# The Research of Deploying Whitelisting Security Mechanism in Smart Grid

ICT Research Laboratory：Cheng-Hung Lin

**The Purpose of the Research**:

A main feature of smart grid (SG) is to apply advanced information & communication standard and technologies to integrate different resources, e.g. generation, transmission, distribution, electricity markets and demand-side decentralized systems.

Through two-way information exchange mechanism, SG realizes automatic real-time monitoring, self-inspection, diagnosis and repair functions. Besides it helps integrate renewable energy and provide high quality/ reliable power networks.

Comparatively communication technology increases complexity of power system, but also the risks of information leaking and tampering between communication networks. These vulnerabilities expose the system to malicious attacks, incorrect control, system damage, accidents, and eventually result in service interruptions and great economic loss to the public.

To protect industrial control networks from cyberattacks, ICS-CERT announced seven strategies to effectively defend ICSs in December 2015. According to a study conducted by ICS-CERT, there were at least 295 industrial network-related intrusions in 2015, and the seven strategies have a good chance to prevent 98% of the incidents reported that year.

Top of the seven strategies is "Deploy Application Whitelisting", which may prevent 38% of incidents. By denying unapproved applications to run on the system, whitelisting enables the network to detect and prevent malware intrusion. This strategy particularly suits for systems carrying fixed functions in OT environment, such as SCADA, human-machine interface (HMI) computers, and database systems.

In view of the said, we decided to implement whitelisting application in IEC 61850 demonstration site of Kinmen Smart Grid, a pilot system architecture between Tashan Power Plant and Sheshan Substation in accordance with the IEC 61850-90-2 substation automation standard, to strengthen the security defence capabilities of IEC 61850 critical equipment and security of power grid operation.

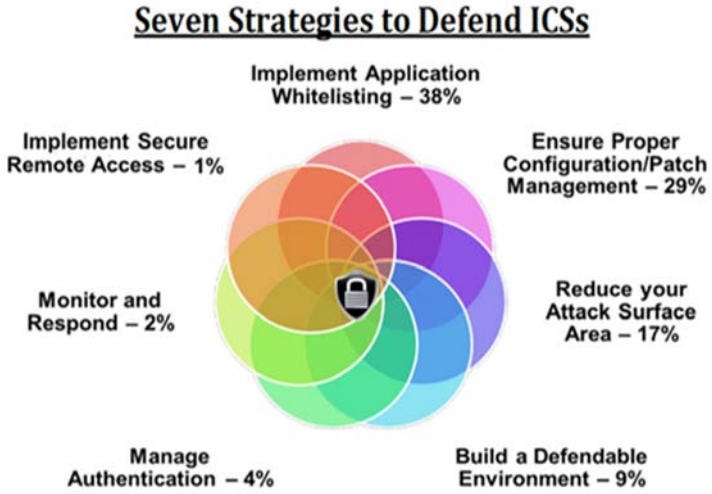


Figure 1 ICS-CERT Seven Strategies to Defend ICSs

**Research results**:

The application whitelisting deployment architecture is shown in Figure 2. The whitelist management servers are redundant hosts installed in IEC 61850 Gateway cabinet of Tashan Power Plant, and connected to the OT network of Sheshan Substation via Switch # 2, capable to manage its own IEC 61850 equipment, which includes 4 IEC 61850 Gateways, 1 IEC 61850 front-end server and 1 IEC 61850 Local SCADA.

The main functions of active whitelisting security protection management platform are as follows:

(1) Remotely enable/disable whitelisting agents for endpoints as shown in Figure 4.

(2) Records and alerts abnormal as shown in Figure 5.

(3) Manages whitelist database.

The whitelist monitoring server has been installed in the DMZ at TPC headquarters. DMZ is a secure network domain between OT network and IT network, capable to prevent hacking risks due to IT network direct access to OT network equipment. It is necessary to perform

vulnerability scan and repair for whitelist monitoring server before it provides services. After confirming no medium or high risk vulnerability, the server may receive logs from the management server through one-way device, and provide APP connection through the Internet to monitor the status of security protection for endpoints anytime and anywhere, as shown in Figure 3.

