Control Decision and Control Development of Hanford Tank Farms First Two ISA-84 Safety Instrumented Systems – 17370

Todd M. Brown
Washington River Protection Solutions

ABSTRACT

Hanford's 242-A Evaporator has had the mission of reducing waste volume in the Hanford Tank Farms since the late 1970s. Until 2014, the Documented Safety Analysis for the 242-A facility considered protection and controls of the collocated worker (workers outside the facility) and the public. In 2010, Tank Farms Nuclear Safety engineers initiated a significant revision of the Documented Safety Analysis to implement DOE-STD-3009, Change Notice 3, which requires the protection of the facility worker in addition to the collocated worker and public. Through the use of an extensive process hazards analysis performed on the facility, it was concluded that it was essential to control conditions in the primary evaporation vessel (C-A-1) such that flammable gasses could not build up to the Lower Flammability Limit, and that another control was necessary to ensure that the C-A-1 vessel could not overflow.

Early control decision meetings held during the development of the Documented Safety Analysis revision yielded no simple solution to the protection of workers from a flammable gas deflagration. Controls selected for the waste overflow accident were all mitigative in nature (i.e. the detection of a waste overflow after it already happened). Engineering could not replace the mitigative controls with preventive controls without attempting to credit some of the existing facility interlocks associated with the C-A-1 vessel operations. Software and hard-wired interlocks had been used at the facility to prevent overheating of the waste and overfilling of the C-A-1 vessel. These interlocks were considered useful to the prevention of the flammable gas deflagration and vessel overfilling accidents, but lacked the pedigree and reliability necessary to credit the interlocks as safety significant.

It was at this stage of the Documented Safety Analysis control decision and control development that engineering became aware of the DOE's acceptance of the ISA-84 instrumented system standard. It became apparent that the ideal solution was not to attempt to credit existing interlock systems, but to develop a new system of "safety interlocks" to the ISA-84 standard. A meeting was held with upper management of both engineering and operations to propose the use of safety instrumented systems at the 242-A facility. URS Corporation (now AECOM), who had recently supported the Savanah River site in developing ISA-84 controls, was consulted to support the development of two new instrumented systems for the 242-A facility. In addition to the use of the newly adopted ISA-84 standard, the failure modes and effect analysis process was implemented in a very effective manner to support the development of the new safety instrumented systems. Through a brand new methodology, and through a very dedicated and hard-working engineering, projects, and operations team, the new controls were designed, built, tested, and commissioned. At this time, five successful waste reduction campaigns have been performed at the facility with the new safety instrumented systems.

During these waste processing campaigns, trips and spurious trips of the SIS have occurred – all of which acted properly.

INTRODUCTION

Background

The Hanford Site tank farms, now managed by Washington River Protection Solutions (WRPS) and owned by the Office of River Protection of the Department of Energy (ORP), is the home of 149 underground single-shell tanks (SSTs) and 28 double-shell tanks (DSTs). These tanks are used to store highly radioactive mixed waste. WRPS mission includes the safe storage of waste in the tanks, and the retrieval of the waste from the older SSTs and transfer of the waste into the newer and more stable DSTs. Since DST space is so limited, waste volume reduction is necessary to the tank farm mission. Waste volume reduction is provided by the 242-A Evaporator facility, located in the 200 East area of Hanford and adjacent to the tank farms.

The function of the 242-A Evaporator facility is to take dilute waste pumped from a designated feed DST, evaporate the waste in a forced circulation vacuum evaporation process, and return the more dense waste slurry back to a different receiver DST. A simplified graphic of the 242-A Evaporator process is shown in Figure I and a simplified process flow sheet in Figure II.

