KV_C012
Villez, K., Venkatasubramanian, V., Spinner, T., Rengaswamy, R., Garcia, H., Rieger, C. (2010). Achieving resilience in critical infrastructures: A case study for a nuclear power plant cooling loop. Proceedings of the 4th International Symposium on Resilient Control Systems (ISRCS2010), Idaho Falls, ID, USA, August 10-12, 2010, 49-52.

Achieving resilience in critical infrastructures: A case study for a nuclear power plant cooling loop

Kris Villez, Venkat Venkatasubramanian
School of Chemical Engineering
Purdue University
West Lafayette, IN 47906
Email: kvillez,venkat@purdue.edu

Tim Spinner, Raghunathan Rengaswamy
School of Chemical Engineering
Texas Tech University
Lubbock, TX 79409
Email: tim.spinner,raghu.rengasamy@ttu.edu

Humberto Garcia, Craig Rieger
Idaho National Laboratory
PO Box 1625, Idaho Falls, ID 83415
Email: humberto.garcia,craig.rieger@inl.gov

***Abstract*—Engineered systems are increasingly equipped with sensing and actuating equipment making the operation ans supervisory task increasingly difficult to handle by means of human interaction alone. In particular, the detection, identification and accommodation of abnormal, potentially harmful, events has been a long-standing challenge. Many scientists in different scientific areas have attacked this problem which has resulted in a plethora of techniques for both Fault Detection and Identification (FDI) and advanced control, each with their strengths and weaknesses. Because of the diverse nature of adopted theory and paradigms and because of a historical separation of FDI specialists and control theoreticians, it remains a challenge to establish automated systems able to handle exceptional events with minimal human intervention. As such, a project has been set up to enable full integration of diverse FDI methods as well as optimal coupling of FDI modules and control modules in the closed-loop supervisory control system. In this contribution, we introduce the basic paradigms of our approach, a strategic plan to achieve this goal as well as some preliminary results.**

I. Introduction

The safeguarding of the integrity of large and complex systems is a long-standing problem in control engineering. The problem is relevant in the context of large-scale systems such as electricity, transportation and communication networks, hazardous processes like nuclear and certain chemical production systems, where resiliency of the designed systems is vital.

The problem has been attacked from many angles, using very different techniques, and by many researchers, applying different schools of thought, theories and assumptions. A particular niche in this research area is the one of fault detection and identification (FDI). An overview of techniques in this area is given in a series of review papers [1], [2], [3]. Likewise, an important research and development opportunity exists dealing with the establishment of control theory and algorithms with increased ability of systems to handle abnormal, potentially harmful, events. Robust control deals with so called passive methods, where the control algorithm is set up in such a way that it can handle a diverse set of anomalies, without further modification. A drawback is that increased robustness is necessarily bargained against performance. It is therefore economically infeasible to handle all possible harmful events by the robust control approach only. Active methods are usually classified under supervisory control systems, where the applied control algorithm is conditional to the awareness of a particular abnormal state of the process. While this delivers more flexibility and allows for higher performance in normal process conditions, this approach depends strongly on the correct assessment of the process conditions, following Fault Detection and Isolation. Unfortunately, bridging the two tasks (FDI and control) is not an easy task, especially as techniques have been developed in different scientific communities. In addition, the FDI community has traditionally developed techniques for open-loop supervision, in which a human operator takes control actions. As a result, many of these techniques are not readily suitable for control. Likewise, control theory offers little on how to translate FDI results into automated control actions.

