Originally appeared in:
June 2015, pgs 71-74.
Used with permission.

HYDROCARBON PROCESSING®

J. LUCAS and S. WHITESIDE, Mangan Software Solutions, Houston, Texas

Cloud computing: The next revolution in process safety

Over the past 25 years, the process safety and functional safety disciplines have evolved from the implementation of safety legislation and the creation of governing authorities, to the development of best practices and the adoption of applicable standards. As the push for operational excellence and process safety spreads across multiple industries worldwide, organizations are continuously looking to technology to offer effective solutions.

Over that time, technological advances have provided new and effective software products that sought to answer this call; yet, emerging process safety methodologies and technical limitations of the 1990s and early 2000s reduced their scope and efficacy. Detailed here are the evolution of information-management technology, the benefits of software innovation over the last 25 years, and the limitations of tactical solutions that led to the search for new products.

Also demonstrated is the evolution from disparate applications and data-management systems to strategically linked, cloud-based solutions. This evolution is allowing thought leaders within the petrochemical industry to reengineer how their plants implement and execute process and functional safety.

The rise of PSM, RAGAGEP and spreadsheets (1990–1997). The early to mid-1990s brought about a sweeping change in the information-management landscape. This change was brought on by lower entry costs for computing platforms and a diverse landscape of software developed for those platforms. Personal desktop computers went from being a support mechanism for management and administrative staff, to being an essential tool for the entire workforce.

At the same time, a number of catastrophic accidents brought the need for process safety management (PSM) and standardization of safety instrumented systems (SISs) to the attention of senior leadership in the chemical industry and the federal government. Many organizations maintained proper documentation of their safety systems and process safety instrumentation.

However, this information was often manually accumulated, via hard copy or other complex technical forms, making it inaccessible to those that could benefit the most from its contents. With the introduction of the Occupational Safety and Health Administration's (OSHA's) PSM standards and its recognized and generally accepted good engineering practices (RAGAGEP), such as ISA-84, IEC 61508 and IEC 61511, the documentation requirements and information that would need to be managed dramatically increased. New procedures and standards for reviewing, changing and managing this information were established, as detailed in TABLE 1.[1]

As the 1990s came to a close, corporate networks and data warehouses became more common. They were rigidly structured and focused primarily on financial and contractual data management. Individual business unit information was stored in the traditional "filing cabinet" paradigm that was entrenched in business culture at the time. The file-and-folder method of information management rarely provided the appropriate context to comprehend the importance or relevance of the data contained within the system documents.

Along with the traditional storage paradigm, this period was marked by widespread adoption of desktop spreadsheet and database-management systems. Tools like Microsoft Excel, Fox-

TABLE 1. History of process safety management

Year	Event
1984	A toxic chemical release in Bhopal, India kills 4,000 people.
1985	Release from a chemical plant in Institute, West Virginia injures 135 people.
	American Institute of Chemical Engineers forms the Center for Chemical Process Safety and publishes *Guidelines for Hazard Evaluation Procedures.*
1989	A Philips 66 chemical plant explosion kills 23 and injures 232 people.
1990	The American Petroleum Institute (API) publishes Management of Process Hazards voluntary guidelines.
	Arco petrochemical plant disaster kills 17 workers.
	OSHA proposes a PSM standard based on API guidelines and recommendations.
	Congress passes the Clean Air Act Amendments, which mandate that OSHA enact process safety rules covering 14 specific areas.
1991	OSHA releases study of the effects of using contract workers in the US petrochemical industry.
1992	The final OSHA PSM standard is issued.
1993	The US EPA releases its risk-management program regulation.
1997	May 26, 1997, was OSHA's deadline for 100% completion of all process hazard analysis. OSHA required companies to identify the processes that pose the greatest risks and begin evaluating those first. At least 25% of the processes needed to be evaluated by May 26, 1994, with an additional 25% completed each year, so that all affected processes were evaluated by the final deadline.
1998	IEC 61508, "Functional safety of electrical/electronic/programmable electronic safety-related systems," is published. This document sets the standards for safety-related system design of hardware and software.
	IEC 61511, "Functional safety of safety instrumented systems for the process industry sector," is also published.

