
DIGISAFE®
DATA DIODE
ST Engineering
Electronics

Recent Cyber Attacks

More devices, systems and people are connected to the internet. While interconnectivity is beneficial to businesses, the increased exposure to cyber threats requires the deployment of cyber security strategies that are practical yet current; ensuring cyber secure networks is not just practical but paramount.

Cyber attacks are escalating in number and magnitude. Recent incidents reveal the overt real-world damage caused by covert digital intrusions.

Jul 2018

Cyber attack at Algonquin College exposes data of more than 100,000 students, alumni, past and present employees via unauthorized and illegal access of database server.

Mar 2018

Ransomware attack shut down online systems in the City of Atlanta, resulting in stoppages of several applications such as bill payments and utility service requests.

Boeing hit by malware, affecting a number of computers used by its Commercial Airplanes division in North Charleston, S.C.

Oct 2017

Hackers managed to siphon $60m from the Far Eastern International Bank in Taiwan by planting a malware on its PCs and servers in order to gain access to its SWIFT terminal.

Jul 2017

Cyber attack on a North American casino though a fish tank, which had sensors connected to a PC and networks, resulted in 10GB of data being stolen.

Jun 2017

A.P. Moller-Maersk was disrupted by cyber attacks, affecting terminals at many ports including Los Angeles and Rotterdam.

Cyber attacks on Heritage Valley Health System hospitals and satellite offices cause surgeries to be rescheduled as well as the closure of laboratories and diagnostic offices.

Apr 2017

Cyber attack on Dallas emergency alarm systems set off 156 sirens routinely used for tornadoes warnings, into 15 90-second activation cycles.

DIGISAFE® DATA DIODE

Protecting the Integrity and Availability of Critical Assets

Powered by Edge-corE NETWORKS

DigiSAFE Data Diode is a unidirectional communication and data transfer gateway that enables organisations to transfer data securely across physically separated networks.

The high performance solution comes in a compact design that integrates seamlessly with users' operational environments.The security design prevents data leakage and eliminates cyber threats by enforcing the one-way data transfer at both the physical and protocol layers.

It complements ST Engineering Electronics' suite of cyber security solutions to enhance the security and resilience of Information Technology and ICS/SCADA infrastructures against cyber attacks.

Information Assurance by Design
Ensures no data leakage due to hardware-enforced one-way communication.

Highest level of Certification and Recognition
Certified under National IT Evaluation Scheme (NITES) by Cyber Security Agency of Singapore (CSA)

