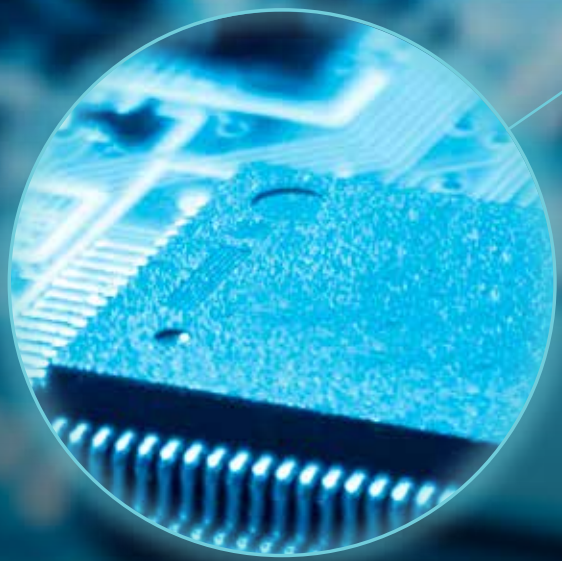
IndustrialProtect™

INTELLIGENT PROTECTION FOR CRITICAL INFRASTRUCTURE.



Applied Intelligence

BAE SYSTEMS
INSPIRED WORK

THE PROBLEM

Thanks to the internet and daily advances in science and technology, society and the way we live is continuously evolving. Technology is changing everything and connectivity between people, companies and systems is becoming ubiquitous. And yet, the systems at the heart of the industries core to all our societies – oil, gas, water, electricity, chemical plants, manufacturing, nuclear plants etc. are commonly based upon industrial control systems that were designed with more focus on operational efficiency and reliability than cyber security.

Worryingly, in an age where connectivity is pervasive, critical industrial systems that were originally not designed with security features capable of resisting malware or cyber attack, are now being connected to the internet, to each other via TCP/IP networks, and to the Cloud.

In the face of threats and risks that were previously irrelevant, but which now endanger the infrastructure upon which society depends, security solutions must now be found that can be implemented in critical systems without adversely affecting their operation.

WHAT IT DOES

IndustrialProtect is one such solution that can help those tasked with building and enforcing effective security measures into the operational technology (OT) which controls industrial systems.

IndustrialProtect™ enables high assurance information exchange between operational technology systems and corporate IT.

IndustrialProtect is built upon the premise that by maintaining secure separation between the IT and the OT (operational technology) networks, the risk and impact of any cyber attack is reduced. The purpose of the solution is to enable secure information exchange between the boundaries of the segmented networks so that business processes can continue to operate between the networks across these boundaries. It enables a remote supervisory network to communicate securely with and control elements within the control system or field systems, and facilitates secure communication between industrial systems and Business Networks, the Enterprise or Corporate LAN.

With industrial systems it is essential that the commands sent from supervisory networks to control, regulate and gather data are authentic and authorised. It is also essential that information sent from control systems to supervisory networks and beyond into the Business or Enterprise, comes from known and authorised sources, ensuring no unauthorised or untrusted data can be introduced to those networks.

In each industry, the control languages and protocols used to communicate between devices within industrial networks are specific and sometimes unique to the applications and devices being controlled. By further ensuring that communications between systems and devices are of the correct format, frequency, structure and protocol and contain only content which is relevant and allowed for communication between those devices and systems, those tasked with securing industrial networks can significantly reduce the risk of their operational technology being compromised.

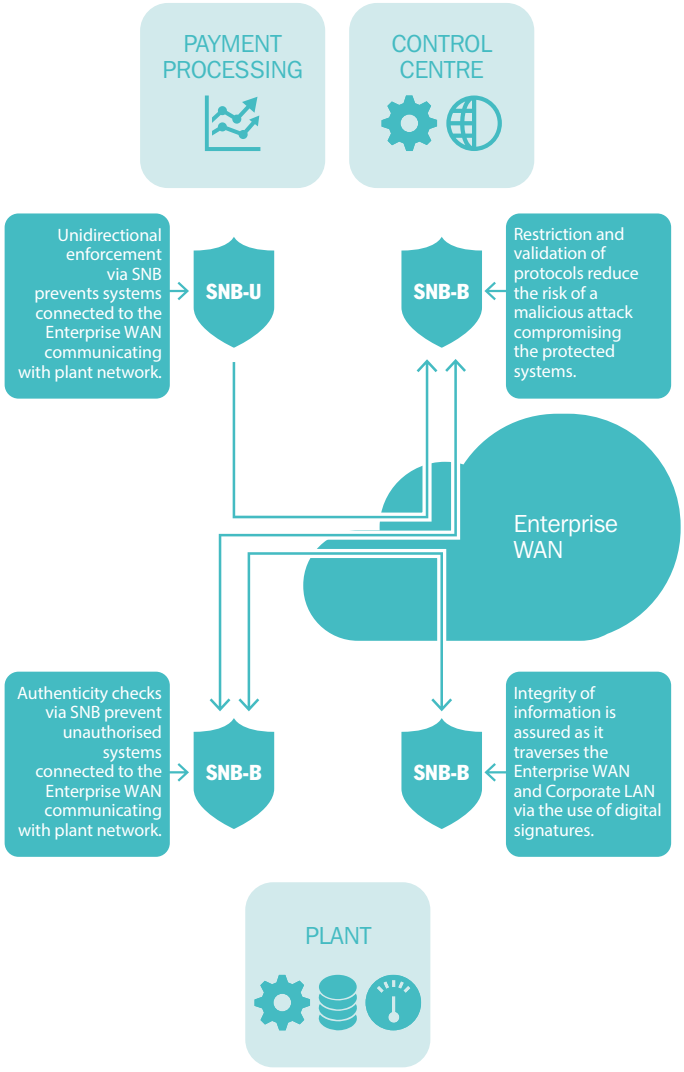
At the core of the BAE Systems IndustrialProtect solution is a hardware appliance (Secure Network Bridge - SNB) which can be deployed at the boundaries between two network segments: i.e. one SNB on the boundary of the supervisory control network or control system in a plant, and another on the Business LAN.

