MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Multi-level Failure, Causality and Hazard Insights via Knowledge Based Systems

Erzsébet Németh, Ian Cameron
School of Chemical Engineering
The University of Queensland,
Brisbane, Australia 4072
Email: itc@uq.edu.au

Keywords: Failure, causal graphs, hazard identification, diagnosis, knowledge based systems, intelligent systems

Abstract

Over many decades there has been a significant development of knowledge-based, intelligent design tools and their use in the design of process systems. Amongst such tools are "intelligent" piping and instrumentation (P&IDs) design environments, coupled to life cycle design environments. These tools can provide opportunities for the development of new, more efficient and re-usable approaches to hazard identification and diagnostic systems. They leverage modern information technology characteristics of such design environments. These considerations are part of a growing trend in industrial digitalization, as reflected in such initiatives as Industry 4.0 in Europe and driven by the Industrial Internet of Things (IIoT).

Within this larger industrial digitalization picture, this work discusses the principles, developments and application of a hazard identification methodology (BLHAZID) that exploits structured representations of the design in the form of ISO15926 data standards. The hazard identification methodology is based in knowledge representations of failure modes of equipment types that are found in many process designs and how those failures subsequently affect the system states and other components. The underlying causal models can be used at various levels of aggregation, model fidelity and component inclusion detail. The aggregation can span across the most detailed view at the smallest component level through subsystem level to plant level perspectives.

The ability to represent and then display failure causation and implications at different levels of granularity allows deeper insight into system failures, and the potential for real-time diagnostic deployment. The importance of failure and subsequent propagation prevention through the use of

safety instrumented systems and other barrier devices is possible. Outcomes can be visualized in informative ways.

The presentation will discuss these intelligent information technology approaches via some a case study, highlighting the advantages and challenges such approaches bring to hazard identification as well as highlighting other application areas such as real-time diagnosis, corporate knowledge capture of failures, operator training and accident investigation.

Motivation

In the following discussion, we highlight some of the motivations to consider computer aided developments driven by the significant focus on industrial digitalization. Increasing digital connectivity and the focus on system life cycle processes.

Challenges in failure, causality and hazard identification:

The hazard identification phase of risk management applied to complex process design systems is still a significant challenge in terms of detail, time, cost, quality of outcomes and efficient re-use of generated knowledge. Today, hazard identification tasks are almost exclusively performed by Hazard and Operability (HAZOP) studies that adopt a particular system representation and methodology. In some industries Failure Mode and Effects Analyses (FMEA) are also used. Both these approaches normally use diverse teams of participants applying a form of critical enquiry around the intended design. A primary source of information is represented in Piping and Instrumentation Diagrams (P&IDs). In the case of HAZOP studies, the basic approach has been accompanied by an ever-growing list of supporting documentation, and extended, rightly or wrongly, into other aspects of systems' analysis, such as non-fluid systems, maintenance, waste considerations, commissioning, emissions and the like.

In a comprehensive critique, Baybutt (2015) discussed a range of potential weaknesses using HAZOP around team issues, meaning and interpretation of design intent, basic issues related to parameters and guidewords as well as technical coverage, operability and specific hazard types. He also shows that many of these insights and concerns have been present for decades. Some things appear to have not changed.

In a recent review of hazard identification methodologies and tools, Cameron et al. (2017) also considered similar issues. The issues can be summarized around recurring challenges for the traditional HAZOP methodology as:

- lack of depth in analysis,
- lack of diversity and imagination within study teams
- lack of completeness in identifying scenarios
- lack of completeness in identifying initiating events
- dealing with the complexity of the process
- poor documentation and communication of outcomes
- loss of focus due to the duration of the studies
- confusion as to the propagation paths of deviation to initiating cause and to consequence
- repetitiveness of the studies
- inadequate assessment of the interactions amongst plant, people, procedures
- review of changes

Jarvis and Goddard (2016) recently did a study of 100 major losses over the 20 year period: 1996-2015, in order to understand the common causes of those losses. Major losses were classed as losses greater than $US50 million (capital plus business interruption), with no consideration of other consequential losses such as civil fines, environmental clean-up, personal injuries and reputational damage. Total losses for the period were in the order of $US25 billion.