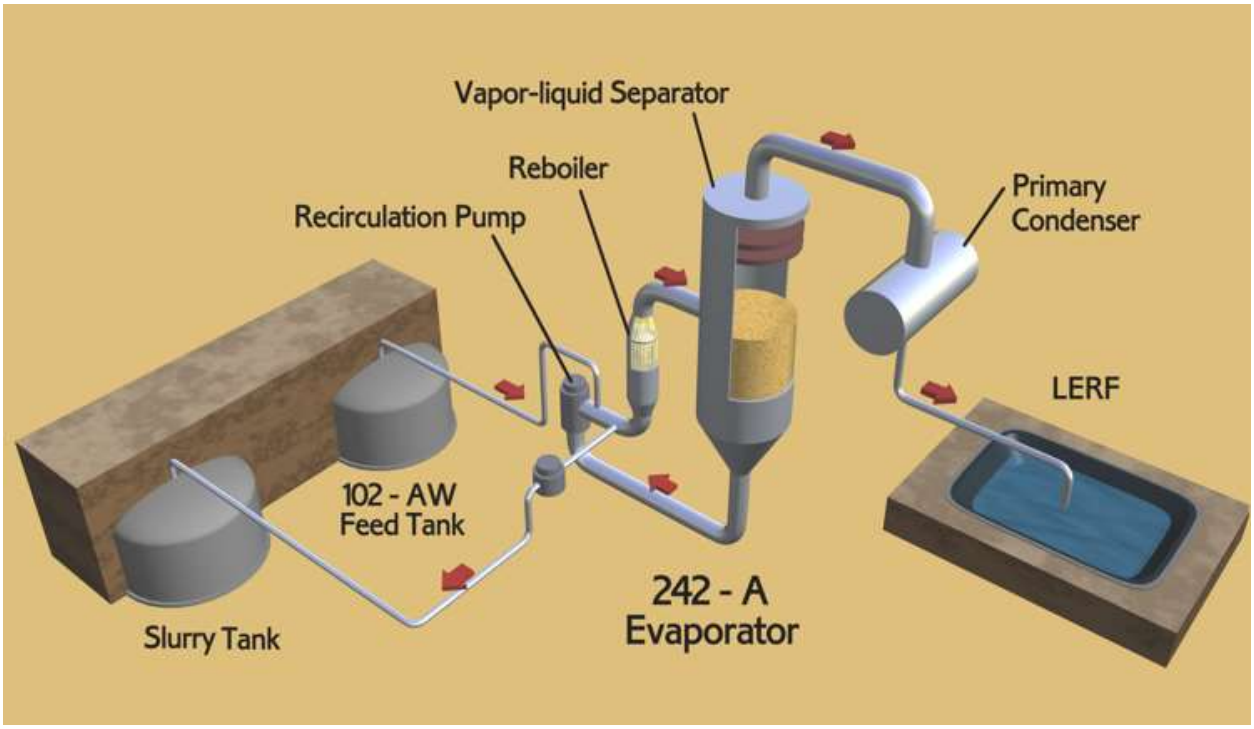

Fig. I. Simplified 242-A Evaporator Process

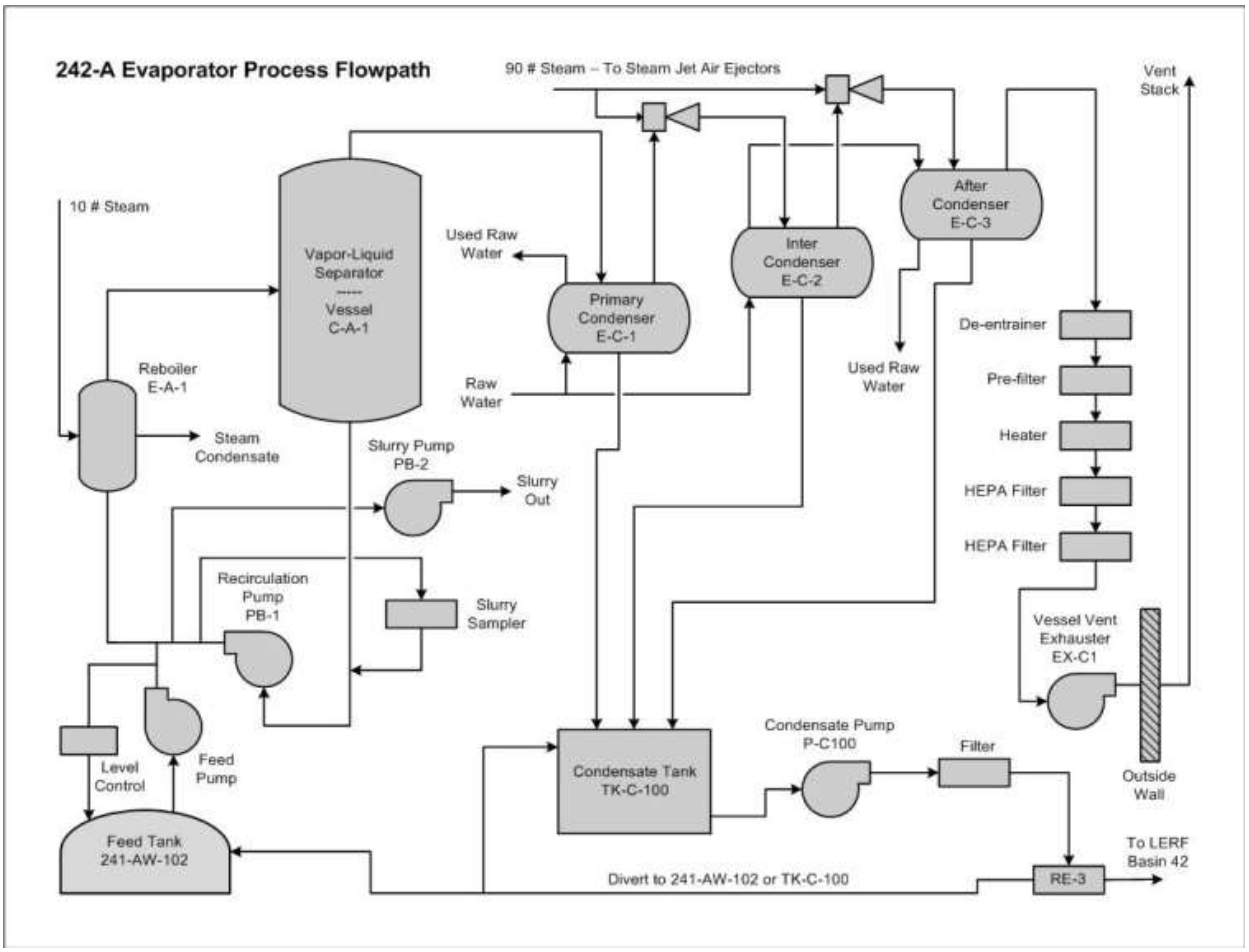

Fig. II. Evaporator Process Flow

Waste is pumped to the facility from the DST feed tank. Waste is fed directly into the recirculation loop, which consists of the primary evaporator vessel (vapor-liquid separator, or C-A-1 vessel), the reboiler (a steam heated shell-in-tube heat exchanger – E-A-1 vessel), and the recirculation pump PB-1 (PB-1). Heat is added to the process at the E-A-1 reboiler. Boiling of the waste occurs at the relatively low temperature of approximately 49°C (~120°F). Low saturation temperatures are achieved by applying a high vacuum to the headspace of the vapor-liquid separator of approximately 8.0 kPa psi (~60 torr) by the means of steam ejectors (shown in Figure II). The evaporation process is a closed loop continuous process, meaning that waste is fed at the same time the waste in the recirculation loop is evaporated. When the waste in the recirculation loop reaches its intended product specific gravity, the waste is pumped from the process (still continuous) to a receiver DST. Boiling occurs at the waste surface in the C-A-1 vessel, and flows to a series of three condensers through two de-entrainer pads (shown in Figure II near the top of the separator vessel, but not labelled). The condensers shown in the figures are actually a three-stage vacuum condenser system. Condensed vapor is

referred to as process condensate, and is pumped to the liquid effluent treatment facility (LERF) and the effluent treatment facility (ETF – not shown) for further treatment before being released to the ground.

