Sin precedente - Niveles de seguridad ciber física para redes

Donde la seguridad importa: Seguridad Cuántica embedida en el hardware

Tradicional cibernética seguridad Soluciones son software basado y hacer no proteger redes más allá de Ethernet y el Internet Protocolos (IP).

Por debajo de este nivel, los sistemas de control utilizan protocolos y lógica que conectan dispositivos del mundo real que a menudo son críticos en tiempo real y de seguridad. El dominio ciberfísico donde Internet interactúa con dispositivos físicos en el entornode las redes.

En un mundo cada vez más conectado, los sistemas de control son los componentes centrales de la infraestructura nacional: el tejido de la sociedad en energía, transporte, fabricación, distribución y centros de datos.

Estas redes también son cada vez másatacadas por los adversarios como un punto débil para acceder a sistemas empresariales bien protegidos, inducir impactos físicos, posiblemente a escala y poner en peligro la vida, las empresas, las economías y la resiliencia nacional.

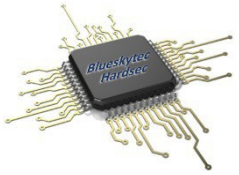
Blueskytec protege de forma única los sistemas de control de los ciberataques a nivel de dispositivo y protocolo de dispositivo. 'Edge Point Cyber Security'.

Las aplicaciones van desde IoT (Internet de las cosas), complejos sistemas de control de IoT industrial (IIoT), tecnología operativa (OT) e infraestructura, incluso sistemas basados en el espacio. Security even contra la próxima generación de ciberataques de inteligencia artificial (IA) impulsados por ordenadores cuánticos.

Una solución de "sistema de sistemas" de bajo costo que proporciona niveles de seguridad sin precedentes a nivel de dispositivo y telemetría independiente para mejorar la resiliencia, la detección de anomalías y la gestión de la configuración central, incluida la adición de aplicaciones.

Seguridad basada en silicio - Hardsec

Blueskytec implementar seguridad en silicio - FPGAs, esto se conoce Como Hardsec (https://hardsec.org).



El software impulsó la revolución de la información, pero contra él vino el problema del problema de la seguridad. El software por sí solo no puede alcanzar los niveles de seguridad, rendimiento y fiabilidad necesarios cuando es importante.

- En el borde de las redes.

Las FPGA proporcionan una solución simple de bajo costo. Procesan decenas de miles de elementos lógicos en paralelo a cada ciclo de reloj donde el software ejecuta línea por línea.

El silicio también proporciona un límite de seguridad inexpugnable que proporciona autenticación al 100% y protección contra manipulaciones para garantizar que los dispositivos No se puedan copiar, modificar o manipular.

T-HUMS de Blueskytec
Módulo de seguridad de punto de borde (EPSM) y rastreador

- ✓ Rastreador ciberseguro de bajo costo y sensor de monitor de salud y uso (Alarmas)
- ✓ También protege los dispositivos perimetrales de rojo de terceros cuando se integra un nivel de circuito o como una aplicación de seguridad de factor de forma
- ✓ Seguridad multinivel y multifunción masivamente escalable, incluso para sistemas heredados
- ✓ Interfaces estándar abiertas contra configurabilidad y actualizabilidad 'Enchufe y encender'
- ✓ La integración contra US-EPM de Blueskytec garantiza una seguridad completa en Internet: sepa que su nube es segura

