Ciberseguridad en la Digitalización de Operaciones de Mantenimiento

Autores

- Fernando Sáenz (Director Gerente en Savvy Data Systems, Investigador Predoctoral Departamento de Arquitectura y Tecnología de Computadores, UPV/EHU)
- José Miguel-Alonso (Catedrático de Universidad, Departamento de Arquitectura y Tecnología de Computadores, UPV/EHU)

Introducción

La nueva era digital está permitiendo una rápida evolución de la industria, a través de la denominada cuarta revolución industrial (*Industry 4.0*). Esta transformación digital también está produciéndose en las operaciones de mantenimiento [1], permitiendo ejecutar ciertos trabajos de forma remota, e incluso pudiendo anticipar ciertas operaciones gracias a la aplicación de inteligencia artificial para la predicción de la vida útil restante (RUL) de un componente [2]. Desde una sencilla telegestión de un SCADA, hasta una asistencia remota utilizando herramientas de realidad aumentada, todas las operaciones de mantenimiento que estén sujetas a una transformación digital deben tener en cuenta la aparición de nuevos riesgos de seguridad inherentes a la digitalización, principalmente debidos a la interconexión de sistemas de diferente naturaleza, pasando en muchos casos por Internet.

El proceso de digitalización de operaciones de mantenimiento requiere la integración de nuevos elementos físicos y lógicos, tales como *cyber-physical systems* (CPS) [3], tecnologías *Cloud*, redes segmentadas, o incluso algoritmos de análisis de datos. Esta constelación de componentes digitales aporta una gran agilidad y versatilidad de operación, al mismo tiempo que incorpora en la cadena riesgos adicionales. Este proceso implica, además, la aparición de nuevos actores que participan activamente en las operaciones, entre los que se incluyen empresas suministradoras de CPS, proveedores *Cloud*, e ingenierías de análisis de datos. Este nuevo entorno multidisciplinar y multiempresa requiere una interconexión y una interoperabilidad sin precedentes, las cuales hacen aflorar dos importantes retos fuertemente interrelacionados: la protección de la infraestructura hardware/software, y la correcta gestión de los permisos de acceso a los datos para cada actor implicado.

El cumplimiento de los tres pilares fundamentales de la ciberseguridad (confidencialidad, integridad, disponibilidad) es un factor clave para poder poner en práctica con garantías un proceso de digitalización de las operaciones de mantenimiento. Para lograrlo es necesario elegir un diseño arquitectónico hardware+software adecuado. Esta ponencia analiza los puntos críticos sobre los cuales suelen concentrarse la mayoría de vectores de ciberataques, y muestra estrategias de diseño de una arquitectura fiable y segura que permita gestionarlos adecuadamente. El diseño propuesto tiene en cuenta la heterogeneidad de los diferentes entornos en los que pueden enmarcarse las operaciones de mantenimiento, cubriendo la custodia de todo el ciclo de vida del dato, desde su origen hasta su análisis en entornos *Edge* o *Cloud*. Finalmente, este trabajo muestra como conclusión la manera en que un diseño de arquitectura por capas intercambiables aporta

un mayor nivel de mantenibilidad de sus componentes, favoreciendo que persevere en el futuro un buen nivel de ciberseguridad.

Mantenimiento y ciberseguridad.

La EFNMS (*European Federation of National Maintenance Societies*) define el término "mantenimiento" como la combinación de todas las acciones técnicas, administrativas y de gestión durante el ciclo de vida de un artículo, destinada a mantenerlo en o restaurarlo a un estado en el que pueda realizar la función que de él se requiere. El mantenimiento es de suma importancia para el comercio, para el medio ambiente y para la salud y la seguridad en general [4].

Complementando la definición anterior, este trabajo también tiene en cuenta aquellas operaciones denominadas como *mantenimiento perfectivo*, a través de las cuales se ejecutan ciertas tareas que no están enfocadas directamente a salvaguardar la correcta operación de un activo industrial, sino a *mejorar su rendimiento*. Un ejemplo podría ser la sustitución de un conjunto de rodamientos, en perfecto estado y operando a su máxima capacidad, por otros que consigan un rendimiento superior, mejorando así la capacidad global de la unidad de producción. Este tipo de operaciones están relacionado con el denominado *mantenimiento evolutivo*, el que se realiza cuando se ejecutan ciertos trabajos para cumplir con una actualización de los requisitos iniciales a los que estaba sujeto el diseño y construcción de la unidad de producción.

En función del momento en el que se realiza el mantenimiento, puede ser de uno de estos tres tipos:

- *Correctivo*: actuación reactiva ante un suceso que ya se ha desencadenado, cuyo objetivo es *restablecer* la capacidad de operación del equipamiento al punto anterior, así como minimizar las consecuencias derivadas del fallo.
- *Preventivo*: actuación preparatoria o profiláctica, cuyo objetivo es *evitar* que se desencadenen sucesos dañinos para la producción o para los activos.
- *Predictivo*: actuación preparatoria basada en una previsión de probabilidad de fallo calculada matemáticamente.

La digitalización de las operaciones de mantenimiento consiste en la adopción de un conjunto de herramientas relacionadas con las Tecnologías de la Información para automatizar y/o agilizar dichas tareas. Entre los diferentes beneficios que debe aportar una digitalización bien ejecutada, podemos destacar la simplificación en la gestión de un gran parque de máquinas muy deslocalizadas, la posibilidad de conocer la situación exacta de un activo antes de ir a visitarlo, pudiendo llevar los recambios adecuados en el momento adecuado (entrega *just in time* de recambios), y la incorporación de ciencia de datos en el mantenimiento, que a su vez habilita la aplicación de analítica descriptiva, diagnóstica, prescriptiva, y predictiva.

Para las empresas dedicadas al mantenimiento industrial, el proceso de adopción comprende la digitalización de dos componentes del negocio:

- *Digitalización de las operaciones de la empresa*: abarca un gran abanico de transformaciones que, potencialmente, inciden sobre diferentes departamentos, desde la implantación más básica de un sistema informático de gestión (ERP), hasta

la integración completa de datos de máquina en tiempo real para el análisis de condición de componentes críticos en línea.
- *Digitalización de la relación con el cliente*: se centra en la adopción de tecnologías digitales para optimizar los puntos de contacto con el cliente. Está muy interrelacionada con la digitalización de las operaciones de la empresa y, lógicamente, afecta en mayor medida a aquellos departamentos que tienen una relación más directa con el cliente.

