Operational Safety in Power Systems: Proven Practices and Common Pitfalls

Egypt Energy & FIREX 2025 Conference
Dr. Ahmed Sharaf
Head of EHS BU

Agenda

1. Operational (process) Safety Definition
2. Why Operational Safety is very important
3. The Pillars of Operational Safety Excellence
4. Proven Practices in power systems
5. Common Pitfalls in power systems & Worldwide Examples

Operational (process) Safety definition

This definition, backed by the references to CCPS, HSE, and ASSP

"The integrated framework of engineering, management, and human factors designed to maintain control over high-energy processes in power systems, thereby preventing potential high-consequence events that could affect personnel, the public, the environment, and asset integrity. It is the discipline of ensuring that our complex systems do not fail catastrophically."

Why Operational Safety is very important?

National Security

Grid resilience and reliability

Reputational Cost

Loss of public trust, investor confidence

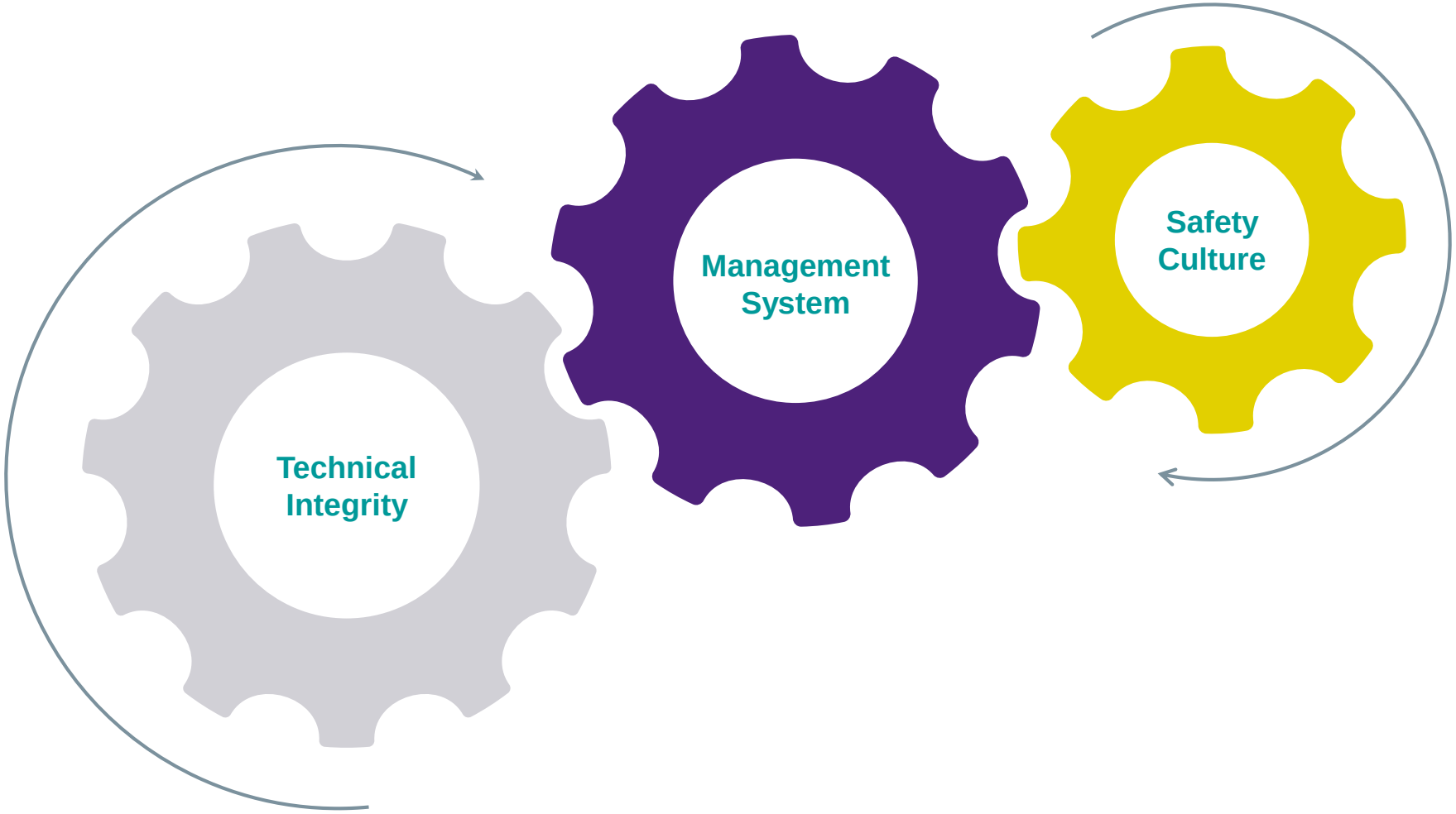
Economic Cost

Downtime, equipment damage, regulatory fines

Human Cost

Worker safety, public safety

The Pillars of Operational Safety Excellence



Pillar 1: Technical Integrity (The Hardware)

Asset Integrity & Reliability

- Maintaining equipment to prevent failures (e.g., corrosion management, mechanical integrity programs)

Process Safety Information (PSI)

- Having accurate and up-to-date documentation on equipment, chemicals, and processes

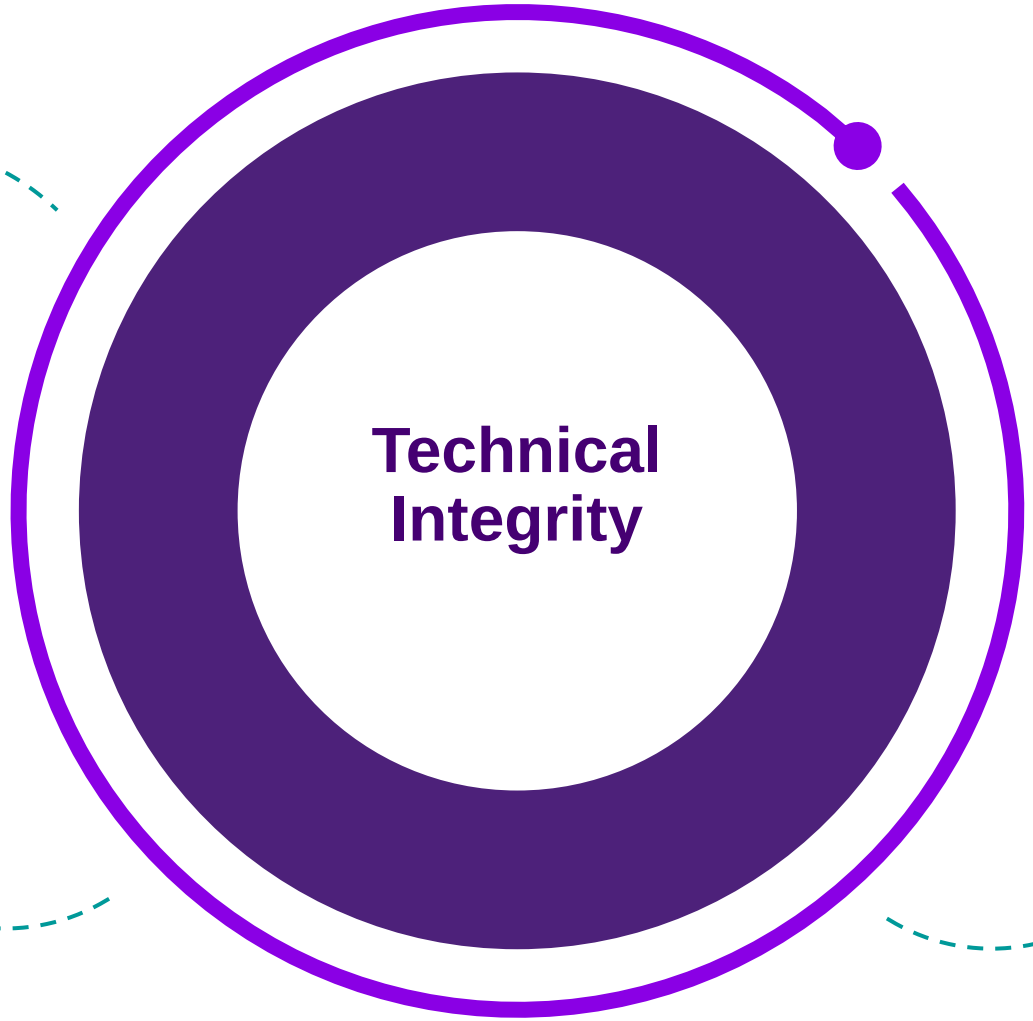
Safer Design

- Designing systems to eliminate or reduce hazards rather than controlling them

Automation & Safety Instrumented Systems (SIS)

