INFORMATION SYSTEM AND NETWORK PROTECTION

With its long-standing experience of projects involving the creation of infrastructure aimed at housing communication systems for strategic command centres, **CEGELEC Défense Infrastructures & Réseaux** has acknowledged expertise in the field of protecting information systems and networks (notably as regards compromising electromagnetic pulse emanations and shielding against compromising parasite signals).

A COMPREHENSIVE APPROACH

Information system security involves ensuring the integrity, confidentiality and availability of the information in the system, as well as the non-repudiation of transactions and the authentication of users. To achieve this, a structured security process is required :

- Identification of threats and vulnerabilities,
- Assessment of the probabilities associated with each threat,
- Assessment of the consequences - Choice of counter-measure.

Deploying a security policy (all measures) requires a comprehensive approach to ensure the coherence between the resources to be used :

- Establishing organizational rules and operating procedures,
- Raising user awareness,
- Implementing technical measures.

CEGELEC Défense Infrastructures & Réseaux works hand in hand with its customers from the design to the deployment of systems, and maintains the security and operating condition of the systems deployed).

SSI

INFORMATION SYSTEM SECURITY AND CYBER-SECURIT

Cegelec Défense has a specific unit devoted to information system security (including industrial information systems) and cyber-security. The unit operates on a cross-functional basis on projects, supporting operations so as to provide services that meet our customers' needs in terms of information security.

Cegelec Défense service offer addresses every phase of a project, in order to provide comprehensive support :

- Management: project management, coordination, drafting of plans, etc.
- Engineering : audit of the organisation, design of the solution, definition and drafting of technical security documents,
- Supervision : inspections, drafting of CRE (IS security) and validations,
- Production : adjusting the security parameters of Operating Systems and monitoring their deployment on site,
- Support : Maintaining the system's security, training and raising user awareness.

Physical security :

- Choice of architecture and network equipment,
- Supervision and hypervision,
- Functional security (redundancy, etc.),
- Equipment infrastructures (Faraday chambers, etc.),
- Security of the premises (access control, anti-intrusion and fire-detection systems, etc.),
- Reinforced work stations,
- Installation rules (zone layout, etc.).

IT security :

- Data,
- Applications,
- Operating systems,
- Encryption techniques,
- Partitioning between users, etc.

TEMPEST

PROTECTION AGAINST COMPROMISING PARASITE SIGNALS

The aim of TEMPEST protection is to remove the risk of malicious operations caused by the propagation of parasite signals, whether by **conduction** or **radiation**.
It involves strict measures as regards the choice and the implementation of the equipment.
Cegelec breaks the approach down into a series of processes aimed at reinforcing the system against threats.

For example :

Use of Faraday cages

- Effectiveness of the shielding qualified in laboratory,
- Protection from radiation by NIDA and cut-off doors,
- Protection from conduction using filters,
- Wall duct via collector plate.

Use of certified materials

- Protected operator stations, printers, scanners, etc.

Installation rules, design of zone layout

- Compliance with coupling zones according to the category of equipment,
- Radio-electrical clarification in premises around coupling zones,
- Installation of protective accessories: copper plates and cowling, electrical filters on the edge of the zone, galvanic isolation,
- Massive use of fiber optics,
- Physical separation of cable ducts (red/black).