Human Performance Engineering

“Sharing best Practices to Protect Electricity Networks from Natural Disasters”

Vienna, July 2nd 2014
Lubomir Tomik

National Critical Energy Infrastructures vary within the different Member States of the OSCE, but they have at least one challenge in common. All are all obliged to ensure that they can continue to function in the most adverse conditions since their breakdown can have catastrophic consequences - as shown during the fatal Fukushima incident.

How can National Critical Energy Infrastructures be protected against man-made or natural threats?

What are the best strategies to manage major blackouts?

How to assess and manage these risks for Critical Energy Infrastructures in the best way?
**Definitions**


- **Article 2, (a), Critical infrastructure’ (ECI)**
  Means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic and social well-being of people, and the disruption or destruction of which would have a significant impact on Member State

- **ECI**:
  - Energy :
    - Electricity
    - Oil
    - Gas
  - Transport :
    - Road
    - Rail
    - Air
    - Waterways & Ocean

- **Article 2, (e), Protection’**
  Means all activities aimed at ensuring the functionality, continuity, and integrity of critical infrastructures in order to deter, mitigate, and neutralise a threat, risk or vulnerability

- **ECI is defined by cross-cutting criteria:**
  - Causalities criterion
  - Economic effect criterion including potential environmental effects
  - Public effect criterion (public confidence, physical suffering, disruption of daily life, loss of essential services..)

---

**Risk matrix**

<table>
<thead>
<tr>
<th>Consequence Categories</th>
<th>Minor to Major</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A</td>
</tr>
<tr>
<td>1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Probability Categories</th>
<th>Minor to Major</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
</tr>
</tbody>
</table>

- Unacceptable
- Tolerable
- Acceptable
What Causes ECI Accidents?

- Nature phenomena (earthquake, tsunami, flooding...) including solar storms
- Underestimation of hazards/risk in all organizational level (lack of Safety culture)
- Design Flaws
- Failure of Control Systems
- Lack of Maintenance
- Operator Fatigue - Human failure
- Poor risk analyses and plan for risk mitigation
- Risk accumulation /multidimensional combination/

Human error and unsafe behaviour accounts for almost 80% of all accidents

Edgar Schein’s Metaphor of Culture

Most of the culture is below the surface

Above the surface we find: the visible aspects of culture: artefacts, people’s actions, language use

Below the surface we find: norms values fundamental assumptions of reality – the shared understandings
Safety culture levels

Focus on performance drivers

Equipment + PEOPLE !!!
James Reason – Five components of Safety Culture

**INFORMED CULTURE**
Those who manage and operate the system have current knowledge about the human, technical, organisational and environmental factors that determine the safety of the system as a whole.

**FLEXIBLE CULTURE**
A culture in which an organisation is able to reconfigure themselves in the face of high tempo operations or certain kinds of danger - often shifting from the conventional hierarchical mode to a flatter mode.

**REPORTING CULTURE**
An organizational climate in which people are prepared to report their errors and near-misses.

**LEARNING CULTURE**
An organisation must possess the willingness and the competence to draw the right conclusions from its safety information system and the will to implement major reforms.

**JUST CULTURE**
An atmosphere of trust in which people are encouraged (even rewarded) for providing essential safety-related information, but in which they are also clear about where the line must be drawn between acceptable and unacceptable behaviour.

---

**Human Performance Engineering**

**Introduction**

**Direct Causes of Events**
- Equipment Failure: 20%
- Human Failure: 80%

**Causes of Human Failures**
- Organizational deficiencies: 70%
- Individual Failures: 30%
What is Human Performance?

A series of behaviors executed to accomplish a specific task.

\[ P = B + R \]

Performance = Behavior + Result

Expected BEHAVIORS are the proper use of these Error Prevention Tools

- Pre-Job Briefings
- Procedure Use and Adherence
- Self Checking
- Peer Checking
- Effective Communications / Phonetic Alphabet
- Questioning Attitude
- ...

---

Human Performance Engineering

Introduction
Desired Attitudes

- Uneasiness for & intolerance of error traps
- Belief in the effectiveness of the rigorous use of error-prevention tools
- Vigilant situational awareness
- The will to communicate
- Value relationships

Attitude Meter

Healthy Uneasiness/Wariness/Alertness

Uncertain/Unsure

Too Certain/Too Sure
**Error Likely Situation**

Unintentional deviation from preferred behavior

**Risk Factors**
• Task
• Work Environment
• Individual Capabilities
• Human Nature

Significant probability of an error due to *risk factors* (error precursors) is an error likely situation.

---

**Principles of Human Performance**

- Humans are fallible . . . even the best ones
- Error likely situations are predictable and error can be avoided
- Organization influences behavior ...
- Behaviors are reinforced ...
- If we understand causes, events are avoidable
Human Performance Concepts

Error-likely Situation “TWIN Model”

Task Demands
- Time pressure (in a hurry)
- High Workload (memory requirements)
- Simultaneous, multiple tasks
- Repetitive actions, monotonous
- Irrecoverable acts
- Interpretation requirements
- Unclear goals, roles, & responsibilities
- Lack of or unclear standards

Individual Capabilities
- Unfamiliarity with task / First time
- Lack of knowledge (mental model)
- New technique not used before
- Imprecise communication habits
- Lack of proficiency / Inexperience
- Indistinct problem-solving skills
- “Unsafe” attitude for critical task
- Illness / Fatigue

Work Environment
- Distractions / Interruptions
- Changes / Departures from routine
- Confusing displays or controls
- Workarounds / OOS instruments
- Hidden system response
- Unexpected equipment conditions
- Lack of alternative indication
- Personality conflicts

Human Nature
- Stress (limits attention)
- Habit patterns
- Assumptions (inaccurate mental picture)
- Complacency / Overconfidence
- Mindset (“tuned” to see)
- Inaccurate risk perception (Pollyanna)
- Mental shortcuts (biases)
- Limited short-term memory
Human Performance Engineering
Defense in Depth

Challenges To the Plant

EVENT

Vision, Beliefs, & Values

Latent Organizational Weaknesses

Mission Goals Policies Processes Programs

Flawed Defenses

Error Precursors

Initiating Action

Human Performance Engineering
Anatomy of an Event
The goal is mutual understanding between two or more people

Especially communication involving technical information related to plant operation or personnel safety

2 tools:
- Three-way Communication
- Phonetic Alphabet
A pre-job briefing is a dialogue between workers and leaders held prior to performing a job to discuss the tasks involved, hazards, and related safety precautions.