The outcomes of this study in regard to the adequacy of Process Hazard Analysis (PHA)[1] were:

- 7% of mechanical integrity failure (MIF) were primarily associated with PHA inadequacies, which was one factor in Management System Failures (MSF) [2]
- 28% of non-mechanical integrity failures (NMIF) were associated with PHA activities, and,
- 48% of totalled MIF and NMIF were associated with PHA activities

These insights into current practice put pressure on maintaining very high quality PHA activities, and also raise questions concerning the long-term suitability of current practices in complex and highly interconnected socio-technical systems. This is especially a challenge around the present growth in systems' connectivity, embedded devices and life cycle perspectives driven by such developments as Industry 4.0 and IIoT. In the context of safety and risk we now briefly discuss some of the current drivers around smart systems.

Drivers from current industrial digitalization and the opportunities they afford:

For more than 25 years there has been a significant acceleration in industrial digitalization, driven primarily by information and communication technologies (ICT) and massive growth of internet technologies. Significant process and business performance is now driven by The Industrial Internet of Things (IIOT) which refers to:

> *"a network of physical objects, systems platforms and applications that contain embedded technology to communicate and share intelligence with each other, the external environment and with people".* (Accenture, 2018)

Key aspects to consider in the context of IIoT are:

- Investment levels in IIoT are predicted to reach $US123B in 2021 (i-scoop, 2018), 2018a).
- Massive sensor deployment and reduced costs – embedded and also wearable. There is predicted to be over 50 billion internet connected devices by 2020 from a base of 17 billion in 2016. (Morgan Stanley 2018a)
- Massive equipment embedding of micro-controller units (MCUs)
- Industrial IIoT adoption rising from about 8% of capital budget to 18%. IIoT is a key driver of market growth. (Morgan Stanley 2018b)

What does all this mean to the process industries and in particular to function and failure of complex systems? For industry, the main IIoT drivers as reported by Morgan Stanley are:

1. Improving operational efficiency (47%)
2. Improving productivity (31%)
3. Creating new business opportunities (29%)

[1] PHA in this study consisted of: HAZOP, LOPA and SIL activities.

[2] The 7 factors in the Management System Failures were: Inspection programs, Materials & Quality Assurance, Operations/Practices/Procedures, Control of Work, PHA and Management of Change, Available Safety Critical Devices.

4. Reducing downtime (28%)
5. Maximizing asset utilization (27%)
6. Reducing asset life cycle costs (18%)
7. Enhancing worker safety (14%)

Given that risk and safety are temporal in nature we need to consider the implications on the methodologies and the nature of the software platforms for safety and risk issues into the future. What was considered acceptable today will be under threat from tomorrow's developments. Transitions to life cycle, smart systems that are based on systems fundamentals will provide a range of benefits not easily achievable today, and fit more effectively into the current digital tools of IIoT.

In the next section we consider the specific area of function, failure, risk and the identification of hazard in complex designs. This is an area with a long and important history which has experienced numerous methodological developments over more than 60 years and more recently the development of software support platforms.

For major projects in the process industries, current practices are struggling to provide efficient and high quality outcomes as attested by recent studies and critiques already mentioned. It is also likely that good, viable solutions will involve an eco-system of integrated approaches: software platforms, knowledge based systems, re-use of prior knowledge, real-time gathering and processing of data and information to continually incorporate deeper and wider knowledge to enhance operational excellence. These will also provide easily accessible and usable corporate memory for future developments.

Function, failure and causation: the role of knowledge representation systems

Dealing with complex, highly interconnected systems subject to failure definitely requires "systems" approaches, conceptualizations and thinking. There are several important considerations to such approaches in the current era of rapid digitalization:

1. System conceptualizations that adequately represent the major elements and their interconnections. This involves not just the physical plant, but also procedural aspects and human factors, people issues.
2. The ability to exploit evolving digital representations and data interoperability standards such as ISO15926[3] that provide access to the evolving design in a neutral format.
3. An approach based on fundamental principles and formal concepts around function, capability, failure and causality, and their organized knowledge representation.
4. Approaches that have applicability across the whole life cycle of product and process, so that maximum benefit can be derived from the insights of designers, managers, operators and other associated staff and personnel.
5. The ability to incorporate learning from failures, to identify, capture and enhance knowledge of the system over time. This aids in capturing corporate memory.
6. The ability of the methodology to be adaptable to different scales of representation, such as:

[3] See the International Organization for Standardization (ISO): https://www.iso.org/search.html?q=15926

a. Access to multiple causal models of varying complexity and fidelity that can be applied as designs develop and mature
b. The ability to look at the system from highest level of detail at the individual component level to more aggregated views
c. The ability to exclude/include process equipment within any failure analysis
d. The ability to estimate system failure propagation time scales or track overall failure frequency or probability estimates.

