ATMEA1

Performant, Proven & Safe

Safety – Security: ATMEA1 reactor coherent approach

Outline of the ATMEA Company

- Company name: **ATMEA S.A.S.**
- Office Location: **Paris La Defense**
- President & CEO: **Benoit Blassel**
- Deputy CEO: **Yoshiki Ogata**
- Establishment: **November 2007**
- Capital: **126 Million Euros**

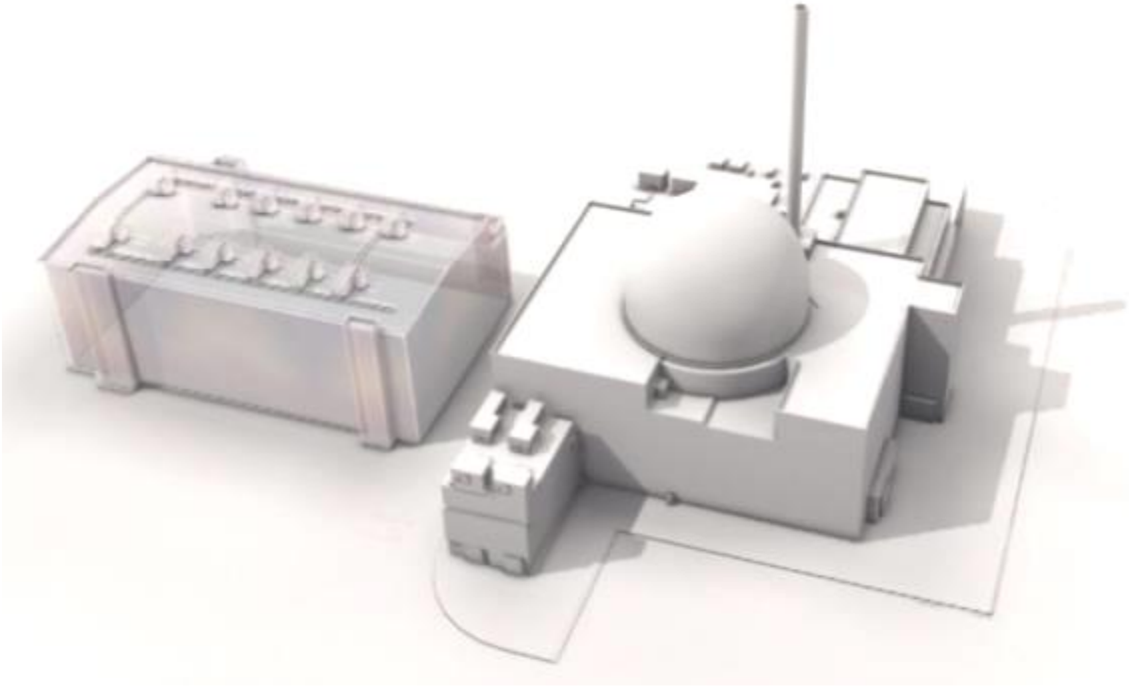
- **Scope of activities**:

  Development, Marketing & Sales, Construction & Commissioning of 1200 MWe class Generation III+ ATMEA1 Nuclear Island

Reminder

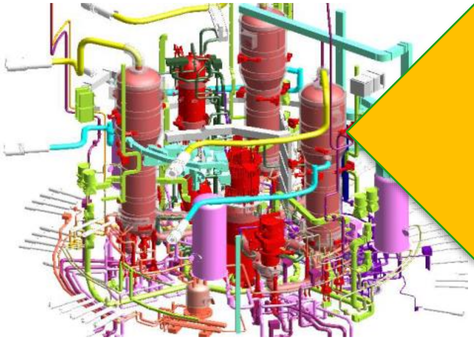
- ATMEA combines the unrivalled experience and competences of world nuclear leaders AREVA and MHI
- The ATMEA1 reactor (1200 MWe class) offers:
  - The highest level of safety for a plant under control in all situations
  - The most advanced medium-sized reactor technology for reliable power production
  - Ready for project start-up and construction
- Advanced techniques experienced in AREVA and MHI are applied to shorten the construction period
- Support of the French and Japanese team ensured on the different levels (Government, SA, TSO, Operators, Vendors, Subcontractors, etc.)
- ATMEA is committed to the success of the Brazilian new build program, capitalizing on the long-standing experience of its Shareholders in Brazil

Contents



Definition of Safety and Security

SAFETY	SECURITY
• The achievement of proper operating conditions, prevention of accidents or mitigation of **accident consequences**, resulting in protection of workers, the public and the environment from undue radiation hazards.	• The prevention and detection of, and response to, theft, sabotage, unauthorized access, illegal transfer or other **malicious acts** involving nuclear material, other radioactive substances or their associated facilities.



Both serve to **protect** the plant with the ultimate aim of protecting people, society, and the environment

IAEA Safety Glossary
Terminology Used In Nuclear Safety And Radiation Protection

Integrated approach during all phases

Siting

Selection based on **both safety and security criteria**:

Site location, geology, demography, infrastructure (road, airport), etc.

Design

Compliance with **both safety and security requirements**:

Division separation and segregation

Protection against Airplane crash

Cyber-security design

Access control

Operation

Integrated management of operation, maintenance, design change, etc.