La digitalización a su vez incide en diferentes apartados técnicos:

- *Electrónica*: nuevos requerimientos en sensórica, dispositivos de captación, enrutadores, unidades de cómputo local (*Edge Computing*), etc.
- *Comunicaciones*: nuevos flujos de datos entre los activos y las empresas encargadas de sus mantenimientos, que pueden ser bidireccionales, y probablemente incluirán en su cadena a terceros actores (proveedores *Cloud*, ISPs, proveedores o departamentos IT de las fábricas de los clientes, etc.).
- *Infraestructura de cómputo*: la adopción de tecnologías digitales requiere un conjunto de servicios de soporte que serán ejecutados por un entorno de computación. Hoy en día la estrategia más habitual suele ser contratar granjas de servidores a empresas especializadas, que cuentan con los recursos físicos necesarios, y los proveen en un modelo IaaS (*Infrastructure as a Service*). Son los comúnmente denominados CPD o Centros de Procesamiento de Datos (*Data Centers*).
- *Ciencia de datos*: la captura, monitorización y recopilación de datos es un medio para lograr un fin. En este caso, la optimización de las operaciones de mantenimiento mediante la predicción matemática de la probabilidad de fallo de un componente, basada en la evolución mostrada por datos recopilados anteriormente. Por ejemplo, el RUL estimado de un componente crítico determina de forma estadística la proyección en el tiempo de la vida útil de dicho componente, información que resulta de vital interés para la planificación de las operaciones de mantenimiento predictivo. La ciencia de datos permite reducir el número de operaciones de mantenimiento reactivo, optimizando el preventivo.
- *Ciberseguridad*: se trata de un elemento transversal que afecta a todos los anteriores apartados técnicos, y cuya misión es garantizar la confidencialidad, integridad y disponibilidad de la información en cada uno de ellos.

La adopción trasversal de un buen nivel de ciberseguridad para todos los apartados técnicos permitirá eliminar, o al menos reducir, el número y alcance de los incidentes que puedan ocasionar los diferentes tipos de ataques a los que el sistema se verá inevitablemente sometido. En la siguiente sección incluimos una lista de las amenazas más comunes en este contexto, así como de las formas de evitar que se materialicen.

La digitalización de las operaciones de mantenimiento supone una oportunidad de negocio de una gran magnitud, dado que aporta un conjunto de beneficios a corto plazo, una previsión de mejora notable a medio plazo, y unas capacidades de evolución muy sustanciales a largo plazo. Todo ello, ya lo hemos descrito, sometido a la aparición de nuevos riesgos, inherentes a la digitalización de cualquier proceso. Por esta razón, resulta vital la elección de un diseño adecuado para la arquitectura de cómputo que dará soporte a tales operaciones. Un buen diseño reducirá notablemente las probabilidades de sufrir incidentes de ciberseguridad, mejorará la mantenibilidad de la plataforma que lo

implemente, y permitirá una mayor adaptación a los nuevos entornos que, sin duda, nos traerá el futuro.

Ciberseguridad: riesgos y técnicas de mitigación

La RAE define el término “seguro” como un adjetivo que indica “libre y exento de riesgo” [5]. Este concepto, denominado *safety* en inglés, es amplio y aplicable a multitud de situaciones y entornos. En lo relativo a las operaciones de mantenimiento industrial, si bien es poco realista pensar que se pueda lograr un entorno o actividad completamente libre y exenta de riesgo, su minimización y gestión se lleva a cabo mediante un conjunto de normas enmarcadas en la disciplina denominada Prevención de Riesgos Laborales. Nos referiremos normalmente a este tipo de seguridad como *seguridad física.*

En lo relativo a la seguridad de la información (*information security* en inglés), su objetivo es la reducción y gestión de los riesgos asociados a la publicación no consentida, bloqueo, destrucción o alteración de la información. Habitualmente su actividad se enmarca en conservar la denominada “*CIA Triad*” sobre la información: confidencialidad, integridad y disponibilidad.

La ciberseguridad o seguridad informática se encarga de gestionar la seguridad de la información en el medio informático. Está contenida dentro de la seguridad de la información, pero conviene no confundirla con ésta, ya que la ciberseguridad tiene su actuación específicamente limitada al campo digital. Así, un usuario que deja su clave apuntada en un *post-it* es un caso de (falta de) seguridad de la información, pero no de (falta de) ciberseguridad.

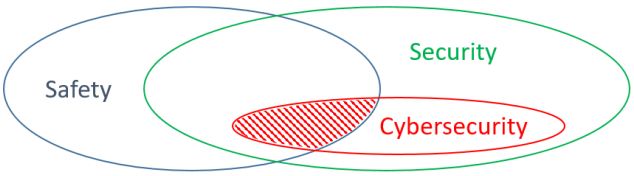

Ilustración 1 - Ciberseguridad y seguridad física (Cybersecurity & Safety)

El carácter intangible de la seguridad digital puede provocar el grave error de considerarla menos relevante que la seguridad física, más aún cuando clásicamente la seguridad en las operaciones de mantenimiento ha incidido principalmente en la seguridad física. Una operación de mantenimiento en un entorno digitalizado a menudo supondrá una conexión remota con un bien físico que ya opera mediante una lógica de control digital. Hay que tener en cuenta que ciertos fallos en la cadena digital pueden desencadenar situaciones que potencialmente transcenderán lo digital, convirtiéndose en fallos de seguridad física que podrían herir a operarios o incluso provocarles la muerte. Las nuevas amenazas inevitablemente introducidas por las nuevas tecnologías saltarán del mundo digital al físico cuando actúen gestionando un activo físico (ej. un torno, una fresadora, una grúa, una forja, un ascensor…). Así, los sucesos físicos peligrosos, que hasta ahora han sido objeto de prevención física, podrán ser desencadenados por un fallo digital que también habrá que comprender, localizar y gestionar. Esta interrelación está representada en la Ilustración 1.

Vulnerabilidades en el software

Todo proceso de digitalización implica el uso masivo de software. Hoy en día la producción de software se lleva a cabo en entornos muy controlados, habitualmente diferenciando etapas en su proceso de diseño, implementación y pruebas que, como mínimo, incluyen *desarrollo*, *preproducción* y *producción*. Todo software es sometido, en cada una de estas etapas, a un conjunto de tests automatizados para la detección de vulnerabilidades, como pueden ser por ejemplo las pruebas unitarias. Además se lanzan versiones alfa y beta para su testeo por personal cualificado.