Despite the important progress in both the FDI and control engineering area, fully integrated control systems which enable the detection, identification and accommodation of abnormal conditions in a process have not been accomplished yet. We are investigating this opportunity in a project that has been set up to make critical advancements in the integration of available techniques for automated management of abnormal events. Our study is particularly focused on a pilot-scale plant, both established in real-life and in simulation, which mimics the hydraulic behavior of a secondary cooling loop in a nuclear plant. Abnormal conditions to be accounted for include control equipment faults (sensors, actuators), process faults (tube rupture, cavitation) and faults in control logic (erroneous control actions). It is crucial that (i) several FDI methods can be used simultaneously and (ii) that robust and supervisory control algorithms are optimally coupled with the information derived from the FDI methods. In addition, validation by means of simulation and real-life testing will make sure that

both theoretical and practical challenges for the project are effectively tackled. By completion of the project, the designed control system will allow to accommodate for abnormal conditions in an automated fashion. This will reduce the impact of fault and failures on the system and its performance, leading to increased resilience [4] and so called graceful degradation. In addition, because of the high level of automation, human efforts are expected to be focused on situations that cannot be recognized or accommodated automatically, thereby making these efforts more effective and efficient.

II. Bayesian supervisory control

Two main problems were sketched in the above paragraphs. One is that a whole range of FDI techniques is available with varying characteristics. For instance, techniques have varying degrees of specificity. Indeed, some methods are set up and tuned for specific types of faults and others are more generic. Many methods are developed for certain faults (e.g. sensor biases, increased noise levels) and need to be combined for a comprehensive approach to FDI. However, the formulation results may vary which makes the integration of results from different techniques a challenge. To solve this challenge a Bayesian Belief Network (BBN) will be constructed. Such a BBN structure is an intuitive way to handle the diverse set of information flows. To apply BBNs to FDI, consider that a set of FDI techniques is implemented in a modular fashion with each of them operating in parallel. These techniques are set up in such a fashion that their outcome is a vector of probabilities or beliefs associated with all or a subset of the considered faults in the system. The BBN takes these probabilities as inputs and integrates the overall probability of each of the faults based on the separate module outcomes. To do this, Bayesian statistical theory is applied straightforwardly. This theory is based on two rules, namely the sum rule and Bayes' rule. The sum rule says that the overall likelihood of an outcome, $L(y)$, is the sum of the products of conditional likelihoods, $L(y|x)$, and corresponding prior likelihoods, $L(x)$:

$$L(y) = \Sigma_x L(y|x) \cdot L(x) \tag{1}$$

Bayes' rule says that the conditional likelihood of a first condition to a second condition, $L(x|y)$, is the same as the likelihood of the second condition conditional to the first multiplied by the prior likelihood of the first condition and the total likelihood of the first, or mathematically:

$$L(x|y) = L(y|x) \cdot L(x)/L(y) \tag{2}$$

Consider that $L(x, y)$ represents the likelihood of a certain fault, x, conditional to available information, y. Then $L(y|x)$ is the likelihood of having obtained that information in this fault case. $L(x)$ the prior likelihood of the considered fault and $L(y)$ the overall likelihood for the obtained information. The latter is computed based on the sum rule above. By using the above two equations for all possible faults one can compute the likelihood for all faults based on the same information. One can then select the fault with maximum value for this likelihood, called the Maximum A Posteriori (MAP) likelihood. When selecting faults this way, one ignores that other faults may also explain the observations to a similar extent, especially when obtained likelihoods are close to each other. Subsequent control actions may therefore not accommodate for the right problem or may make things worse. To avoid such conditions, the likelihoods for each fault, rather than the MAP selected fault will be communicated to the controller module in the supervisory control system. In a similar fashion to the Bayesian FDI strategy above, the controller will then evaluate the best control actions by integrating the expected performance function over the range of considered conditions. The likelihoods for each fault then function as weights in the decision process. By doing so, the risk associated with wrong fault identification and subsequent actions is reduced in the supervisory control loop, thereby increasing the resilience of the whole system to accidental or willful faults and failures.