- Using technology as a layer of protection against catastrophic failures

Pillar 2: Management Systems (The Software)



Management of Change (MOC)

A formal process for reviewing and approving changes to equipment, procedures, or personnel

Operating Procedures & Safe Work Practices

Clear, accurate, and accessible instructions for all operational and maintenance tasks

Audit, Assurance, and Continuous Improvement

Regularly checking the system's health and learning from performance

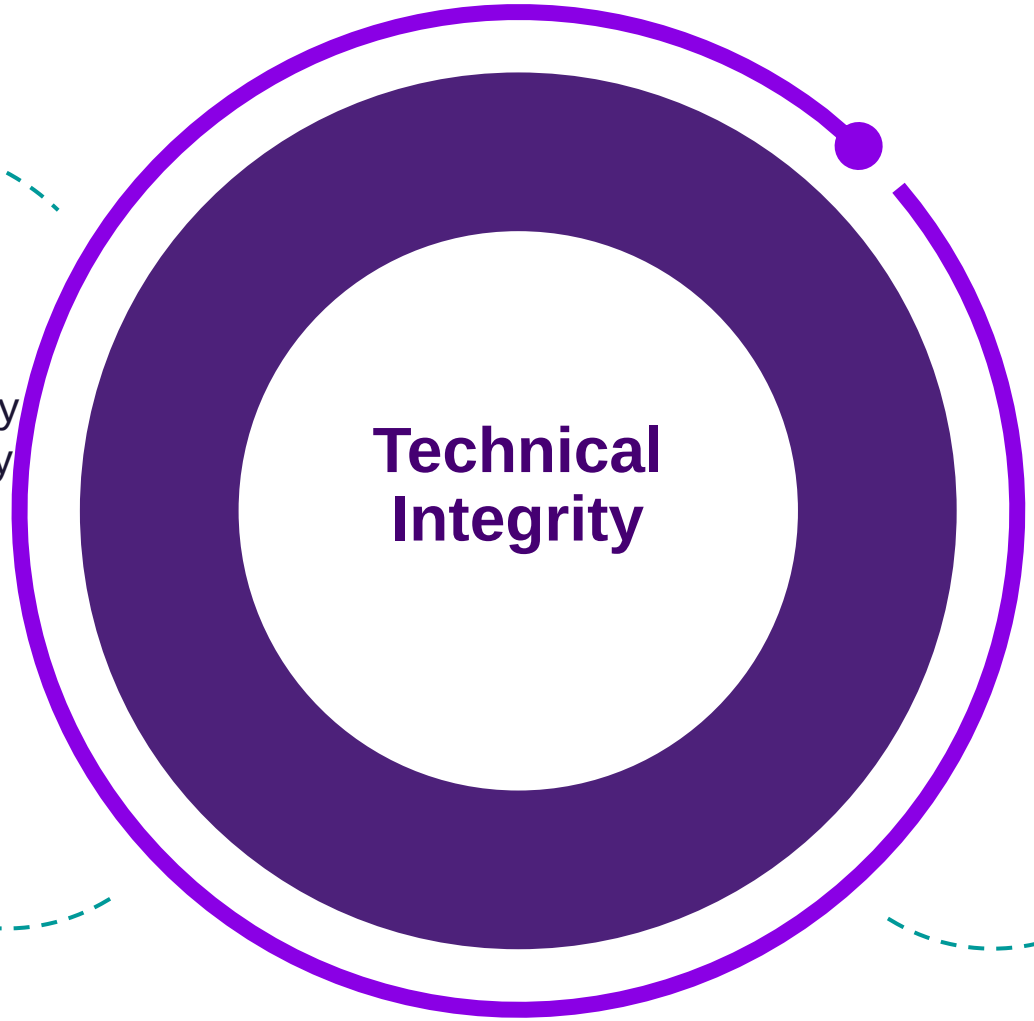
Emergency Preparedness & Response

Having plans and resources to effectively respond to incidents

Risk Assessment & Management

Proactively identifying and mitigating risks (e.g., through HAZOP, FMEA, FTA).