Pese a ello, cabe recordar que el software sigue siendo diseñado y programado por personas, lo que introduce el error humano en su codificación. Por convención (y por estadística) se sabe que todo software tiene entre 3 y 10 bugs por cada 10KLOC (*Thousand Lines of Code*) [6]. De esos bugs, se sabe que entre el 1% y el 5% son potenciales vulnerabilidades de seguridad. Por tanto, un software que tenga unos 2MLOC (*Million Lines of Code*) tendría unas 420 potenciales vulnerabilidades de seguridad, aproximadamente una cada 5KLOC [7]. Inevitablemente, siempre hay un cierto número de fallos que consiguen avanzar por todas las etapas de la creación del software sin ser detectados, razón por la cual la búsqueda de vulnerabilidades sigue activa en la fase de producción. Una prueba de ello es que todas las empresas comercializadoras de software de cierto tamaño cuentan con programas de retribución para premiar a aquellos usuarios que encuentren vulnerabilidades y las reporten debidamente a la compañía.

La detección de fallos en programas informáticos que ya están en producción genera una base de datos que se encuentra actualmente formalizada en una lista conocida como “CVE” (*Common Vulnerabilities and Exposures*) [8]. Incluye información registrada sobre las vulnerabilidades conocidas, junto con una puntuación según la criticidad percibida. Las vulnerabilidades publicadas en los CVEs son un arma de doble filo. Por un lado permiten saber cuándo es necesario actualizar un software, pero también son muy utilizadas por los atacantes para determinar si una versión concreta de software contiene una vulnerabilidad explotable, e incluso conocer su forma de explotación. Se trata de una herramienta indispensable que todo gestor digital debe dominar. Es de una importancia vital consultar la lista regularmente (suscribirse), y automatizar tests periódicos (por ejemplo, OpenVAS [9]) basados en las novedades de esta base de datos.

Ataques más comunes

Antes de poder diseñar una arquitectura realmente efectiva en lo relativo a la Ciberseguridad, es necesario identificar, comprender y valorar el alcance de los tipos de ataques que más comúnmente sufren las plataformas digitales. Estos ataques suelen ser también los más efectivos, ya que los no efectivos van desapareciendo o evolucionando paulatinamente.

Cabe destacar que es poco habitual encontrar un caso en el que un intento de explotación de una vulnerabilidad se esté produciendo de forma aislada. Lo habitual es que los ataques estén más elaborados, organizados en vectores formados por una combinación de diferentes tipos de intentos de explotación.

Ataque de fuerza bruta o diccionario para la autenticación

Consiste en la automatización de un gran número de intentos de autenticación consecutivos, siguiendo un orden o patrón, con la intención de encontrar una combinación de usuario y clave válida en el sistema. La plataforma debe contar con una herramienta

para detectar esta situación y activar bloqueos tempranos, incluyendo bloqueos por ráfaga y control de rango temporal de los ataques. El sistema puede avisar al usuario legítimo, pero siempre controlando el número de avisos. Se debe evitar bloquear la cuenta del usuario legítimo, ya que de hacerlo se provoca un nuevo tipo de ataque dirigido contra el usuario (y del que la plataforma además sería partícipe). Los bloqueos tienen que comenzar desde lo más específico y avanzar hacia lo más genérico. Inicialmente debe intentarse el bloqueo por sesión de navegador (cookie), el siguiente paso puede ser incluir un *captcha* [10] para todas las peticiones desde la dirección IP del posible atacante con el fin de evitar intentos de acceso automatizados y, como paso final, proceder al bloqueo temporal de la dirección IP. Hay un riesgo de estar bloqueando a usuarios legítimos, de ahí que las medidas más restrictivas siempre deben ser el último recurso, cuando el vector de ataque persiste. Una decisión inteligente a este respecto es que el sistema no permita a los usuarios establecer claves demasiado sencillas o que puedan ser encontradas en un diccionario de claves.

Robo de credenciales

Son diversas las posibilidades para que un atacante haya podido obtener las credenciales de acceso de un usuario legítimo (*phishing*, *man in the middle,* ingeniería social…). Una vez logradas, el atacante intentará hacer uso de esas credenciales para proseguir con sus intentos de explotación. Un buen diseño puede incluir medidas adicionales para poner más barreras a un atacante que ya dispone de credenciales robadas. Tal es el caso de las herramientas 2FA (*Two Factor Authentication* - Autenticación de Dos Factores). Un sistema que implementa alguna de estas herramientas concede acceso al usuario por: 1) lo que sabe (usuario y clave) y 2) lo que tiene (dispositivo físico). El usuario se autentica mediante sus credenciales, pero además también debe autorizar sus dispositivos de acceso. Un dispositivo no autorizado (o revocado) no puede acceder a la plataforma. Desde su panel de usuario podrá gestionar sus dispositivos, renombrarlos (facilitando su reconocimiento) o revocarlos. Muchas plataformas utilizan el correo electrónico del usuario como elemento de identificación unívoco, lo cual es de fácil aplicación siempre que todas las cuentas de usuario sean nominales. Se debe evitar el uso de cuentas no nominales para poder identificar a la persona física responsable de la utilización que se da a sus credenciales. Existen muchas otras formas de implementar 2FA (SMS, aplicaciones móviles, tarjetas de coordenadas), si bien el correo electrónico es muy utilizado por su relación coste-comodidad-seguridad.

Acceso utilizando credenciales por omisión

Este tipo de ataque es de especial incidencia en plataformas digitales para la gestión de activos industriales. Es muy habitual en dispositivos IoT, que están configurados de fábrica con unas credenciales de gestión pre-establecidas y conocidas. Este tipo de ataque ha sido ampliamente exitoso en diversos entornos, desde cámaras de video vigilancia hasta autómatas de control – PLCs [11]. Para limitar su impacto, la plataforma puede integrar una herramienta de barrido de credenciales. Mediante esta herramienta, se van cambiando cada cierto tiempo las claves de acceso a los dispositivos IoT, creando claves aleatorias. El personal autorizado puede solicitar el establecimiento de una clave conocida en un dispositivo dado, de forma temporal. Tras operar con el mismo, la plataforma volverá automáticamente a aleatorizar la clave. Alternativamente, puesto que las claves temporales están guardadas en un repositorio protegido, es posible acceder a ellas y utilizarlas, siempre por un tiempo limitado.

