
BLUESKYTEC

# Complete protection against cyber-attacks for your infrastructure


***Complete protection against 'known' and 'unknown' cyber-attacks on infrastructure***

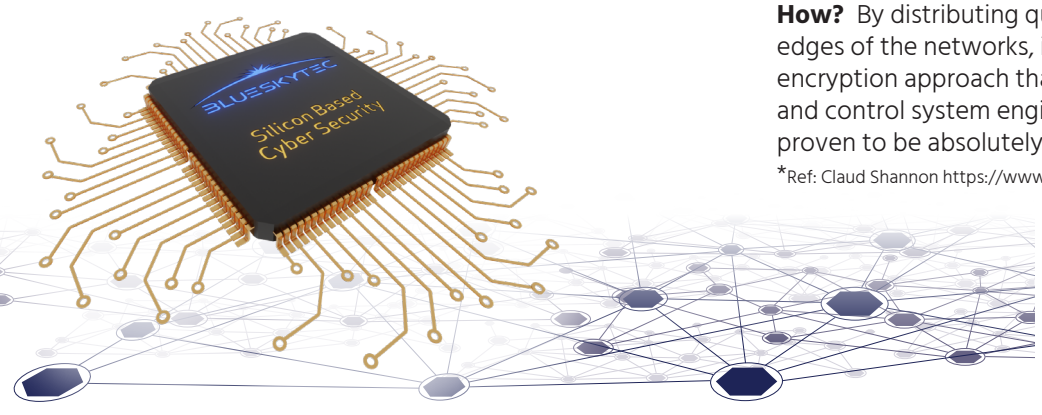
**Blueskytec provide complete cyber security protection for industrial control systems (ICS) and Operational Technology (OT), the core of your infrastructure and critical national infrastructure.**

The technology has been demonstrated to the most discerning of customers to fully secure ICS/OT against all the 'known' attacks documented in the globally definitive database - MITRE ATT&CK.

Infrastructure is subject to specific types of cyber-attacks. These include nation state advanced persistent threats (APTs), 'Zero-day' attacks and quantum computer/AI attacks that attempt brute force and decipher any encryption. Blueskytec technology, uniquely protects against these attacks – even the 'unknown' ones.

**How?** By distributing quantum derived encryption keys to the edges of the networks, in physical devices. A 'fire and forget' encryption approach that is easy to install and supported by field and control system engineers, yet one that is mathematically proven to be absolutely secure*.

*Ref: Claud Shannon https://www.itsoc.org/about/shannon




BLUESKYTEC

BLUESKYTEC Ltd, Eveleigh Waterside West,
Spring Gardens Road, Bathwick, Bath, BA2 6FL UK.
t: +44 (0) 1225 484580 w: www.blueskytec.com
e: enquiries@blueskytec.com

Central key management solutions are complex and difficult to manage. The keys can be denied or stolen and the system latency is inappropriate for real-time ICS/OT systems. With Blueskytec, without the correct key there is simply no access to the ICS/OT systems or devices.

Distributed key encryption requires that the keys are protected. Blueskytec has been granted the patent for their integrated quantum random number generator and anti-tamper solution that uses similar mechanisms throughout the design to those utilised by the military in cryptographic devices at the highest level of security.

The modern cyber security paradigm of 'zero trust' is implemented to the limit. Authentication, segmentation and audit can be at the level of every device, every user, even every transaction.

The Blueskytec KeySpace™ technology is suitable for small and large, complex, legacy systems. Fully integrated with enterprise information technology and cyber security operation centres, the technology provides security and AI to correlate the virtual and physical world through independent telemetry of the physical system.

Even if your IT becomes compromised - your ICS/OT is secure.

