Revista Innovación y Software
Vol. 3, No. 2, Mes Septiembre-Febrero, 2022
ISSN: 2708-0935
Pág. 132-139
https://revistas.ulasalle.edu.pe/innosoft

Tipo de artículo: Artículos originales
Temática: Gestión de software
Recibido: 18/07/2022 | Aceptado: 02/09/2022 | Publicado: 30/09/2022

Identificadores persistentes:
ARK: ark:/42411/s9/a73
PURL: 42411/s9/a73

Gestión de riesgos para el desarrollo de proyectos de sistemas críticos

Risk management for the development of critical systems projects

Guillermo José Aleman Zambrano[1][0000-0001-5471-4226], Marvik Irzovic Del Carpio Lazo[2][0000-0002-0019-2458], Daniel Gustavo Mendiguri Chávez[3][0000-0002-0588-6520], Daniela Carolina Vílchez Silva[4][0000-0002-7896-8228]

[1] Universidad La Salle. Arequipa, Perú. galemanz@ulasalle.edu.pe
[2] Universidad La Salle. Arequipa, Perú. mdelcarpiol@ulasalle.edu.pe
[3] Universidad La Salle. Arequipa, Perú. dmendiguric@ulasalle.edu.pe
[4] Universidad La Salle. Arequipa, Perú. dvilchezs@ulasalle.edu.pe

[*] Autor para correspondencia: galemanz@ulasalle.edu.pe

Resumen

Hoy en día podemos encontrar distintos sistemas críticos en diferentes campos como en la salud, militar, espacial, seguridad, etc., dónde peligra la vida y economía de muchas personas debido a las consecuencias que pueden surgir de alguna falla en estos sistemas. Por ello es importante identificar, analizar y tratar los riesgos relacionados a los proyectos de sistemas críticos, procesos típicos de la gestión de riesgos. En este artículo mostramos y analizamos distintas técnicas y modelos aplicados en diferentes ámbitos como la medicina y el campo militar, reconociendo conceptos y similitudes sobre los sistemas críticos y la gestión de riesgos. Finalmente determinando que no existen metodologías definidas para la gestión de riesgos en estos sistemas, siendo en muchos casos necesaria la aplicación de opciones hibridas y dinámicas.

Palabras clave: *Gestión de riesgos, Riesgos, Sistemas críticos, Software*.

Abstract

Today we can find different critical systems in different fields such as health, military, space, security, etc., where the lives and economy of many people are in danger due to the consequences that may arise from a failure in these systems. For this reason, it is essential to identify, analyze and treat the risks related to critical systems projects and typical risk management processes. In this article, we show and explore different techniques and models applied in different environments, such as medicine and the military field, recognizing concepts and similarities in critical systems and risk management. Finally, determining that there are no defined methodologies for risk management in these systems, in many cases necessary to apply hybrid and dynamic options.

Keywords: *Critical Systems, Risks, Risk Managment, Software.*

Revista Innovación y Software
Vol. 3, No. 2, Mes Septiembre-Febrero, 2022
ISSN: 2708-0935
Pág. 132-139
https://revistas.ulasalle.edu.pe/innosoft

Introducción

Los sistemas críticos son aquellos en los que un error podría llegar a significar pérdidas económicas de gran tamaño, daños al medio ambiente, ocasionar daños físicos o amenazar la vida. Muchos sistemas de información modernos están llegando a ser críticos para la seguridad en un sentido general porque pueden producirse pérdidas financieras e incluso la pérdida de vidas debido a su falla. Los futuros sistemas críticos para la seguridad serán más comunes y poderosos [1]. En pocas palabras para entender que es un sistema crítico debemos enfocarnos en sus consecuencias, si la falla de un sistema puede tener consecuencias que se consideran inaceptables, entonces el sistema es crítico para la seguridad. En esencia, un sistema es crítico para la seguridad cuando dependemos de él para nuestro bienestar [1]. También se considera que algunos subsistemas que conforman el sistema crítico pueden llegar a ser considerados sistemas críticos dependiendo de las consecuencias provocadas por su falla.

Estos sistemas los podemos encontrar en el campo militar [2], médico [3], espacial [4], seguridad [5] y entre otros [1], al contar con consecuencias graves es importante aplicar una gestión de riesgos a este tipo de proyectos, para así determinar el alcance de los daños y los controles que se aplicarán para disminuir o eliminarlos.

