# Risks of AI Interfaces in Process Plants

There has been much concern lately that Artificial Intelligence may introduce new risks to society and might even result in the replacement of mankind by robots. Although this may be possible in the far future, I believe that in the foreseeable future, these risks are manageable.

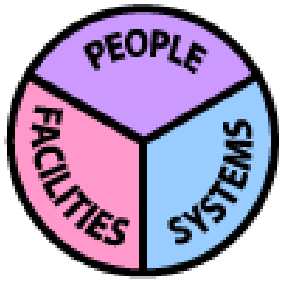
It is true, however, that the recent accelerating rate of AI technology development and application justifies careful consideration. This article therefore addresses some of these risks along with measures that have addressed similar risks that have been effectively dealt with using PERA principles that were defined many decades ago.

**For example:**

**1) Eventually, there will not be enough people to deal with upsets or emergencies.**

Automation is the process of reducing the number of people in the Enterprise compared to the facilities and systems they must manage. As AI becomes increasingly capable, there is a risk that this may result in inadequate staff to deal with emergency situations such as upsets or emergencies.

Over decades, dramatic reductions in staffing levels have proven manageable. It must be noted, however, that this process has been very gradual allowing evolution of operating procedures and improved training. Development of new communication technology has also improved remote technical support, and centralized Network Operations Centers (NOC) have proven feasible.

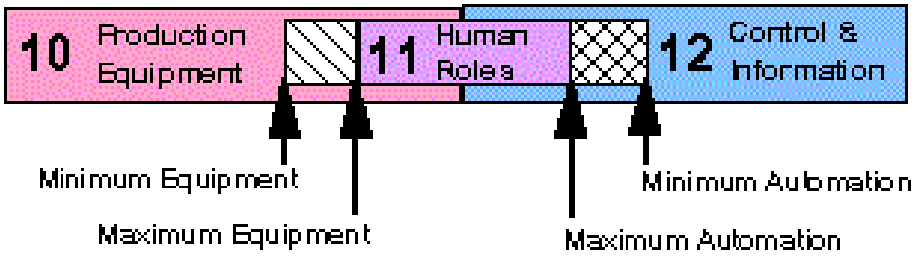



The accelerating rate of AI application does however increase risks. This risk may be reduced with careful design. The PERA methodology is designed to improve enterprise architecture, and PERA master planning emphasizes human roles and organizational design.

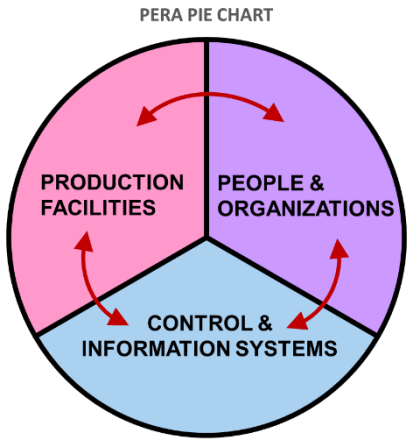
2) **Changes in the "Line of Automation" may create risks**

There are actually two "Lines of Automation, each of which may be set anywhere between Maximum and Minimum:

1. Replacing people with Equipment (conveyors, packaging equipment or other automated equipment), and
2. Replacing people with control and & information systems.




Where these lines of automation are established is important because most operating problems and errors occur at the human interfaces.



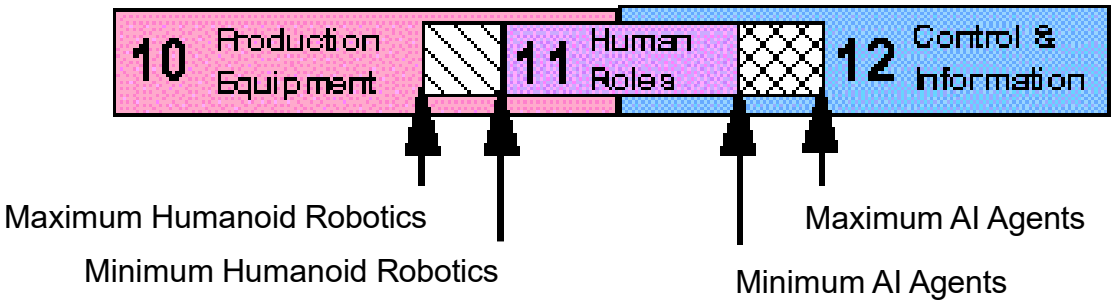

It has even been suggested by companies like Neuralink that physical connections between human brains and control and information systems will be necessary in the future.