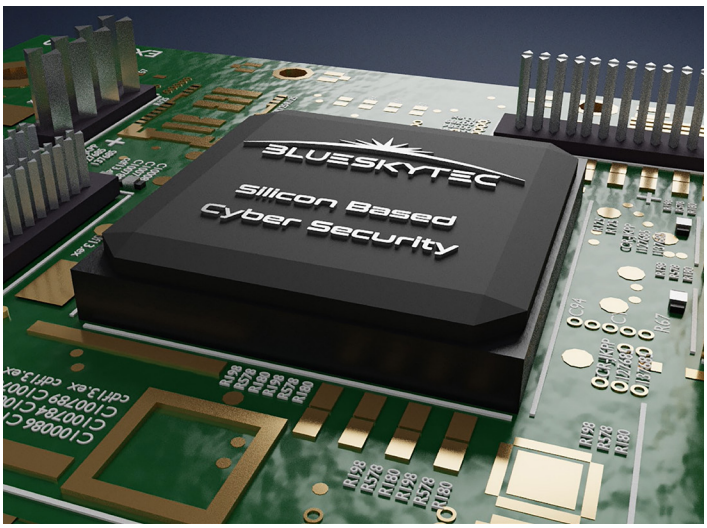
Complete security and peace of mind that your core infrastructure is secure.

## Cyber-security in silicon

Blueskytec believe that more software could simply provide new vulnerabilities for cyber-attacks to exploit - so the complete solution is based in silicon.

Protection at the level that software executes that also provides orders of magnitude more security, resilience, performance and reliability.

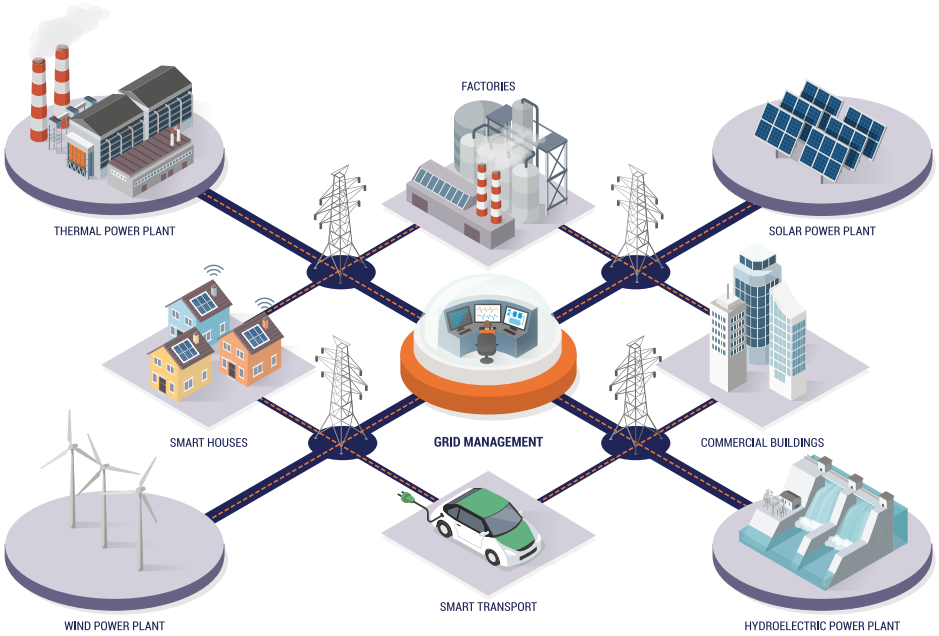
Referred to as 'Hardware Security' (Hardsec) the approach is new to the market but is now rapidly becoming adopted. The new Google phone for example now promotes the use of hardware security to provide more protection than any other phone on the market.




## Operational Technology

The Internet is probably mankind's greatest invention to date. Everyday new applications impact all aspects of modern life - globally.

IT/OT integration enables a hyper connected world and new levels of automation and resilience. Data continuously informs AI to ensure the resilience of infrastructure to faults and for example, to optimize the efficient generation, distribution and consumption of electricity.



However, the technology and levels of integration also enable new vulnerabilities and exploits for criminals and nation states intent on economic, political and military advantage. Many agencies responsible for national infrastructure are concerned that IT/OT integration could accelerate access to traditionally less well protected networks.