Pillar 3: Human Factors & Safety Culture (The Heartware)



Competence & Training

Ensuring personnel have the necessary knowledge, skills, and experience

Fatigue Management & Human Factors Engineering

Designing tasks and systems to account for human limitations and strengths.

Just Culture (Speak Up)

Fostering an environment where people are encouraged to report errors and near-misses without fear of punishment

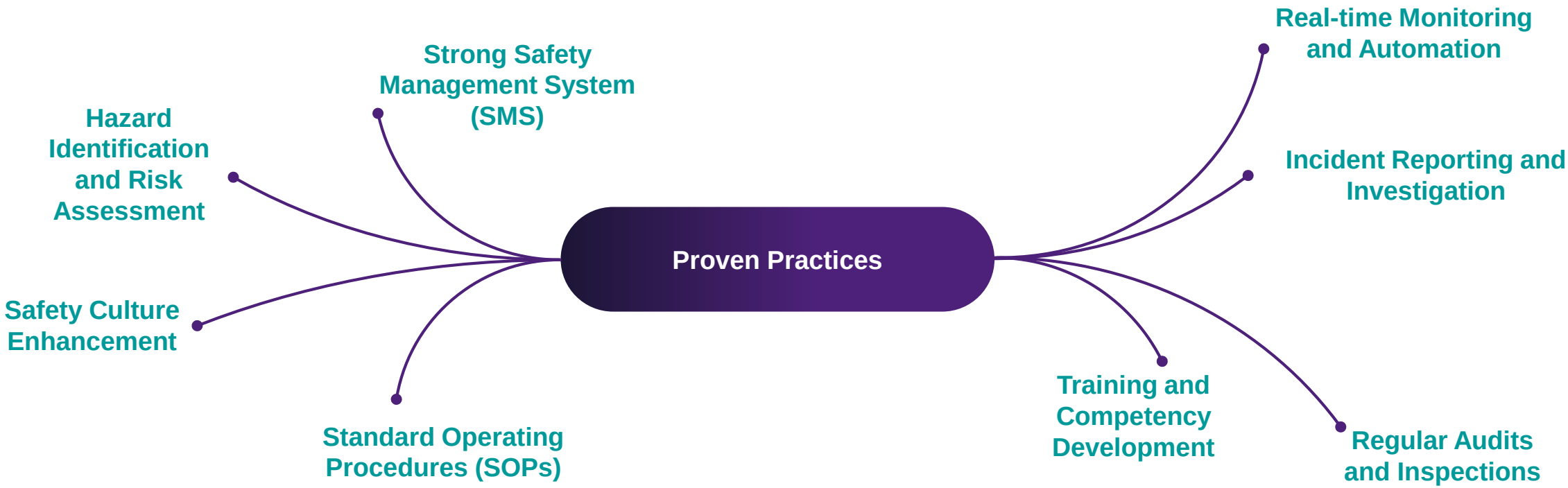
Strong Safety Culture

An environment where safety is deeply valued and is everyone's responsibility

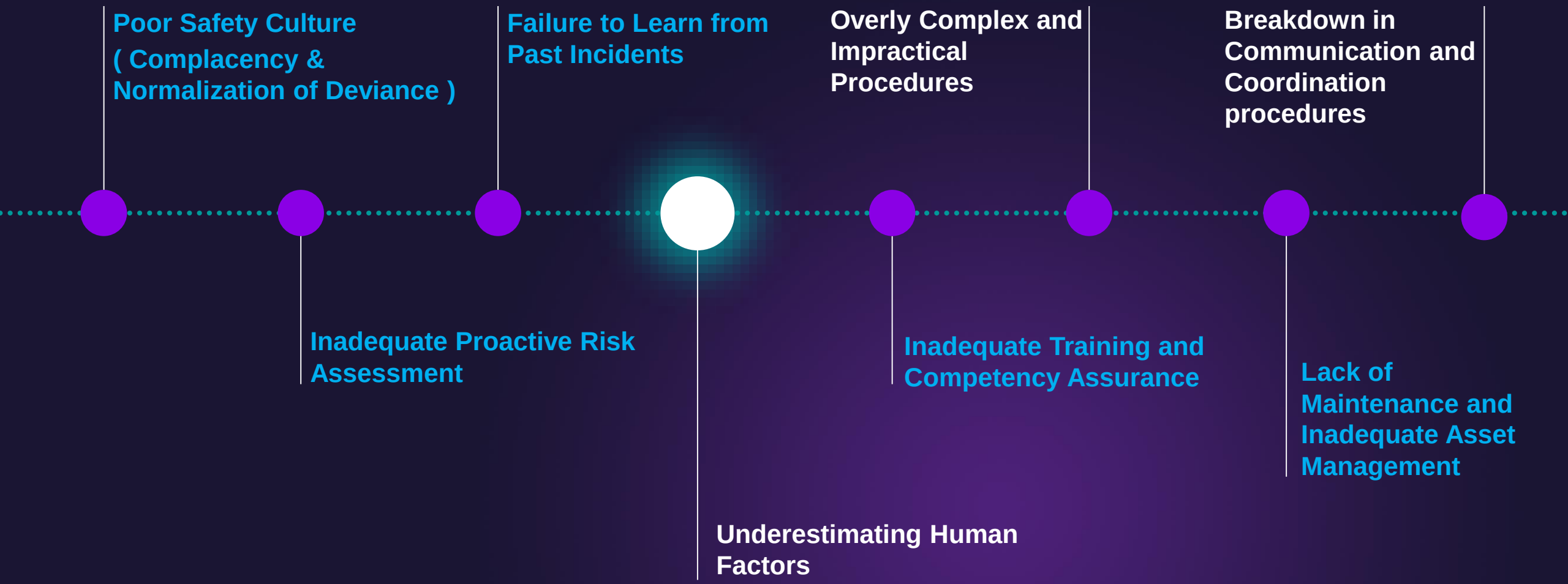
Leadership & Commitment

Visible and felt leadership from the top down that actively promotes and resources safety

Proven Practices in power systems



Common Pitfalls in power systems



Example #1: Chernobyl Nuclear Disaster (1986, USSR/Ukraine)

On April 26, 1986, at the Chernobyl Nuclear Power Plant in Ukraine, operators began a late-night safety test on Reactor No. 4 to assess its ability to generate backup electricity during a power outage.

During the test, operators disabled key safety systems and ignored established protocols, leading to an unstable reactor condition.

Due to the defected RBMK reactor design—particularly its positive void coefficient—the reactor power surged in non-controlled way.

Within seconds, two massive explosions blew apart the reactor vessel and roof, igniting a fire that released radioactive materials into the atmosphere.

The disaster expanded rapidly, with first responders rushing in without adequate protection and being exposed to lethal doses of radiation.

References: IAEA (1992), INSAG-7; WHO/IAEA/UNDP (2006); World Nuclear Association (2021); Medvedev (1991).

Pitfalls That Caused the Accident

1.Poor Safety Culture (Complacency & Normalization of Deviance):