Phishing y técnicas de engaño

Las técnicas de *phishing*, normalmente llevadas a cabo a través de mensajes de correo electrónico engañosos, tratan de obtener de forma fraudulenta credenciales de acceso a sistemas. Se hace creer a un usuario que accede a una página web legítima cuando en realidad accede a otra con la misma apariencia, pero falsa, que pide credenciales que, luego, se usarán para realizar actividades ilegítimas haciéndose pasar por el usuario víctima del ataque. Dichas actividades pueden ser de mucha gravedad, en función del nivel de privilegios de la víctima. La prevención de estos ataques, en los que interviene un factor humano, pasa por examinar e-mails sospechosos, bloquear ciertos enlaces, revisar los accesos, imponer políticas seguras de autenticación, etc.

Man in the middle

Se trata de un ataque dirigido al cifrado del canal de comunicación. Existe un enorme número de técnicas de este tipo. De hecho se trata de auténticos vectores de ataque completos en sí mismos. El ataque requiere interceptar las comunicaciones, lo que permite acceder a información sensible cuando el canal no esté debidamente cifrado. Su inicio suele depender del origen y destino del ataque, pudiendo iniciarse mediante una técnica de *ARP poisoning*, un *DNS flooding* de un router, o incluso un ataque directo a un PC para la instalación de certificados maliciosos a través de un *plug-in* de un navegador. Para evitar este tipo de ataques es indispensable que toda comunicación utilice siempre cifrado no inferior a TLSv1.2, gestionando adecuadamente los certificados, la validez, la firma por una autoridad reconocida, y la posible revocación. Dentro de las familias de algoritmos de firma y cifrado admitidos en TLSv1.2, el sistema debería permitir únicamente aquellos que sigan el RFC 7525 [12].

DoS y DDoS

Los ataques de denegación de servicio tienen como objetivo saturar la capacidad de procesamiento (habitualmente mediante saturación del tiempo de procesador, capacidad de memoria y/o comunicaciones) de aquellos dispositivos que estén dando servicio a los usuarios de la plataforma. Su método habitual de ataque es realizar un número masivo de peticiones contra su víctima, intentando que cada una de ellas requiera el máximo esfuerzo por parte del sistema informático. Cuando el ataque es localizado, cualquier firewall o IPS comercial es capaz de detectarlo y neutralizarlo. Cuando el ataque es distribuido (típicamente desde una *botnet*) suele ser más complicado contenerlo, dado que el método más efectivo es la anulación del acceso al recurso objeto del ataque, lo que requiere que el servicio responda a las peticiones de gestión (lo que no siempre es posible: recordemos que está siendo sometido a una enorme carga y, por tanto, saturado). La contención efectiva suele requerir métodos más avanzados, como firewalls o balanceadores capaces de interpretar las comunicaciones a nivel de aplicación.

Escaneo de puertos

Todo sistema digital debe permitir que sus clientes, digitales o humanos, se puedan conectar a sus servicios. Para ello, establecen unos números de puerto (relacionado con los protocolos de transporte TCP y/o UDP) que son utilizados para diferentes aplicaciones. Estos puertos, indispensables para el funcionamiento de los sistemas interconectados, son también puntos a través de los cuales equipos y servicios quedan expuestos. Muchos vectores de ataque comienzan por un barrido de puertos, con la intención de encontrar aquellos abiertos para dar servicio. Tras este reconocimiento, el ataque evolucionará hacia formas específicas para los servicios detectados.

Muchos servicios incluyen en sus protocolos mensajes de saludo, en los que se anuncia información como el nombre, tipo y versión del software que presta el servicio. En ciertos casos también se incluye en el anuncio un listado de capacidades o *plug-ins* que tenga activos dicho software. Esta información es de enorme valor para los atacantes, ya que les permite centrarse en vulnerabilidades efectivas y específicas, listadas en las listas CVE, en vez de en otras más genéricas.

Las contramedidas más efectivas suelen estar relacionadas con los elementos de seguridad de red, tales como cortafuegos y sistemas de detección y prevención de intrusiones. Estas herramientas pueden detectar patrones de escaneo de puertos y bloquear el tráfico sospechoso. También es importante configurar las aplicaciones para que en su saludo no envíen información sensible, o lo hagan de forma controlada y codificada, para evitar dar pistas a los posibles atacantes.

Control de servidores, intrusión en la red (rootkits)

A través del ataque a las aplicaciones que conforman la plataforma un intruso podría hacerse con el control de un servidor mediante herramientas conocidas como *rootkits* y, en función de la topología de red de la plataforma, podría propagar después su ataque hacia otros servidores del sistema. Este tipo de ataques suele darse principalmente a través de aplicaciones auxiliares, a las que suele prestarse menos atención pero que, una vez comprometidas, sitúan al atacante en una posición privilegiada para infectar el resto de sistemas desde dentro. Hay que recordar que toda aplicación que conforme el sistema, sea crítica o auxiliar, incluye potenciales brechas de seguridad. Una buena gestión de red, que incluya reglas muy restrictivas, ayudará a evitar accesos públicos a servicios y servidores internos. El acceso a todas las aplicaciones auxiliares debe estar debidamente protegido a través de conexión VPN, IPSec, o reglas de conexión para orígenes controlados. También se deben integrar herramientas de escaneo y detección de *rootkits*, para poder realizar una detección temprana de cualquier ataque exitoso y aislar el sistema comprometido antes de que su propagación resulte catastrófica.

Ataques físicos contra dispositivos IIoT

La seguridad digital también se puede ver comprometida por una acción física, como puede ser la conexión de un dispositivo USB a uno de los aparatos IIoT (*Industrial Internet of Things*) conectados a la plataforma. Un ataque típico sería conectar una llave USB con un sistema operativo "*live*", reiniciar el dispositivo, iniciar el nuevo sistema operativo y, desde él, acceder al contenido del disco físico, que podría incluir software sensible, credenciales de acceso, certificados de firma, etc. Para evitarlo, las placas base de los dispositivos IIoT deben estar correctamente configuradas (p. ej. desde su sistema BIOS) para no permitir la conexión de ningún dispositivo físico no autorizado.