Process Hazards and Accidents to be Considered

The Documented Safety Analysis (DSA) [1] is a contractual document between the tank farms contractor (WRPS) and ORP that defines how workers in tank farm facilities, as well as the public and the environment, will be protected from nuclear waste hazards. In 2010, Tank Farms Nuclear Safety engineers initiated a significant revision of the DSA to implement DOE-STD-3009, Change Notice 3 [2], which requires the protection of the facility worker in addition to the collocated worker and public. In the case of the evaporator, the facility worker is considered as the worker inside the facility and the collocated worker as workers outside of the facility. The basis for the development of the new DSA revision was an extensive process hazards analysis which was performed on the 242-A Evaporator process. Several hazards were identified during this process, of which only two are in the scope of this paper (high waste level and flammable gas).

Accident scenarios were postulated that involved a release of material associated with the identified hazards. Most postulated accidents were prevented and/or mitigated through the use of mechanical safety significant equipment (such as backflow preventers and pressure relief valves) or through the use of administrative (procedural) controls (note that throughout the rest of this report, safety significant refers to any device or system that is relied on for safety in the DSA). However, two different hazards (and associated accidents) were identified that could not easily be prevented or mitigated with the use of the standard mechanical devices or administrative controls that were typically used in past controls strategies at tank farms. These hazards, and the difficulties associated with each, will be discussed in the rest of this section.

<u>High waste level in the vapor-liquid separator vessel and waste spill-over:</u> Waste in the C-A-1 vessel is typically well-controlled by operations personnel to a specified waste level. The operating waste level of the vessel is well below the de-entrainer pads, so as to ensure the pads do not get wetted by tank waste (waste exposure to the pads can cause plugging). Operations personnel ensure that the in-flowing waste feed rate and the out-flowing slurry rate are controlled in such a way as to keep the waste level in the evaporator vessel in a steady operating range. However, under abnormal operating conditions, waste could flow-over, boil-over (waste at saturation temperature), or even foam-over (waste not at saturation temperature) in such a way that it could flow through the de-entrainer pads and over the top of the C-A-1 vessel into the condensers, and end up in the condensate tank (tank TK-C-100 on Figure II). Waste in this location is a hazard to facility workers through direct radiation exposure or due to its highly caustic nature if a worker had skin contact with the waste.

Flammable gas deflagration in the C-A-1 vessel or in the process condensate tank TK-C-100: The other hazard that proved difficult to mitigate or prevent through traditional controls is flammable gas generation in the waste vessels. Tank waste in the C-A-1 vessel and process condensate in the TK-C-100 vessel can both generate hydrogen and other flammable gasses if left unventilated long enough. The rate of hydrogen generation is a function of temperature. A flammable gas deflagration in either of these vessels has been determined to be a significant hazard to both facility workers inside the building and tank farm workers outside of the building.

DISCUSSION

This section will discuss the issues that were faced by facility engineering and nuclear safety personnel in selecting controls for the waste spill-over hazard, the flammable gas hazard, and their associated accidents. It will also discuss the implementation and use of ISA-84 Safety Instrumented System (SIS) controls in the facility.

Difficulties Encountered in Selecting Accident Controls

When 242-A facility engineering began the process of selecting controls for the waste high level spill-over accident, it became evident that the traditional equipment or administrative controls used in the past for nuclear safety accidents would not function well. Inherently safe mechanical devices to stop the overflow, boil-over, or foam-over of waste in the C-A-1 vessel could not be identified, particularly for back-fitting into an operating facility. Administrative procedural-type controls were deemed to be unreliable, since waste level increases above operational limits were likely to occur in process upset conditions when facility operations personnel would be fully occupied dealing with the abnormal conditions. Two boil-over events had already occurred in the mid-1990s. These events happened quickly, and without the operator even aware of the boil-over until after it had happened. A preventive control for waste flow-over, boil-over, or foam over would have to be very fast acting.

As a result of the foregoing considerations, initial control selection meetings selected radiation monitoring of the condenser piping, and area radiation monitoring of the condenser room, as the spill-over event control.

