CENTRO DE INNOVACION UC
ANACLETO ANGELINI

TERRA QUANTUM TECHNOLOGY

Failover y continuidad operacional en redes industriales

***Abstract*—En redes industriales, la continuidad operacional depende de la capacidad del sistema para mantener conectividad incluso cuando un enlace falla o se degrada. El failover permite redirigir automáticamente el tráfico hacia un camino alternativo, reduciendo el impacto de una interrupción sobre la operación. Este artículo explica, desde una perspectiva divulgativa, cómo funcionan los mecanismos de detección, conmutación y estabilización en redes resilientes aplicadas a entornos críticos como la minería subterránea.**

I. Introducción

En sistemas industriales, la comunicación debe ser confiable, estable y capaz de responder ante fallas. No basta con que una red funcione correctamente en condiciones ideales; también debe mantener operación cuando aparecen interrupciones, degradaciones o cambios inesperados en el entorno [1].

Esta necesidad es especialmente importante en minería subterránea, donde la conectividad permite monitorear sensores, coordinar equipos, transmitir alertas, registrar eventos y apoyar la seguridad del personal. Una pérdida de comunicación puede afectar directamente la continuidad operacional y la capacidad de respuesta ante incidentes.

Para enfrentar este desafío, las redes industriales utilizan mecanismos de redundancia y conmutación automática. Uno de los más relevantes es el failover, que permite cambiar el tráfico desde un enlace afectado hacia otro enlace disponible [1], [2].

II. Concepto de failover

El failover es la capacidad de un sistema para redirigir automáticamente el tráfico cuando detecta que el enlace principal ha fallado o ya no cumple condiciones mínimas de operación. Su objetivo es evitar que una falla puntual provoque la interrupción total del servicio [1].

Por ejemplo, una red puede utilizar un enlace óptico como camino principal y un enlace inalámbrico como respaldo. Si el enlace óptico se interrumpe por bloqueo, desalineación o pérdida de señal, el sistema puede enviar el tráfico por el enlace alternativo [3], [4].

Este proceso debe ocurrir sin intervención manual. Para ello, el sistema necesita monitorear continuamente el estado de los enlaces, detectar cambios de disponibilidad y actualizar la ruta utilizada para transportar datos.

En una arquitectura híbrida, el failover permite que distintas tecnologías trabajen de forma coordinada. No se trata solo de tener más enlaces, sino de gestionarlos inteligentemente.

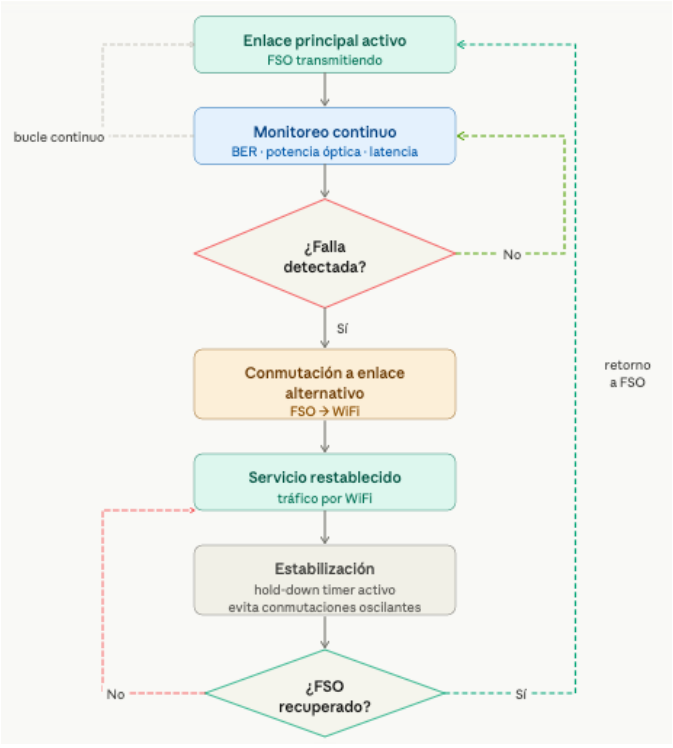

Fig. 1. Secuencia de failover con monitoreo, conmutación a enlace alternativo, estabilización y failback controlado.

