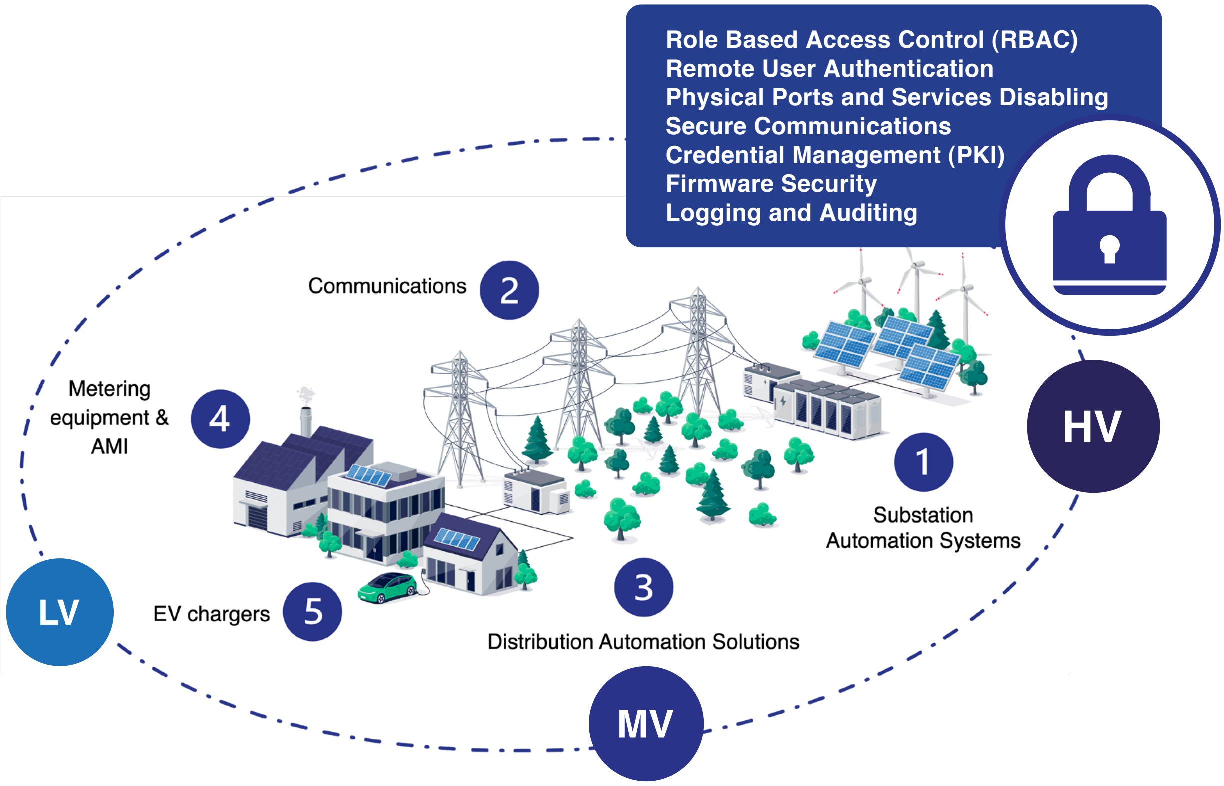
Cybersecurity

that applies to all of the company procedures & products

Cybersecure solutions in devices for smart HV, MV & LV networks

ZIV cybersecurity solutions have been created utilising the latest OT cybersecurity standards and guidelines, such as IEC 62443, IEC 62351, IEEE 1686 and NERC CIP



