Lessons Learned for Application of AI in Plants

Industrial control and optimization is projected to be among the most highly profitable applications of "real world" Artificial Intelligence (AI). However, as "AI agents" gain direct or even indirect control of industry, the risks of a malfunction or malicious acts rise even more quickly than potential benefits. To address these risks, corporate leaders of this emerging technology have urged that governments take measures to ensure the safety of AI, especially where it controls critical infrastructure.

Several of these AI leaders have even suggested that government regulation is required before any such applications are implemented. It has also been suggested that a "kill switch" should be a minimum requirement of all AI systems. While a public dialog on these topics is necessary, I believe that it is essential that experts in Automation and Control Systems (or ACS) always be a key part of this dialog.

I also believe that government regulation of ACS is both impractical and unnecessary.

- **<u>It is impractical</u>** because industrial regulations typically take years to formulate and AI is developing so quickly that regulations cannot possibly get ahead of AI development. Even worse, if AI leaders in the US and Europe "hold back", they will be overtaken by less regulated, and probably more authoritarian regimes. This will increase AI risks rather than reduce them.

- **<u>It is unnecessary</u>** because industry has been applying increasingly sophisticated control and optimization for many decades. In fact, it can be argued that AI is not a revolution, but rather an evolution that has been going on for 50 years. During this time we have learned to maintain safe operations even when physical equipment is controlled by extremely sophisticated technology.

Rather than talking in generalities, I thought it better to describe actual examples from Operational Technology (OT) and Automation and Control Systems (ACS) that I have personally led. In each case, although new technology introduced risks along with benefits, these risks were effectively dealt with by engineers with the required knowledge and experience. The real risk is not from errors that AI may make, but rather from failure to apply the knowledge described below.

Here are some examples of sophisticated industrial control and optimization. In each case, I describe the issues we encountered and resolutions that were applied:

- In the early 1970's, **Linear Programming Optimizers** were used for optimizing shipping schedules and refinery production planning. These used large linear matrices to maximize an objective function (usually profit in $). These models were so large that they would "take over" our entire corporate data center (then an IBM 370-158) for nearly an hour.
  - **Issue:** Local maxima and simple data errors could have large economic impacts.
  - **Resolution:** Humans who had done these schedules in the past, reviewed the recommended actions and deleted "outliers".

- In the mid 1970's **Non-Linear optimizers** allowed even more sophisticated relationships to be modelled and maximized for problems such as gasoline blending.
  - **Issue**: Since relationships could be non-linear, there was no practical way for even experienced blenders to reject invalid optima.
  - **Resolution**: "Test engines" were used to verify proposed blends in a routine quality control procedure before actually blending large volumes of product.

- By 1980 **advanced digital control algorithms** were developed that could stabilize fast loops and incorporate analyzer feedback more quickly and efficiently than operators and traditional analog control.
  - **Issue**: If model-based control failed, the operator of a high-pressure polyethylene reactor could not control pressure quickly enough to prevent a "decomp release" that was known to break windows a mile from the plant. Shutdown interlocks or a "Kill Switch" would probably destroy the ethylene compressor house, killing everyone inside.
  - **Resolution**: On loss of reactor control, automated high speed "sequences" return the unit to a safe state. These "state-based" sequences recognize the plant status and automatically, ramp down, hold, or resume high-pressure circulation.

- In the 1990s **Expert Systems** used a large number of "rules" provided by the "best" operator(s) to control the process units at that site. A complex algorithm then used real-time process conditions as inputs to find a "best solution" for process performance.
  - **Issue:** The urea reactor Operators often did not understand the resulting plant control actions.
  - **Resolution:** Traditional "alarms" and "alarm procedure books" ensured that unsafe situations were dealt with promptly using carefully considered response scenarios. As a further backup, the "Lead Operator" supervised actions of the Expert System as he would have done for the (replaced) operator.

- In the 2010's **"digital twin" simulations** of the plant were available that could anticipate operating problems and "pre-test" proposed solutions to plant upsets.
  - **Issue**: Digital Twin simulations were more sophisticated than operators could quickly understand. Even plant engineers often could not modify or troubleshoot these mathematical models.
  - **Resolution**: High speed networking technology allowed remote specialists to quickly provide 24 x 7 support. Process engineers at the central response center were responsible for development and maintenance of the digital twin model, thus ensuring that they remained highly skilled.

- In 2020 we began to see **cyber-attacks** on industrial infrastructure that were faster and that probed more vulnerabilities than any human. In order to cope with these challenges, AI-based cyber defense systems were developed.
  - **Issue**: Soon, Plant Operators will not be able to respond rapidly enough to participate in cyber defense. In fact, without help, they may never realize that an attacker had penetrated their facility.
  - **Resolution:** Control and optimization systems must incorporate measures to deal with both malicious and inadvertent cyber events. Network Operations Centers (NOCs) will be needed to watch for unusual traffic and respond when cyber incidents are suspected.

It is important to realize that in each of the above examples, safe operation requires a deep understanding of that plant, its control dynamics, and safety interlocks. What matters is not the optimization technology used. Instead, what is required is a clear understanding of human-machine interfaces (HMI), process hazards, operating practices and engineering standards of that industry.

AI applications are now gaining the ability to "self-improve" without human direction. This is potentially both a blessing and a curse. It may be beneficial, making AI more effective in industrial applications; however, it also brings the risk that AI applications may "improve" plant operations in ways that were not intended. We must therefore ensure that humans always retain the ability to control plant safety. This can be accomplished using established engineering and operating practices. It will also require training and certification of operating and maintenance personnel.

More articles that address the use of AI in ACS and OT may be found at https://www.pera.net/Ind_tech.html .

Author

Gary Rathwell has more than 40 years of experience with enterprise integration and optimization projects, including PERA master planning and project management.

As one of the initial authors of the PERA Handbook of Master Planning, he has used PERA Enterprise Architecture and Master Planning methodologies throughout his career including control and information systems for oil production, pipelines, refining and marine loading, petrochemicals, coal, gas, and oil-fired power plants, polyethylene, ammonia, explosives, paint, pulp and paper, food and beverage, and pharmaceuticals.

LNG facilities included world-scale arctic, European, and US Gulf coast complexes. infrastructure facilities included Fire, Police, and Emergency Response systems for major US cities, as well as emissions reporting and trading systems for more than 100 US Power Plants,