There are numerous knowledge based system perspectives and conceptualizations that can be adopted to address function, failure and causation. Many had their origin in the 1980s when AI and expert systems were making some headway. An early AI based HAZOP system using the Prolog declarative language appeared in the 1980s (Cameron, 1986), and other work at Loughborough University in the UK has led to commercial realization in the form of the *hazid* software platform[4]. These approaches essentially took the HAZOP methodology at the time and applied structure and some aspects of artificial intelligence tools to aid users in performing their tasks.

Many of these approaches are highlighted in the recent review by Cameron et al. (2017), and the reader is referred to that for more information. What follows here, is a discussion around the conceptualization, development and application of a functional systems framework (FSF) that has formed the basis of our own research into looking at the issues around plant, people and procedures and their inter-relationships. It needs to be emphasised that this is one of many systems based approaches built on knowledge management and use.

The fundamental conceptualization is seen in Figure 1, with basic concepts drawn from fundamental system concepts of entities, properties, function, failure and causation (Bunge 1997). The framework provides a firm foundation to pursue systems related investigations.

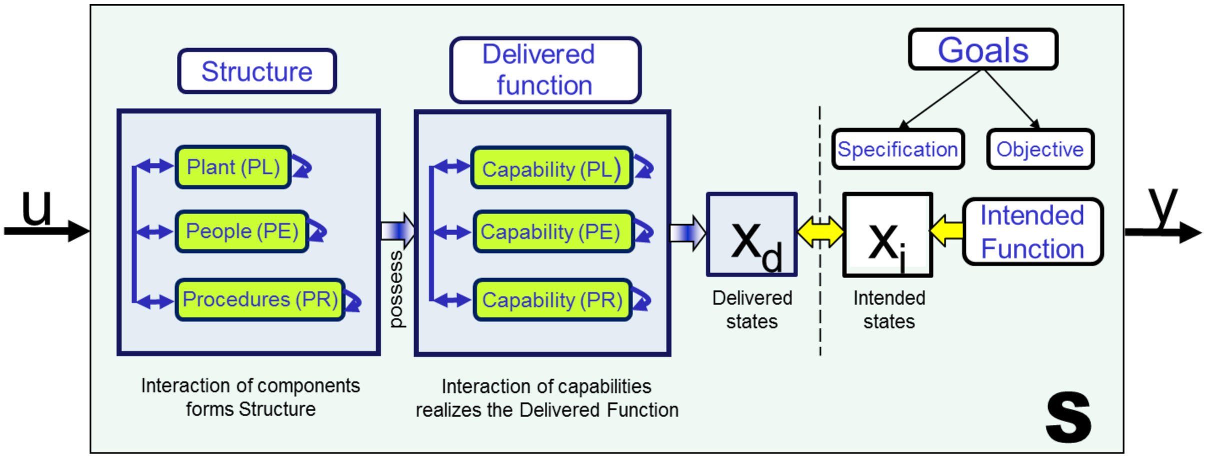

Figure 1 A functional systems framework (FSF)

[4] See: https://www.hazid.com/

The FSF pictures key components of plant, procedures and people, highlighting components capabilities, function and intended system goals. This has been discussed by Seligmann et al. (2012) in which he developed a blended hazard identification methodology that combined aspects of HAZOP with FMEA to generate deeper insights and better hazard coverage than either individual method. It was tested on a commercial design of a Benzene Saturation Unit.

The underlying causal model that considers the plant components (equipment) and the streams is seen in Figure 2. This considers that properties of both plant equipment and streams give rise to a set of system capabilities. It is those capabilities, acting together, that deliver the relevant system functions for a particular process structure, and these address design intentions as reflected in the intended states. Plant components and streams interact in complex ways. Loss of capabilities can lead to failures in components and hence impacts on stream properties and vice versa.