Selection of vital area and equipment

Emergency preparedness and response

Training and awareness program for personnel

Periodic reviews, continuous improvement

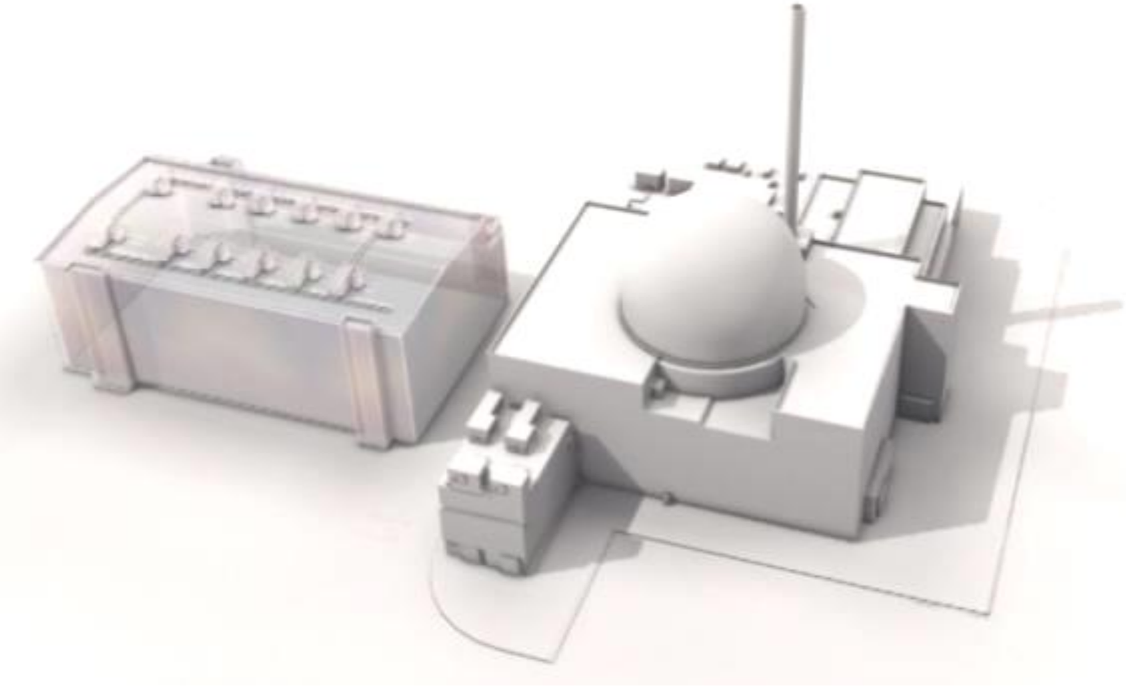
IAEA INSAG-24 The interface between Safety and Security at NPPs

Effective and coordinated **involvement** of safety and security specialists

Synergies and interrelations

Design features	Impact on safety	Impact on security
Redundancy and diversity	Improve system reliability (e.g. single failure criterion, common cause failure)	Reduce impact of malicious acts
Segregation	Increase independency of divisions/trains	Delay malicious acts
Zoning / Control access to vital area	Reduce exposure to worker	Prevent malicious acts in vital area
Robust Containment	Provide a barrier against radiological release	Protect against malicious acts (e.g. terrorist, APC)
Passive safety systems	Improve system reliability (not required power or human action)	Mitigate effects of malicious acts
Digital technology of Instrumentation and Control (I&C) system	Reduce operator workload and increase the reliability of the I&C system	Prevent malicious acts with a solid cyber security management

Contents



Integrated approach in ATMEA1 design

All external and internal hazards including human induced events are **considered**

Earthquake	Extreme condition	External flooding	Internal flooding	Rupture of piping	Fire	Explosion	Explosion wave	Airplane crash

Nuclear Safety principle:
- Protection of workers and the public in all plant conditions
- Prevention – detection – mitigation of accident consequences

+

Nuclear Security principle:
- Protection against unauthorized removal and sabotage
- Mitigation effects of sabotage