Ransomware y técnicas de extorsión

Un equipo infectado por un virus o un gusano puede ser objeto de un robo de información, o de un bloqueo en el acceso a la misma tras cifrarla. El atacante promete revertir la situación tras pagar un determinado rescate. Los efectos en la organización pueden ser devastadores, especialmente si el gusano se propaga por la red corporativa utilizando vulnerabilidades de los sistemas conectados. La prevención pasa por políticas y mecanismos de mantenimiento de copias de seguridad de la información, y también por la actualización permanente de sistemas (para reducir las vulnerabilidades). El coste de recuperar un sistema atacado se puede reducir con sistemas ágiles de despliegue de

servicios. A modo de ejemplo, si se ataca una máquina virtual, es relativamente sencillo destruirla y crear rápidamente una nueva a partir de una copia maestra.

Arquitecturas para la digitalización en los procesos de mantenimiento

La digitalización en los procesos de mantenimiento requerirá en la mayoría de los casos el diseño, desarrollo, e integración de multitud de herramientas de software. Nos encontramos ante un escenario de *plataforma*, entendida como un único ente que agrupa y coordina la operación de un cierto número de programas informáticos. En el caso de las operaciones de mantenimiento, cabe esperar además que dichas plataformas requieran una arquitectura distribuida, en la que encontraremos software cuya operación se realiza en un entorno *Cloud*, software diseñado para operar en entorno *Edge*, software de gestión de comunicaciones, y seguramente diversas herramientas que requieran la operación en los tres entornos de forma coordinada. Por tanto, al tener en cuenta la gestión de la ciberseguridad en una plataforma, estamos hablando no solo de abordar su gestión en multitud de elementos de software, sino también en sus interrelaciones.

Capacidades específicas de una arquitectura cibersegura

Listamos aquí una serie de propiedades que consideramos fundamentales para una arquitectura orientada a la digitalización del mantenimiento, teniendo en cuenta la necesidad de que permita un funcionamiento seguro:

- Capas desacopladas: nuestra propuesta plantea un diseño basado en capas desacopladas para crear una arquitectura modular, híbrida y altamente deslocalizada.
- Gestión de enlaces entre capas, con un control exhaustivo sobre qué sistemas pueden comunicarse con cuáles, y cómo deben hacerlo.
- Elección de componentes: en la arquitectura, en caso de que sea necesario, un componente puede ser reemplazado por otro con la misma funcionalidad. Por ejemplo, si utilizamos un módulo software de un determinado proveedor que no actúa de forma ágil ante una vulnerabilidad detectada en su módulo, podremos cambiar de proveedor.
- Mantenibilidad: el diseño modular permite el reemplazo de cualquiera de sus componentes, lo cual incrementa sustancialmente la mantenibilidad del software.
- Tecnología *future-proof*: el reemplazo de componentes por otros nuevos con capacidades mejoradas permite que la arquitectura evolucione progresivamente.
- Segmentación de la información: se propone la utilización de un repositorio central con una arquitectura distribuida multi-datacenter, o *Data Lake*, que cuente con la capacidad de crear segmentos estancos para la gestión de la información. Así, una operación de escritura o de lectura de un origen concreto siempre quedará confinada al segmento al que pertenece, no pudiendo evadir esta restricción ni siquiera ante el fallo humano de un programador.
- Ciberseguridad interna: la arquitectura por capas añade un componente adicional de seguridad porque, al estar desacopladas, impide que las vulnerabilidades de una capa se propaguen al resto. La ciberseguridad en el software puede verse como una cadena cuya robustez viene determinada por el eslabón más débil. El diseño por capas reduce la longitud de los tramos de dichas cadenas. Así, el propio diseño puede contener la propagación de vulnerabilidades que puedan existir en el software sus componentes.

- Control de despliegue: una arquitectura deslocalizada requiere la gestión de las partes de su software que residen en entornos *Edge*, por lo que incluye mecanismos para la actualización ágil de los mismos.
- Orquestación de aplicaciones: una arquitectura híbrida debe aportar capacidad de cómputo cerca de las máquinas (ej. cálculo de RUL de un componente, análisis de condición...). Para poder realizar dichos cálculos, la plataforma permite y controla el despliegue de aplicaciones de terceros a entorno *Edge*, lo que requiere de un sistema de orquestación controlado, que no introduzca puntos de vulnerabilidad adicionales en la plataforma.
- Mecanismos de control de autenticación: la implementación del diseño debe incluir características de detección y bloqueo temprano ante ataques de fuerza bruta o diccionario, y un sistema de autorización de doble factor o *2FA*.
- Integración de terceros sistemas de ciberseguridad: la plataforma operará bajo firewall e IPS, configurados de forma que detecten y neutralicen ataques de denegación de servicio y escaneo de puertos, entre otros. Se incorporará además un segundo nivel de firewall software que trabaje a nivel de aplicación para todas las peticiones que utilicen protocolo HTTPS (accesos web, accesos vía API y otros servicios). También integrará terceros sistemas de análisis, como por ejemplo detectores de *rootkits*.
- Ciberseguridad en dispositivos electrónicos: la producción de todos los dispositivos que forman parte de la plataforma incluirá la configuración en modo seguro de sus puertos físicos, imposibilitando el arranque desde medios extraíbles, y clave de acceso para gestión de BIOS. El software de gestión IIoT dispondrá de un subsistema que garantice que el dispositivo no opere utilizando claves por omisión, y se coordinará con un servicio central de aleatorización de claves.
- Cifrado de canales: todas las comunicaciones se harán usando TLSv1.2 siguiendo el estándar RFC 7525
- Redundancia y copias de seguridad: todos los datos gestionados por el sistema estarán sometidos a tres niveles de copias, uno *en línea* o constante, otro a nivel de servidor completo, y otro deslocalizado (codificado y cifrado). Todos los servicios deben operar en clústeres multinodo redundados, con el fin de garantizar el nivel de servicio o *SLA.*

Propuesta de diseño de arquitectura

A partir de los requisitos anteriores, describimos en esta sección una propuesta más concreta de arquitectura para la digitalización de las operaciones de mantenimiento.

Ciclo de vida del dato

El diseño propuesto desacopla diferentes capas por las que el dato tendrá que ir transcurriendo en su ciclo de vida, desde su captura hasta su análisis, tal y como se representa de forma resumida en la Ilustración 2.