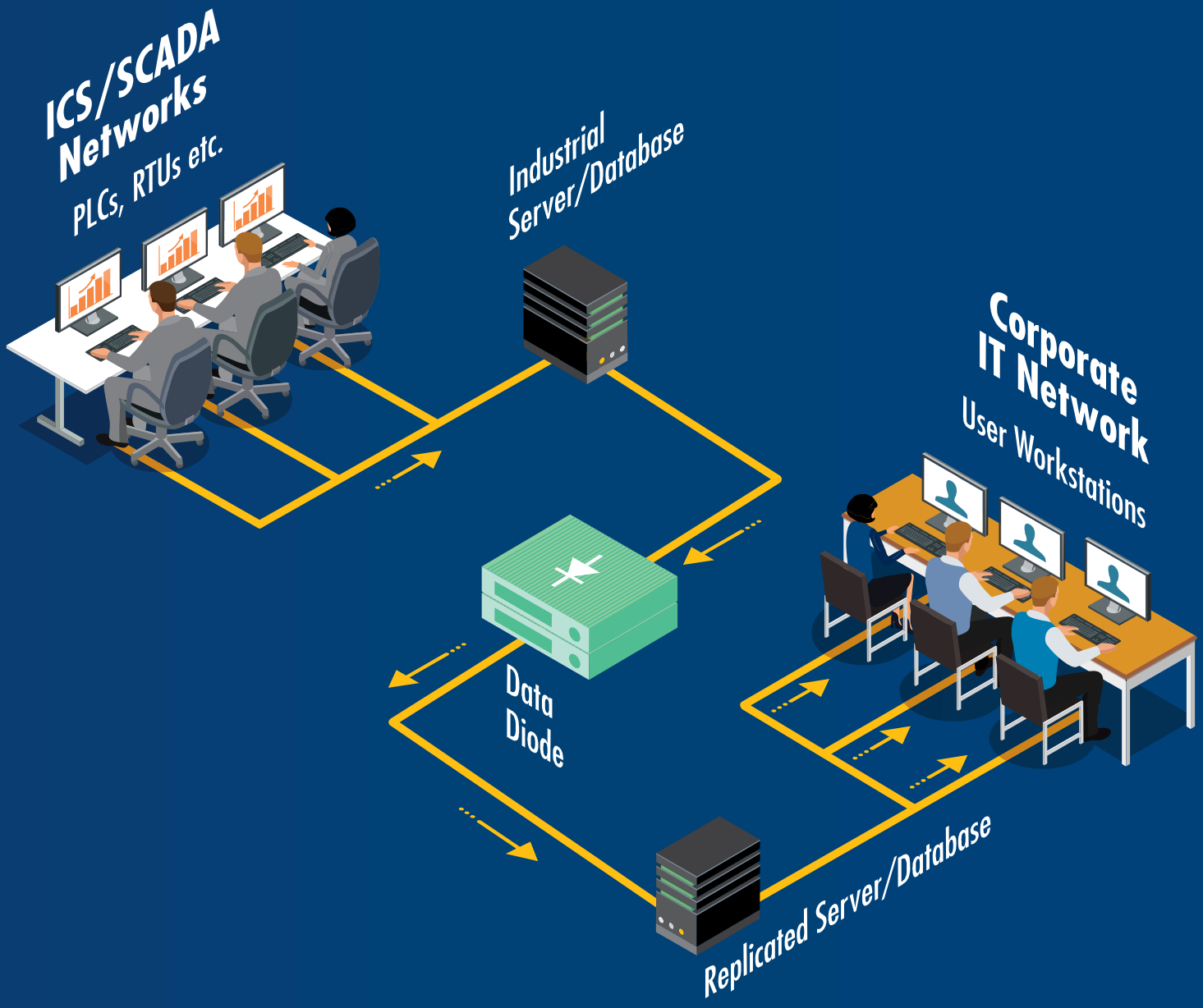
Compact Design
Reduces space required when deployed as all functionalities can be encapsulated within the servers

High Throughput & Robust Performance
Configurable for High Availability

Ease of System Integration & Customisation
Supports multiple IT and ICS/SCADA networking protocols and can be customised for any operational requirement

Protecting Industrial Control System (ICS) / SCADA Networks

Cyber threats to critical information infrastructure are on the rise. Cyber criminals have been exploiting vulnerabilities in these cyber-physical systems to cause disruption and damage.