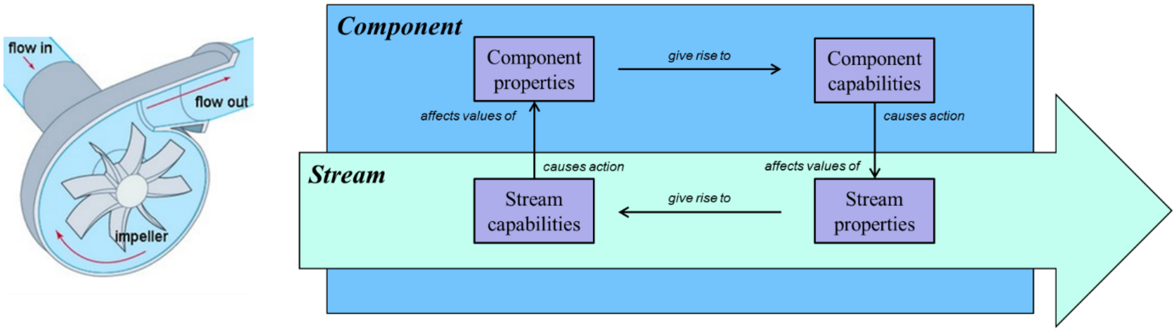

Figure 2 Causal model for failures and failure propagation

With reference to Figure 1, HAZOP considers ‘intended function’ in terms of the stream properties and looks at the difference between important ‘intended’ and ‘delivered’ states, typically expressed as stream values that can include such properties as pressure, flow, temperature, level and concentration. This leads to HAZOP ‘deviations’, which are then traced to causes and consequences. In a complementary manner, FMEA starts with failure modes with potential failure mode causes, then tracing through to system to identify impacts on function. This typical drives left to right in Figure 1, whilst HAZOP drives from right to left.

The original, overall strategy followed a general workflow which included:

- Efficient extraction of design information from P&IDs using a neutral format standard. In this case: ISO15926, that is now an agreed interoperability data standard between major CAD-CAPE software vendor systems.
- Structured decomposition of the topological information into interconnected subsystems that are amenable to investigation and analysis around failure, causes, implications and causal pathways.
- The ability to build, use, modify and extend knowledge based representations of plant component models that incorporate known failure modes. These can be built with various levels of detail and fidelity.
- The application of those models to the system design to illicit potential failure types, causes and implications across the system.
- Various forms and levels of visualization and representation of outcomes to understand implications for design thinking and operational performance.

The original implementation of this methodology as an experimental tool required the use of several information and knowledge representation and management systems that included:

- Formal description of equipment capability sets (see Figure 3)
- Use of failure modes (FM), failure mode causes (FMC) and failure implications (FMI).
- Development of causal descriptions that link component failures to stream failures and vice versa, leading to causal triplets: {cause, mode, implication}: <FMC><FM><FMI>.
- Development of causal models for common operational modes that incorporate: stream inputs and outputs, internal states, FMs and their interconnections. (see Figure 4).

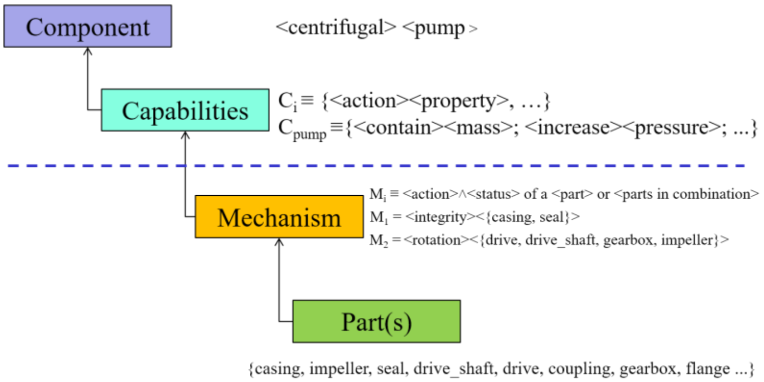
Component
<centrifugal> <pump>
Capabilities
$C_i \equiv$ {<action><property>, …}
$C_{pump} \equiv${<contain><mass>; <increase><pressure>; ...}
Mechanism
$M_i \equiv$ <action>∧<status> of a <part> or <parts in combination>
M_1 = <integrity><{casing, seal}>
M_2 = <rotation><{drive, drive_shaft, gearbox, impeller}>
Part(s)
{casing, impeller, seal, drive_shaft, drive, coupling, gearbox, flange ...}

Figure 3 Component capabilities structure

Within the approach taken in this work there is the possibility of adopting multilevel perspectives that relate to:

- *Causal model fidelity*: providing simple to complex models of the causal relations for a component
- *System aggregation level*: providing high level views down to highly detailed views into the causal structures
- *Inclusion detail*: which provides the ability to include or exclude nominated components from the subsystems, such as every pipe segment in a subsystem

These levels of consideration are supplemented with the ability to consider a range of operational modes that can affect the failure modes of component. Other temporal factors related to causal interactions as well as failure frequency/probability can be considered.