Para poder mitigar los riesgos en diferentes sistemas, se aplica un concepto de sistema superviviente, el cual consiste en asegurar la confiabilidad del software a través de una alta disponibilidad de sus servicios, de forma tal que sean siempre por lo menos óptimo. Así un sistema crítico superviviente puede dar la seguridad de continuar incluso en caso de fallas, dentro del sistema global. Esto se logra dando prioridad a los subsistemas que hacen critico a todo el sistema, sacrificando al resto de subsistemas cuando sea necesario [7]. Así hacer que un sistema crítico puede aplicarse a los distintos ámbitos de clasificación de sistemas críticos.

Los pueden ser clasificados por Tradicionales y no tradicionales. Los primeros sistemas críticos incluyen la atención médica, los aviones comerciales, la energía nuclear y los armas. La falla en estas áreas puede conducir rápidamente a que la vida humana se ponga en peligro, la pérdida de equipos, etc. [1] Los segundos son aquellos sistemas que a simple vista no son sistemas críticos, pero podrían llegar a serlo si su falla se prolonga o sus consecuencias escalan [1]. Un ejemplo que [1] muestra es la pérdida del sistema telefónico que a simple vista no puede causar la muerte de personas. Pero una pérdida prolongada del servicio 911 sin duda resultará en lesiones graves o la muerte. El servicio de

emergencia 911 es un ejemplo de una aplicación de infraestructura crítica. Otros ejemplos son el control del transporte, los sistemas bancarios y financieros, generación y distribución, telecomunicaciones y la gestión de los sistemas de agua.

Una mala planificación de la gestión de riesgos dentro de la elaboración del proyecto implicaría fallas que, si se llegan a lanzar a producción, llegaría así a ser contraproducente para la empresa y en caso de no llegarse a culminar el proyecto implicaría grandes pérdidas por la inversión que implican el desarrollo de proyectos orientados a sistemas críticos. Existen varios ejemplos de fallas en sistemas críticos que han ocurrido, incluidos la falla de la cuenta regresiva del transbordador espacial en el primer lanzamiento, la falla del lanzamiento del Ariane V/5 [8] y las pérdidas del Mars Polar Lander [9] y el Mars Climate Orbiter [10]. Podemos encontrar otros ejemplos documentados en el texto de Neumann [11] que analiza una gran colección de problemas experimentados a lo largo del tiempo y proporciona ideas que pueden ser útiles para evitar tales consecuencias en el futuro.

Para el PMBOK [6] del Project Management Institute el riesgo es un evento o condición incierta que sí ocurre, tendrá un efecto positivo o negativo en los objetivos del proyecto. De aquí la necesidad de su gestión para promover las ventajas o mitigar las desventajas que estén relacionadas a cada riesgo que se puede identificar. Una buena gestión de estos asegura que los recursos empleados en el proyecto tengan un alto rendimiento sobre el logro de los objetivos planteados para el desarrollo.

Entonces al existir diversidad de riesgos a identificar, su clasificación es parte importante para una correcta gestión, es así que este trabajo evalúa las técnicas aplicadas a la gestión de riesgos en distintos campos donde se desarrolla proyectos orientados a sistemas críticos.

Materiales y métodos o Metodología computacional

Esta investigación se basó en una metodología descriptiva, basándonos en los sistemas críticos y sus aplicaciones como objeto de estudio mismo. El documento se estructura en dos secciones base para finalizar en la conclusión. La primera parte consiste en la recopilación de información sobre sistemas críticos en diversos ámbitos como la medicina, las aplicaciones militares, los usos en el transporte, y sistemas ciber físicos en general que permiten el control del entorno real a través de la administración de mecanismos controlados por software.
La segunda parte consiste en la abstracción de los conocimientos adquiridos y la comparación de estos para mostrar los resultados obtenidos. Logrando esto a través del consenso de ideas entre los distintos autores, y la identificación de sus diferencias clave, que contribuyen al enriquecimiento de ideas sobre el tema.

Finalmente se explican las conclusiones consecuencia de la información y abstracción del conocimiento de las dos primeras partes. Comparando previamente resultados y propuestas de las aplicaciones de los sistemas críticos estudiados.