To improve system operation reliability, active whitelisting security protection management platform adopts virtualized fault tolerance technology Cuju, which is a technology capable to provide high availability of virtualized systems to ensure uninterrupted services. When the main host fails without warning, e.g. for the reasons of power off, shut down or hardware failure, service requests will be automatically transferred to the backup host to take over immediately.

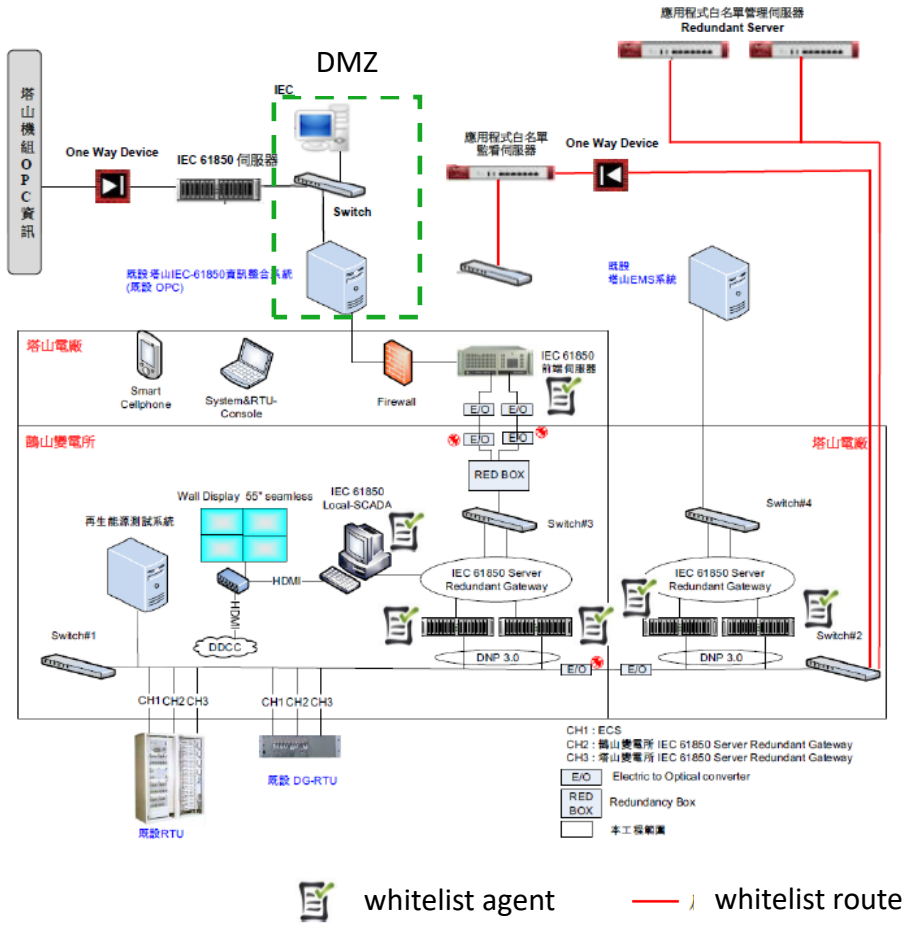


Figure 2 Application Whitelisting Deployment Architecture in Kinmen Smart Grid

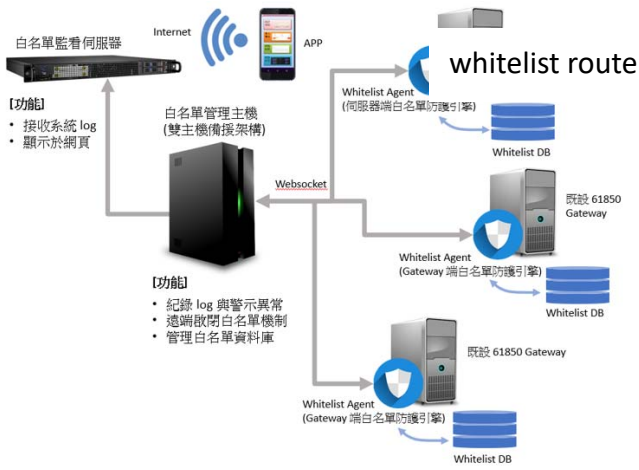


Figure 3 Application Whitelisting System Workflow


Figure 4 Enable the Whitelisting Agents for Endpoint


Figure 5 Display the Protection Status and Abnormal Statistics of Endpoints