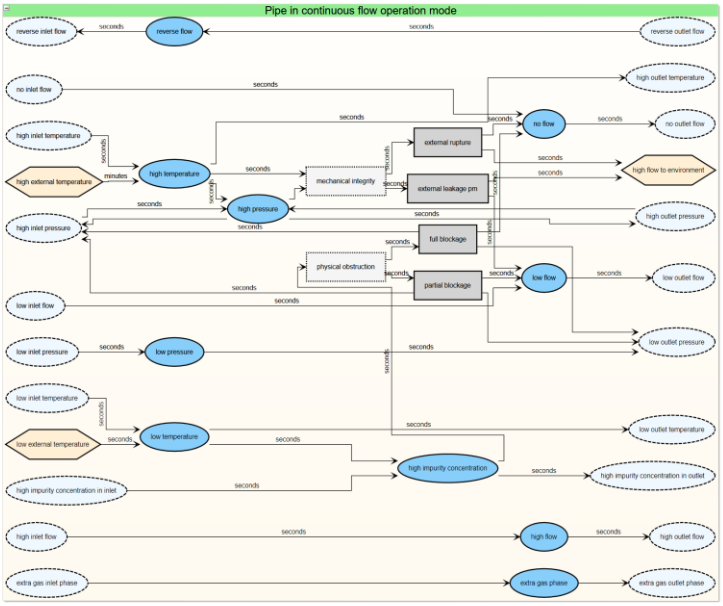

Figure 4 A causal model for a pipe segment

In the following section we discuss how these knowledge representations can be put to work when looking at a particular engineering design to understand failure propagation in the system.

Application and observations

The knowledge representation contained in approaches such as BLHAZID or similar methodologies can be used to consider a range of failure and hazard issues related to process plant. In this case we look at a bulk liquids storage and handling facility that is described in two separate, but linked P&IDs.

P&ID topology is imported via ISO15926 data exchange XML files and automatically analysed, decomposed into a series of interconnected subsystems that link inputs to internal subsystems and major mass and energy inventories and then to system outputs. Figure 5 shows the P&IDs and the first 3 levels of decomposition that is possible. These cover the overall system, the major subsystems and then further detail within a chosen subsystem. Disaggregation can proceed down to the finest level of every individual component in a Piping Network Segment.

Individual component types within a subsystem are automatically identified, and can be associated with models in a knowledge base (KB). The particular operational mode of the subsystems can be chosen, as well as the level of fidelity of model to be used as well as what specific components can be overlooked in the causality analysis. These overlooked items might be all pipe segments within a subsystem, where their failures modes are regarded as not significant.

Investigations can be performed on either, or both component failures (CF) in the form of failure modes (FM) in process equipment, or functional failures (FF) in the form of changes in stream properties. Search algorithms can then be used over the system topology to enumerate the possible causes and implications of a nominated failure. The outcomes of the search methodologies are shown as causal graphs. Other tabular outputs are also possible.

Figure 6a shows a situation where the issue of ‘no level’ in one of the main storage tanks (T-3) was investigated. The subsystem in which the initial failure occurs is highlighted by a yellow background and the specific failure by a yellow chevron shape. The live causal graph can be then traced through various intermediate failures to other functional or component failures, which are associated with other connected subsystems. In this case the two primary functional failures are related to ‘no inlet flow’ to T-3 and an ‘extra gas phase inlet flow’ which raises tank pressure, causing tank failure, and loss of containment.

The detail in Figure 6 is shown at a high level of aggregation. Finer details can be observed by opening other subsystem, as seen in Figure 7 where ‘component failures” in the main feedline subsystem can be seen. This involves numerous items of plant equipment. This methodology is using the causal model shown in Figure 2.