- Ensures understanding of task scope.
- Ensures understanding of roles and responsibilities.
- Anticipates problems and identifies responses.
- Discusses plant and/or industry lessons learned and operating experience.
- Minimizes the potential for making mistakes.

Peer checking

- It is a series of actions by two individuals working together at the same time and place, before and during a specific action – critical step, to prevent an error by the performer.

- Involves two people (performer and peer) self-checking in parallel, agreeing together that the action is the correct action to perform on the correct component.

- The peer, an individual familiar with the activity, may see hazards the performer does not see.
Procedure adherence means understanding the procedure’s intent and purpose and following its direction.

The user performs all actions as written in the sequence specified by the document. If it cannot be used as written, then the activity is stopped and the procedure is corrected before continuing.

Place Keeping
- Prevents omitting or duplicating steps in a document.
- Maintains a record of steps completed and those not yet performed.
- Helps procedure users to return to the last step performed after interruptions or delays.

Self-checking helps the performer focus attention on the appropriate component, think about the intended action, understand the expected outcome before acting, and verify the results after the action.

1. **Stop** – Focus on the task’s objective.
2. **Think** – Understand what will happen when the correct action is taken on the correct component.
3. **Act** – Perform the correct action on the correct component.
4. **Review** – Verify anticipated result obtained.
A questioning attitude fosters situational awareness, encouraging thought about safety before action is taken.

1. **Stop, Look, and Listen** – Proactively search for work situations that flag uncertainty.

2. **Ask** questions – Gather relevant information.
   - Use Qualification, Validation, & Verification (QV&V)

3. **Proceed if sure** – Continue the activity if the uncertainty has been resolved with facts. Otherwise, STOP!

4. **Stop when unsure** – If inconsistencies, confusion, uncertainties, or doubts still exist, do the following:
   - Stop the activity, place equipment and the job site in a safe condition.
   - Notify your immediate leader.

---

**Culpability tree implementation**

**Just Culture Principle**

**What it is?**

How it is related to safety culture reinforcement?
Industry statistics

- 8 from 10 safety significant events were caused with contribution of human failure
- 75% reported events at is caused by human error
- 15% - 20% of production loss are results of incorrect company decisions
- Trust is important factor in reporting

Why?

Confidential reporting

* Indicates a 'System' induced error. Manager/supervisor must evaluate what part of the system failed and what corrective and preventative action is required. Corrective and preventative action shall be documented for management review.
How it is related to safety culture reinforcement?

Goal?

- **Initiate regular discussion** between management and employees on safety issues.

- **Reinforce a risk awareness** environment

- **Reinforce an involvement and responsibility** of each employee for SC improvement

- **Achieve common understanding** and implementation of values and behaviors which support SC principles
• When lifting, slinging and handling loads safety is a priority

- Safe behaviour examples
  - I only carry out lifting and slinging work with the required qualification.
  - As a slinger I monitor the whole path of the load. I make sure it is not transported over people working below and I myself do not stand under the load.
  - As a slinger I warn people about the load moving above them in a timely manner.
  - When a load is lifted in a complex environment, an independent supervisor is called for.
  - Before working with lifting equipment I review its functioning and make sure there are no unsecured objects that may fall.

- Risks and unacceptable behaviours
  - Persons passing under the moving load do not avoid the load being transported.
  - When transporting the load, the slinger does not move along with the load to warn the persons passing by.
  - Managers are not trained about the basic rules of load lifting and slinging.
  - Issues and near-misses related to slinging and lifting are not reported or investigated.

Safety Message of the Week

Area: Occupational Health and Safety
Author: Maintenance – B2000

Continues improvement processes

Self-assessment (Proactive approach)
Work
Human factor, Behavior (at work)
Equipment reliability
Corrective action program (Reactive approach)

Results
Safe and reliable operation

Human performance
Operating experience
Work management

Human performance
Operating experience
Work management
HuPI Program Structure

- **Roles and responsibilities**
  - Managers
  - Supervisors
  - Workers

- **Process controls**
  - Written expectations, ...
  - Procedures, guidelines, work plans, ...
  - Training – classroom & practical (dynamic training)

- **Performance monitoring**
  - Event Free Clock Program

Human Error prevention

Tools and Observation Program

- **Situation Awareness**
  - Observation and coaching
  - Self-checking
  - Procedure Adherence
  - Three-way communication
  - Phonetic alphabet
  - Pre-job Briefing
  - Peer-checking
  - Independent verification
  - Flagging
  - Place keeping
  - Turnover
  - Task preview
  - Job-site preview
  - Questioning Attitude
  - Post-job Critique
To date the power energy infrastructure so far has shown an appropriate reliability level, but new threats can be foreseen. Some of the threats are internal to the infrastructure, mainly due to the increasing complexity of many technical and market components, such as:

- the institutional fragmentation among the different states,
- menace of terrorism in the form of cyber attacks,
- human failure,
- nature phenomena