**3) Increased Automation may prove more hazardous at lower Levels in the Enterprise Architecture**

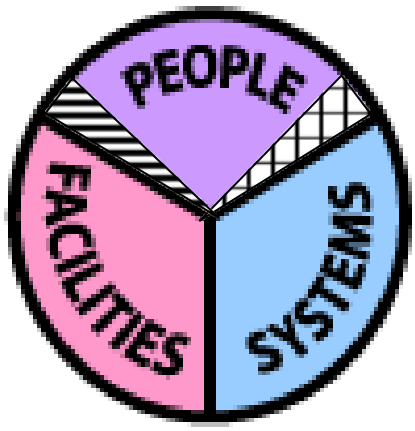
The chosen Line of Automation at IACS levels may be different than at MES or Office levels. This may be because of safety at lower levels, but the economic consequences may also be high for a production scheduling or quality control errors at the MES or even corporate level. Whatever level of automation is chosen, it is important to carefully consider sampling rates and loop stability across related control and information systems at all levels in the Enterprise Architecture.

### 4) Artificial Intelligence Introduces new Human Interface Problems

After the line of automation is decided during enterprise design, and even after the enterprise is in operation, introduction of AI makes possible significant changes in the role of people. This can occur at any level in the Enterprise, but it can have particularly serious consequences in industrial Automation & Control Systems,




This introduces new interfaces for human operators. Traditional human interfaces to Control and Information systems and to plant equipment have been evolved over many years and are thoroughly understood and well documented in the plant design. However, the Reliability, Response, Resolution and Repairability of these new AI interfaces may not be known and may even be unpredictable.




The new AI interfaces may even be faster and better than a human. For example, an AI agent monitoring network traffic might detect and even deal with an intrusion more quickly than a human. However, if the operator does not understand what is happening, the result will be confusion and the operator will no longer be in control.

Ultimately, the human role may be (almost) completely replaced. Anthropomorphic robots can walk out and open or close valves, or move a drum of lubricants from storage and connect it to a compressor. Control and optimization systems are already in widespread use that are operating at a level that most operators cannot replicate. It is quite reasonable to expect that planned facilities to produce rocket fuel on the moon will be completely “unmanned”.

# Key Messages Looking Forward

Accelerating rates of AI adoption will require more careful design and analysis of human roles.

There is a need for a classification system for AI systems, particularly where they involve control of critical infrastructure

The Line of Automation must be a carefully considered and documented choice at all architectural levels.

The Line of Automation must be established during the appropriate enterprise design phase and documented along with other “Engineering Deliverables”.

After startup, any change in the Line of Automation must be subject to the appropriate “management of change” process in that facility.

There can be serious consequences if control is taken from the Plant Operator. Operating procedures have evolved over many years to ensure that operators can always intervene to maintain safe operation.

At the very least, AI agents or humanoid robots must inform the operator “after the fact” of any initiative that it has taken and the reasons for its actions.

Perhaps what is also needed is an assessment of the probability of the AI agent’s answer being correct or even truthful.

It has been suggested that truthfulness must be the first law of AI. (Elon Musk). Otherwise, we will have no hope to monitor an AI agent that may be smarter, faster and more knowledgeable than we are.

A key issue is what may happen when AI exceeds human capabilities. Clearly Isaic Asimov’s early “laws of robotics” are already obsolete. Even early AI systems already harm humans or through inaction cause humans to be harmed (ask anyone in the Ukraine or Russia 😉).

At the very least, we must design “watcher“ applications (that can see and report unusual actions or communication). These must be independent systems in AI Agents and Robots, that communicate to human operators. Such systems have been used for decades in traditional plant control and optimization and are even codified in standards such as ISA-18, Instrument Signals and Alarms.

To help manage AI risks in Process Industries, it is proposed to establish a classification system and identify common risks associated with each AI type.

Some of these AI technologies include:

1. Large Language Models (e.g., GPT-4 or GROK to interface technical manuals)

2. Real-world Navigation (e.g., for anthropomorphic robots, or to guide service vehicles to remote installations)

3. Vision (for image analysis of flares or infrared plant images)

4. Speech to Text AI (to deliver maintenance instructions to field workers)

5. Translation (voice to voice, voice to text, and text to voice for emergency response centers)

6. Text to image AI (to create graphics to improve training and maintenance materials)

7. Computation & numerical analysis (e.g. Wolfram's Alpha AI for process modelling or Fast Fourier curve fitting).

8. Generative AI (for optimization algorithms or Expert Systems for troubleshooting)

9. AI-Powered Engineering (to accelerate and enrich design practices)

It is also proposed to establish an "AI Applications List" to identify opportunities and risks associated with use of AI in plant design and operations.

This AI Applications List will be established in conjunction with the PERA Industry Classification System. In this way, it will be possible to manage AI and cybersecurity risks according to the hazards, terminology and culture of that industry.

Initially an AI Application List will be developed for "Process Industries" as defined in the PERA Industry Classification System; however, with time (and knowledgeable volunteers), AI Applications Lists will be developed for other Industries.

Gary Rathwell