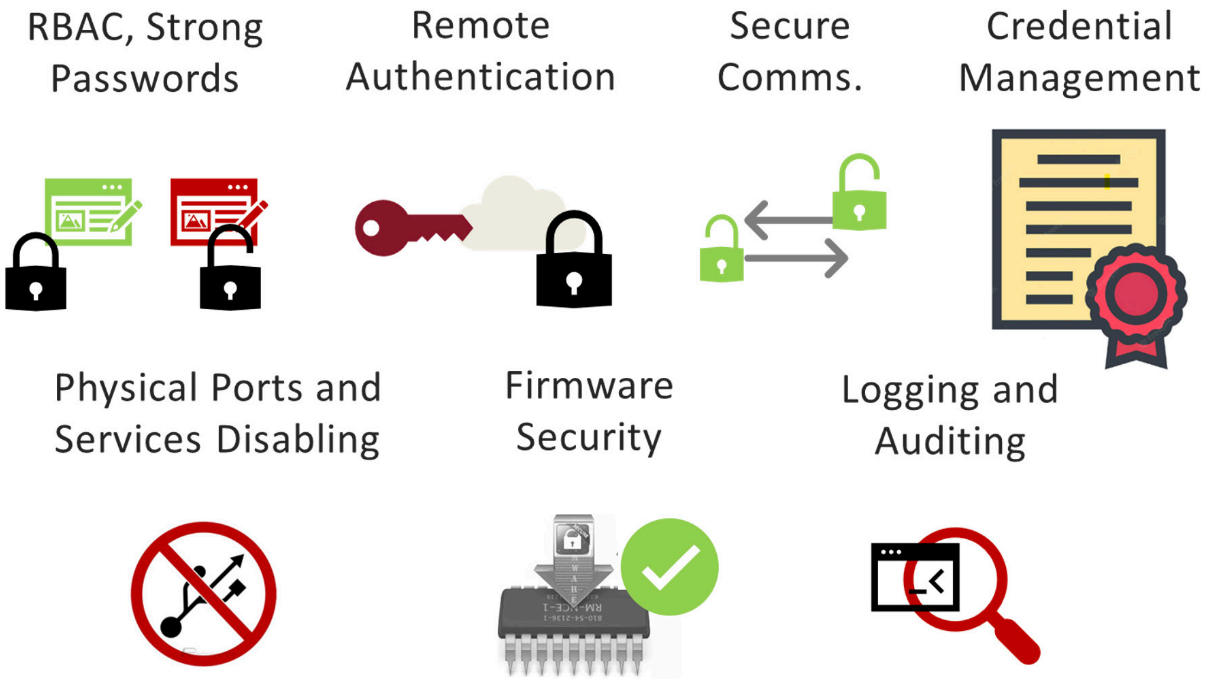
Role Based Access Control (RBAC)
Remote User Authentication
Physical Ports and Services Disabling
Secure Communications
Credential Management (PKI)
Firmware Security
Logging and Auditing

Communications 2
Metering equipment & AMI 4
HV
1 Substation Automation Systems
3 Distribution Automation Solutions
LV
EV chargers 5
MV

Cybersecurity is not just a set of functions implemented in a device, it equally applies to all the company procedures and departments.

ZIV focuses on cybersecurity throughout the entire life cycle of its products from design, implementation, testing, and manufacturing through to deployment, operation, maintenance and disposal.

Key Features



Role Based Access Control (RBAC)

Up to 10 roles can be configured in the devices, each ontaining one or more permissions (up to 7) to comply with least privilege and segregation of duty policies. Permissions are largely based on IEEE 1686.

Local and Centralised User Authentication

Users can be authenticated against LDAP or RADIUS centralised repositories, or against local user databases in the device, where up to 20 local users can be defined applying strong password policies. Return to local authentication when centralised repositories are not available can be enabled.

Physical Ports and Services can be configured, so that unused ports and services can be disabled.

Secure Communications

Secure versions of the protocols are available in the devices (SSH, SFTP, HTTPS, PROCOME over TLSv1.2, LDAPS/StartTLS). Mutual authentication is available in TLS communications.

Credential Management (PKI)

Each device has a unique X.509 identity, signed by ZIV's Certificate Authority. Trusted Certificate Authorities can be configured (CAs). Revocation (based on CRL) and expiration of remote certificates are checked during TLS communications and firmware upgrade processes.

Firmware Security

The firmware of the devices is digitally encrypted and signed by ZIV based on X.509 certificates using CMS/PKCS#7 DER format, so that only authorised and valid firmware can be uploaded to the devices.

Logging and Auditing

A wide range of cybersecurity events are generated, stored, and sent to centralised servers (up to 3) using Syslog, complying with RFC 5424, using a format largely based on IEC 62351-14 and complying with IEEE 1686 and IEC 62443 standards.