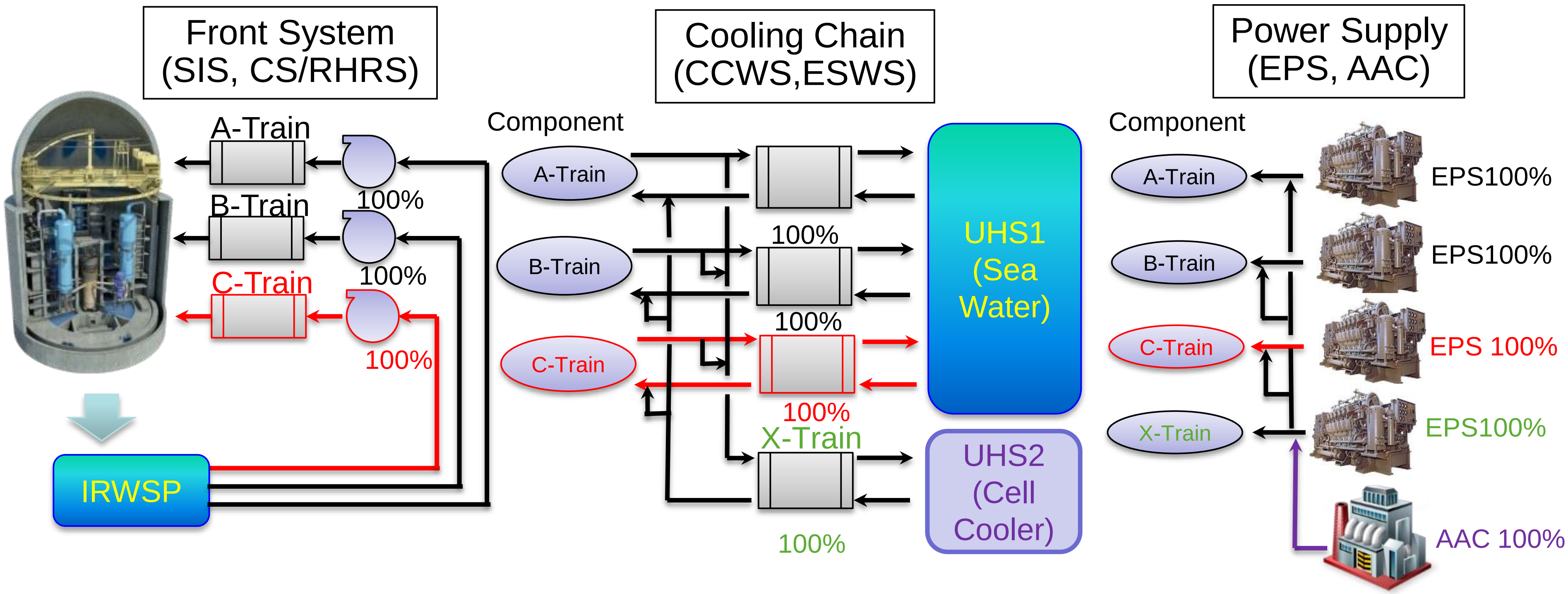
ATMEA1

Reinforce the design (e.g. extended redundancy and separation, APC shielding)

Redundancy and Diversity

Reduce impact of malicious acts

- Safety Design based on existing and **proven technologies** with increased redundancy and diversity



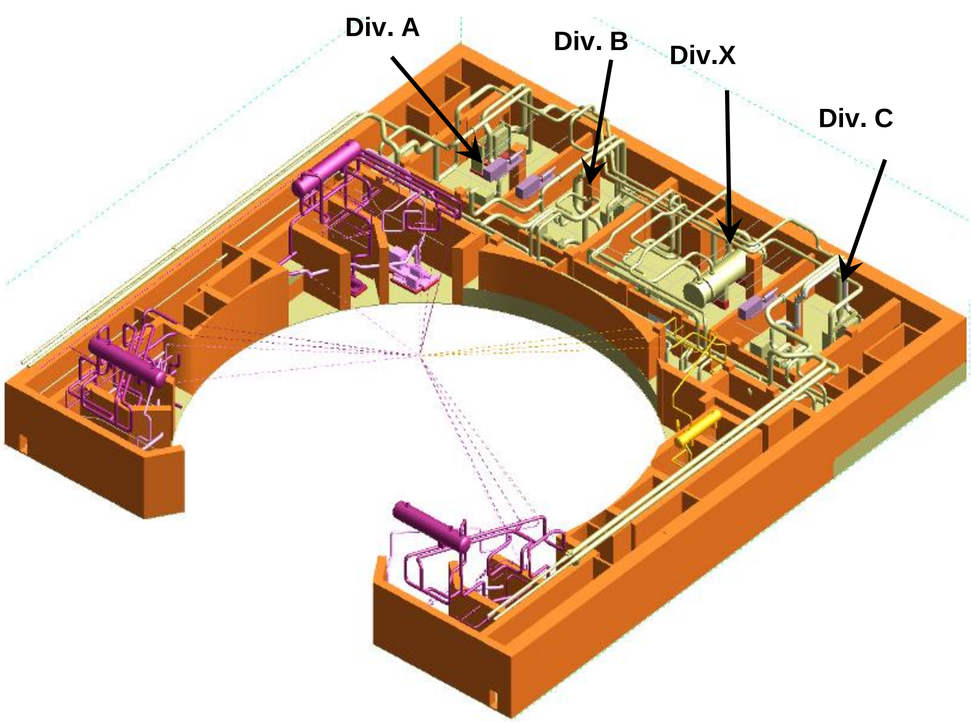
SIS: Safety Injection System
CS/RHRS: Containment Spray System / Residual Heat Removal System
IRWSP: In-containment Refueling Water Storage Pit