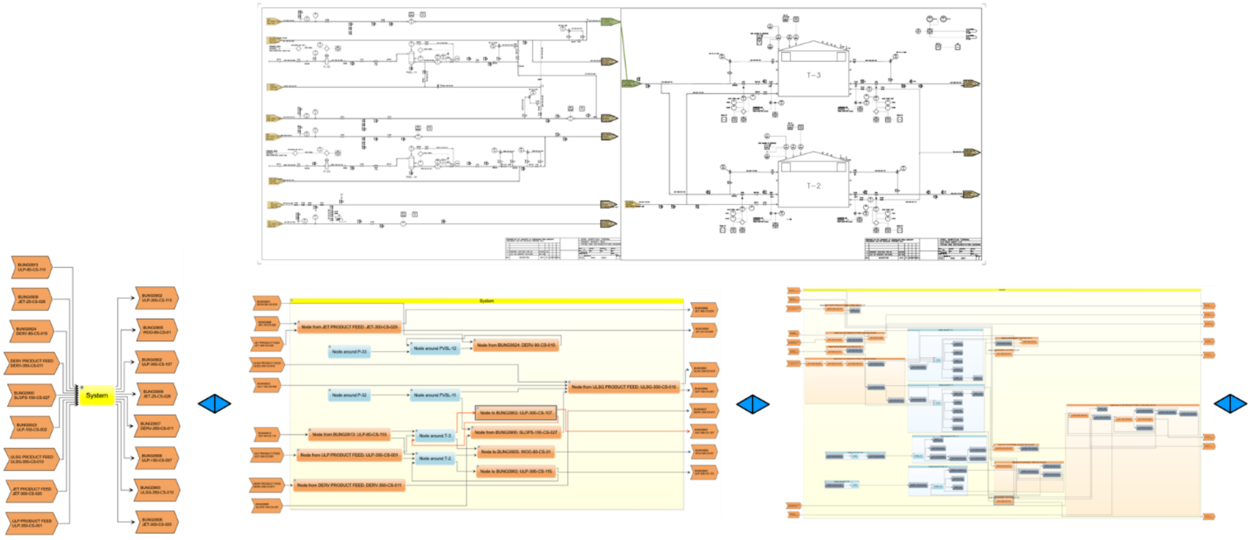

Figure 5 P&ID import and levels of system detail

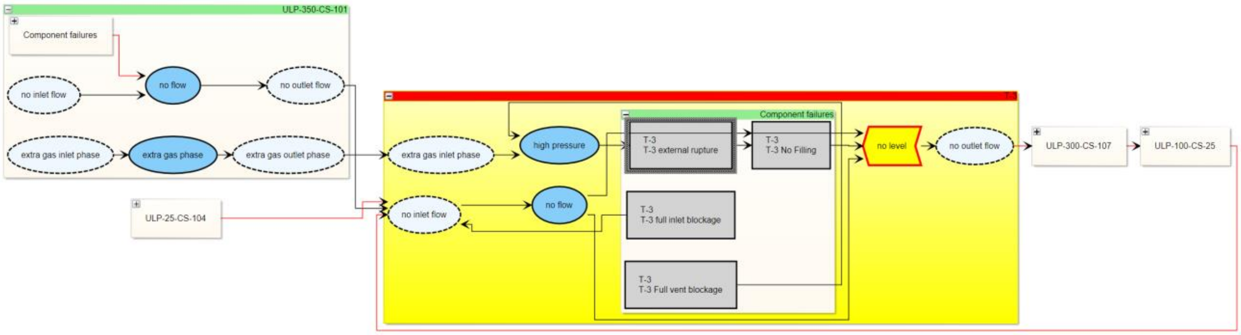

Figure 6a Possible causes of 'no level' (in subsystem T-3) storage tank

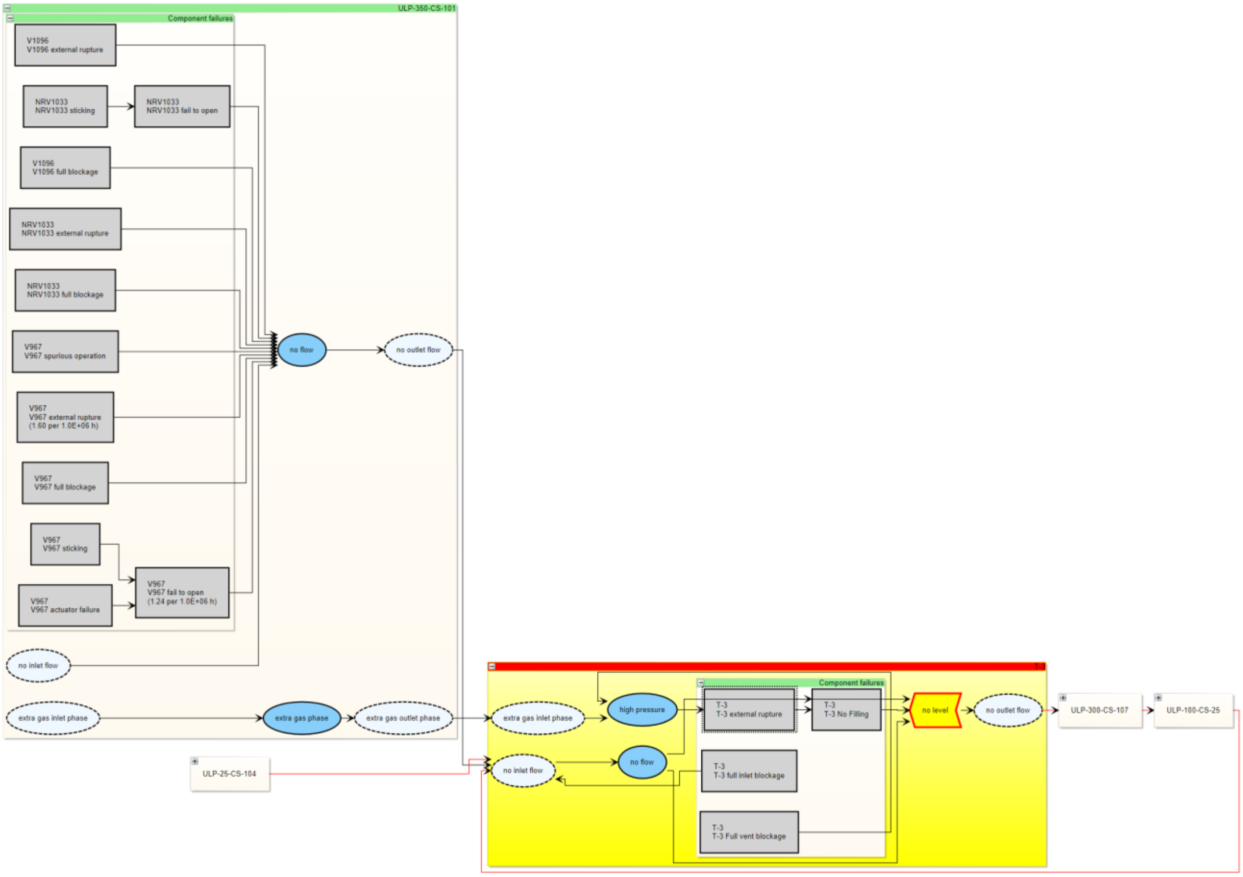

Figure 7 finer detail of component failures in feed subsystem that induce 'no flow' conditions to T-3

Besides the functional failures related to states within major equipment or streams be investigated but given the blended nature of the methodology failure modes in plant components