Resultados y discusión

Luego de la realizar una ardua investigación pudimos observar que en el campo de la medicina encontramos un ejemplo de proyecto [12] que tiene como objetivo analizar la aplicación de la metodología FMEA (Análisis de Modos de Falla y Efectos) y sus efectos de mejora en un sistema médico para distribución de medicamentos.

> *FMEA es un proceso de mejora de la calidad que se concentra en el sistema general en un entorno en lugar de asignar todos los errores al error humano. Esta técnica divide un proceso determinado, como un sistema de distribución y administración de medicamentos, en pequeños pasos. Los métodos de aseguramiento de la calidad utilizados en otras industrias, como sacrificar un porcentaje de un lote de producto para la prueba, no se pueden aplicar en situaciones de administración de medicamentos que involucran a seres humanos. El objetivo de FMEA es utilizar la experiencia de las personas en el campo para evaluar un sistema y anticipar las posibles formas en que puede fallar. Una vez que se han establecido los modos y mecanismos de falla básicos, se clasifica la importancia relativa de cada uno para el sistema general [12].*

El caso de estudio se realizó en el Hospital Sir Charles Gairdner [12] y para aplicar la técnica se instauró un observador farmaceuta, quien era encargado de registrar todos los hallazgos de las áreas del proceso involucradas en el sistema de suministro de medicamentos. con estos hallazgos se detectaron los riesgos y fallas junto a su área perteneciente. Además, gracias a la técnica se pudo determinar la tasa y los tipos de errores de medicación que ocurrían en el sistema de existencias del hospital. Las posibles fallas se identificaron prediciendo qué acciones incorrectas podría realizar una persona, cuáles podrían ser los resultados de esas acciones incorrectas y cómo se podrían prevenir las acciones incorrectas, gracias esto se identificó las deficiencias del sistema y desencadenó a desarrollar un nuevo sistema. En cuanto a los resultados "*El análisis del sistema de administración y distribución de medicamentos identificó 12 fallas del sistema. Se eliminaron o redujeron una serie de posibles errores de medicación al pasar del sistema de existencias*

de la sala al nuevo sistema. Las limitaciones del estudio incluyen el hecho de que menos del 100% de las enfermeras se ofrecieron como voluntarias para ser observadas durante el estudio" [12].

Se observa que la técnica aplicada demanda la atención e intervención de una persona, ya que al ser parte de un sistema crítico no podemos aplicar técnicas débiles para el análisis e identificación de riesgos, porque cualquier error desencadenaría consecuencias graves. Para el caso de estudio los resultados de la aplicación de FMEA obtuvieron nuevos requisitos y mejoras que lo llevaron a desarrollar un nuevo y mejorado sistema.

Otra aplicación con respecto al campo de medicina en la gestión de riesgos fue encontrada en el campo de Internet de las Cosas Médicas (IoMT), con una interconexión de dispositivos médicos [13]. Debido a la naturaleza del campo y a que los dispositivos IoMT se conectan a sistemas para su comunicación e integración, esto los vuelve parte de sistemas críticos. Además, estos sistemas manejan una gran data y están estrechamente relacionados con pacientes por lo que desencadenaría consecuencias desastrosas. Se utiliza una matriz de Severidad-Probabilidad que permite detectar los fallos gráficamente, cruzando ambos criterios para determinar si el riesgo es aceptable, razonablemente práctico-tolerable, e intolerable [13].
Demostrando que aplicar estos criterios mejora la confiabilidad de sus sistemas, ya que esta demanda un alto nivel de seguridad, al estar inmersa en las redes es vulnerable a una gran cantidad de ataques. Claramente se ve la necesidad e importancia de una gestión de riesgos en este campo de la tecnología.

