INL/CON-16-38935
PREPRINT

Failure Diagnosis for the Holdup Tank System via ISFA

2016 ANS Winter Meeting and Nuclear Technology Expo

Huijuan Li, Shannon Bragg-Sitton,
Carol Smidts

November 2016

The INL is a
U.S. Department of Energy
National Laboratory
operated by
Battelle Energy Alliance

Idaho National Laboratory

Failure Diagnosis for the Holdup Tank System via ISFA

Huijuan Li[1*], Shannon Bragg-Sitton[2], and Carol Smidts[1]
[1]*Department of Mechanical and Aerospace Engineering, The Ohio State University, 201 W. 19th Ave, Columbus - OH 43210*
[2]*Idaho National Laboratory, PO Box 1625, Idaho Falls, ID 8341, USA*
**email: li.6131@osu.edu*

This paper discusses the use of the integrated system failure analysis (ISFA) technique for fault diagnosis for the holdup tank system. ISFA is a simulation-based, qualitative and integrated approach used to study fault propagation in systems containing both hardware and software subsystems. The holdup tank system consists of a tank containing a fluid whose level is controlled by an inlet valve and an outlet valve. We introduce the component and functional models of the system, quantify the main parameters and simulate possible failure-propagation paths based on the fault propagation approach, ISFA. The results show that most component failures in the holdup tank system can be identified clearly and that ISFA is viable as a technique for fault diagnosis. Since ISFA is a qualitative technique that can be used in the very early stages of system design, this case study provides indications that it can be used early to study design aspects that relate to robustness and fault tolerance.

INTRODUCTION

The integrated system failure analysis (ISFA) technique was initially introduced as an integrated approach to the failure analysis of a system containing both hardware (HW) and software (SW) subsystems in [1]. The ISFA technique integrates the functional failure identification and propagation (FFIP) method for fault propagation and effects analysis of the HW subsystem as well as the failure propagation and simulation approach (FPSA) method for the fault-propagation analysis in the SW subsystem. ISFA bridges the HW and SW domains by introducing missing concepts and mapping classes, attributes, enumerations and data types. As software-based digital systems are slowly pervading the nuclear industry, the capabilities of methods such as ISFA for the design and analysis of robustness and fault tolerance properties of such systems early in the system life-cycle should be explored.

The holdup tank system has commonly been used in the research literature as a simplified test case for the investigation of reliability, failure propagation and risk assessment methods and will be used in this paper. The system consists of a tank containing a fluid whose level is controlled by two components: an inlet valve and an outlet valve. Failure of the holdup tank system is determined by the fluid level of the tank. Several component failures from either the HW or SW subsystem may lead to a similar system failure.

In this paper, we apply the ISFA technique to the holdup tank system. First, we introduce the component model for the holdup tank system in [1]. We then quantify the main parameters of the simulation process. Finally, we simulate possible failure-propagation paths. To demonstrate ISFA's ability to diagnose faults, it must be shown that each underlying component failure will have unique failure-propagation characteristics, distinguishable by IFSA and that all component failures can be identified clearly. The results in this paper demonstrate ISFA's diagnostic capability for the holdup tank system.

DESCRIPTION OF WORK

We implement the ISFA technique for failure diagnosis of the holdup tank system. We use the ISFA model for the holdup tank system, quantify the corresponding parameters and simulate the failure-propagation paths. We show that we can predict whether there is a failure in the holdup tank system, identify which component failure leads to the system failure and repair the faulted components.

ISFA Model of the Holdup Tank System

The holdup tank system is a hypothetical system composed of an inlet valve with a position sensor, four pipes, a tank with a pressure sensor, an outlet valve with a position sensor, and a SW-based computer controller. The schematic of the holdup tank system is shown in Fig. 1. The ISFA component model of the holdup tank system is shown in Fig. 2. The function of the holdup tank system is to regulate the fluid's flow and to maintain the desired fluid level in the tank. The holdup tank system is a simplified representation of the steam generator in the secondary loop of a nuclear power plant. If the water in the steam generator (holdup tank system) falls below a certain level for more than a specified time, the core may overheat and the pressure in the primary loop would rise above critical, leading to system failure. In this case study, for simplicity and demonstration of the ISFA method, the input steam is assumed as water in liquid state.