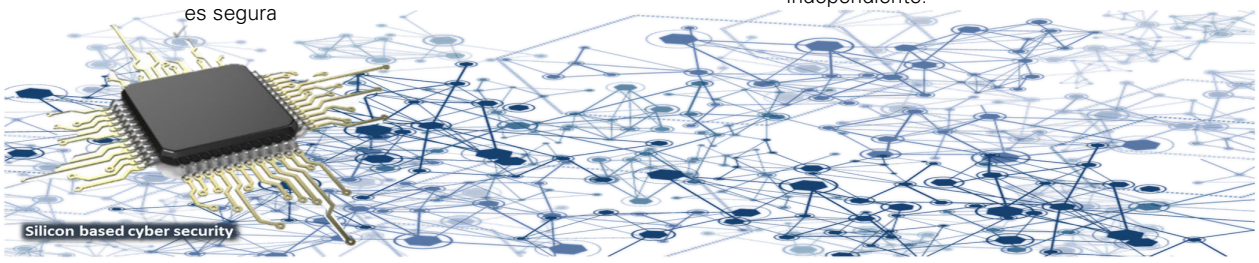
Módulo de seguridad de punto de borde T-HUMS (EPSM) de Blueskytec

El *T-HUMS EPSM* de Blueskytec asegura los dispositivos de punto de borde, también es un rastreador autónomo y un sistema de monitoreo de salud y uso (HUMS) para mantenimiento y resiliencia.

El módulo IoT de factor de forma pequeño proporciona una seguridad completa a los dispositivos de punto de borde y sussensores de eemetría independientes (GPS, voz, ruido, vibración, potencia y corriente) proporcionan una protección adicional contra anomalías que también puede ser utilizada por los ingenieros de sistemas de control para proporcionar características y aplicaciones adicionales del sistema .

Para ilustrar el grado único de re-configuration disponible en estos pequeños dispositivos, Nuestro cliente ONU utilizó T-HUMS como rastreador ciberseguro para sus activos a través de la 'Nube' y luego nos pidió que implementáramos puntos de venta sin efectivo en los activos, todos configurados centralmente, distribuidos de forma remota y seguros utilizando T-HUMS.

El control de los dispositivos de punto de borde se puede configurar para que sea totalmente pasivo o completamente activo para proteger los dispositivos de punto de borde y evitar todo acceso a cualquier interfaz de alimentación, señal, hombre-máquina o configuración. Todas las Interfaces hijo entonces física y electrónicamente seguras, protegidas contra manipulaciones y monitoreadas de forma independiente.



BLUESKYTEC
BLUESKYTEC LTD
18a James St West,
Bath, BA1 2BT, UK.
t: +44 (0) 1225 471086
w: www.blueskytec.com
e: enquiries@blueskytec.com

Sin precedente - Niveles de seguridad ciber física para redes

Gestor de puntos finales ultra seguros de Blueskytec (US-EPM)

Blueskytec's Ultra Seguro Fin Punto director (ULTRA SECURE-EPM) *conecta decenas de miles de T-HUMS EPSM para monitorear y proteger sus activos y proporcionar control central y comunicaciones. También puede ser Utilizado en el borde de la nube para garantizar que sus servicios en la nube sean ultraseguros, independientemente de quién los opere.

Esta conectividad puede ser un servicio alojado desde el sitio seguro de Blueskytec o en sus propias instalaciones.

Para indicar el grado de escalabilidad disponible, cada US-EPM puede tener una, dos, tres o más unidades de rack de altura y cada unidad puede acomodar de seis a ocho módulosque pueden acomodar decenas de miles de dispositivos, puntos de borde y puntos finales (IP).

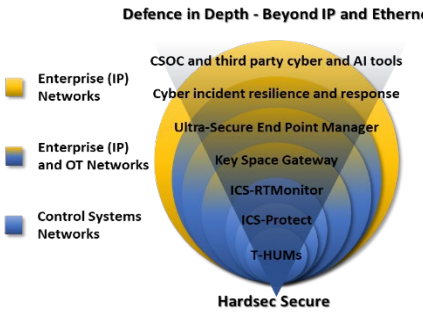
Cada módulo proporciona toda la funcionalidad segura de Key Space Gateway (KSG)* de Blueskytec, lo que permite configurar grupos o roles de usuarios cerrados seguros e ilimitados para la seguridad multinivel y multifunción.

