DigiSAFE Data Diode

The Data Control Solution to Safeguard Your Mission Critical Systems

The Fourth Industrial Revolution (Industry 4.0) has been the driving force towards the convergence of computer networks. The main notion behind Industry 4.0 is to leverage on big data analytics and machine learning to create business value and spur productivity growth. Concurrently, the growth of the "Internet-of-things" (IoT) has seen the emergence of more communication devices and platforms ride on the expanding internet bandwidth and connectivity. These have led to Smart City initiatives in numerous metropolitan cities and urbanised areas, where the seamless flow of information is being harnessed to manage assets and utilise resources more effectively and efficiently. However, due to the ease of interaction and increased connectivity among platforms, people and devices have laid the perfect conditions for cyber attacks to take place.

Over the last decade, cyber attacks have grown in both frequency and scale. In 2017 alone, there were 5,207 breaches reported, exposing approximately 7.89 billion records and these have led to heavy financial losses and damages to corporate reputation.[1] Furthermore, as more Critical Information Infrastructure (CII) systems such as transportation and utilities become connected, the impact of cyber attacks can have greater disastrous consequences. In an investigation conducted by Verizon, hackers were able to infiltrate the water treatment system and modify the chemical levels in the plant by exploiting the vulnerabilities in the Supervisory Control and Data Acquisition (SCADA) system. Fortunately, the utility company detected the abnormality early, and halted the attack before consumers were affected. The ramifications to this act of cyber intrusion into public/civilian utility infrastructure would have been terrifying due to the high probability of the loss of lives.[2]

Solution architects generally deploy firewalls when connecting networks. A firewall acts as a barrier against external threats by regulating the flow of network traffic based on a set of predefined rules. However, if any threat disguises itself to adhere to the predefined rules, it will be able to infiltrate the

[1] Data Breach QuickView Report, Data Breach Trends – Year End 2017, Risk Based Security, Inc

[2] Data breach digest, Verizon - http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest_xg_en.pdf

networks. Furthermore, if a firewall malfunctions or is brought off-line, an open and free-for-all connection may result among the networks. Another mitigating measure against cyber-attacks is to isolate the critical systems from enterprise IT networks with a physical air-gap. Although this would represent the maximum safeguard against cyber threats originating from unsecured networks, it goes against the grain of the Industry 4.0 movement.

Data Diode - A Unidirectional Data Control Solution

A data diode is a hardware-enforced unidirectional data control network appliance which enables the transfer of data across physically separated networks to be done securely without the risks of any data leakage. Data is transmitted using one-way fibre optic communication thus it is physically impossible for data to flow in the opposite direction, even if the data diode malfunctions. The control of data flow is also enforced at the application layer by deliberate selection of appropriate communication protocols.