En el nivel *Edge*, una instancia de un módulo de captura intercambiable realiza la lectura de los datos originales desde su origen. La capa de gestión de módulos de captura encapsula los datos para su gestión adecuada por el resto de la plataforma. El dato avanza en paralelo hasta las capas de preprocesado, prefiltrado y gestión de *triggers*.

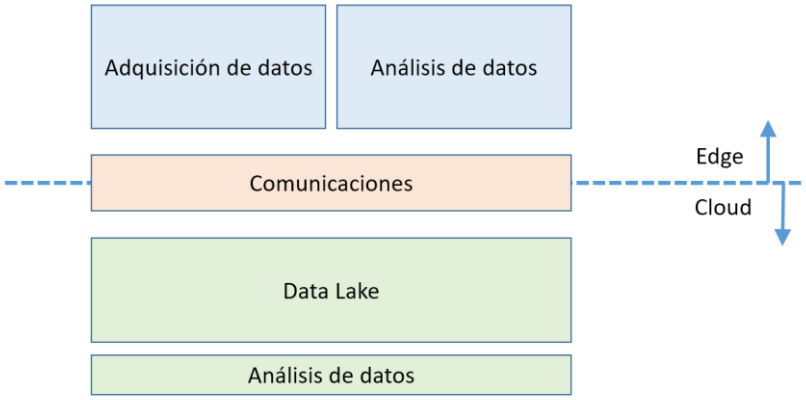

Ilustración 2 - Diagrama básico de diseño híbrido Edge-Cloud

Tras su tratamiento inicial, el dato avanza y se bifurca en "Y". Una copia pasa a la capa de interoperabilidad, desde la cual puede ser consumido por terceros sistemas en planta, puede formar un flujo de entrada para las aplicaciones Edge que estén desplegadas en el dispositivo, y también habilita una salida hacia una capa de persistencia local basada en un SGBD sin esquema, no relacional. La persistencia local supone un apoyo importante para los análisis que se llevan a cabo por parte de las aplicaciones Edge. La segunda copia del dato (recordemos la bifurcación en "Y") se lanza hacia el Cloud a través de la capa de control de transmisión. Este diseño puede verse en la Ilustración 3.

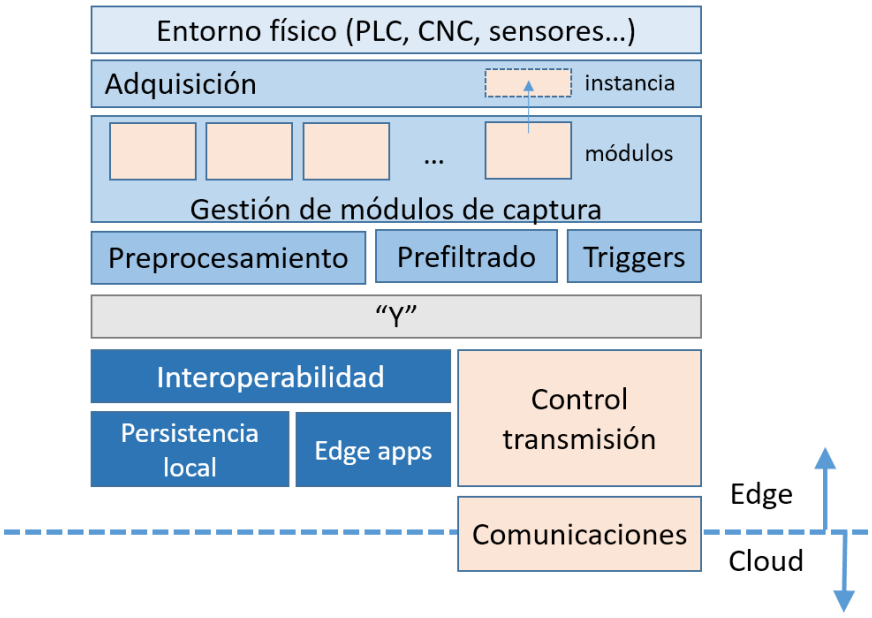

Ilustración 3 - Arquitectura del nivel Edge

En lo relativo a las operaciones de mantenimiento, la tecnología *Edge* es un integrante imprescindible en la arquitectura, ya que soluciona uno de los grandes problemas relacionados con el uso de tecnologías *Cloud*: la dependencia de la disponibilidad, calidad y capacidad de la conexión a Internet. El entorno *Edge* se encuentra directa y físicamente conectado a la máquina, lo que posibilita la adquisición de grandes flujos de datos, evita las

latencias y cortes de conexión derivados de la conectividad a Internet, y permite cerrar el lazo con la máquina de una forma más segura, rápida y fiable [13].

Las aplicaciones *Edge* no solo pueden consumir información, también pueden publicarla a través de un módulo de captura específico que les permite hacer "*push*" o publicación de datos en el flujo principal. Así, los datos calculados por las aplicaciones *Edge* entran de nuevo en el flujo principal, lo que permite su transmisión hacia el *Cloud*, su interoperabilidad hacia terceros sistemas, o su consumo por parte de otras aplicaciones *Edge* (o incluso la misma).

Un ejemplo de aplicación sería el de un sistema digital de análisis de condición de máquina o CMS, tal y como se presenta en la Ilustración 4, que permite conocer si el activo se encuentra en un buen estado de operación, y determinar si alguno de sus componentes necesita mantenimiento. El dispositivo electrónico donde se ejecuta el software Edge lee datos desde acelerómetros a una frecuencia de muestreo de 30Khz, y los procesa con una primera aplicación Edge que realiza una transformada rápida de Fourier (FFT). El resultado (espectro) se publica de nuevo en el flujo, siendo recibido por una segunda aplicación Edge (siguiente nivel) que aplica una serie de filtros para segmentar la señal en diferentes frecuencias. Una tercera aplicación Edge realiza un proceso de obtención de características sobre los datos segmentados (ej. severidad o energía de la vibración en cada frecuencia, picos altos y bajos, etc.). Finalmente, una cuarta aplicación recibe esas características y las combina con datos originales provenientes de otros módulos de captura para realizar un análisis estadístico y decidir si la situación se encuentra dentro de la normalidad o no. Esta aplicación de mantenimiento generará unas señales digitales de aviso que, a través de la capacidad de interoperabilidad de nuestro diseño, podrán ser enviadas al sistema de gestión de mantenimiento de la planta (GMAO), o a la empresa encargada de las operaciones de mantenimiento del activo monitorizado (utilizando nuestro entorno Cloud). Al detectar desviaciones en la normalidad, aporta al mantenimiento la capacidad de detección muy temprana (incluso predictiva) de posibles fallos de operación en el activo. Esto supone una mejora sustancial respecto a los trabajos de mantenimiento que no incorporan componente digital, dado que introduce la capacidad de evitar paradas no programadas, y permite planificar con antelación una actuación de mantenimiento muy precisa, realizando el recambio en la máquina de aquellos componentes físicos específicos que el sistema digital ha marcado con una alta probabilidad de fallo futuro (por ejemplo rodamientos, husillos, cabezales, etc.). Por otra parte, una rotura total de un componente de máquina generalmente aumenta el peligro físico, tanto en el momento de operación de la máquina como en la operación de mantenimiento para su reparación. Evitar la rotura total y poder hacer una reposición cuando el componente deteriorado aun es semi-funcional supone un aumento en la seguridad física de operarios de producción y de mantenimiento.