## Cyber-attacks

Attacks on ICS/OT and infrastructure are increasing in frequency and sophistication. In April 2022 the most sophisticated and extensive set of such nefarious tools to date were discovered - PIPEDREAM.

**Increasing frequency and sophistication of Industrial Control Systems (ICS) and Operational Technology (OT) attacks**

**2010**
STUXNET
Sophisticated malware able to disrupt nuclear enrichment projects globally, and specifically targeted at Iran's Natanz facility randomly destroying centrifuges cause similar effects

**2013**
Dragonfly & Havex
Espionage targeting electric power and petrochemical installations using OPC (Open Platform Communications) to map ICS networks for attack

**2015**
BLACKENERGY2
Attacked three energy companies in Ukraine to disrupt electricity grid operations of 225,000 customers and delay restoration efforts

**2016**
CRASHOVERRIDE & INDUSTRYOYER
Specifically design to attached high voltage electricity sub-stations. Impacted 20% of the power capacity of Kyiv, Ukraine.

**2017**
TRITON
Modified a critical safety instrumented system (SIS) in a Perto-chemical plant in Saudi Arabia designed to cause an explosion

**2022**
PIPEDREAM & INDUSTROYER 2
A complex series of capabilities designed to take control of programmable logic controllers (PLCs), target OPC (Open Platform Communications) and IEC-104 protocols to cut power

Cyber security requires complex specialist skills but exploits have been commoditized on the Internet. Now anyone can access these skills and tools, including terrorists seeking the next major incident at scale. It is surprisingly easy to search for and impact ICS/OT on the Internet, the search engines show you how.

Nation state exploits are highly classified and closely guarded until they are needed. However, even sophisticated government agencies tools have been leaked or stolen and are now commoditized on the Internet.

Together, this level of integration, complexity, vulnerability and availability of exploits creates an unfortunate 'perfect storm', a significant risk to the very fabric of society. Securing ICS/OT is not an option.

## Traditional cyber-security

Cyber security tools traditionally look for known vulnerabilities or exploits. They identify the malware by their signatures, hashes, code comparison or anomalous behaviour and look to block, remove or quarantine any malicious content.

These sophisticated technologies, cyber security tools and sophisticated cyber security operations centres (CSOCs) monitor the networks, identify anomalies, analyse the attacks and their motives and defend against them.

For cyber security professionals, monitoring the networks and understanding the issues is an important element of a strong cyber security posture. The approach works well in the enterprise IT environment where billions of people are accessing billions of web sites - a non-determinant environment. ICS/OT systems are determinant, known assets and physical devices controlled by known control systems.

However, for the 'unknown unknowns' of nation state and zero-day attacks (vulnerabilities with no identified fix available or where the vulnerability or attack approach has not been seen before) requires a different approach.

The traditional cyber security paradigm of monitoring, identifying vulnerabilities, fixing and patching them works for IT. However even the patching process could introduce new vulnerabilities and security is reliant on the brand reputation of the major IT vendors. Brands that often state in their end user licences that the software is "provided AS IS without any warranty of any kind".

Operational technology has additional concerns validating the scope and impact of the changes, down time and potential need to re-certify the system, particularly where real-time systems and safety is a concern.

The ICS/OT networks require an approach based on protection - This is where Blueskytec specialise.

## Zero Trust Architecture (ZTA)

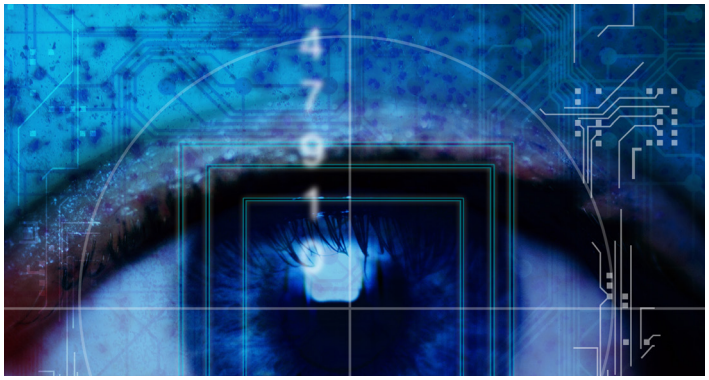
1. Know your **ARCHITECTURE**
2. Create a single strong **USER ID**
3. Create a single strong **DEVICE ID**
4. **AUTHENTICATE** everywhere
5. Know the **HEALTH** of devices
6. Focus **MONITORING** on devices
7. Set **POLICIES** according to value
8. Control **ACCESS** to your device
9. Don't trust your **NETWORK**
10. Choose **ZERO TRUST** services