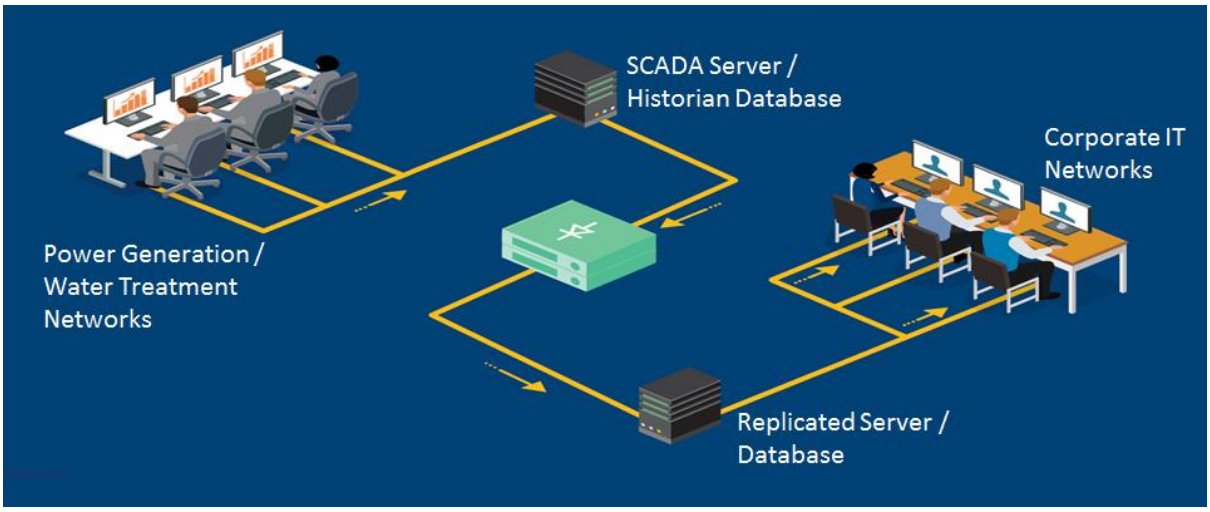

Figure 1 Securing Critical Information Infrastructure

A common application of the data diode is to protect secured networks from external threats. In such cases, it is critical for the systems to be working properly rather than to ensure that the data being transmitted is secured. Examples of such use cases would be in the CII sectors such as utilities. By connecting the SCADA networks to the enterprise IT networks securely with a data diode, operational statuses of individual utility plants can continue to be monitored centrally while remaining isolated from any cyber threats.

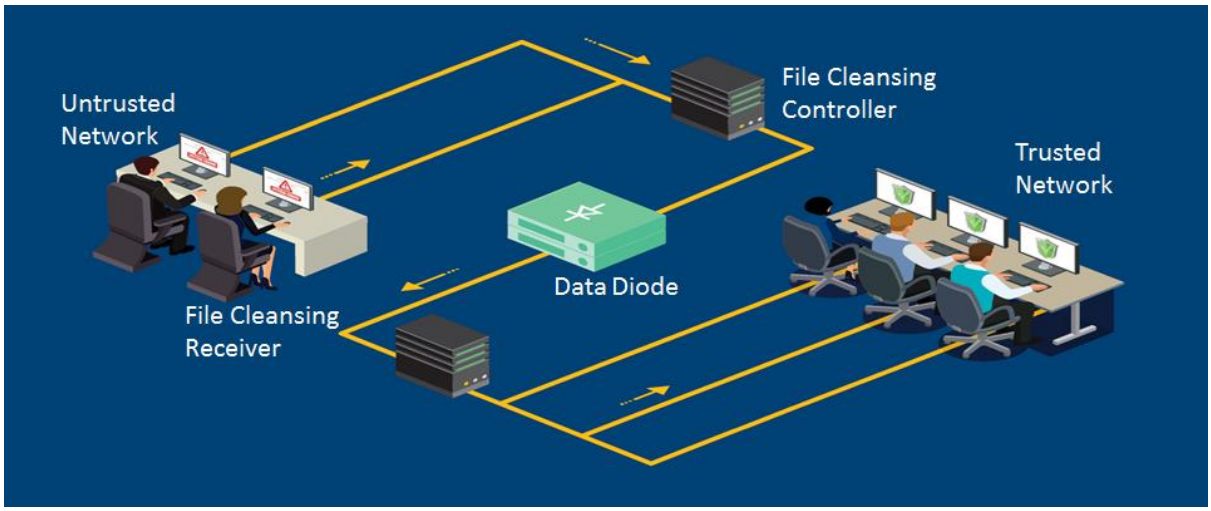

Figure 2 Securing Information and File Transfer

Another application of the data diode is to protect highly confidential or sensitive information. Common examples of such use cases would be in defence or banking sectors. The data diode will ensure a unidirectional transfer of data from an unsecured network (e.g. internet) to a trusted or closed network (e.g. intranet). In addition, the data diode can be deployed together with a file cleansing solution to ensure that malware does not infiltrate the closed network.

DigiSAFE Data Diode – Built To Support Operations

Aside from all the advantages a data diode can bring in terms of network security, there remain challenges that have prevented its implementation in many organisations. These include integration and compatibility issues which may affect the reliability of the system. Moreover, as a unidirectional data control solution, the lack of feedback on the integrity of the data transfer creates an additional problem of data loss.

DigiSAFE Data Diode has a comprehensive suite of networking protocols for ease of system integration. It is compact and can achieve a high end-to-end throughput. This allows organisations to enjoy the benefits of seamless network integration without the risk of cyber-attacks or data leakage.

DigiSAFE Data Diode is engineered with high reliability in mind to meet the most stringent operational requirement. It also has a pending patent, built-in

self-monitoring capability, which allows users to be notified in the rare event of a file or packet loss.

Certified under the National IT Evaluation Scheme (NITES), the DigiSAFE Data Diode is designed to meet stringent security of governments and financial institutions. DigiSAFE Data Diode complements ST Engineering Electronics' suite of cyber security solutions to enhance the security and resilience of Information Technology and Operation Technology infrastructures against cyber-attacks.

ST Electronics (Info-Security) Pte. Ltd.
100 Jurong East Street 21, Singapore 609602
T: (65) 6568 7118 F: (65) 6568 7226
(Regn. No.: 199902746G)