Key Danfoss PLC / iC7 Security Features

Here are some of the key security features of Danfoss iC7 drives / PLC-like controllers:

1. **Hardware crypto chip** (on control unit) for cryptographic operations. Danfoss
2. **Tamper-resistant hardware** to prevent physical or side-channel attacks. Danfoss
3. **Secure / trusted firmware**: only verified (signed/authentic) firmware is executed; encrypted firmware storage. Danfoss
4. **End-to-end encrypted communication**: TLS/SSL for communication between drive and commissioning tool (MyDrive Insight). Danfoss
5. **Public key certificates / PKI-based identity**: device identity, mutual authentication. Danfoss
6. **User management / role-based access** (least-privilege principles), per IEC 62443. The remote monitoring guide specifies principle of least privilege. Gross Automation
7. **Secure firmware updates / patching**: remote monitoring manual recommends using latest firmware, encrypted connections, certificate management. Gross Automation
8. **Security management / risk analysis**: iC7 user guide describes performing continuous risk assessments, defining countermeasures, audit, etc. Danfoss
9. **System-level guidance**: integrator/OEM guidance for achieving targeted security level (SL-T), based on IEC 62443-3-3. Danfoss
10. **Functional safety separation**: While not purely cybersecurity, the iC7 has Safe Torque Off (STO) SIL3, isolating safety function. Danfoss

IEC 62443 Key Concepts & Stakeholders

- **IEC 62443 is a family of standards for cybersecurity in Industrial Automation & Control Systems (IACS).**
- **It defines roles / stakeholder responsibilities: e.g., product suppliers (component vendors), system integrators / OEMs, service providers, and asset owners.**
- **Key parts:**
  - ***IEC 62443-4-1*: Secure Product Development Lifecycle (SDLC) for component suppliers.**
  - ***IEC 62443-4-2*: Technical Security Requirements (component-level).**
  - ***IEC 62443-3-3*: System-level requirements (for design, zones, conduits, foundational requirements (FR)).**
  - ***IEC 62443-2-1*: Security program for asset owners (operations).**

Recommended OEM Responsibilities:

OEMs (system integrators) should:

1. **Perform risk assessments** in the context of their system, determine SL-T (target security level) per zone, using IEC 62443-3-2/3-3.
2. **Configure and provision** Danfoss devices appropriately (keys, certificates, accounts, roles) to meet the SL-T.
3. **Establish patch management processes**, using secure update channels, handling rollback, and testing.
4. **Design network architecture** (zones, conduits, segmentation) so that confidentiality, integrity, and availability requirements are met.
5. **Validate security** during factory and site acceptance: ensure firmware authenticity, encryption, certificate use, user access, etc.
6. **Specify incident response and recovery strategies**, such as for firmware corruption or certificate expiration.
7. **Maintain security governance**, including periodic reassessment of risk, auditing of access, and re-certification if needed.

Additional Notes & Considerations

- Danfoss has explicitly aligned its iC7 security management with **IEC 62443** and **ISO 27001**.
- According to the *iC7 User Guide*, most drives are assigned a target security level (SL-T) of **SL-1**, even though the hardware is capable of supporting higher levels.
- For very high-security applications, the OEM may choose to design for **SL-2, SL-3, or SL-4**, but they must verify that all components (including Danfoss drives) are configured, and the system architecture supports that.
- Because Danfoss provides both component-level support (certified product development, component security features) and system-level guidance, the OEM should leverage Danfoss documentation (guides, mitigation lists) heavily.

Gross Automation | sales@grossautomation.com | +1 (262) 252-1600