The problems with this control were:

- The control was mitigative, meaning that the radiation detection instruments would not notify facility personnel of the waste spill-over until the spill-over event had already occurred and personnel were already potentially exposed to the harmful waste or radiation.
- Facility engineering had no experience in qualifying instrumentation as safety significant equipment. Facility engineering was aware of no method of

evaluating instrumentation reliability or determining the reliability of the instrument loop (the signal from the element to the transmitter to the operations monitor or to alarms).

The control selection of the flammable gas hazards was also problematic:

- Mitigative controls were not acceptable. The consequence of a flammable gas deflagration or explosion is too severe. Therefore, controls for the flammable gas accidents in the 242-A facility had to be preventive.
- Detection of flammable gasses in an existing vessel that had been designed with no such requirements, and that had already been built and operated, proved difficult. Physical modification of the vessel was not preferred due to the radiological access issues. Sample ports could not easily be added to the side of the vessel, and a representative sampling location of the build-up of hydrogen and other flammable gasses could not be made with confidence.

In order to accommodate the above considerations and provide a fully preventative solution, the installation of an "in-vessel" purge air system using existing pipe penetrations was deemed to be the best course. However, qualifying a purge air system as safety significant was difficult since it relied on reliable power to air compressors, including generator back-up. It was determined that the monitoring of the purge air flow would provide the best solution since it did not require the qualification of the air system. Relying on a flow instrument to detect the loss of purge air does, however, result in the same problem – how to qualify instrumented systems.

After an extensive search for an adequate set of controls, and experiencing numerous setbacks, the team established that the only adequate way of preventing waste spill-over and flammable gas accidents was to somehow qualify instrumentation as safety significant, and also qualify the "interlocking" functions of that instrumentation as safety significant.

ISA-84 Safety Instrumented Systems

ISA-84 is used in this report to refer to the Instrumentation, System, and Automation Society (ISA) standard ANSI/ISA-84.01-2004, "Functional Safety: Safety Instrumented Systems for the Process Industry Sector" [3]. ISA-84 was originally developed for the chemical processing industry. A SIS, as developed by the ISA-84 standard, is an instrumented system used to implement on or more safety instrumented functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s), which are defined as:

- Sensor – a device or combination of devices, which measure the process condition (examples: transmitter, transducers, process switches, or position switches).
- Logic solver – that portion of a SIS that interprets the sensor input, and activates the final elements based upon a pre-determined logic function(s).

This function can be performed by solid state devices (relays or trip modules), programmable logic controllers (PLC), or even by humans.
- Final elements – part of the SIS which implements the physical action necessary to achieve a safe state (examples: opening a valve to relieve pressure or drain a vessel, or shutting off a pump).

Sensors, logic solvers, and final elements are combined together in a SIS to create a system that will detect an adverse or unsafe condition, and will apply a preventive or mitigative response via activation of the final element(s).

The ISA-84 standard recognizes that the consequences or probability of every accident is different, and therefore uses a graded approach to the development of its controls. The standard refers to different levels of protection of the SIS control, referred to as safety integrity level (or SIL). SIL levels identify the minimum required risk reduction factor of the system, or the failure on demand of the system. Although the standard identifies four levels of SIL protection (SIL-1 through SIL-4), tank farms adopted two SIL levels (SIL-1 and SIL-2) in their implementation of the standard. The SIL-3 and SIL-4 levels were not adopted, since only safety significant and not safety class controls are required at tank farms. Different SIL levels are met for a SIS in various ways, but primarily by the amount of redundancy in the system, the reliability of the instrumentation, logic solvers, or final elements used, or the simplicity of the design. Table I shows the method used to determine the SIL-level of tank farm SISs, giving consideration to the probability and consequence of the accident, and who is affected (facility worker, collocated worker, or the public).

TABLE I. Safety Integrity Level (SIL) Determination

Consequence	**Frequency**		
	Anticipated	**Unlikely**	**Extremely Unlikely**
Public [offsite]	SIL-2	SIL-2	SIL-1
Co-Located Worker [onsite]	SIL-2	SIL-1	SIL-1
Facility Worker	SIL-1	SIL-1	SIL-1

Note that this table is particular to the tank farms application of ISA-84, and is commensurate with the material that is accepted at tank farms facilities (including the evaporator). Tank farms implementation of ISA-84 was not performed to DOE-STD-1195 [4], because that standard was not in the WRPS contract.