The direction of data flow across a boundary can be enforced to provide unidirectional or bidirectional transport.

As data enters the bridge between the network segments, the appliance acts as a proxy for the communication and repackages the data into a verifiable format, enforcing a complete protocol break. It then analyses the type, content and structure of that data, and after comparing with a white-list of authorised communications, will block any that are not agreed, relevant or correctly formatted. It then digitally signs the communication, to help provide assurance of the authorisation and integrity of the message before it leaves the system.

When the data arrives at the other side of the boundary, the recipient SNB will unpack the data, inspect it to ensure that it is from a known source and check that the data has not been changed in any way since it left that source. It will verify the information conforms to a white-list before accepting the information into that segment.

An important feature of the bridge is that the security functions are implemented in hardware, and are hence immune to software attack. These security functions assure communications between the bridges are resistant to many types of cyber attack including man-in-the-middle and malicious content injection attacks, which are common attack vectors for this type of system.



PROTOCOL SUPPORT

The protocols used to communicate will vary depending upon the industry, application and control system. IndustrialProtect currently supports OSISoft PI and JDBC protocols with additional protocols planned for release in 2014 and beyond. Our easily extensible Protocol Connector architecture allows new protocols to be added rapidly and without the need for significant change to security enforcing elements of the product.

IMPLEMENTATION AND MAINTENANCE

Implementing security solutions into existing plant operations and control systems can be risky. IndustrialProtect includes a range of services that ensure our customers can achieve the benefit of the solution with minimal operational disruption: these include consultancy and support for design, installation and transition to live operation, with a managed support and maintenance package that matches the criticality of the systems we protect.

SOLUTION BENEFITS

- Reduces the risk of ICS compromise without disrupting existing business processes
- Allows for secure two way flows of information, reducing the need for local manual processes
- Can be simply extended for other control system protocols
- Centralised management interface to simplify large scale deployments and facilitate simple management, and maintenance of remote systems
- Designed to be simple to install and integrate for rapid deployment

SUPPORTED PROTOCOLS:

- Database Apps
  - JDBC
- SCADA
  - OSISoft PI
- Monitoring
  - SNMP
  - Syslog

ABOUT US

BAE Systems Applied Intelligence delivers solutions which help our clients to protect and enhance their critical assets in the connected world. Leading enterprises and government departments use our solutions to protect and enhance their physical infrastructure, nations and people, mission-critical systems, valuable intellectual property, corporate information, reputation and customer relationships, and competitive advantage and financial success.

We operate in four key domains of expertise:

- Cyber Security – helping our clients across the complete cyber security risk lifecycle
- Financial Crime – identifying, combating and preventing financial threats, risk, loss or penalties
- Communications Intelligence – providing sophisticated network intelligence, protection and controls
- Digital Transformation – creating competitive advantage and enhancing operating performance by exploiting data and digital connectivity

We enable organisations to be more agile, increase trust and operate more confidently. Our solutions help to strengthen national security and resilience, for a safer world. They enable enterprises to manage their business risks, optimise their operations and comply with regulatory obligations.

We are part of BAE Systems, a global defence, aerospace and security company delivering a wide range of products and services including advanced electronics, security and information technology solutions.

Global Headquarters UK
BAE Systems Applied Intelligence
Surrey Research Park
Guildford
Surrey GU2 7RQ
United Kingdom

Australia: +61 (0) 1300 027 001
Dubai: +971 4369 4369
Malaysia: +60 3219 130 84
UK: +44 (0) 1483 816000
USA: +1 (617) 737 4170

E: learn@baesystems.com
W: www.baesystems.com/ai

www.twitter.com/baesystems_ai

www.linkedin.com/company/baesystemsai

Victim of a cyber attack? Contact our emergency response team on:

UK Freephone: 0808 168 6647
Australia: 1800 825 411
International: +44 1483 817491
E: cyberresponse@baesystems.com

CREST
CESG Certified Service Cyber Incident Response
CPNI Centre for the Protection of National Infrastructure