Pro and Access, as well as Lotus Software's Lotus 123 (now part of IBM), provided users the ability to organizationally store data and information in a structured manner (**FIG. 1**). These tools marked the beginning of the transformation of how process safety data and information could be managed and stored. No longer was safety information a static piece of paper.

In the late 1990s, process safety focused on compliance activities. The new OSHA regulations and International Electrotechnical Commission (IEC) standards required a great deal of resource-intensive data gathering to identify functional safety gaps that had not been scrutinized in the past. This effort led to a large number of non-standardized methodologies for managing the increased volume of data that was being created to reach compliance. Some organizations built "libraries" of documentation that housed all safety-management-related information, and, despite the security risks and potential for human error, these items became the *de facto* mechanism.

While these libraries served as a cost-effective solution, individual business units quickly began to amass libraries of spreadsheets and databases filed in an ever-growing network of disparate storage locations. Important data lived on individual engineers' desktops, and information began to reside in silos across multiple business units, decreasing access to critical information. It would take another five years before web technology would enable centralized systems to maintain standardized, accessible data.

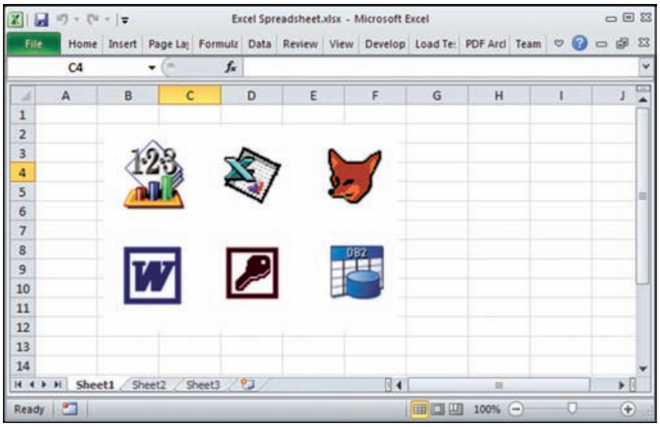

FIG. 1. Tools like Excel, FoxPro, Lotus 123 and Access provided users the ability to store data in a structured manner.

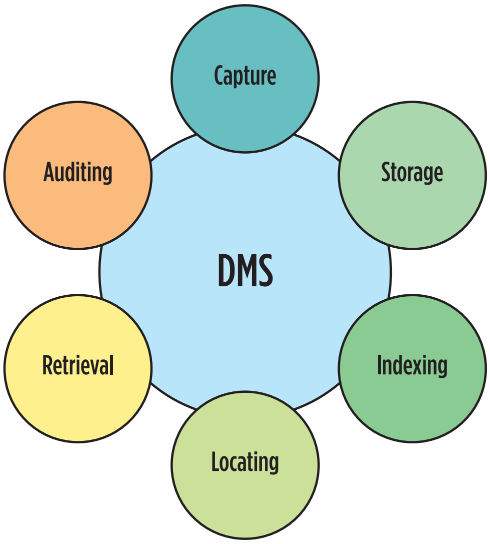

FIG. 2. Document-management system components.

The move to desktop applications and the intranet (1998–2005). By late 1996, the World Wide Web (www) had begun its meteoric rise. Initially, the web was a rudimentary system of linked documents and information with little interactivity. However, the industry quickly capitalized on the web's capability to share information across the corporate landscape.

Early web-based technologies quickly outpaced most businesses' ability to implement a lasting strategy for information management. This was due to several factors; web technologies were immature and in a constant state of flux. While web-based systems could be developed and deployed within an organization, underlying technologies were changing so fast that the compatibility and longevity of the systems were always at odds. Also, tools for manipulating and managing massive data and for making the data readily available were still in their infancy.

Many companies forged ahead, commissioning multi-year projects to manage the growing mountain of information, only to realize that their systems had become obsolete just prior to deployment.