'Zero Trust Architecture (ZTA)' is the modern security paradigm that is designed to overcome the limitations of 'perimeter security' (stopping access to the network at the network boundary).

ZTA assumes that the network is already compromised, that the assailant is already in the network and through segmentation the ability to traverse the network is limited.

Zero Trust looks to authenticate at the lowest possible level with multi-factor authentication and not to assume implied authentication once access is granted to the network. To always authenticate every user, data or device transaction at the lowest possible level.

So, is there a way to benefit from automation and hyperconnectivity in infrastructure and operational technology without inheriting software vulnerabilities?



## Blueskytec - encryption at the edge of the networks


Blueskytec have created 'disruptive technology' to effectively neutralise the threat of cyber-attacks against infrastructure.

Blueskytec's technology protects the infrastructure without the need for the cyber-security specialists and tools and is cost effective and readily installed and supported by field engineers and control system engineers.

The approach secures the networks to the device level and their control protocols. A 'bottom-up' approach as opposed to the traditional cyber-security solutions that take an enterprise IT 'top-down' approach that often can not reach beyond the Ethernet and Internet Protocols.


Encryption in industrial control systems remains relatively new. Blueskytec's technology applies ZTA policy all the way down to the edge, and, if required segments and authenticates to a level of every user, every device, every data transaction, all enforced by 'hi-grade' encryption.

Legacy and new systems alike can be protected and segmented into limitless 'crypto-zones', closed user groups or virtual networks, all with 100% authentication and anti-tamper enforced by encryption at device level.

Latency is negligible unlike in central key management systems like PKI or QKD where latency is inappropriate for real-time, safety-critical control systems. Key management is distributed and protected by stringent anti-tamper techniques. Blueskytec have been granted the patent for this integrated solution.

## Protecting society itself

Blueskytec talented team comes from a background of leading roles in global technology integrator companies in industrial control systems, electronic warfare, UK/US 'high grade' cryptography (military grade), national cyber projects and acquiring UK and US cyber businesses. They developed their vision for securing infrastructure from their passion in innovation and technology with an understanding of future threats from classified briefings.

Blueskytec was formed specifically to protect infrastructure from cyber-attacks from the outset. The result is a fully engineered solution that is available now and being fielded with partners in the UK, US, Middle and Far East and leading industrial control system vendors at a global scale.

No one wants to imagine a really bad day on the Internet - communications and transit systems down, fake news broadcasting global catastrophe, stock exchanges, ATM's, power, utilities and data centres and major networks all down. However, occasionally maybe we should imagine the unimaginable to inform our defence strategies - 9/11 taught us this. Any one of these 'bad day on the Internet' scenarios would seriously shake the very foundations of society.

Blueskytec's technology is applicable from IIoT (industrial IoT) sensors in the field, throughout the complete protection of power, infrastructure in our factories, logistics and transit systems and national infrastructure all the way into space. Yes, there is even a SpaceWire version.

The technology is available as an 'add-on' appliqué or integrated with infrastructure vendors equipment and architectures or deeply integrated/licensed in client circuits and silicon. Being industrial control system encryption, it is free from export controls (except for military specific variants).

Securing the future is not an option, however Blueskytec's KeySpace™ technology certainly is.


Eveleigh Waterside West,
Spring Gardens Road, Bathwick, Bath, BA2 6FL
t: +44 (0) 1225 484580
w: www.blueskytec.com
e: enquiries@blueskytec.com