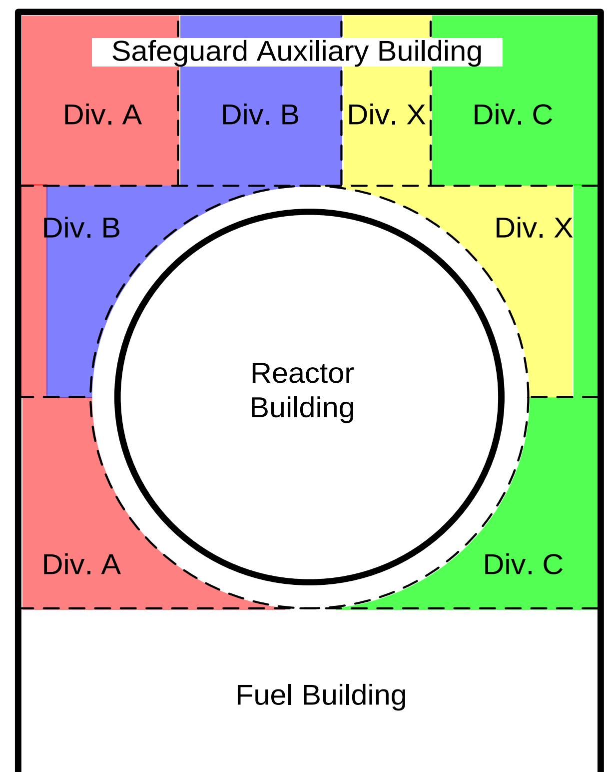
CCWS: Component Cooling Water System
ESWS: Essential Service Water System
UHS: Ultimate Heat Sink

EPS: Emergency Power Source
AAC: Alternative AC power source

Segregation of divisions

- Separation of divisions
  - Each safety train is located in dedicated areas, called divisions
  - Each division is physically separated from the others (walls, floors ..) to avoid spreading of internal hazards from one division to another

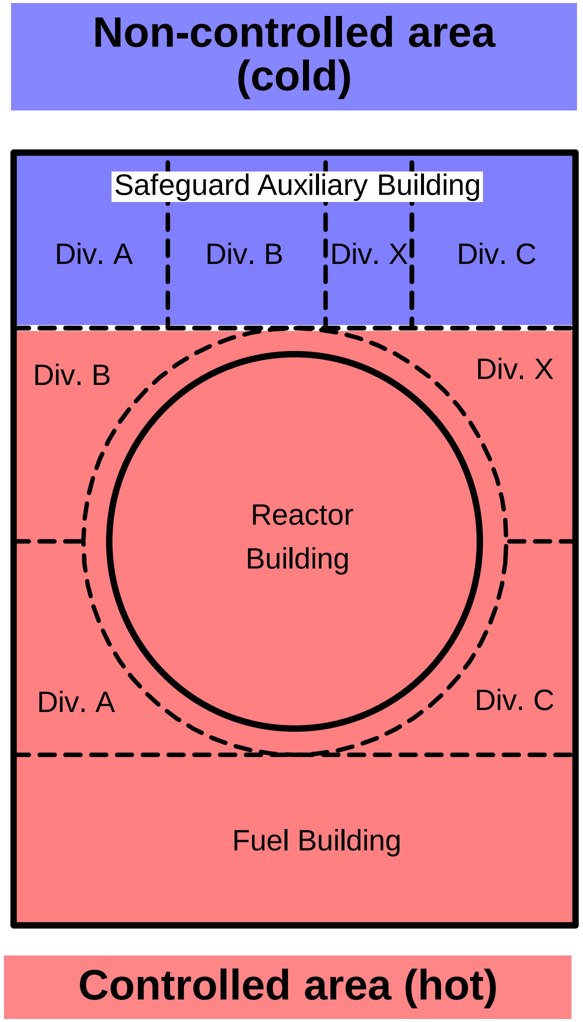




Radiological Zoning

Prevent malicious acts in vital area

- **Access control zonings** are established
  - to regulate access to radiation areas
  - to define the required radiation shielding and monitoring during operation, shutdown, and accident conditions.
- Separation between controlled and non-controlled areas
  - Radioactive systems (SIS, RHRS, SAHRS..) are located in the four quadrants surrounding the Reactor Building ⇒ **Controlled area**
  - Non-radioactive systems (CCWS, ESWS, electrical systems ..) are located in the north part of the building ⇒ **Non-Controlled area**



Airplane Crash Protection

Protect against malicious acts

Airplane Crash protection features

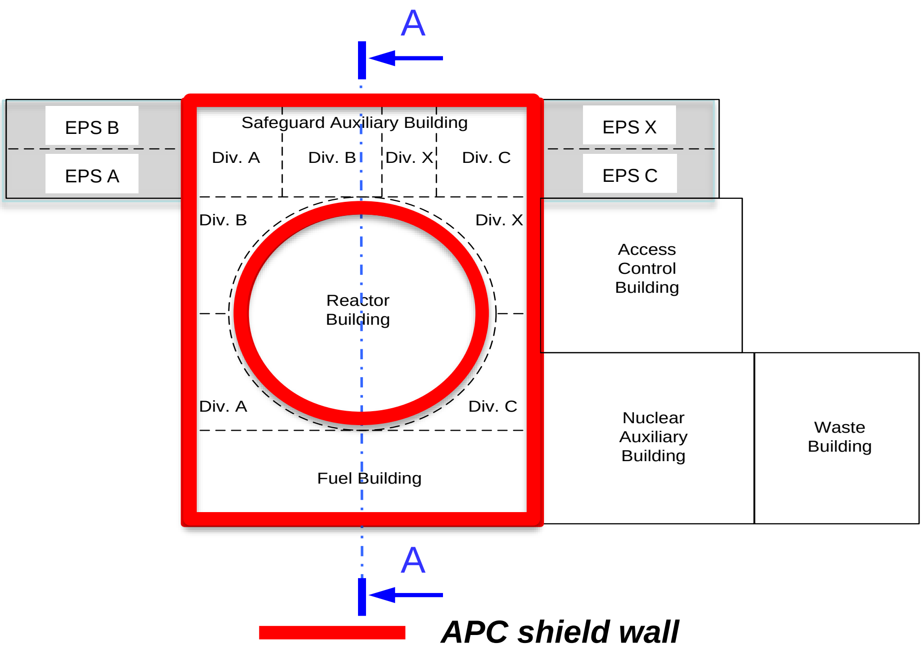
ATMEA1 buildings are protected :