The software industry quickly realized that information management—and document management, in particular—was becoming a burden on organizations. This drove innovation and the development of content-management and document-management systems (DMSs). These new tools provided collaboration, versioning, standardization and, most importantly, centralized storage of information (**FIG. 2**).

For some in process safety management (PSM), web-based document and content management immediately stood out as solutions to the complexities of storage, versioning and centralized access of safety information. DMSs represented the first real opportunity to actively manage process safety information across a complete organization.

While these solutions helped organize information and provide basic search and linking mechanisms, usability problems persisted. The unreliable structure of documents and datasets made it difficult to provide meaningful risk analysis data or performance metrics.

To make matters worse, a lack of standardized and intuitive naming conventions for files created nomenclatures that made it nearly impossible to identify relevant and up-to-date data (**FIG. 3**).

DMSs also forced organizations to continue the emphasis on spreadsheets. According to a 2010 study by the Aberdeen Group, "Accessing data stored in different home-grown systems and spreadsheets can be extremely time consuming and affect the quality of data."[2]

During this same timeframe, desktop applications were being developed to focus on specific compliance tasks in the market. These tools focused specifically on individual, standalone compliance tasks, and they became industry standard for facilities and engineers in the process safety and SIS lifecycle-management field.

Process hazard analysis (PHA) and hazard and operability (HAZOP) software rapidly decreased the time required to execute HAZOP studies, reducing costs and plant resources allocated to these studies. Desktop applications provided the quick and reliable means to execute safety integrity level (SIL) calculations, but the lack of collaborative features limited usability to the individual engineer sitting at a workstation.

Intranet-based management of change (MOC) software offered good tracking tools and easy-to-use interfaces, but a lack of rigid taxonomies in the software and links to corresponding process safety information limited the organization's ability to conduct accurate and timely hazard assessments.

While saving plants and engineers precious time, these tools lacked standardization capabilities and desired output formats. Exports from these tools were often complex, incomplete or confusing, causing firms to turn to consulting agencies to produce extensive paper reports, typically offsetting any savings the tools should have realized.

Many organizations attempted to offset the lack of standardization by producing internal standards and requirements, only to see them ignored as HAZOP teams quickly adopted the methodology of the third-party facilitator's parent company. This process resulted in risk-reduction strategies that varied from plant to plant and even from study to study. The lack of efficiency affected not only the efficiency of the processes themselves, but also the risk-reduction strategies, preventing the ability to prioritize gap closure.

These early software solutions suffered from a series of unintentional flaws that were mainly due to the lack of expertise with the overall subject matter. Engineering companies, lacking the resources to fully fund software products, created small utility applications as key differentiators or profit centers that could be used to bridge the gap to larger safety engineering projects. Software companies, lacking the engineering and plant-level expertise and resources, typically developed products that provided tactical solutions, such as risk assessment, hazard identification and information storage.

Several engineering companies attempted costly acquisitions, and a few software companies partnered with specialty consulting firms or embedded their applications within their engineering tools. None were truly successful.

In the end, these software tools gave leadership a false sense of security that they were managing and monitoring risk effectively. The limitations of these applications and the early attempts at sharing information had an unintended negative impact: reinforcing the silo culture while simultaneously frustrating leadership, management, engineering and operations.

Ascending to the cloud (2006–present). In 2006, a new methodology in business and information computing began to take form. It was a consolidation of past ideas. Early mainframe and terminal virtualization combined with the ever-increasing density and capacity of hardware environments. A single system could easily emulate tens to hundreds of individual systems, and they could easily and instantaneously be turned on and off.

This "virtualization" of hardware and its instant-on nature made it possible for service providers to quickly deploy hardware and software technology services. Companies like Google, Amazon, Apple, Force.com and Microsoft began to call this instant-on, everywhere computing capability "the cloud."[3]

Cloud technologies and software architectures became a means of sharing information and data, as well as infrastructure and services (FIG. 4). These tools opened new and powerful collaboration, analytics and data-mining opportunities that continue to this day. Information and data are no longer represented as a series of spreadsheets or data tables. They have become contextualized into data objects that can describe, share and interrelate information to other data objects within the cloud.