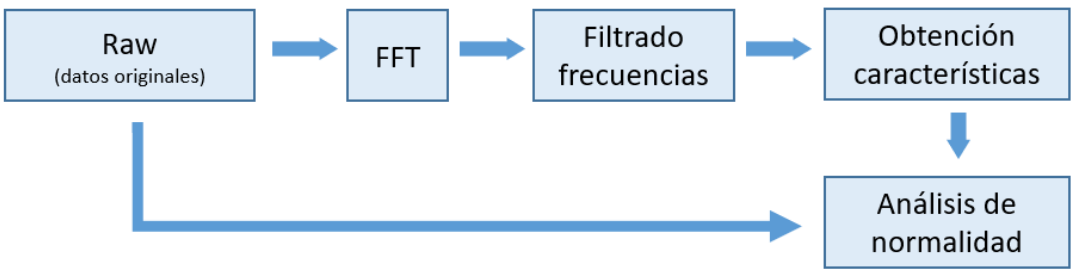

Ilustración 4 - Ejemplo de aplicación CMS ejecutada en niveles Edge

Los datos provenientes desde el entorno Edge son recibidos por el entorno Cloud a través de canales debidamente cifrados utilizando TLSv1.2 según el estándar RFC 7525, incluyendo además una correcta gestión de los certificados (validación, firma y revocación), con el fin de evitar cualquier tipo de ataque Man in the Middle. Los datos son debidamente almacenados en el Data Lake tras pasar por las capas de “Autorización y Segmentación” y “Registro Forense”. Estas capas garantizan la autenticidad del origen de los datos recibidos, aseguran que sean almacenados en el lugar correcto (segmento correcto, ver Ilustración 5), y crean en el registro forense una entrada reflejando la actividad llevada a cabo. El Data Lake está formado por un conjunto de granjas multi-clúster multi-nodo, tal y como se muestra en la Ilustración 6. Cuenta con un entorno relacional para sus necesidades internas de administración, y tres meta-niveles de almacenamiento que explotan la localidad temporal y espacial de los datos: UFDL (Ultra-Fast Data Lake), BBDL (Big Block Data Lake), LTDL (Long-Term Data Lake).

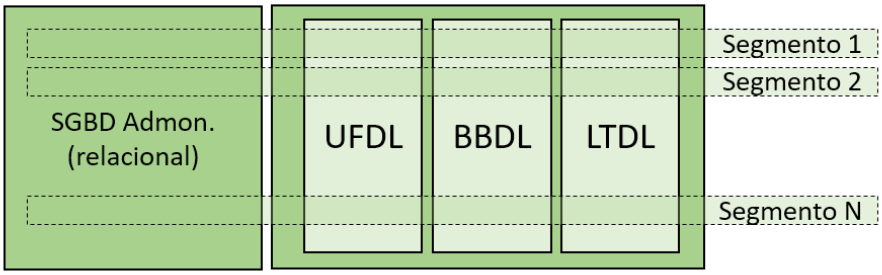

Ilustración 5 - Segmentación de la información en compartimentos estancos

El *Data Lake* es un entorno de persistencia de datos con una gran capacidad de escalar, tanto en dimensión como en rendimiento. Su diseño permite que se encuentre distribuido entre diferentes centros de datos. De él recogen los datos todos los sistemas de análisis, cuyas peticiones deben atravesar igualmente las capas de *Autorización y Segmentación*, y *Registro Forense*. Así, todo dato que entre o salga del repositorio será fuertemente controlado, y su movimiento quedará registrado.

La arquitectura escalable y distribuible del *Data Lake* permite que su operación física pueda estar localizada en diferentes CPDs. Esta característica aporta un alto nivel de redundancia ante fallos de servicio en los CPDs, y capacita al *Data Lake* para que pueda operar utilizando redes de comunicación diferentes (consideremos por simplicidad que cada CPD aporta una única red). Todo ello aumenta la resiliencia del sistema completo para mantener el nivel de servicio frente a ataques para el control de servidores, mejora la contención frente a ataques de intrusión en la red, aumenta la resistencia frente a ataques DDoS, y mejora la capacidad de mantener el nivel de servicio y revertir la situación en caso de ataques por *ransomware*.