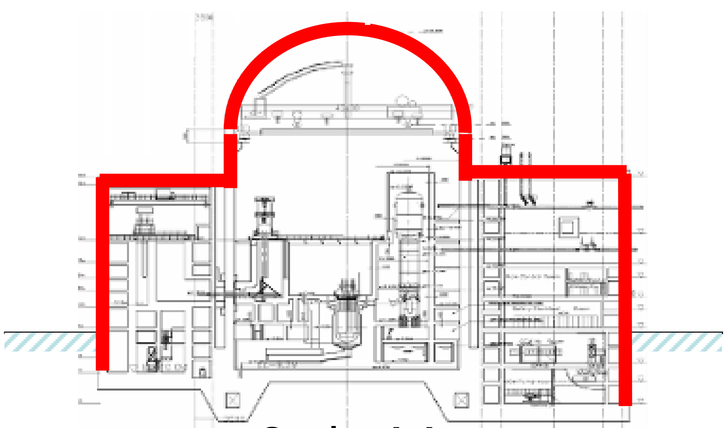
- By shielding (APC wall) : RB, FB, SAB
- By segregation : EPS buildings, AAC building

Airplane Crash protection objectives

Ensures that:

- The reactor core remains cooled, the containment remains intact
- Spent fuel cooling and spent fuel pool integrity are maintained
- No-offsite countermeasures necessary





