MOVEMENT GUIDANCE AND CONTROL SYSTEMS (2003).

Eurocae. (2010). TECHNICAL SPECIFICATION FOR WIDE AREA MULTILATERATION (WAM) SYSTEMS.

Eurocae. (2012a). ED-217, Object-oriented technology and related techniques supplement to ed-12c and ed-109a.

Eurocae. (2012b). Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management.

FORCE, J. T., & INITIATIVE, T. (2010). Guide for applying the risk management framework to federal information systems NIST special publication (Vol. 800, pp. 37).

FORCE, J. T. I., TRANSFORMATION. (2013). Security and privacy controls for federal information systems and organizations NIST special publication (Vol. 800, pp. 8-13).

ISO. (2015a). ISO/NC 31000 Gestión de Riesgo - Principios y Directrices Oficina Nacional de Normalización, La Habana, Cuba, .

ISO. (2015b). SO/IEC 27001 Information technology – Security techniques - Information security management system - Requirements International Organiation for Standardization, Geneva, Switzerland.

McGregor, J. D., & Silva, R. S. (2017). Building Safety-Critical Systems Through Architecture-Based Systematic Reuse. Paper presented at the Mastering Scale and Complexity in Software Reuse: 16th International Conference on Software Reuse, ICSR 2017, Salvador, Brazil, May 29-31, 2017, Proceedings.

MORENO QUINTANA, V. (2017). Desarrollo de un simulador de sistemas de multilateración para vigilancia aérea en TMA.

Moteff, J., Copeland, C., & Fischer, J. (2003). Critical infrastructures: What makes an infrastructure critical?

"Multilateration (MLAT) Concept of use". (2007).

Doc 9859 - Manual de gestión de la seguridad operacional (2013).

RTCA. (2012). DO-178C, Software Considerations in Airborne Systems and Equipment Certification.

Stergiopoulos, G. (2016). Critical Infrastructure Protection tools: Classification and comparison. . Paper presented at the En Proc. of the 10th International Conference on Critical Infrastructure Protection.

Stouffer, K., Falco, J., & Scarfone, K. (2011). Guide to industrial control systems (ICS) security NIST special publication (Vol. 800, pp. 16-16).

Technology, N. I. o. S. (2014). Framework for Improving Critical Infrastructure Cybersecurity SP-800 53.