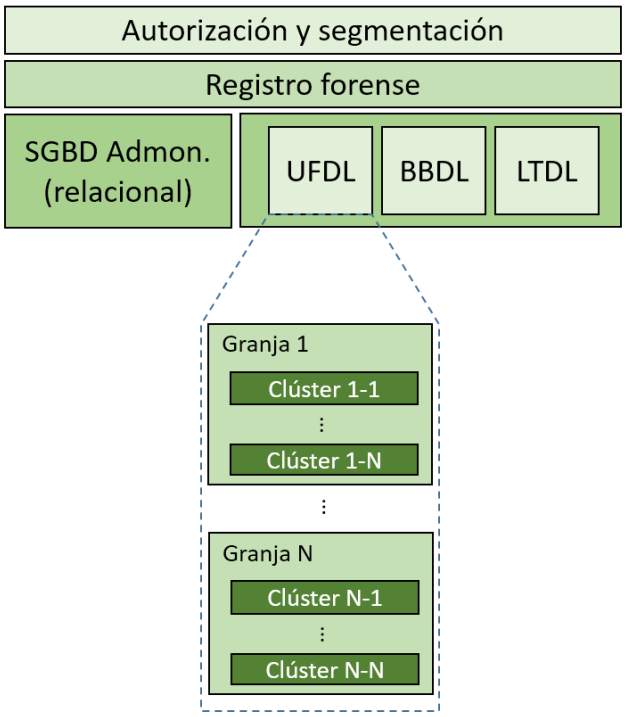

Ilustración 6 - Diseño multi-granja del Data-Lake con tres meta-niveles

El registro forense asocia toda acción a unas credenciales validadas de usuario, lo que permite detectar de forma temprana cualquier (intento de) uso indebido de credenciales. El diseño propone un sistema de autenticación de dos factores (2FA), lo cual, unido a la capacidad de bloqueo de ataques de fuerza bruta o diccionario que le aporta la sincronización de la aplicación de gestión de credenciales con los elementos de control de red, hace que crezca de forma exponencial la dificultad de lograr éxito con un vector de ataque basado en descubrimiento de credenciales. Por tanto, la detección de actividad indebida a través del registro forense habitualmente estará relacionada con un robo de credenciales realizado mediante técnicas de engaño (*phishing*, ingeniería social). Este registro aporta también un componente de advertencia psicológica importante para el usuario, ya que éste queda advertido a través de la aceptación del EULA (*End User License Agreement*) de que su cuenta es nominal e intransferible, de que sus acciones quedan registradas y son su responsabilidad, y de que es su obligación mantener un correcto esmero en lo relativo a la elección de sus contraseñas y la forma de salvaguardarlas.

Centralizar en un único repositorio los datos de condición y operación de un parque de máquinas muy deslocalizado permite analizar información sobre el comportamiento de componentes de máquina similares en entornos diferentes. La variabilidad de los datos resulta muy útil al utilizar algoritmos matemáticos para la creación de los modelos de predicción. Así, cuando una empresa o departamento de mantenimiento que haya digitalizado sus operaciones despliegue la última versión de un modelo predictivo en el entorno *Edge* instalado en una máquina, su "inteligencia digital" no estará basada únicamente en los sucesos registrados en ese dispositivo *Edge*, sino que tendrá el conocimiento adquirido desde los datos históricos de todas las máquinas que hayan enviado información al entorno *Cloud* y que utilicen componentes similares.

En la arquitectura que proponemos, el aprendizaje de nuevos modelos matemáticos se realiza en el nivel *Cloud*, donde podemos aprovechar su gran capacidad de cómputo y

flexibilidad en el dimensionamiento de recursos. La ejecución de los modelos se realiza habitualmente en el nivel *Edge*, dado que es conveniente ejecutar el modelo aprendido "cerca de la máquina" por eficiencia y para evitar trasiego de datos por Internet.

Administración y orquestación

Un canal trasversal debe administrar y desplegar las instrucciones pertinentes para cada una de las capas que forman parte del ciclo de vida del dato. Así, un dispositivo *Edge* sabrá qué módulo de captura debe instanciar, qué protocolo deberá utilizar, y a qué origen de datos deberá conectarse, porque recibirá la información de configuración oportuna a través del canal de administración. Todas las capas cuentan con un conector a través del cual pueden intercambiar información con dicho canal de administración, que está gestionado por un sistema central, pero que también es utilizado para el intercambio de mensajes de administración entre capas.

Recordemos que las aplicaciones *Edge* habitualmente se complementan entre sí formando niveles de procesamiento. El sistema de orquestación permite desplegar de manera eficiente conjuntos de aplicaciones usando contenedores, tanto en dispositivos *Edge* como en entorno *Cloud*. También gestiona para las aplicaciones la comunicación entre ambos entornos, y añade un canal de telegestión para el personal técnico.

Conclusiones

En este artículo hemos identificado las posibles amenazas de seguridad a las que pueden ser vulnerables las plataformas de digitalización de las operaciones de mantenimiento, así como las diferentes contramedidas que se pueden utilizar para afrontarlas. Estas medidas deben estar integradas en una arquitectura por capas desacopladas que garantice un funcionamiento seguro de dichas operaciones, ofreciendo características beneficiosas adicionales como mantenibilidad de la plataforma, alta escalabilidad, garantías de evolución a futuro, y posibilidad de elección de componentes. Las empresas y departamentos de mantenimiento industrial que implementen e implanten de forma adecuada el diseño de arquitectura aquí propuesto optimizarán de forma significativa sus operaciones, y lograrán un aumento en su seguridad física, manteniendo bajo control los riesgos digitales derivados de desplegar una plataforma de estas características.

Referencias

[1] Jiafu Wan et al, «A Manufacturing Big Data Solutions for Active Preventive Maintenance,» *IEEE Transactions on Industrial Informatics.*

[2] Jun Zhu et al, «A new data-driven transferable remaining useful life prediction approach for bearing under different working conditions,» *Mechanical Systems and Signal Processing,* vol. 139, 2020.

[3] Jazdi, N., «Cyber physical systems in the context of Industry 4.0,» *IEEE International Conference on Automation, Quality and Testing, Robotics,* 2014.

[4] European Federation of National Maintenance Societies, «European Federation of National Maintenance Societies web site,» [En línea]. Available: https://www.efnms.eu/about-us/what-does-efnms-stand-for/. [Último acceso: 23 01 2020].

[5] Real Academia Española, «Seguro, ra,» [En línea]. Available: https://dle.rae.es/seguro. [Último acceso: 25 01 2020].

[6] McConnell, Steve, Code Complete, Microsoft Press.

[7] Kan, Stephen H., Metrics and Models in Software Quality Engineering.

[8] MITRE Corporation, «Common Vulnerabilities and Exposures,» [En línea]. Available: https://cve.mitre.org/. [Último acceso: 10 01 2020].

[9] Greenborne Networks, «OpenVAS - Open Vulnerability Assessment Scanner,» [En línea]. Available: https://www.openvas.org/#about. [Último acceso: 23 01 2020].

[10] Wikipedia, «Captcha,» [En línea]. Available: https://es.wikipedia.org/wiki/Captcha. [Último acceso: 17 01 2020].

[11] Shodan, «Shodan,» [En línea]. Available: https://www.shodan.io/. [Último acceso: 01 02 2020].

[12] Y. Sheffer et al, «Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS), RFC 7525,» *Internet Engineering Task Force (IETF).*

[13] Behrad Bagheri et al, «Cyber-physical Systems Architecture for Self-Aware Machines in Industry 4.0 Environment,» *Center for Intelligent Maintenance Systems, University of Cincinnati Cincinnati, OH, USA.*