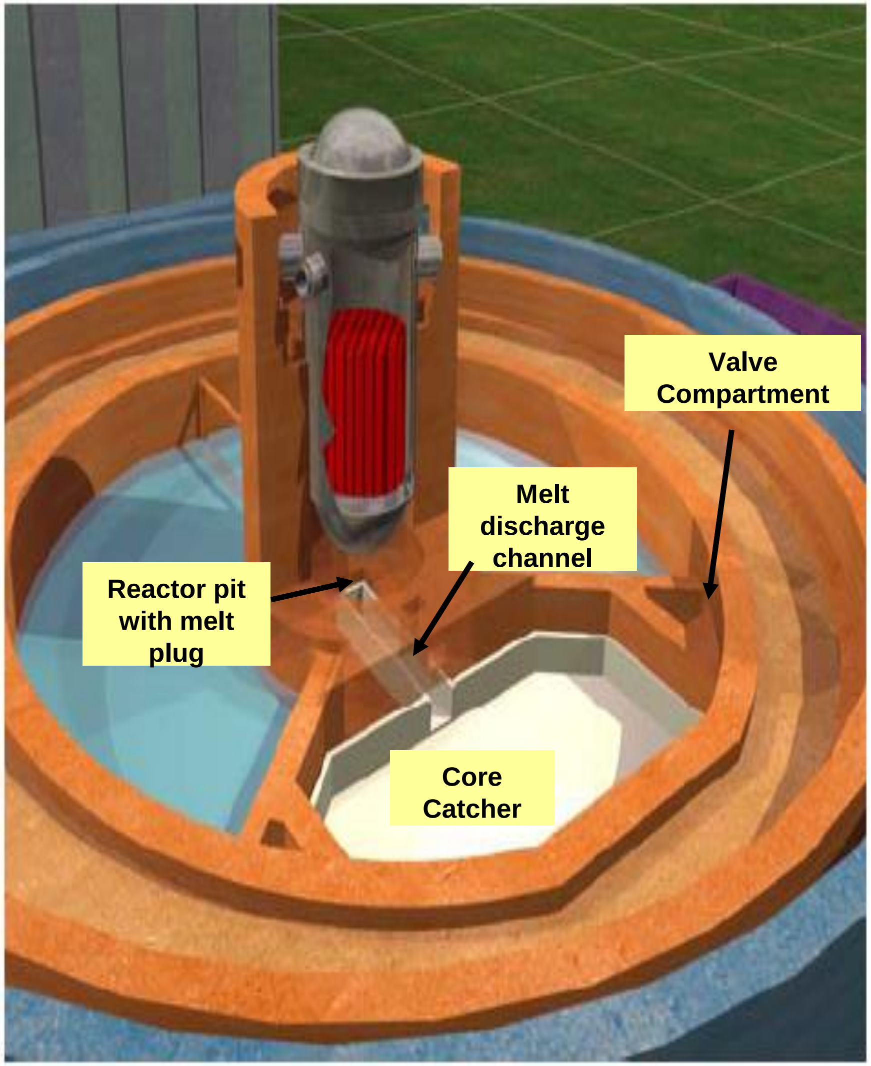
Section A-A

Mitigate effects of malicious acts

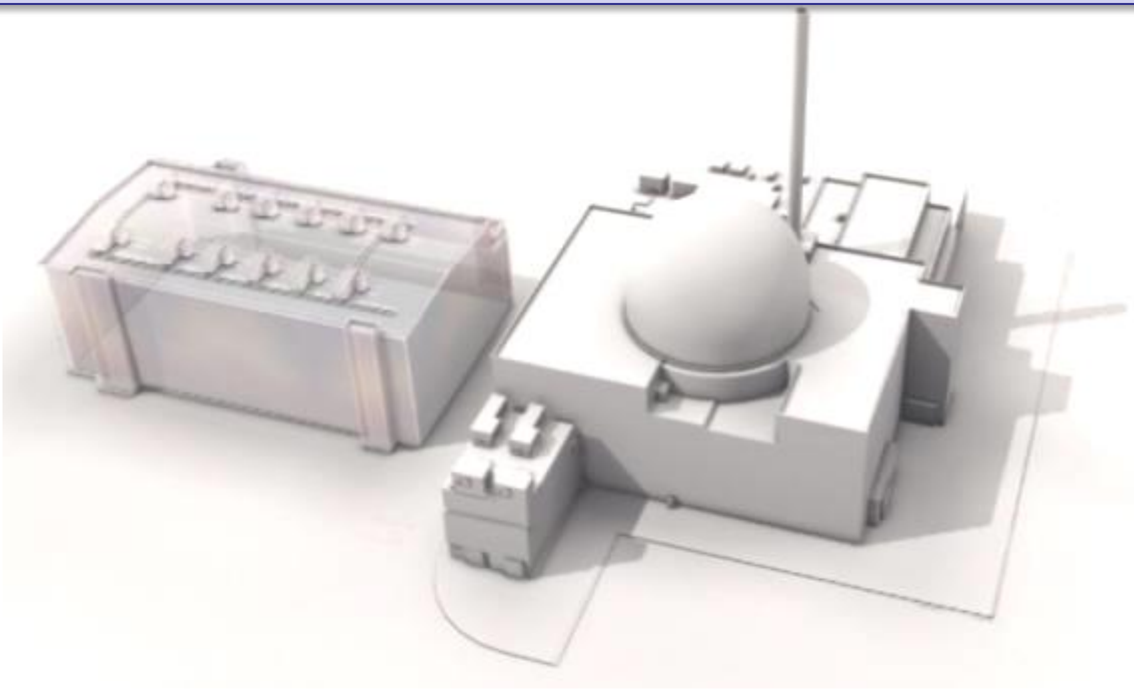
Core melt stabilization system

- All stages are **fully passive** (retention, spreading, flooding, cooling)

  - **Phase 1**: Accumulate corium and temporarily retain it in the reactor pit. Delayed melting of a melt plug located at the bottom of the reactor pit (Al plate and silicious sacrificial concrete)
  - **Phase 2**: Spread the corium on a large surface outside of the reactor pit: ~80m² metallic core catcher with cooling channels (cast iron elements with a layer of sacrificial concrete)
  - **Phase 3**: Flood and cool the spreading area by IRWSP water after trigger of redundant spring loaded flooding valves



Contents



Cyber Security Management

- Cyber Security is one aspect of Nuclear Security

- Cyber Security strategy is applied during **all design steps** to protect from a cyber threat on:
  - Safety-related and important-to-safety functions (e.g. I&C)
  - Security functions
  - Emergency preparedness functions, including offsite communications

- Security measures are periodically:
  - Updated (e.g. requirements, risk analyses)
  - Audited (e.g. procedures, compliance)
  - Monitored