III. Monitoreo y detección de fallas

Para aplicar failover, primero es necesario detectar que un enlace presenta problemas. Esto puede realizarse mediante pruebas periódicas de conectividad, medición de pérdida de paquetes, latencia, jitter, estado de interfaz o disponibilidad de un gateway [1].

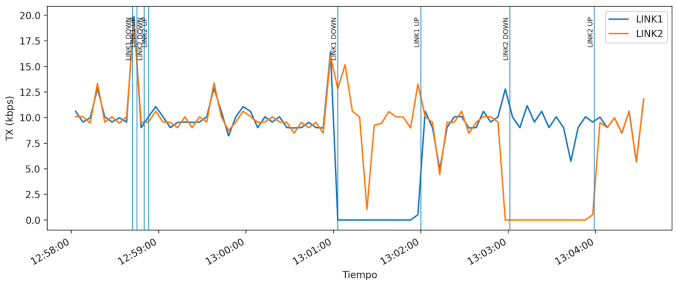

Fig. 2. Registro temporal de eventos UP/DOWN y tasas de transmisión por enlace, utilizado para analizar detección de fallas, recuperación y estabilidad post-conmutación.

Un router industrial puede ejecutar mecanismos de health-check para verificar si cada ruta sigue operativa. Si un enlace deja de responder durante un tiempo definido, el sistema puede declararlo en estado DOWN. Cuando vuelve a responder de forma estable, puede declararlo nuevamente en estado UP.

Dos indicadores importantes son T_{detect} y T_{switch}. El primero representa el tiempo que tarda el sistema en detectar la falla. El segundo corresponde al tiempo necesario para restablecer el servicio mediante un enlace alternativo.

Mientras menores sean estos tiempos, menor será la interrupción percibida por la aplicación. Sin embargo, si los umbrales son demasiado agresivos, el sistema puede reaccionar ante variaciones momentáneas que no representan una falla real.

IV. Conmutación hacia un enlace alternativo

Una vez detectada la falla, el sistema debe redirigir el tráfico hacia una ruta disponible. Esta conmutación puede realizarse modificando rutas, cambiando prioridades, desactivando gateways no alcanzables o aplicando políticas de selección de camino.

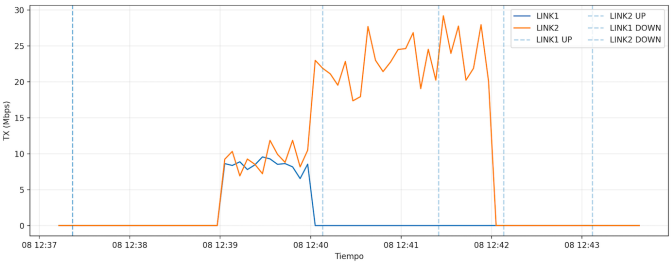

Fig. 3. Comportamiento de tráfico por enlace durante una prueba de conmutación: ante la caída de LINK1, el tráfico se sostiene por LINK2, evidenciando continuidad mediante enlace alternativo.

En redes IP, los routers pueden mantener varias rutas posibles hacia un destino. Cada ruta puede tener una prioridad diferente. Si la ruta principal pierde disponibilidad, el tráfico puede migrar hacia la ruta secundaria.

En algunos escenarios, la conmutación puede afectar de forma distinta a los flujos existentes y a los nuevos flujos. Por ejemplo, ciertas políticas mantienen sesiones ya establecidas por el mismo camino hasta que finalizan, mientras que nuevas conexiones pueden usar el enlace recuperado o alternativo.

Por esta razón, no basta con observar si un enlace vuelve a estar disponible. También es necesario analizar cómo se redistribuye el tráfico después de una falla y cómo se comportan las aplicaciones durante la recuperación.

V. Estabilidad post-recuperación

Cuando un enlace vuelve a estar disponible, el sistema debe decidir si retorna inmediatamente al camino original o si mantiene el tráfico por el enlace alternativo durante un tiempo. Esta etapa se conoce como failback.