III. Benchmark model and pilot-scale plant

A pilot-scale Machine Condition Monitoring (MCM) plant has been constructed for real-life experimentation and testing within the context of automated process state awareness and resilient control. The setup mimics the hydraulics of a nuclear plant service water system at 1/400 scale and consists of a water reservoir, pump, a butterfly valve equipped with a torque sensor, a gate valve and a series of ball valves that control the flow direction, connected by means of PVC pipes with diameter of 3 inch. The setup can be manipulated based on sensor signals (temperature, pressure, flow) and by means of several actuators (pump speed, valve positions). Automated controls and faults in the sensors and actuators (bias, drift, stiction) are added artificially in LabView. In addition, ball valve positions can be adjusted so to emulate tube ruptures or to introduce pump cavitation. An open-loop model of the same system has been set up by means of the ASPEN 7.1 package. All controls are programmed in Matlab, which reads sensor signals and sends actuator signals to the open-loop model at a simulated time interval of 2 seconds. Several fault models are included in the model, including sensor bias and drift, valve stiction and tube ruptures. Figure 1 shows the open-loop model in ASPEN.

Default low-level control includes a simple PID control of the butterfly valve based on a single flow measurement in both simulation. However, the envisioned supervisory control will have the authority to change the pump speed, gate valve position and ball valve positions to achieve system resiliency by means of control reconfiguration. A particular example of such resiliency may consist of altering the operation of pump and valves (changes in and level of set point) so that maximal flow is achieved while maintaining expected pump longevity. This will be set up and tested in simulation first, then in the pilot-scale plant.

IV. Strategic plan

Three major phases are identified in the project. The first phase, modeling, aims at the matching of the model with

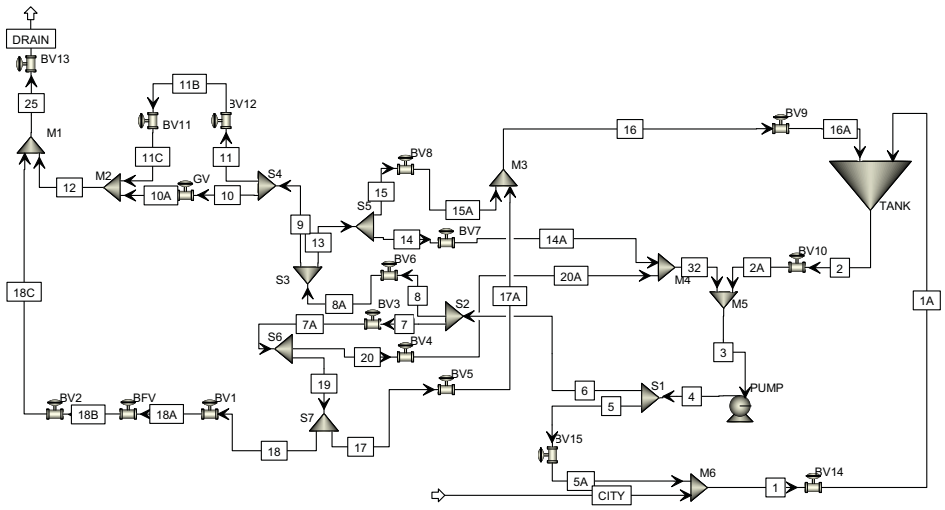

Fig. 1. ASPEN Model of the MCM testbed

experimental data, including fault models. In the second phase, Fault Detection and Identification (FDI), the above described strategy to integrate FDI techniques will be developed, integrated and tested. The third phase, resilient control, entails the development of control algorithms that can accommodate the considered faults and failures under uncertainty will be developed and coupled with the FDI modules.

A. Phase 1: Modeling

An experimental campaign has been set up to enable the verification and adjustment of the ASPEN open-loop model as well as the fault models. In particular, the experimental campaign includes the generation of:

- Open-loop response to changes in the butterfly valve position and closed-loop responses to changes in flow rate set point.
- Open-loop and closed-loop responses of the system to faults in sensors and actuators, including faults of the bias, drift and stiction type.
- Open-loop and closed-loop responses of the system to process faults, including emulated tube ruptures and pump cavitation.

By means of the generated data, the parameters of the ASPEN model as well as detailed fault models will be set up and validated. Figure 2 shows the open-loop flow rate measurement response to a closing and opening of the butterfly valve.