En el campo militar [2] encontramos un ejemplo de proyecto que tiene como objetivo el poder reconocer todos los posibles riesgos que podrían presentarse en el software de aeronaves militares y en este caso utilizaron Software Hazard Analysis (SWHA) esta metodología se centra en la identificación de los riesgos asociados con el diseño en el que se evaluarán restricciones operativas para mejorar aún más los requisitos de diseño y los esfuerzos de prueba para el software crítico para la seguridad, en conclusión el SWHA es esencialmente un análisis de requisitos de seguridad, el SWHA utiliza un índice de riesgo de software el cual sirve como una guía para la ingeniería de seguridad, el proceso de desarrollo e integridad y la gestión de programa que otorgan la cantidad adecuada de esfuerzo para garantizar la seguridad del sistema, también utiliza la evaluación de riesgo, esta nos indica el nivel de gravedad del percance dentro del contexto del sistema y de la organización, para ello se utiliza la tabla de condición de falla donde se categoriza la gravedad de los accidentes por catastróficas, criticas, marginales y negligentes, la siguiente clasificación es la control de software esta nos muestra la condición en la que se encuentra por cuatro niveles, el primer nivel nos indica que la

falla ante la prevención de un evento nos podría conducir directamente a un peligro, el nivel dos se divide por en dos, primero nos dice que se debe dar tempo para la intervención de un sistema de seguridad independiente para mitigar el peligro para luego tener una acción inmediata para mitigar el peligro, el nivel tres indica que se necesita de una acción humana para completar la función de control para luego con ayuda del sistema que genera información crítica poder tomar una decisión y por último el nivel cuatro el cual es el que muestra mayor independencia e indica que el software directamente no controla el sistema crítico y no proporciona información que nos ayude a tomar decisiones por ende el sistema es totalmente independiente al riesgo, estas dos tablas son fundamentales para generar la matriz del índice de riesgos de software, gracias a este análisis se pudieron encontrar las fallas y poder generar una correcta clasificación de riesgos.

También pudimos observar que en el artículo [5] se plantean diversas opciones para la gestión de riesgos en sistemas ciber físicos (CPS), estos son sistemas inteligentes que incluyen redes de interacción diseñadas de componentes físicos y computacionales, en otras palabras, en un mecanismo (sistema físico) controlado o monitorizado por algoritmos basados en computación y que a menudo el intercambio de datos lo realizan por medio de internet en tiempo real. Ejemplos de sistemas ciber físicos serían los famosos IOT o Internet de las cosas. Estos sistemas podrían ser considerados como críticos al producir consecuencias muy graves en el bienestar de las personas tanto a nivel económico y salud. Los CPS abarcan distintos dominios los cuales incluyen sistemas biomédicos y de salud, sistemas de transporte, sistemas automotrices, y sistemas de fabricación [5]. Los sistemas ciber físicos se encuentran expuestos a una serie de riesgos que importante controlar. Por ejemplo, al estar integrado a internet podría sufrir ataques cibernéticos, posible robo de información, etc. Para ello el artículo [5] plantea que es importante aplicar diferentes técnicas la para evaluación de riesgos, así como técnicas de reducción. También recomienda que las herramientas e instrumentos desarrollados para la gestión de riesgos deben ser rápidos, rentables y prácticas. Mencionan a su vez que recibieron diferentes propuestas para esta gestión de riesgos entre las que destacan la de Aakarsh Rao y sus colegas quienes en [14] presentan un enfoque dinámico de gestión y mitigación de riesgos basado en la estimación probabilística de amenazas. Con el objetivo de garantizar la seguridad, la protección y la privacidad en presencia de amenazas de seguridad desconocidas, los dispositivos deben detectar y evaluar el riesgo de forma dinámica y, posteriormente, tomar medidas de mitigación automatizadas cuando el riesgo sea elevado, Aakarsh Rao y su equipo propuso un modelo incorporado un novedoso detector de amenazas en tiempo real con una metodología de evaluación de riesgos adaptativa para garantizar una mitigación de amenazas completa durante la implementación de dispositivos. Para la demostración de su funcionamiento desarrollaron un prototipo de marcapasos con conexión inteligente en la cual implantaron un

programa maligno. Los componentes críticos necesarios para el rendimiento esencial del marcapasos incluyen el marcapasos, el sensor y el componente de cómputo de estimulación. El middleware hardware-software facilita la transferencia segura de datos y señales entre modos operativos. El middleware también es responsable de analizar la detección de amenazas en tiempo de ejecución, la actualización del modelo de riesgo y la determinación de qué estrategia de mitigación invocar cuando se detecta una amenaza.

Conclusiones

La gestión de riesgos para los sistemas críticos se basa principalmente en la determinación y valoración de riesgos como consecuencia de una metodología determinada. Justamente esta metodología varía según cada investigación, dando como resultados en todas ellas mejoras de los análisis de riesgos lo que permitió mitigar los riesgos, o al menos mejorar los ámbitos donde se desencadenan para mitigar sus efectos.