The water level of the tank is controlled by the input and output valves according to a SW-controlled logic. If the pressure is below a critical value, the output flow must be stopped and the input flow must start (and vice versa), so that the water level is within the desired range. The pipe i (i = 1, 2, 3, 4) is used to transfer fluid with one inflow (Q_{in}^{i}), one outflow (Q_{out}^{i}), and none are transaction signals. A transaction is an instance of a signal and defines the communication details of the HW-SW interaction. The transaction status vector can take the values *Active, Inactive, Complete, Incomplete, Never started or Impossible*. The inlet valve regulates the fluid. It has two inputs, Q_{in}^{iv} and transaction <<signal>> T4 or T5, which indicate the status of the function that closes or opens the inlet valve, and one output, Q_{out}^{iv}. The position sensor *j* (*j* = 1, 2) measures position with one inflow Pos_{iv}^{j} and two outflows, Pos_{ov}^{j} and transaction <<signal>> T6 (T7), which indicate the status of the function reading the position. The holdup tank stores and supplies fluid with one inflow (Q_{in}) and one outflow (Q_{out}). The pressure sensor has one function, to measure pressure with one inflow P_{in} and two outflows, P_{out} and transaction <<signal>> T1, which indicates the status of the function reading the pressure. The outlet valve regulates fluid with two inputs, Q_{in}^{ov} and transaction <<signal>> T2 or T3, which indicates the status of the function that closes or opens the outlet valve, and one output Q_{out}^{ov}. Table I lists some examples of HW and SW components of the holdup tank system and their behavior rules (i.e. express component behavior as a function of physical variables) and function failure logic (relate component behavioral modes to function behavior). An extended table can be found in [1].

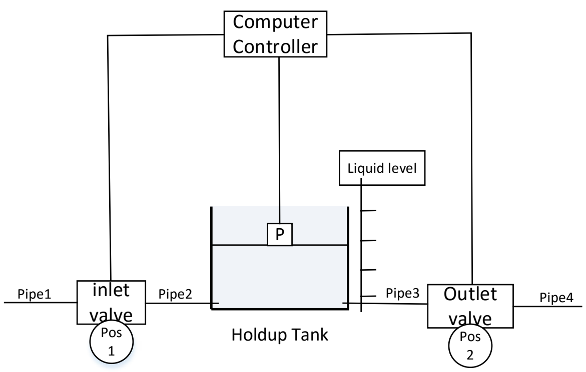

Fig. 1. A schematic of the holdup tank system

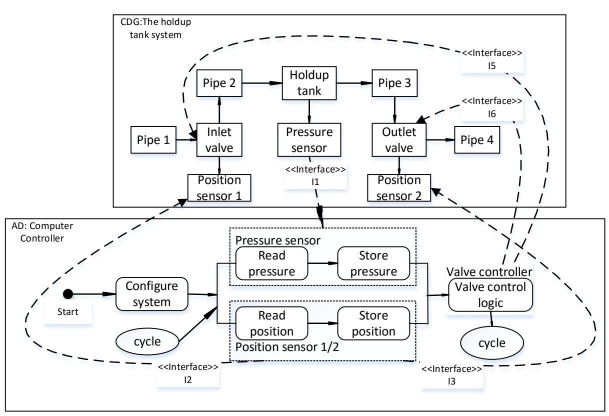

Fig. 2. The ISFA model of the holdup tank system

Parameter Quantification

After introducing the ISFA model of the holdup tank system, our next step is to simulate all possible failure-propagation paths and identify different failure characteristics. In order to better understand the simulation process, it is necessary to quantify some parameters of the holdup tank system. To do so, we consider a scaled-down model where it is assumed that the height of the holdup tank is H = 180cm and the tank is initially half full. The limit range of the level is ±6cm around the initial height. The diameter of the tank is D = 4cm. Pipes are at the bottom of the tank and the diameter of the pipes is d = 0.64cm.