Operators routinely ignored safety rules and protocols, and risk-taking had become normalized.

2.Inadequate Risk Assessment & Scenario Planning:

The reactor design was inherently unstable at low power, but this risk was not fully assessed or mitigated.

3.Failure to Learn from Past Incidents:

Previous operational warnings and smaller incidents in Soviet reactors were not incorporated into safety improvements.

4.Insufficient Training:

Operators lacked adequate understanding of reactor physics and emergency protocols, leading to fatal misjudgments during the test.

5. Defected design:

The defected RBMK reactor design—particularly its positive void coefficient—the reactor power surged in non-controlled way.

These pitfalls combined to create a situation where human error, poor design, and weak oversight, resulting in an uncontrolled power surge and reactor explosion.

Consequences of the Accident

The Chernobyl disaster caused immediate deaths of two plant workers on the night of the explosion and 29 firefighters and staff within weeks from acute radiation syndrome. Long-term, the World Health Organization and UNSCEAR report thousands of cases of thyroid cancer and other radiation-related health effects, particularly among children.

Radioactive fallout spread across much of Europe, forcing the permanent evacuation of around 116,000 people and the resettlement of another 230,000. A 30-km exclusion zone remains uninhabitable to this day.

The accident severely damaged trust in nuclear power worldwide, leading to policy shifts, delays in nuclear expansion, and stricter international safety regulations (IAEA, 2006; WHO, 2016).

Example #2: Fukushima Daiichi Nuclear Disaster (2011, Japan)

On March 11, 2011, a massive 9.0 magnitude earthquake struck off the coast of Japan, followed by a destructive tsunami that reached heights of up to 15 meters.

