THE SAFETY FIRST IMPERATIVE FOR UTILITIES

Infosys®
Navigate your next

The Utilities industry has accorded top priority to the safety of the public, customers, and the workforce. Yet, there have been several incidents some of which resulted in fatalities. According to the U.S. Bureau of Labor Statistics, the Utilities industry registered 28 workplace injuries / illnesses per 100 full-time workers in 2020. While a majority of incidents affected employees in operations, maintenance and building of facilities, some affected the public, such as the waterworks accident at Abbeystead, Lancashire in 1984. Even when there are no fatalities, incidents can have long-term and far-reaching consequences such as the contamination of water supply at Camelford, Cornwall in 1988. Workplace safety continues to be an issue at Utilities plants. In December 2020, an explosion at a wastewater plant of Wessex Water at Avonmouth, Bristol claimed the lives of four workers.

Mitigating IT and OT risks

For Information Technology (IT) professionals, such issues, while a cause for concern, may seem remote. On the other hand, safety of coding has been a long-standing concern for professionals involved in automation or Operational Technology (OT). Supervisory control and data acquisition (SCADA) systems have rigorous design and testing protocols. However, even in domains with a robust safety ethos, errors and omissions have resulted in serious consequences. Moreover, with the growing adoption of Artificial Intelligence (AI) and transition towards autonomous asset management, safety can be affected by many IT systems.

IT professionals need to undertake the risk analysis and testing associated with automation and OT. The IT industry adopts ISO 27001, a global information security standard for risk mitigation. Although it is an important standard and set of procedures, ISO 27001 only covers the security aspects of a deployment. Managing other risks, specifically in safety matters, is more nuanced. Enterprises expect subject matter experts (SMEs) to set safety standards for projects. But, as IT becomes more complex, particularly as more AI is deployed, SMEs may not have the requisite knowledge to address potential risks.

Applying HAZOP in Utilities

Utilities can take a cue from the engineering industry which has established several safety processes and procedures. The hazard and operability (HAZOP) methodology developed by the ICI Group of Companies helps manage risks in the design, operation, maintenance and decommissioning of chemical plants. The Institution of Chemical Engineers (IChemE) further codified the procedures and provides training courses to apply HAZOP in a working environment.. IChemE sets out the fundamentals of HAZOP as well as pitfalls of the process and how they can be managed. However, any HAZOP study needs to be led by an experienced practitioner.

Let us evaluate an IT system offering real-time control of a sewer network. AI may be deployed to support such a control system, but AI needs to be set with specific parameters. For example, a control gate could be opened in a storm situation leading to flooding and pollution downstream.. This could cause environmental damage, health risk (contamination) and potentially, risk to life. This IT system should be designed within parameters that remove, or at least reduce, the risk. Other risks include the danger of equipment startups to staff during maintenance. A properly enacted HAZOP 'teases out' such risks, so that they can be appropriately managed and incorporated into design, build and testing. Apart from HAZOP, utilities can evaluate the merit of incorporating other security mechanisms, notably, Failure Mode and Effects Analysis (FMEA) or Failure Modes, Effects and Criticality Analysis (FMECA) and the 'Swiss Cheese' model that ring-fences IT systems with multiple levels of security to prevent dysfunction.

Learning from the Aviation industry

The number of times IT errors have caused safety issues is difficult to estimate, mainly because many of these events are not reported. Aviation has been in the spotlight after several mishaps resulted in fatalities. The aviation industry has undertaken studies detailing errors, which are a combination of human and automation (i.e. software), leading to incidents. Software control systems were a factor in the Boeing 737 MAX crashes. Moreover, it is not simply errors in the setup that can cause issues, but also on how the system interacts with the user of the system. For example, in 2009, the complex information presented to pilots of Air France 447 when they took over from autopilot mode resulted in the aircraft crashing into the Atlantic ocean.

Artificial Intelligence (AI) presents opportunities as well as risks. A study by the Center for Security and Emerging Technology at Georgetown University shares examples of what can go wrong. It describes where things have gone wrong, sometimes with fatal consequences. The study recommends best practices for avoiding such issues.

Managing emerging risks

In the Utilities industry, the area that presents the gravest direct risk is the electricity flexibility market. As a prime enabler for Net Zero initiatives, such as Electric Vehicles (EVs) and Distributed Energy Resources (DERs), flexibility will be a major area of investment and requires innovations on the IT front. It also presents several risks, primarily in the area of asset and workforce safety. With two-way electricity flows, multiple sources and demands, and complex switching, not to mention an exponential growth in sensors (Internet of Things), control will require use of complex computations, often involving AI. The potential for life threatening scenarios is huge, from switching on circuits under maintenance / overloading circuits to switching off circuits with vulnerable customers at risk. Comprehensive risk identification and management will be vital to prevent loss of life or injury. Moreover, these risks will need to be assessed against other risks such as security and privacy risks.

There are also indirect risks which endanger life and property. For instance, the network effect of social media has its positives as well as a downside. The viral effect of social media perpetuates several 'myths' about water and electricity. However, social media uses algorithms originally designed for retail applications. When a retail website directs customers to products similar to those just viewed, the risk is low. However, if a social media app directs users to information that reinforces the 'myth', users can believe it to be the truth. A likely solution can be algorithms directing users to contrarian views, so that people can make more informed choices.

IT professionals need to adopt an appropriate safety mechanism for designing, building, and testing IT for Utilities. Safety should not be 'someone else's problem' but our watchword in everything we do, so that our solutions are truly 'safe by design'

About the Author

Mike Jones
Principal Consultant, Utilities

For more information, contact askus@infosys.com

Navigate your next