Para entornos IIoT exigentes que requieren más interfaces y procesamiento, T-HUMS EPSM y US-EPM se pueden complementar con ICS Protect* de Blueskytec y ICS Monitor* de Blueskytec para proteger, monitorear y analizar de forma independiente los sistemas de control e identificar anomalías utilizando el módulo de inteligencia artificial y aprendizaje automático (AIMLM*) de Blueskytec.

US (ULTRA SEGURO) – EMP

- ✓ Seguridad completa en la nube
- ✓ Integración segura de puntos de borde, puntos finales, OT/IT y redes empresariales
- ✓ Seguridad multinivel y multifunción masivamente escalable, incluso para sistemas heredados
- ✓ Interfaces estándar abiertas contra configurabilidad y actualizabilidad 'Enchufe y encender'

La gama completa de seguridad cibernética de Blueskytec impulsada por Hardsec



- ✓ Protección de seguridad cibernética para millones de puntos de borde y en toda la nube
- ✓ Protección más allá de IP y Ethernet para controlar sistemas y dispositivos físicos
- ✓ Alternativa de bajo costo a los costosos CSOC y especialistas cibernéticos
- ✓ Ciberacondicionamiento y gestión de incidentes
- ✓ Hardsec - donde la seguridad cibernética realmente importa

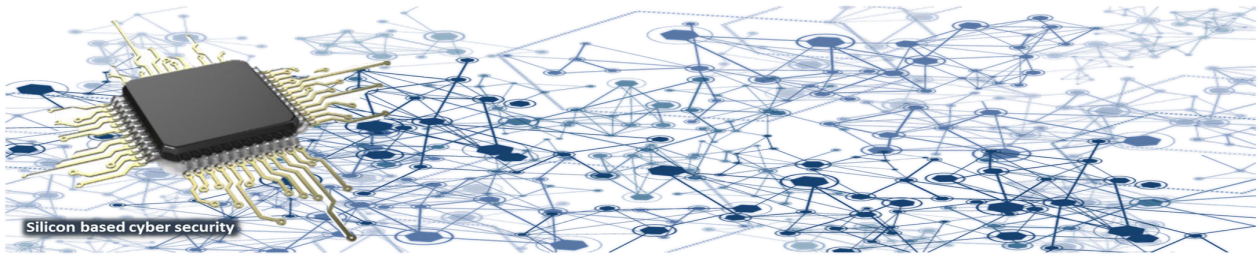
La defensa completa de Blueskytec en profundidad de la gama Hardsec

Para una confianza total en la seguridad Cibernética de toda su empresa, el sistema de Resiliencia y Respuesta a Incidentes Cibernéticos (CIRR*) de Blueskytec proporciona una alternativa de bajo costo a los Centros de Operaciones de Seguridad Cibernética (CSOC) y a los profesionales de seguridad Cibernética. Estos activos son complejos, caros y altamente especializado.

Sin embargo, cuando dichos recursos están disponibles, la gama de productos Blueskytec protégé sus redes y proporciona de manera única los sensores para su CSOC, herramientas de IA y analistas mucho más allá de IP y Ethernet y profundamente en los sistemas y dispositivos de control.

En tiempo real, CTIR identifica los incumplimientos en sus redes de TI, OT y sistemas de control frente a las políticas de seguridad, las suyas propias o las políticas de seguridad de código abierto (Cyber Essentials o NIST, por ejemplo). CIRR también identifica el riesgo contra las bases de datos de inteligencia de vulnerabilidades y amenazas (CVE, por ejemplo) y permite la priorización de cualquier acción correctiva requerida.

CIRR también proporciona una herramienta integrada de respuesta a incidentes que se puede utilizar para ejercicios técnicos y de Ciberseguridad de escritorio que integran la sala de juntas, TI, equipos operativos y soporte externo. Una forma muy rentable de garantizar una seguridad real y el retorno de la inversión.



BLUESKYTEC LTD
18a James St West,
Bath, BA1 2BT, UK.
t: +44 (0) 1225 471086
w: www.blueskytec.com
e: enquiries@blueskytec.com