Security for Projects and for Products

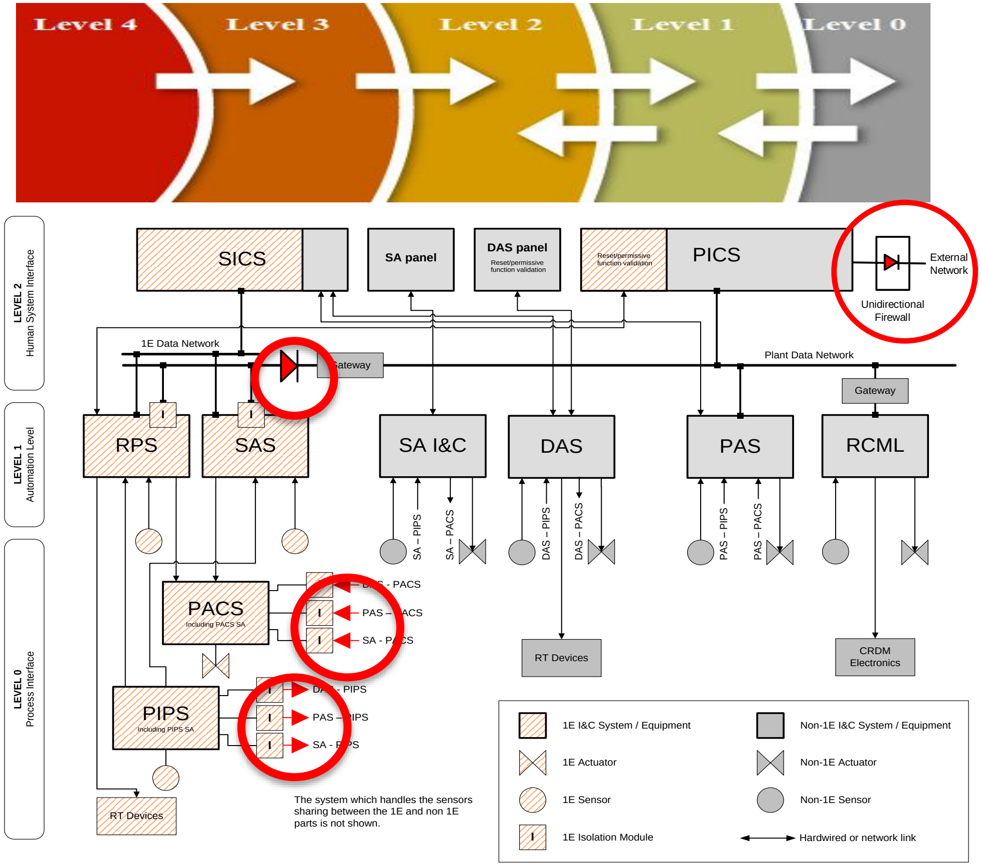
- **Project security**: Best practices in information security is included in the Integrated Quality, Environment and Information Security Management System (SM QESI) of both ATMEA parents companies:
  - main AREVA entities have the certification for Quality (ISO 9001), the Environment (ISO 14001) and Information Security (ISO 27001),
  - Continuous Cyber Security awareness training.

- **Product security**: The ATMEA1 reactor implements proven safety I&C technology. Security risk analysis up to the implementation of the countermeasures and protective techniques have been performed based on recommendations and guidance of NIST Industrial Control Systems (ICS) security guides.

Cyber Security defensive architecture

Defensive architecture includes several cyber security defensive levels separated by **security boundaries** (e.g. firewalls and diodes) at which digital communications are **monitored and restricted**.

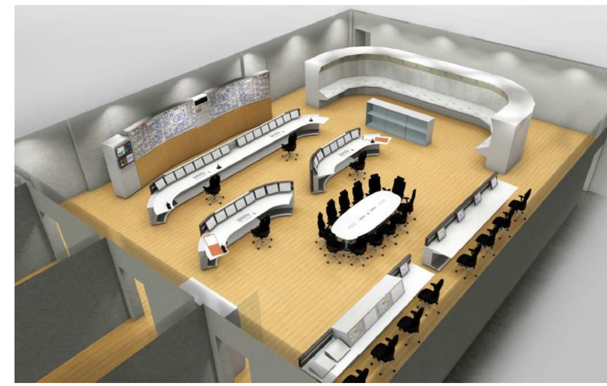
- Connections between non-safety-related I&C networks and external plant networks are via a **unidirectional firewall.** Remote access to the I&C systems is not possible.
- **No direct connections from external networks** to the safety-related I&C systems.
- **Communications independence** between the safety related I&C and non-safety-related I&C.



I&C Access control

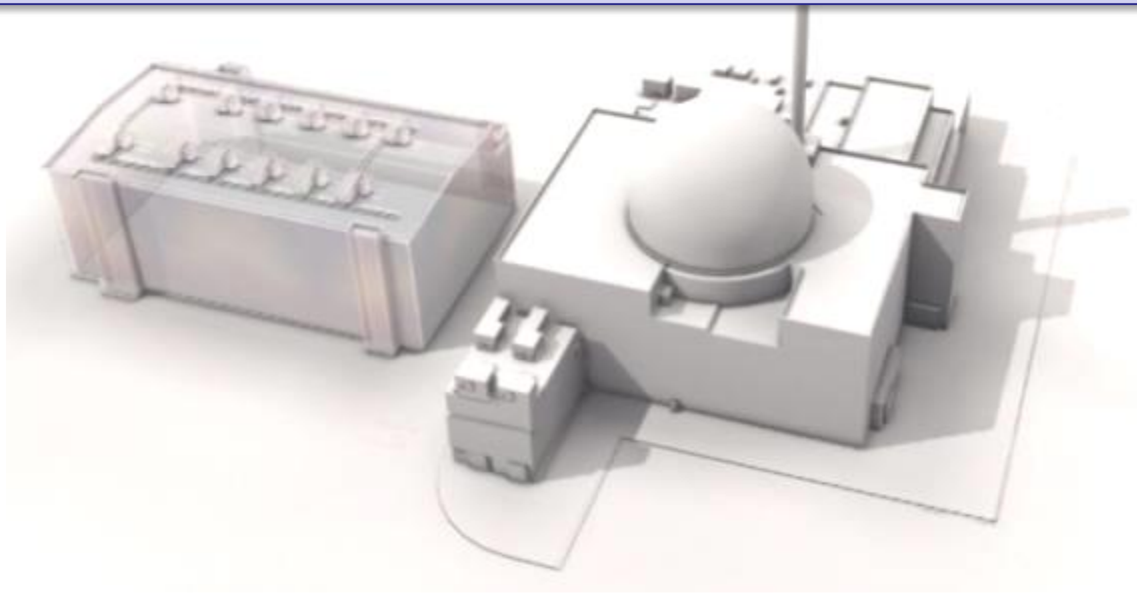
I&C systems important to safety are protected from unauthorized physical or logical access