First, we will discuss the flowrate of the water in the holdup tank. The density of the water in the holdup tank is considered constant and the flow can be considered as an incompressible streamline flow. The flow in the holdup tank conforms to Bernoulli's equation as follows:

$$p + \frac{1}{2}\rho v^2 + \rho g h = constant \qquad (1)$$

where *v* is the water flow speed at a point, *g* is the acceleration due to gravity, *h* is the elevation of the chosen point, *p* is the pressure at the point, ρ is the density of water. Then let *h(t)* and *V(t)* be the height and volume of water in a tank at time *t*. If water leaks through a hole with area A_h at the bottom of the tank, the flow rate of this water can be deduced from equation (1) as follows:

$$\mathrm{Q(t)} = \left|\frac{\mathrm{dV(t)}}{\mathrm{dt}}\right| = A_h\sqrt{2gh} \qquad (2)$$

Considering that the water level is within a narrow depth range, we can regard the water flowrate as constant. Based on the above flowrate data, the Reynolds number of the flow is $\mathrm{Re} = \frac{Q(t)\mathrm{D}}{\frac{\mu}{\rho}\mathrm{A}_D} \approx 925 \ll 2000$ (where, μ is the dynamic viscosity of the water at 25°C and 1atm, and A_D is the tank's cross-sectional area), which validates the assumption that the flow is an incompressible streamline flow. Given that the diameter of the pipes is d = 0.64cm, the inflow and outflow of the pipes are $Q_{in}^{i} = Q_{out}^{i} \approx 13.51 mL/s$. If there is a hole with diameter d=2.8mm at the bottom of the tank, the leakage speed in the tank is $Q_{leak\ of\ tank} \approx 2.59 mL/s$. If there is a hole with the diameter d=2mm on the pipe, the leakage velocity of the pipes is $Q_{leak\ of\ pipe} \approx 1.32 mL/s$. The volume of water is linearly related to the pressure of water measured at the bottom of the tank with $\mathrm{V} = \mathrm{Ah} = \frac{\mathrm{P}}{\rho \mathrm{g}} A = 0.128P$ (where, A is the area of the base of the tank). Rescaling the various quantities in a manner that conserves proportions to describe the water flowrate, we obtain: $Q_{in} = Q_{out} = 10$ units of volume/unit of time, $Q_{leak\ of\ tank} = 2$ units of volume/unit of time, $Q_{leak\ of\ pipe} = 1$ unit of volume/unit of time, the initial pressure of water measured at the bottom of the tank is P_0=900 units of pressure and the limit range of the pressure is $P_{LTh} = 840$ units of pressure, $P_{UTh} = 960$ units of pressure.

TABLE I. Behavior rules and function failure logic (C-Complete, IA-Inactive, O-Operating, L-Loss of function)

