I. PROYECTO OMNISEC

En una compañía de gas, los oleoductos de sus instalaciones transportan distintos tipos de gas. Existen sensores electrónicos que monitorean hidrocarburos en esos oleoductos. Estos sensores monitorean continuamente y reportan datos en tiempo real, garantizando que exista precisión y consistencia en los mismos.

Los datos recolectados se envían a un computador industrial, que puede almacenar hasta 8 reportes y enviarlos a una impresora local o remota. Los reportes se pueden generar a diario, cada hora o bajo demanda. Un operador ingresa los datos desde el reporte impreso a un sistema de información de la compañía para realizar análisis de datos operacional y para persistencia de los mismos.

Sin embargo, este proceso no está excento de amenazas, tales como modificación de los datos por parte de ciertos operadores o indisponibilidad de los mismos, debido a algún tipo de negligencia o ineficiencia humana.

Para abordar estas amenazas, se diseñó un Sistema Ciberfísico (CPS) que recolecta, procesa, integra y reporta los datos de los sensores a usuarios finales y sistemas externos (ERP)

A continuación se especifican los requisitos no funcionales del proyecto:

- **Integridad.** El sistema debe contar como mecanismos para prevenir acceso no autorizado por parte de terceros para manipular los datos asociados a los reportes, configuraciones y recursos del sistema operativo. Debe garantizar la consistencia de los datos almacenados. Adicionalmente, los canales de comunicación deben estar seguros para evitar la manipulación de los datos.
- **Confidencialidad.** Sólo los usuarios autorizados deben poder acceso de leer información de los recursos de OmniSEC, incluyendo reportes, configuraciones, accesos a sistema operativo. Los canales de comunicación deben tener mecanismos para prevenir que sean interceptados durante la transmisión de datos.
- **Disponibilidad.** El sistema debe proveer continuidad operacional incluso si alguno de los componentes, ya sea de hardware o software fallan.
- **Auditabilidad.** El sistema debe permitir a usuarios autorizados reconstruir y supervisar eventos en curso o históricos.
- **Performance:** El sistema debe tener un tiempo de respuesta aceptable para no impactar negativamente en las métricas que se supervisan en tiempo real.
-

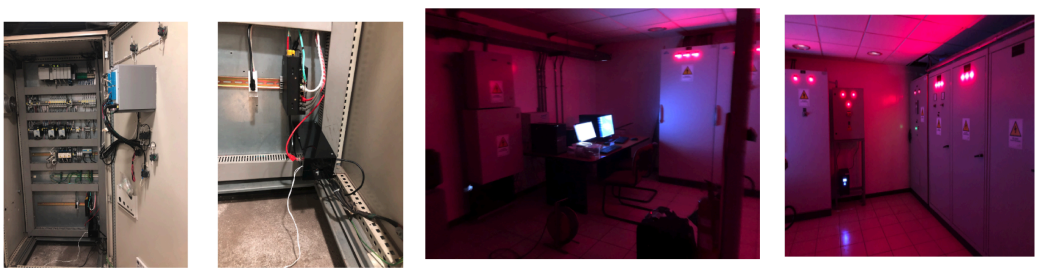
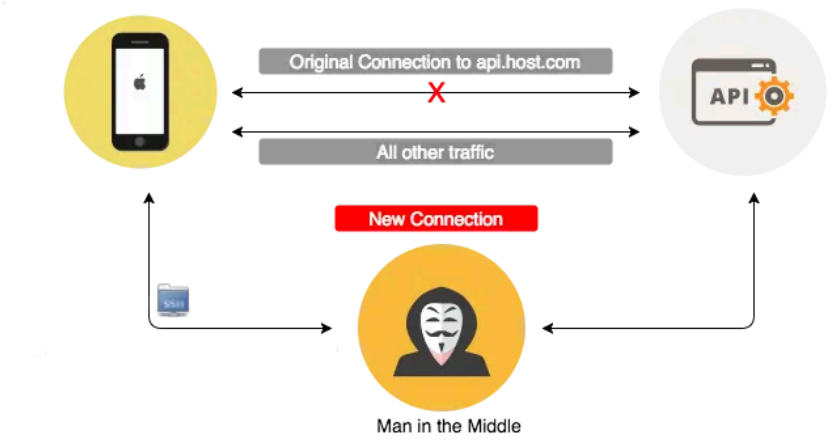


Fig 1. Sala eléctrica de Compañía de Ga

II. ESCENARIO: MAN IN THE MIDDLE



Un adversario ataca la comunicación entre dos componentes (normalmente, cliente y servidor) para alterar u obtener datos de las transacciones. Un método general consiste en que el adversario se coloque dentro del canal de comunicación entre los dos componentes. Esta interposición es transparente, lo que hace que los dos componentes afectados no sean conscientes de la posible corrupción o fuga de sus comunicaciones.

En términos generales se tiene el siguiente escenario:

- **Origen:** Un usuario malicioso que es externo a la organización
- **Acción:** El usuario realiza un ataque para leer, capturar y eventualmente modificar datos.
- **Elementos comprometidos:** Servicios de sistema, datos recolectados por estos sistemas y transmitidos hacia servidores
- **Entorno:** El sistema está conectado a Internet, totalmente operativo.