can also be investigated to look at subsequent implications. Figure 8 shows the situation where a major inlet flow control valve (v1096) has a major failure (rupture). This generates several implications: high flow to the environment, no flow to the tank with potentially low level or no level in the tank. The inlet valve failure can also induce a reverse flow from the tank into the prior subsystem.

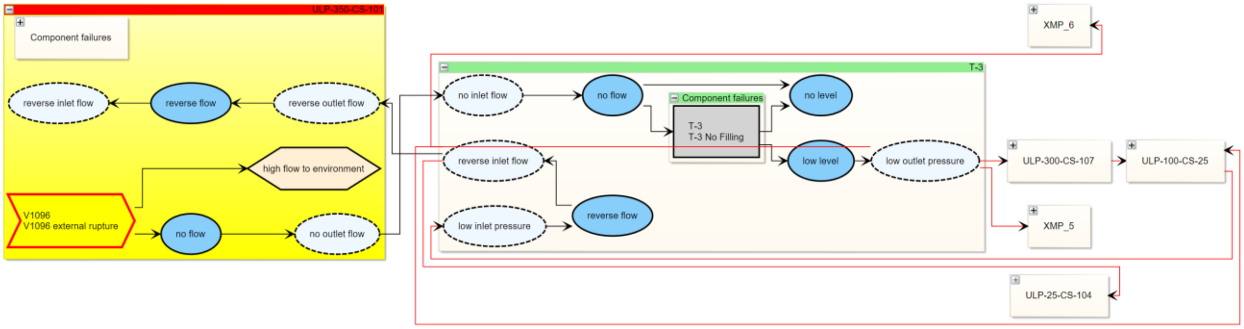

Figure 8 Implications of a major loss of containment through inlet feed control valve.