Si el retorno al enlace principal ocurre demasiado rápido, puede producirse oscilación entre rutas. Este fenómeno se conoce como flapping y ocurre cuando un enlace cambia repetidamente entre estados UP y DOWN.

Para evitarlo, se utilizan mecanismos como histéresis y hold-down. La histéresis evita declarar cambios de estado ante variaciones breves o poco significativas. El hold-down define un tiempo mínimo de espera antes de volver a utilizar un enlace recuperado.

Estos mecanismos permiten que la red sea más estable y evitan decisiones apresuradas frente a condiciones temporales del entorno. En minería subterránea, donde pueden existir bloqueos momentáneos, polvo o vibración, esta estabilidad es fundamental.

VI. Continuidad operacional en minería

En minería subterránea, la continuidad operacional no depende únicamente de la velocidad del enlace. También

depende de la capacidad del sistema para sostener servicios críticos cuando las condiciones cambian.

Un sistema resiliente debe ser capaz de detectar fallas, conmutar tráfico, estabilizar el servicio y registrar evidencia de lo ocurrido. Esta trazabilidad permite analizar el comportamiento de la red y mejorar su configuración en futuras pruebas.

Por ejemplo, si un enlace FSO pierde línea de vista, el tráfico puede migrar hacia un enlace WiFi punto a punto. Si luego el enlace óptico se recupera, el sistema puede esperar un tiempo antes de volver a utilizarlo, evitando oscilaciones innecesarias.

De esta forma, la red no se diseña solo para transmitir datos, sino para mantener operación bajo condiciones reales. Este enfoque es esencial en ambientes industriales donde la pérdida total de comunicación puede afectar seguridad, productividad y control.

VII. Conclusión

El failover es un mecanismo clave para mantener continuidad operacional en redes industriales. Permite que el tráfico se redirija automáticamente hacia un enlace alternativo cuando el camino principal falla o se degrada.

Para que este proceso sea efectivo, se requiere monitoreo continuo, criterios claros de detección, tiempos de conmutación adecuados y mecanismos de estabilización post-recuperación. Conceptos como T_{detect}, T_{switch}, histéresis, hold-down y control de flapping son fundamentales para interpretar el comportamiento de la red.

En minería subterránea, donde el entorno puede afectar la disponibilidad de los enlaces, el failover permite pasar de una falla total a una degradación controlada. Así, la arquitectura de comunicación se vuelve más resiliente y capaz de sostener servicios críticos aun frente a condiciones adversas.

Proyección y pilotaje

Los mecanismos de failover deben validarse mediante fallas inducidas, mediciones de tiempos de detección y conmutación, y análisis de estabilidad post-recuperación. El pilotaje permitirá comprobar si la arquitectura puede sostener servicios críticos bajo condiciones más cercanas a la operación minera. Conoce más sobre las oportunidades de pilotaje y validación tecnológica que TerraQuantum busca desarrollar junto al ecosistema minero:

Leer la nota completa en Reporte Minero

References

[1] S. Scanzio, L. Wisniewski, and P. Gaj, "Heterogeneous and Dependable Networks in Industry—A Survey," *Computers in Industry*, vol. 125, Art. no. 103388, 2021, doi: 10.1016/j.compind.2020.103388.

[2] G. Cena, S. Scanzio, and A. Valenzano, "Experimental Evaluation of Seamless Redundancy Applied to Industrial Wi-Fi Networks," arXiv:2210.16404, 2022.

[3] Y. Wu, M. Jiang, G. Li, and D. Kong, "Systematic Performance Analysis of Hybrid FSO/RF System over Generalized Fading Channels with Pointing Errors," *Photonics*, vol. 9, no. 11, Art. no. 873, 2022, doi: 10.3390/photonics9110873.

[4] J. Shao, Y. Liu, X. Du, and T. Xie, "Adaptive Modulation Scheme for Soft-Switching Hybrid FSO/RF Links Based on Machine Learning," *Photonics*, vol. 11, no. 5, Art. no. 404, 2024, doi: 10.3390/photonics11050404.

Proyecto apoyado por

CORFO