- By **physical control access:** control room in the middle of SAB; only one access to SAB
  - to a specific list of authorized persons in designers' premises during the conceptual phase and in the utilities premises during plant exploitation



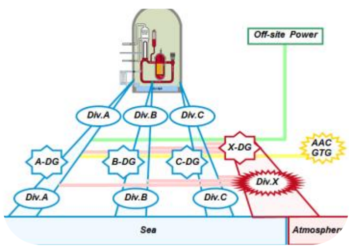
- By **logical control access** including no connection to any network external to the test bay and use of logins and passwords
  - to workstations and network,
  - to the engineering server and the tools installed on the server,
  - to the tested I&C systems and test equipments by physical restrictions.

Contents



Conclusion

- **Safety and Security synergies** benefit from each other mutually and strongly
- **ATMEA1** reactor implements a **robust and integrated design** addressing both safety and security



Extended redundancy and separation

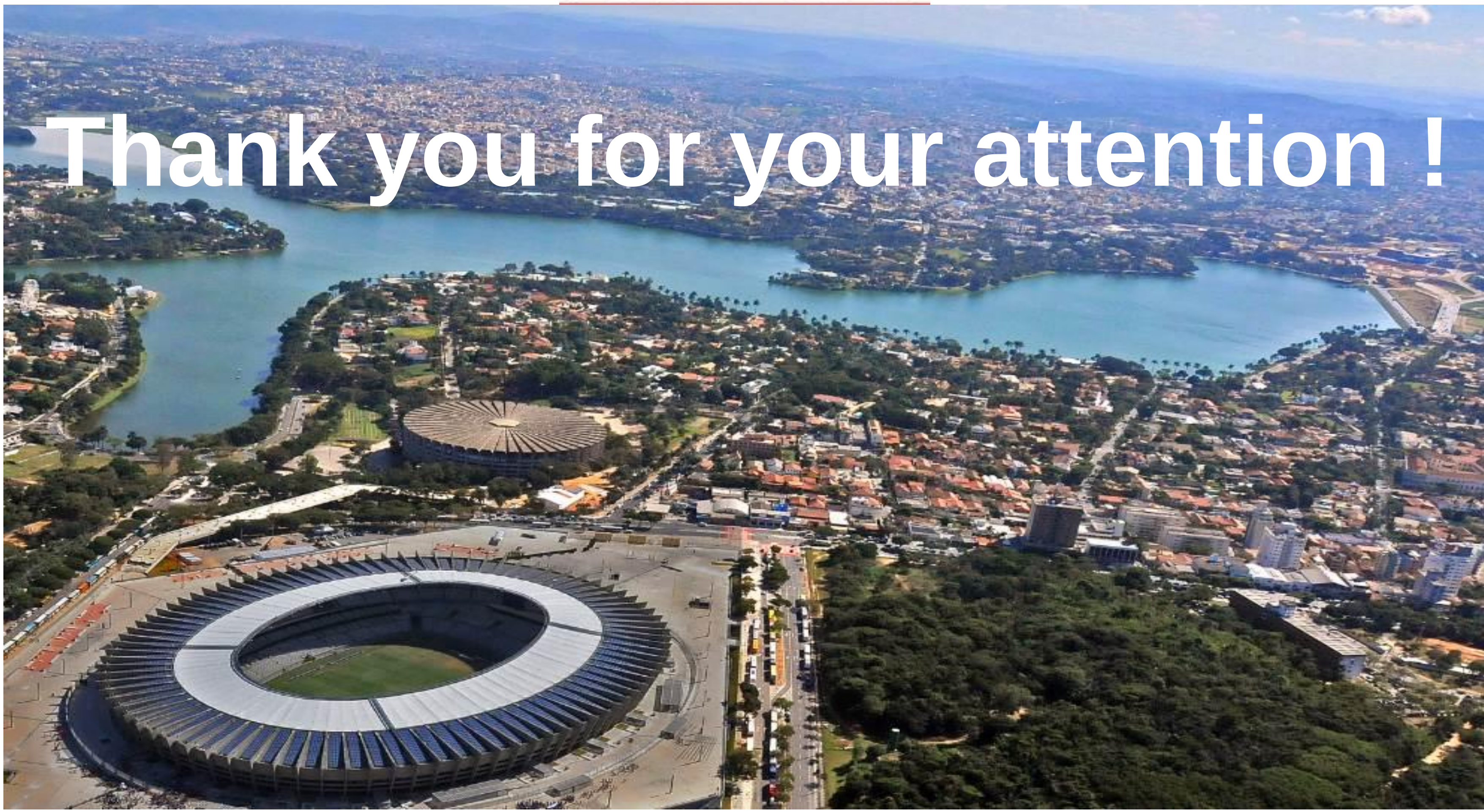
Effective zoning control

Robust design against hazards

Reliable and proven passive systems

Solid Cyber security program

ATMEA1



Visit our website at: www.atmea-sas.com