B. Phase 2: Fault Detection and Identification (FDI)

In the second phase, existing FDI methods are adopted for the particular system and integrated by means of the above described Bayesian Belief Network strategy. Selected FDI techniques include:

- Process history methods such as Principal Component Analysis, e.g. [5]
- Qualitative Trends Analysis (QTA), e.g. [6], [7]
- Model-based fault identification, e.g. [8]
- Signed Directed Graphs (SDGs), e.g. [9]

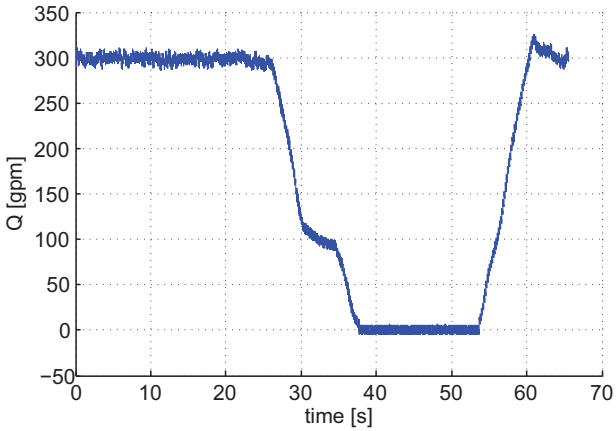

Fig. 2. Open-loop response of the flow rate measurement to full closure and opening of the butterfly valve

The first two methods require historical data to be trained against. The data generated for fault modeling in Phase 1 will be used to this end. In contrast, model-based fault identification and SDGs require process knowledge which will be derived from the detailed model implemented in the combined ASPEN/Matlab platforms. In addition, each of the methods needs to provide a likelihood function for each of the possible faults, rather than a crisp classification result. To this end, minor adjustments are required for the QTA and SDGs methods. For the other two methods, statistical theory provides these likelihood functions directly. On top of the resulting modules will be the Bayesian Belief Network, as described above which will deliver the overall likelihood of each considered fault. An experimental campaign will be set up to complete the FDI phase. In this experimental campaign the on-line performance of the FDI developments will be tested. The generated data will function as additional training data or to adjust the methods for those faults for which the performance is not acceptable.

Figure 3 displays the Bayesian strategy graphically. At the left one finds the system which delivers various sensor signals

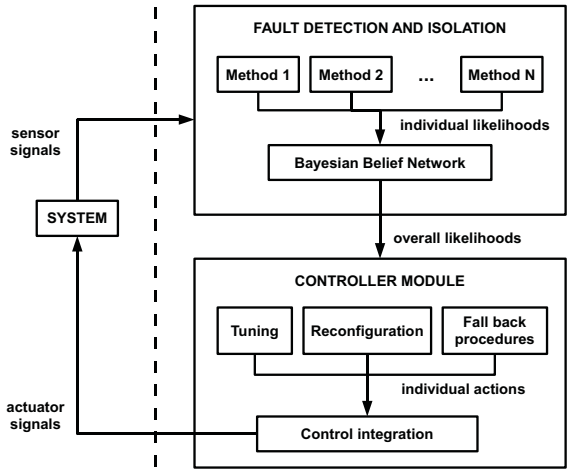

Fig. 3. Feedback and propagation of information through the Bayesian Supervisory Control system

to the control system. This information is passed on to the FDI modules first. Several methods will individually inspect these data for anomalies and associate likelihoods with potential faults. The Bayesian Belief Network then integrates the results of the different methods to obtain overall likelihoods of all considered faults and passes them on to the control module.

C. Phase 3: Supervisory control

Supervisory control aimed at overall system's resilience will consist of the following strategies:

- Tuning: these strategies adjust existing control loops in a parametric way. They may exist of adjusting the set point or speed (e.g. time constant) of a controller. This is done when lowering system performance is a valid option to regain normal operation.
- Reconfiguration: these strategies are applied when by re-routing of the information flows through the control system, system performance can be guaranteed at a certain level, possibly lower than the normal operation level. These strategies are more flexible than the tuning strategies above. This flexibility becomes limited as the degree of redundancy in sensing and actuating equipment are reduced (e.g. by series of equipment failures). Selected implementations will be based on a rule-base and on-line evaluation of RGAs (Relative Gain Arrays, [10]).
- Fall back procedures: this is a planned out strategy in which parts of the system (e.g. a certain control loop) are switched off so to guarantee safety. Switching off parts of the process and/or the control system may help to isolate a problem, preventing further propagation of disastrous effects or may help to guarantee a certain minimum level of performance.