Additionally, the instant-on nature of these systems and services dramatically reduces or eliminates the traditional IT burden of management and maintenance. Businesses can now easily integrate technologies into their ecosystems without the high capital investment of infrastructure, custom development or specialized support staff.

Reengineering the software approach to process safety. Process safety and functional safety engineers are fully aware of the benefits and limitations of each of the technologies that have emerged over the past 20 years. Many of those engineers have used their experiences to develop new solutions that utilize the best attributes of each of these past technologies and merged them into the cloud.

Using an underlying database as the foundation of the software, with data objects linked across different functional modules, these cloud-based solutions have added easy-to-use software workflows that can be configured to an organization's engineering practices and processes, facilitating user adoption and increasing the efficiency of their teams.

Safety management with live data. The integration of cloud technology with the database systems and software tools of the past has transformed process safety and functional safety management.

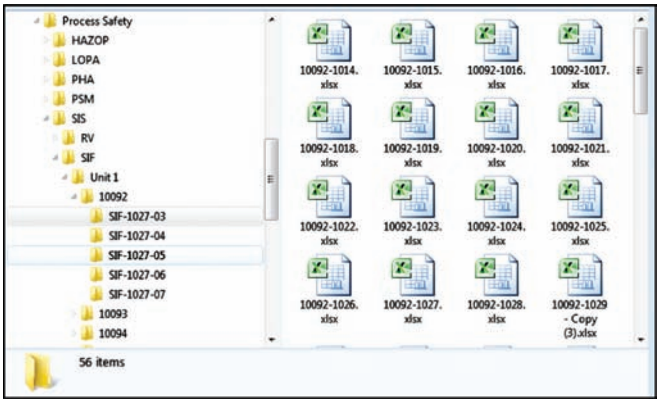

FIG. 3. A lack of standardized and intuitive naming conventions for files created nomenclatures that made it nearly impossible to identify relevant files.

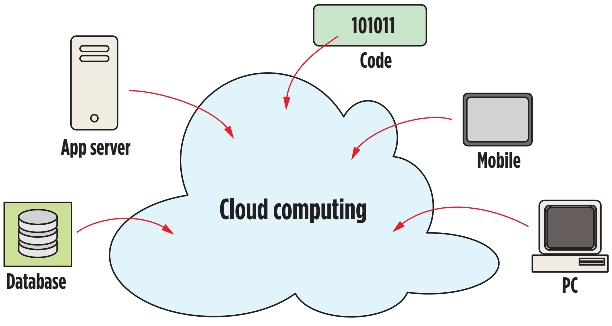

FIG. 4. Cloud technologies and software architectures have become a means of sharing information and data, as well as infrastructure and services.

For the first time, cloud-based software programs are offering unprecedented collaboration capabilities, automating and standardizing engineering processes, enabling easy visibility for management, and facilitating expert execution of risk-barrier assurance.

Cloud computing allows more meaningful and contextual data to be delivered in real time, allowing industrial owners and operators to realize focused results.

For example, in 2011, engineers working on the largest OSHA abatement project in history were able to meet tight deadlines by leveraging cloud technology. With thousands of independent protection layers to assess to meet compliance within a limited timeframe, engineers from multiple companies augmented refinery staff and were able to execute these compliance processes in one cloud-based solution.

Management was able to accurately forecast resources to meet the looming deadline; engineers had instant access to process safety information and were able to execute their assessments regardless of their physical location. Reports generated from the system and the results of the assessments provided the refinery with the audit trail it required to satisfy the federal government's compliance team.

Automation improvements. Cloud-based software offers standardization and automation features that were not feasible with previous desktop solutions. Help features on the interface provide guidance written by subject matter experts (SMEs), allowing less-experienced engineers to navigate processes effectively, while permitting SMEs more time to consult and also ensuring conformance to standard procedures.