The ISA-84 standard consists of 19 sections referred to as "clauses", which include:

- Introductory sections and definitions.
- Requirements that are programmatic in nature for establishing a program to comply with ISA-84.
- Technical requirements for life-cycle implementation of an ISA-84 compliant Safety Instrumented System.

Development of New ISA-84 Systems for the 242-A Evaporator

In 2008, the WRPS contract was written to require compliance with ISA-84, and in 2009 the WRPS process and controls system (P&CS) engineering group started drafting procedures to implement ISA-84 at the tank farms facility. However, it was not until 2012 that the 242-A facility engineering and nuclear safety engineering concluded that fully developed ISA-84 SIS controls were the answer to the flammable gas and high waste level hazards. In 2012, 242-A facility engineering began working with P&CS engineering and with URS Corporation (now AECOM) to develop and implement Hanford's first two SIS controls in the 242-A evaporator facility.

The flammable gas SIS was developed using the following assumptions and inputs:

- When the C-A-1 vessel is at high vacuum (operating) conditions, the head space atmosphere has been largely evacuated, and what little atmosphere remains is primarily water vapor. Therefore, unless the temperature of the waste increases to an amount that results in high flammable gas generation (see below), a high vacuum condition in the vessel (pressure < 26.7 kilopascal (kPa) - or 200 torr) is considered to be a safe condition.
- When the pressure in the vessel is above the normal operating range (i.e. vacuum is off), then a purge air system must be running. It was determined that a purge air flow rate over 85 standard liter per minute (Lpm)(3.0 standard cubic feet per minute or cfm) would adequately evacuate flammable gas from the vessel.
- Regardless of the pressure in the vessel, or of the flow rate of purge air running into the vessel (first two bullets), it was determined that an elevated waste temperature of ≥ 71.1°C (160°F) was not safe and should trip the SIS. The rate of flammable gas generation increases rapidly when waste temperatures start to exceed this amount.
- Therefore, the C-A-1 vessel is in an assumed unsafe condition if the vacuum in the vessel is lost AND there is insufficient purge air, OR if the waste reaches an unsafe high temperature. In any of these conditions, the SIS must trip, meaning that the SIS will activate its final elements to bring the facility to a safe state.

A trip of the flammable gas SIS results in the following actions:

- Immediate shut down of the feed pump and of the recirculation pump P-B-1.

- Immediate closing of a steam safety isolation valve, immediately bringing steam off of the reboiler.
- Immediate opening of a slow draining dump valve (this is actually the feed line isolation valve, which provides a dump path of waste back to the feed tank).
- After 30 minutes, fast draining dump valves open which complete the vessel draining within minutes. The 30 minutes provides time for the operators to take actions such as restoring purge air before the final dump of the vessel occurs.

The hazard analysis of the flammable gas deflagration showed that the flammable gas deflagration is an "anticipated" event, and that it could potentially cause harm to a collocated worker (worker outside of the 242-A building). From Table 1, it can be seen that the flammable gas deflagration in the C-A-1 vessel should be controlled with a SIL-2 level SIS. This was accomplished by providing redundancy in the system components (two sets of purge air flow sensors, two sets of vessel head-space pressure transmitters, two sets of temperature indicators in the waste, and two independent dump line paths – each with its own set of dump valves). A graphical representation of the flammable gas SIS is shown in Figure III (note that not all components of the SIS are represented – this just provides a visual for better understanding).