Each of the above approaches will operate separately based on the input from the FDI module in the system (see Figure 3). As discussed in the above section, the FDI results will be provided as likelihoods for each fault class. These likelihoods will be propagated through the control decision logic to account for uncertainty in the FDI results. Each of the separate control modules will account for the uncertainty associated with the FDI likelihoods and deliver likelihoods associated with several potential control actions. These may be interpreted as the likelihood that the proposed control action is optimal. This likelihood will be based on knowledge-based representations of the system. Similar to the BBN for the FDI task, a control integration module will select one set of actions for execution. This necessarily corresponds to selecting the maximum likelihood action as the system under study can only accept one single control signal value per manipulated variable.

V. Expected impact and perspectives

Several expected results will have important impacts on control engineering of complex and safety-critical systems. First, the real-life validation of existing FDI techniques coupled with automated control logic will enable to validate accepted scientific results that have only been established in silico. Second, the Bayesian developments for integration of FDI methods and to account for uncertainty in the control decision logic will provide the necessary tools to enable supervisory control under uncertainty. In addition, the modular FDI structure achieved by means of the BBN allows to add and activate new modules for FDI in a straightforward fashion. This allows to incorporate several methods with different theoretical bases into the same framework. Third, we expect the integrated system for condition awareness and resilient control to be one of the first real-life implementations of a closed-loop control system in which fault detection and identification as well as fully automated accommodation is achieved on this scale. By means of empirical testing, existing barriers between simulation-based research and real-life control engineering are expected to be alleviated along the way.

References

[1] V. Venkatasubramanian, R. Rengaswamy, and S. Kavuri, "A review of process fault detection and diagnosis - part i: Quantitative model-based methods," *Comput. Chem. Eng.*, vol. 27, pp. 293–311, 2003.

[2] V. Venkatasubramanian, R. Rengaswamy, and S. Kavuri, "A review of process fault detection and diagnosis - part ii: Qualitative models and search strategies," *Comput. Chem. Eng.*, vol. 27, pp. 313–326, 2003.

[3] V. Venkatasubramanian, R. Rengaswamy, and S. Kavuri, "A review of process fault detection and diagnosis - part iii: Process history based methods," *Comput. Chem. Eng.*, vol. 27, pp. 327–346, 2003.

[4] C. Rieger, D. Gertman, and M. McQueen, "Resilient control systems: Next generation design research," in *2nd Conference on Human System Interactions*, pp. 632–636, 2009.

[5] T. Kourti, "Process analysis and abnormal situation detection: from theory to practice," *IEEE Control Syst. Mag.*, vol. 22(5), pp. 10–25, 2002.

[6] S. Dash, M. Maurya, and V. Venkatasubramanian, "A novel interval-halving framework for automated identification of process trends," *AIChE J.*, vol. 50, pp. 149–162, 2004.

[7] K. Villez, C. Rosén, F. Anctil, C. Duchesne, and P. Vanrolleghem, "Qualitative representation of trends: an alternative approach to process diagnosis and control," *Wat. Sci. Technol.*, vol. 57(10), p. 15251532, 2007.

[8] J. Prakash, S. Narasimhan, and S. C. Patwardhan, "Integrating model based fault diagnosis with model predictive control," *Ind. Eng. Chem. Res.*, vol. 44, pp. 4344–4360, 2005.

[9] M. A. Kramer and B. L. Palowitch Jr., "A rule-based approach to fault diagnosis using the signed directed graph," *Chem. Eng. Sci.*, vol. 61(6), pp. 1790–1810, 2006.

[10] F. G. Shinskey, *Process Control Systems*. McGraw-Hill, New York, 1988.