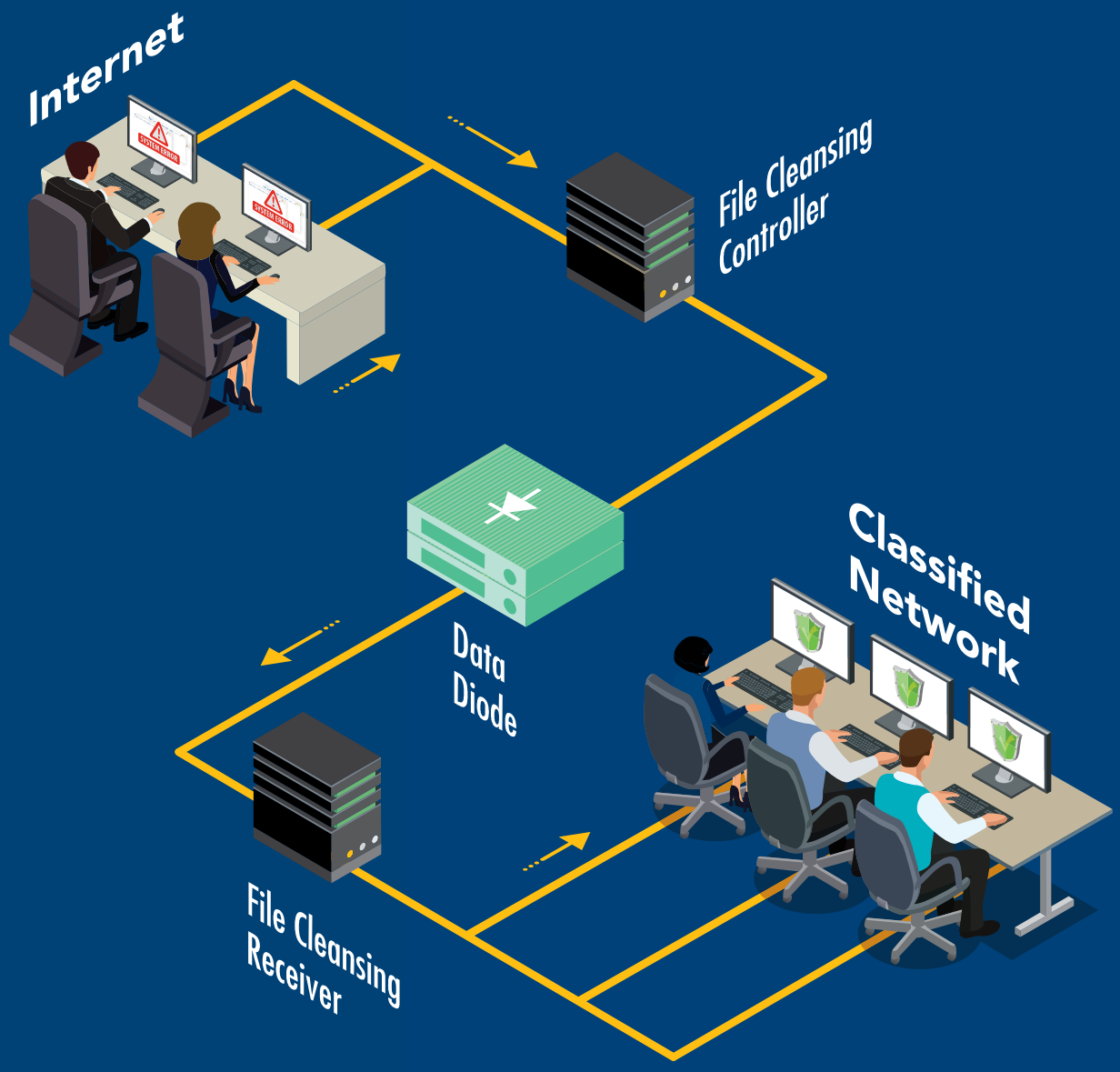


Industry 4.0 is driving the convergence of ICS/SCADA networks and corporate IT networks due to emphasis in Big Data analytics and machine learning to support productivity growth. Nonetheless, this integration of networks increases organisations' vulnerability to cyber attacks, threatening the availability and integrity of critical systems.The integration of networks increases organisations' vulnerability to cyber attacks, threatening the availability and integrity of critical assets.

DigiSAFE Data Diode is a high assurance hardware-enforced, one-way data transmission solution that protects against data leakage and enables network segregation for each of the connected networks. This allows organisations to integrate ICS networks to their corporate IT networks securely without the risk of cyber attacks.

Protecting Classified Information Systems

Protecting confidential information from leakage and networks from malware are constant challenges. The ultimate protection – complete isolation from Internet connectivity – is an impractical solution and an impediment to businesses.



DigiSAFE Secure Files Transfer solution enables trusted networks to be protected from malware intrusion and information leakage. Users are thus able to transfer files securely between networks, such as Internet and Corporate Intranet.

The solution is designed based on the principles of isolating good data, and using signature-less malware detection engines; hence simplifying the operational IT management. Integral to the solution is our DigiSAFE Data Diode. This enables very high throughput and lossless data transfers across the physically separated networks.

About ST Engineering Electronics

ST Engineering Electronics has deep engineering expertise to ensure critical infrastructures are protected, secured and responsive in dealing with such threats. We provide a holistic approach in the mitigation of risks against cyber attacks and deliver comprehensive solutions that incorporate protection, detection, response and recovery capabilities. We specialise in the design and development of advanced info-assurance and digital authentication products with emphases on people, process and technology in the formulation of an integrated cyber defence framework. We design, build, implement and operate Cyber Security Operation Centre for both government and commercial organisations.

ST Engineering Electronics has a Cyber Security Academy to address the critical shortfall of cyber security professionals. This centre offers cyber security training to enhance and strengthen the operational competencies of cyber security professionals in responding to real-life cyber threats and attacks.

ST Engineering Electronics

Singapore Technologies Engineering Electronics Limited
100 Jurong East Street 21, ST Electronics Jurong East Building S(609602)
T: (65) 6568 7118 Fax: (65) 6568 7226
E: mktg.infosec@stee.stengg.com W: www.stengg.com