Los sistemas críticos están presentes en diferentes campos y aplicaciones, teniendo todas en común la importancia de conservar sus sistemas funcionando constantemente y de manera correcta.

Muchos sistemas no son críticos de forma individual, sin embargo, pueden ser relacionados un sistema crítico, o incluido como parte de uno. En el primer caso el software no critico se vuelve crucial, al ser un soporte critico de un sistema crítico, lo que por transitividad ambos sistemas se vuelven críticos. En el segundo caso el planteamiento es similar, con la única distinción que el software no critico es incluido en el software crítico, siendo un soporte embebido en contraposición al primer caso.

A diferencia del punto anterior también se puede se puede dividir los sistemas en subsistemas, permitiendo identificar los subsistemas críticos y no. Lo que contribuye a una gestión de riesgos más incidente sobre lo realmente crítico, derivando tiempo y recursos a lo más importante. Esto a su vez permite la creación de sistemas supervivientes que siempre estén disponible a un nivel óptimo de servicio, aunque no sea el mejor todo el tiempo.

El análisis de riesgos presenta varias técnicas para su identificación, no se puede determinar una técnica ideal para aplicar a todos los proyectos. Esta técnica dependerá del ámbito, especialidad y contexto de desarrollo del proyecto, incluso aplicará en determinadas ocasiones aplicar técnicas hibridas, o dinámicas para adaptar las metodologías y lograr los mejores resultados.

Referencias

[1] Knight, J. C. (2002, May). *Safety critical systems: challenges and directions. In Proceedings of the 24th international conference on software engineering* (pp. 547-550).

[2] Oh, H. J., & Hong, J. P. (2012). A Study of Software Hazard Analysis for Safety Critical Function in Military Aircraft. *Journal of IKEEE*, *16*(2), 145-152.

[3] Gatouillat, A., Badr, Y., Massot, B., & Sejdić, E. (2018). Internet of medical things: A review of recent contributions dealing with cyber-physical systems in medicine. *IEEE internet of things journal*, *5*(5), 3810-3822.

[4] Albee, A., Battel, S., Brace, R., Burdick, G., Casani, J., Lavell, J., ... & Dipprey, D. (2000). Report on the loss of the Mars Polar Lander and Deep Space 2 missions.

[5] Biro, M., Mashkoor, A., Sametinger, J., & Seker, R. (2017). Software safety and security risk mitigation in cyber-physical systems. *IEEE Software*, *35*(1), 24-29.

[6] Guide, A. (2001). *Project management body of knowledge (pmbok® guide). In Project Management Institute* (Vol. 11, pp. 7-8).

[7] Knight, J. C., & Strunk, E. A. (2004). Achieving critical system survivability through software architectures. In *Architecting Dependable Systems II* (pp. 51-78). Springer, Berlin, Heidelberg.

[8] Lions, J. L., Luebeck, L., Fauquembergue, J. L., Kahn, G., Kubbat, W., Levedag, S., ... & O'Halloran, C. (1996). Ariane 5 flight 501 failure report by the inquiry board.

[9] Albee, A., Battel, S., Brace, R., Burdick, G., Casani, J., Lavell, J., ... & Dipprey, D. (2000). Report on the loss of the Mars Polar Lander and Deep Space 2 missions.

[10] Board, M. I. (1999). Mars Climate Orbiter Mishap Investigation Board Phase I Report November 10, 1999.

[11] Neumann, P. G. (1994). Computer-related risks. Addison-Wesley Professional.

[12] McNally, K. M., Page, M. A., & Sunderland, V. B. (1997). Failure-mode and effects analysis in improving a drug distribution system. American Journal of Health-System Pharmacy, 54(2), 171-177.

[13] Gatouillat, A., Badr, Y., Massot, B., & Sejdić, E. (2018). Internet of medical things: A review of recent contributions dealing with cyber-physical systems in medicine. *IEEE internet of things journal*, *5*(5), 3810-3822.

[14] Rao, A., Carreón, N., Lysecky, R., & Rozenblit, J. (2017). Probabilistic threat detection for risk management in cyber-physical medical systems. IEEE Software, 35(1), 38-43.