One refining company was able to automate its functional safety assessment processes through workflows configured to its standards. Assessment teams were able to reduce the duration of the company's projects, enabling it to gradually transition from expensive third-party engineering certification of their systems to internally conducted reviews. Leadership was able to review the level of conformance and the results of the assessment, and align the facilities with the company's governance strategies.

Overall plant safety boost. With cloud technology, operators are able to realize real-time access to timely and accurate information, reliable mobile capability, automated RAGAGEP processes and reduced dependence on third-party consultants. However, the biggest impact that cloud-based software will have surrounds the overall safety of the plant. It significantly increases the performance capability of safety systems through enhanced risk-reduction analysis and increased awareness of unmitigated hazard scenarios.

Engineers now have the ability to monitor risk to their facilities with tools that identify gaps in their independent protection layer (IPL) mitigation strategies, using data from layers of protection analysis (LOPA) studies. Corporate-level and site-level SMEs can drill down into the data and conduct unprecedented analysis on how facilities manage their risk-reduction efforts.

Some organizations have begun using LOPA data and cloud-based software to identify unmitigated hazardous scenarios, enabling engineers and managers to prioritize their gap-closure projects. An added bonus for these teams is that they can use this information as tangible proof in their business justifications when they appeal to senior leadership for funding.

Risk management. New software tools and innovative interfaces also graphically communicate hazardous and unmitigated scenarios. Organizations are now configuring these tools to visually display risk matrices and detail the number of LOPA scenarios at each intersection. Some of these tools are dynamic and serve not only as an organization's risk register, but also as a real-time risk-monitoring application. In using such tools with data objects linked to an underlying database, an operator who places a safety function in bypass can visually review the impact of this decision and make accurate and timely assessments using HAZOP and LOPA data before executing an override.

Engineers can instantly build and view bowtie models using LOPA data uploaded to the system and visually map out the plan to manage commercial, safety and environmental risks. Communicating these plans, identifying these risks and assessing these barriers are now possible with these new innovations.

Takeaway. Over the last 25 years, software technology and PSM systems have grown and matured. From paper processes and filing cabinets to spreadsheets stored in web-enabled DMSs, the nature of the way information about process safety is used and accessed has evolved. Now, with the advent of cloud technologies and the lessons learned from previous decades, a new age of information-management and collaboration has arrived, where data can be analyzed and used to refine safety processes and best practices.

The continued integration of software technologies with cutting-edge engineering practices will reduce the complexity and expense of process safety, and usher in a new era of empowerment and confidence for safety professionals. HP

LITERATURE CITED

[1] McAteer, D. and L. Whiteman, "Learning from Hamlet: The case for a national safety and health board," *New Solutions,* Vol. 3, No. 2, 1993.

[2] Aberdeen Group, "The role of software in asset performance management: Reduce maintenance cost, downtime and safety incidents," October 2010.

[3] Rae, I., "Future of computing: Forecast calls for partly cloudy," Bitcurrent.com, June 12, 2008.

JEREMY LUCAS, chief technical officer for Mangan Software Solutions (MSS), is responsible for leading the architecture, design, development and data intelligence teams. He has been leading teams developing software and system architectures in the oil and gas and life science industries for the past 20 years. Prior to his role at MSS, Mr. Lucas spent 15 years providing innovation and technology solutions that helped drive efficiency and cost savings to Mangan Inc.'s clients and industry portfolio.

STEVE WHITESIDE, president of MSS, is responsible for the overall success of the company, implementing business strategy, recruiting innovative personnel and determining the vision of the organization and its software products. He has over 15 years of leadership and management experience in the oil and gas and construction industries. Prior to his role at MSS, Mr. Whiteside worked with some of the world's top oil, gas and chemical companies, helping them align their organizations with process and functional safety practices and compliance requirements. Mr. Whiteside holds a BS degree in systems engineering from the US Military Academy at West Point, New York.

Eprinted and posted with permission to Mangan Software Solutions, Inc. from *Hydrocarbon Processing*
June © 2015 Gulf Publishing Company