Component	Function	Behavior Rules	Function Failure Logic
Holdup tank	Store and supply fluid	Nominal: $Q_{out} = Q_{in}$ Dry-out: $P < P_{LTh}$, Overflow: $P > P_{UTh}$	O: Nominal, L: Dry-out or Overflow
Pipe *i* (*i* = 1, 2, 3, 4)	Transfer fluid	Nominal: $Q^i_{out} = Q^i_{in}$, Clogged/Leak: $Q^i_{out} < Q^i_{in}$ Burst: $Q^i_{out} = zero$	O: Nominal, D: Clogged/Leak, L: Burst
Pressure sensor (HW)	Measure pressure	Nominal: $P_{out} \neq null$, Breakdown: $P_{out} = null$	O:Nominal, L:Breakdown
Position sensor *j* (*j* = 1,2) (HW)	Measure position	Nominal: $Pos_j \neq null$, Breakdown: $Pos_j = null$	O:Nominal, L:Breakdown
Inlet valve (Outlet Valve) (HW)	Regulate fluid	Nominal Open: $Q_{out} = Q_{in}$, Nominal Closed: $Q_{out} = zero$ External Burst: $Q_{in} \neq zero$ and $Q_{out} = zero$ Leak: $Q_{out} < Q_{in}$	O: Nominal Open or Nominal Closed, D: Leak, L: External Burst
Pressure Sensor (SW)	Read pressure	Nominal: <<signal>> T1.status = C Faulty: <<signal>> T1.status ≠ C	O:Nominal, L: Faulty
	Store pressure	Nominal: $P_{out} \neq null$, Faulty: $P_{out} = null$	O:Nominal, L: Faulty
Position sensor *j* (*j* = 1,2) (SW)	Read position	Nominal: <<signal>> T6 (T7).status = C Faulty: <<signal>> T6 (T7).status ≠ C	O:Nominal, L: Faulty
	Store position	Nominal: $Pos_j \neq null$, Faulty: $Pos_j = null$	O:Nominal, L: Faulty

Additionally, we need to calculate the failure time of the input and output valves. Failures of various components of the tank system can lead to the over-usage of the inlet or outlet valves and therefore to system failure. The failure time of the holdup tank system depends greatly on the failure time of the input or output valves. The inlet (outlet) valve of the holdup tank system can be regarded as a motor-operated valve (MOV). A MOV is a valve normally held open and it is controlled to be closed or open by motor-operated equipment with no need for manual intervention. The failure modes of a MOV are failure to open or close. In [2], the failure parameter λ_N(failure rate per demand) of a MOV conforms to a Beta distribution with α=2.05 and β=2.123E+03. So the mean number of demands $\bar{N}$ till failure of a typical MOV is $\bar{N} = \frac{1}{E(\lambda_N)} = \frac{1}{\frac{\alpha}{\alpha+\beta}} = \frac{\alpha+\beta}{\alpha} = \frac{2.05+2.123\times10^3}{2.05} = 1036.61$ demands (where, $E(\lambda_N)$ is the expected value of λ_N). The system failure time is determined by the period of the open-close cycle and the mean number of demands till failure of the inlet or outlet valves.

Failure Simulation

We will now discuss how the failures propagate within the ISFA models and lead to system failure. We analyze in detail two different faults: a tank leak and a SW modification error in the presence of a tank leak. The initial conditions (*t* = 0) include: no faults injected, all HW and SW components exhibit nominal behavior, all transactions are inactive, the holdup tank is half full, and the inlet and the outlet valves are in a status Nominal Open. At *t* = 1 unit of time, a tank leak and a SW modification error in the presence of a tank leak are respectively injected into the system. Table II and Table III provide in a simplified form the simulation results obtained for each fault injected.

TABLE II. Simulation results of a tank leak (C-Complete, IA-Inactive, O-Operating function, L-Loss of function, Cl-Close, Op-Open)

Time	Pressure	Outlet Valve		Inlet Valve		System Function
		T2 (Cl)	T3 (Op)	T4 (Cl)	T5 (Op)	
0	900	IA	IA	IA	IA	O
1	900	IA	IA	IA	IA	O
32	838	C	IA	IA	IA	O
39	908	IA	C	IA	IA	O
…	…	…	…	…	…	…
39369	908	IA	C	IA	IA	O
39400	838	C	IA	IA	IA	O
39500	638	C	IA	IA	IA	L

TABLE III. Simulation results obtained for a SW modification error in the presence of a tank leak

Time	Pressure	Outlet Valve		Inlet Valve		System Function
		T2 (Cl)	T3 (Op)	T4 (Cl)	T5 (Op)	
0	900	IA	IA	IA	IA	O
1	900	IA	IA	IA	IA	O
32	838	IA	C	IA	IA	O
39	824	IA	C	IA	IA	O
132	638	IA	C	IA	IA	L

