zenitel

Vipedia/Integra Public Address and Voice Alarm

Cybersecurity should be Built in, not bolt-on

zenitel.com

Intelligent Communication Meets **Cybersecurity Excellence**

Zenitel, as a technology leader in unified critical communication solutions, recognizes the growing complexity and severity of cyber threats in today's safety and security landscape. Our mission has always been to empower people and businesses to communicate clearly and securely, without the burden of managing technological complexity.

That's why we believe that having a strong cybersecurity design ethos shall be foundational for any safety and security communication solution providers. Our multi-layered defence in depth approach to security incorporates multiple layers of defence to help you with facing emerging cyber threats and keep your operations safe and secured.

Vipedia/Integra PAVA Cybersecurity

Key **Benefits**

Certified and proven solutions

We are committed to meeting and exceeding regulatory standards, compliance requirements, and industry best practices. Our adherence to **ISO 27001 and IEC 62443** ensures you peace of mind with your security concerns.

Technology leadership

Our market and technology driven approach to cybersecurity enables us to deliver industry-leading public address and voice alarm solutions with latest cybersecurity features embedded into the platform.

Expert Team

Through collaboration with leading cybersecurity organizations, Zenitel has developed in-house expertise in designing and building cyber secure public address and voice alarm solutions. With this, we assist your cybersecurity needs by providing security guidance, training, and tools aligned with industry best practices.

Helping your cybersecurity strategy through a multi-layer security approach

System availability

Ensuring system integrity from the initial boot process, preventing tampering, and verifying software authenticity.

Protect privacy of everyone

With strong key cryptography technologies, all sensitive data at rest and in transit are encrypted.

Trusted data available to the right user

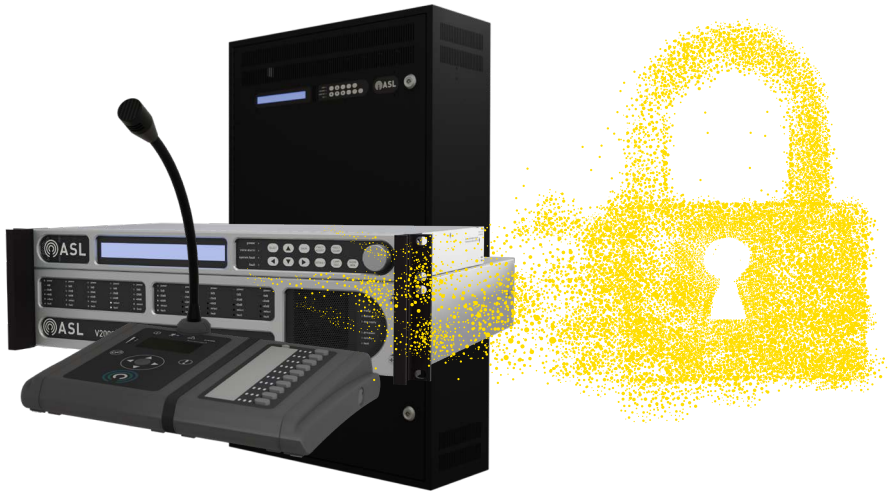
Enforcing least privilege, giving user accounts or processes only those privileges which are essentially vital to perform its intended functions

Never trust, always verify

“Never trust, always verify” principle
Stronger password Policy with multi-factory authentication.

Network access limitation

Restricting unauthorized network access and reducing the attack surface with port security



zenitel

Vipedia/Integra PAVA Cybersecurity

Feature **Highlights**

Authentication

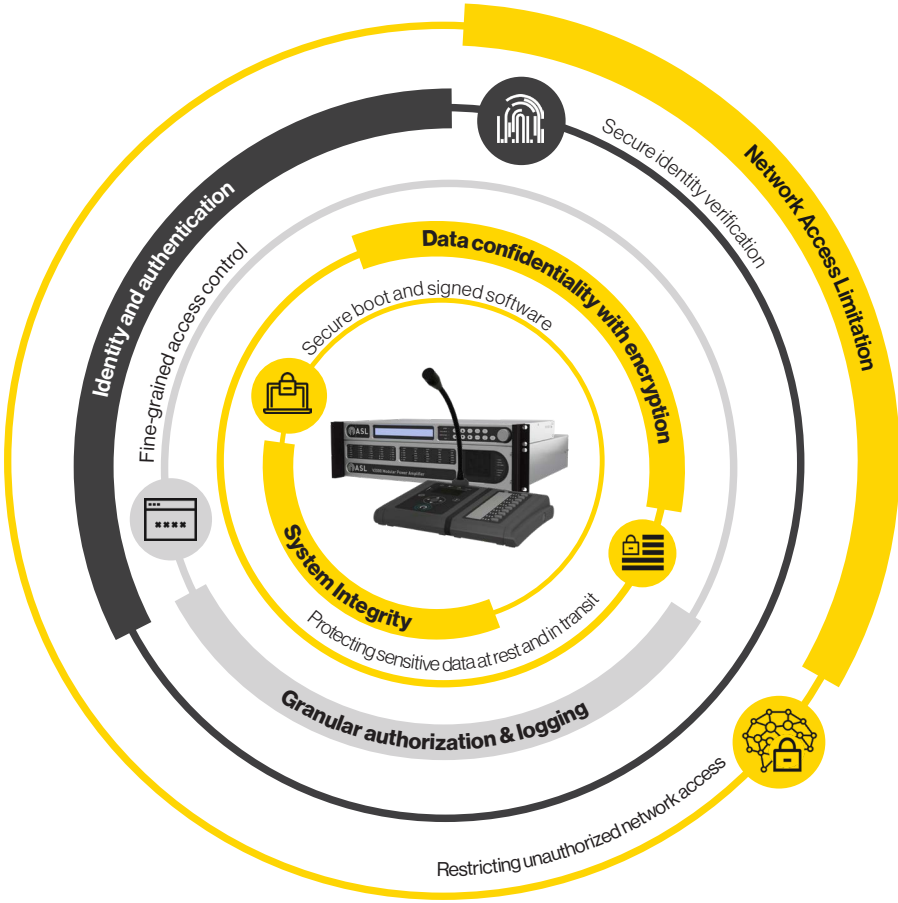
- Multi-factor authentication using PIN, site password, and offline 2FA
- Requirement for stronger 6-digits front panel PINs
- Non-default PINs are required for protected level access
- 2FA with time-based-one time password using Microsoft authenticator or Google Authenticator
- Logging of all activities for each user
- Centrally managed keys
- End devices authenticated before access
- Authenticated communication with external services/API calls

Authorization

- User and user group management
- Restricted scope of activities for operators
- Partitions to determine what users can see
- Privileges to determine what users can do

Encryption

- End-to-end encryption of all internal and external data communication
- All sensitive data at rest and in transit are encrypted



zenitel

Zenitel Public Address & Voice Alarm

Secured Communication, Certified Compliance

ISO/IEC 27001

CIS

IEC 62443-4-2

NDAA

zenitel.com