These rather straightforward examples illustrate the use of formal knowledge based systems that in this case span two P&IDs. More P&IDs can be handled, which potentially allows failure pathways to be tracked across significant sections of process plant.

The quality of the outcomes is clearly measured in terms of the underlying causal models, but the ability to trace causal links through the design can be very important in unravelling the behaviour of the design under numerous failure conditions. It can also be done over many interconnected P&IDs.

Using causal graphs is often a much easier means of visualization than equivalent tables, although these are also generated when the analyses are performed. Early experience with plant operators was encouraging, as they could see the nature of causation visually rather than textually, which required much more effort to interpret.

Higher fidelity models can be used to give more detail, and operational modes can be easily set to investigate what is often a difficult issue in more traditional techniques. Numerous other applications are possible.

Where to from here?

This paper has discussed the need for new approaches that can provide knowledge based tools for understanding failure implications in process designs. Given the growing complexity of information and interconnectedness of process systems, efficient investigation tools as part of risk management that deliver high quality and economically efficient outcomes are required.

Such knowledge based approaches should:

- Support human decision making across the whole life cycle from early conceptual design through detailed design and operations
- Adapt and grow as accumulated operational knowledge is integrated back into systems that can then easily exploit that knowledge in new situations.
- Provide advice in operational circumstances and also for new projects
- Are integrated with plant information systems, including real-time sensor data to provide pro-active functions that can help guide operators' decisions based on causal representations. This leads to real-time diagnostic tools, and the potential to build operator guidance systems off the outcomes of failure analyses.
- The ability to consider how barriers or lack of barriers affect failure propagation and the likelihood of such situations.

Whatever the approach to be taken in this era of IIoT and knowledge systems, it highly likely that the resultant systems will integrate numerous interoperable methodologies into real-time systems that continue to grow over the life cycle of the plant and product. It is also clear that the current digitalization emphasis of Industry x.0 (Schaeffer, 2017) or smart manufacturing will also include high fidelity quantitative modelling and simulation to complement the qualitative and semi-quantitative approaches.

References

Accenture (2015), Winning with the Industrial Internet of Things, How to accelerate the journey to productivity and growth. See: https://www.accenture.com/t20160909T042713Z__w__/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_11/Accenture-Industrial-Internet-of-Things-Positioning-Paper-Report-2015.pdfla=en   Accessed September 10.

Baybutt, P. (2015) A critique of the Hazard and Operability (HAZOP) study, Journal of Loss Prevention in the Process Industries, 33, 52-58

Bunge, M. (1977) Treatise on Basic Philosophy, Vol 3: Ontology I, The Furniture of the World, D. Reidel Publishing Company, Dordrecht, Holland

Cameron, I.T. (1986), Expert Systems for Hazard and Operability Studies, Proceedings of the Australian Institute of Petroleum Conference on Control and Prevention of Major Hazards, Brisbane, Australia, pg. 1-12, 1986

Cameron, I, Mannan, S, Nemeth, E., Park, S, Pasman, H, Rogers, W, and B. Seligmann (2017) Process hazard analysis, hazard identification and scenario definition: Are the conventional tools sufficient, or should and can we do much better?, Process Safety and Environmental Protection 110, 53-70, August.

i-scoop (2018) See: https://www.i-scoop.eu/internet-of-things-guide/industrial-internet-things-iiot-saving-costs-innovation/   Accessed September 10.

Jarvis, R. (2015). An analysis of common causes of major losses in the onshore oil, gas and petrochemical industries. Retrieved from http://www.icheme.org/communities/special-interest-groups/safety%20and%20loss%20prevention/events/2015/large-losses-7-july.aspx#.W1kHDdIzY2w Accessed September 9, 2018

Jarvis, R. and A. Goddard (2016). An analysis of common causes of major losses in the onshore oil, gas and petrochemical industries: Implications for insurance risk engineering surveys, Lloyd's Market Association, Version 1.0, September.

Morgan Stanley 2018a, See https://www.morganstanley.com/ideas/microcontrollers-semiconductors-internet-of-things.html Accessed September 10

Morgan Stanley 2018b, See: https://www.morganstanley.com/ideas/industrial-internet-of-things-and-automation-robotics.html

Schaeffer, E. (2017) Industry X.0: Realizing Digital Value in Industrial Sectors, Redline Verlag, Munich, Germany.

Seligmann, B., et al. (2012) A blended hazard identification methodology to support process diagnosis, J. Loss Prevention in the Process Industries. 25, 746-759