The Fukushima Daiichi Nuclear Power Plant, located in the Fukushima city, automatically shut down its three operating reactors as designed.

However, the tsunami overcome the plant's seawall defenses and flooded the backup diesel generators, which were located in low-lying areas exposed to water ingress. With both grid power and backup generators disabled, the reactors lost critical cooling capabilities.

This "station blackout" led to rising core temperatures, hydrogen buildup, and ultimately partial meltdowns in Units 1, 2, and 3.

Hydrogen explosions destroyed reactor building roofs, releasing radioactive materials into the environment.

The disaster expanded over several days, forcing widespread evacuations and leading to a major nuclear crisis.

References: IAEA (2015) *The Fukushima Daiichi Accident*; National Diet of Japan (2012) *The Official Report of the Fukushima Nuclear Accident Independent Investigation Commission*; World Nuclear Association (2022).

Pitfalls That Caused the Accident

1.Inadequate Risk Assessment & Scenario Planning:

The plant risk profile did not include the worst-case natural disasters, leading to insufficient flood protections.

2.Poor Emergency Preparedness & Crisis Management:

Emergency response plans were not properly prepared / implemented.

3.Insufficient Training:

Workers were lacking clear guidance and the knowledge on how to handle prolonged station blackout conditions.

These pitfalls collectively allowed the disaster to escalate: underestimating natural hazards, failing to prepare for worst-case emergency scenarios, and neglecting to implement strong emergency procedures all combined into a catastrophic failure when the tsunami struck.

Consequences of the Accident

The accident caused three reactor meltdowns and multiple hydrogen explosions, releasing large quantities of radioactive material into the environment and the Pacific Ocean. More than 150,000 citizens were evacuated. The disaster caused contamination of land and food, disrupted energy supply, and economic costs exceeding $200 billion. Globally, Fukushima triggered stricter emergency preparedness standards, and a reevaluation of nuclear power’s role in national energy policies, with countries such as Germany deciding to phase out nuclear energy altogether.

Example #3: Sayano–Shushenskaya Hydroelectric Plant Accident (2009, Russia)

On August 17, 2009, at 8:13 a.m., Turbine No. 2 at Russia's Sayano–Shushenskaya Hydroelectric Plant catastrophically failed while operating at full capacity.

Years of chronic vibration had weakened the bolts securing the turbine cover.

That morning, the bolts suddenly released, and the 920-ton turbine cover was ejected with high power.

Pressurized water surged into the turbine hall, destroying equipment and structures.

The hall was rapidly flooded, the roof collapsed, and multiple turbines and generators were damaged.

Workers inside the turbine hall were swept away by the torrent, while electrical explosions and fires compounded the devastation.

References: Federal Environmental, Industrial and Nuclear Supervision Service of Russia (Rostechnadzor) – *Investigation Report on Sayano–Shushenskaya Accident* (2010).

Pitfalls That Caused the Accident

1.Poor Safety Culture (Complacency & Normalization of Deviance):

Chronic turbine vibration problems had been frequently ignored, and unsafe operations were normalized.

2.Inadequate Risk Assessment & Scenario Planning:

The risks of catastrophic turbine failure were underestimated, with no robust preventive measures in place.

3.Failure to Learn from Past Incidents:

Similar mechanical and vibration issues in turbines had been reported at other plants, but corrective lessons were not applied.

4.Lack of Maintenance and Upgrade:

Equipment was outdated and requiring maintenance or replacement, inspections were inadequate, and critical bolts were left exposed to fatigue and failure.

Together, these pitfalls meant that a preventable mechanical issue escalated into a catastrophic failure that destroyed the plant.

Consequences of the Accident

The accident killed 75 workers and injured dozens more. The plant was forced to be out of service, causing major power shortages in the grid. Around 40 tons of transformer oil spilled into the Yenisei River, causing significant environmental pollution. The destruction of the turbine hall required years of reconstruction and billions in repair costs. (Russian Federal Environmental, Industrial and Nuclear Supervision Service, 2010; IEA Hydro, 2011).

Prepared by:

Dr. Ahmed Mohamed Sharaf

Head of EHS
Siemens Energy

Burullus CCPP 4800 MW

Phone: +201275095396
+201278693025

Engahmedsharaf2015@Gmail.com