The periodicity of the pressure, inlet valve position and outlet valve position signals for each example of failure displays unique characteristics which can help identify which underlying failure leads to system failure in the failure diagnosis analysis. In Table II, the tank leak leads to frequent open-close cycles of the outlet valve. The valve becomes faulty and gets stuck, for instance in an 'open' state. This results in the tank level going below the threshold causing a system failure. The pressure variable and the outlet valve close & open transactions in Table II display a stable periodicity during an extended period of time. This characteristic indicates that the system is affected by a tank leak and the faulted component can be repaired before the system loses its function. The pressure variable and the outlet valve close & open transactions in Table III show that there is a SW code error in the outlet valve control logic, the variable *Pos* was erroneously set from {1,0} to {0,1} corresponding to {Close, Open} instead of {Open, Close}.

RESULTS

The above model and simulation method can be used for the failure diagnosis of the holdup tank system. Possible component failures of the holdup tank system include: the holdup tank leak, pipe *i* clogged, pipe *i* leak, pipe *i* burst (i = 1, 2, 3, 4), pressure sensor breakdown, position sensor *j* breakdown (j = 1, 2), inlet valve stuck open, inlet valve stuck closed, inlet valve internal leak, inlet valve external leak, inlet valve external burst, outlet valve stuck open, outlet valve stuck closed, outlet valve internal leak, outlet valve external leak, outlet valve external burst, inlet valve control logic error, outlet valve control logic error, pressure sensor control logic error and position sensor *j* control logic error (j = 1, 2).

By simulating all the above failure-propagation paths and comparing the characteristics of measured signals, most component failures and software failures can be classified clearly. However, 7% (34 out of 465) combinations of failures occur in components which are located next to each other and have similar effects that cannot be classified, such as the two input pipes clogged, the two output pipes clogged, the pipe 2 and 3 leak/burst, the input pipes burst and the inlet valve external leak/burst, the output pipes burst and the outlet valve external leak/burst. Such undistinguishable failures can be easily classified just by visual observation and inspectors can be sent to observe and repair the failed component on the scene. Additional sensors can also be added to discriminate the remaining failures.

CONCLUSIONS

The integrated system failure analysis (ISFA) technique was shown to be viable for the failure diagnosis of the holdup tank system. In the holdup tank system, most component failures display different periodic characteristics with respect to measured level (i.e. pressure) and inlet and outlet valve position signals. Therefore, most underlying failures can be clearly identified and the faulted components can be repaired before the system function is lost.

However, several component failures in the holdup tank system can still not be identified clearly. We can send inspectors to observe and repair the failed component on the scene. Some faulted components can be repaired before the system function is lost but some cannot. For example, ruptured pipes lead to rapid system failure and cannot be replaced before the loss of system function. On the other hand, a tank leak leads to the system failing slowly and repairs can be undertaken before system failure.

In the future, we will improve the ISFA technique and apply it to more complex nuclear power plant systems. In order to identify failures in a more complex system, we can combine the ISFA technique with conventional failure detection and diagnosis methods to improve the failure analysis process. The combination would explore the use of conventional failure detection and diagnosis methods for the faults ISFA cannot resolve.

ACKNOWLEDGMENTS

This work was funded by the INL Laboratory Directed Research & Development (LDRD) Program under DOE Idaho Operations Office Contract DE-AC07-05ID14517.

REFERENCES

1. C. MUTHA, D. JENSEN, I. TUMER and C. SMIDTS, "An integrated multidomain functional failure and propagation analysis approach for safe system design," *Artificial Intelligence for Engineering Design, Analysis and Manufacturing*, **27**, 317 (2013).
2. Component Reliability Data Sheets, from U.S.NRC: https://nrcoe.inel.gov/resultsdb/publicdocs/AvgPerf/ComponentReliabilityDataSheets2010.pdf (2012).