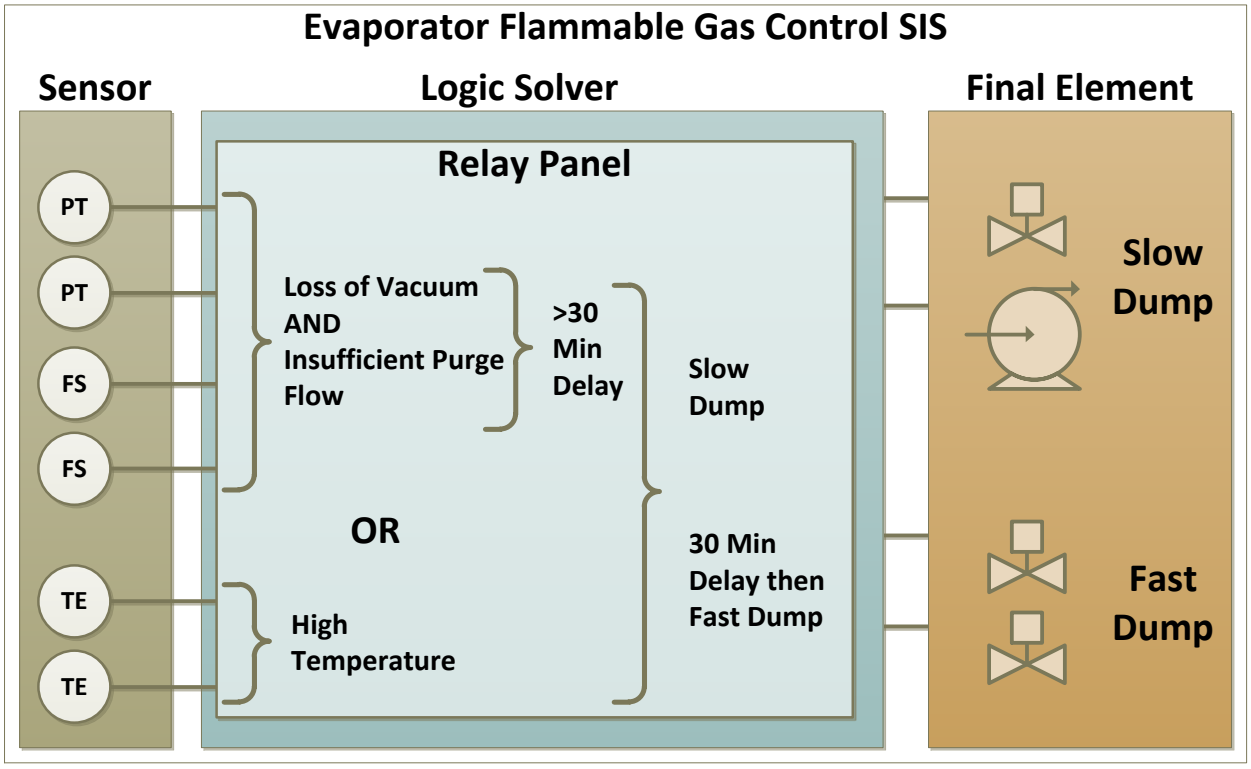

Fig. III. Flammable Gas Control SIS

The high level (waste overflow) SIS was developed using the following considerations and inputs:

- Level instrumentation for the C-A-1 vessel is based upon dip tube bubbler technology. This instrumentation relies upon the differential pressure between a sensing line that passes into the head space of the C-A-1 vessel and another sensing line that bubbles into the waste at a known elevation. The level is proportional to the measured differential pressure. The problem with using this type of an instrument for activation of the SIS is that it will not detect boil-over or foam-over events, since the mass of waste above the lower sensing line does not change in a boil-over or foam over.
- A similar measurement that provides a much better detection of waste level increase, boil-over, or foam-over is a measurement of the differential pressure across the de-entrainer pads at the top of the C-A-1 vessel. Although this measurement is still provided by a differential pressure transmitter, it will detect boil-over, foam-over, and a true waste high level event. The trip point for differential pressure is 20.3 cm water gauge (8.0 in W.G.).
- To ensure that the dip tube sensing lines from the vessel to the transmitter have not become plugged with waste, or that sensing line air flow is not excessive, a flow switch on each sensing line ensures that the sensing line air flow is in the range of 5.9 to 23.6 standard cubic cm per second (0.75 to 3.0 standard cubic feet per hour – SCFH).
- Therefore, the C-A-1 vessel is in an assumed unsafe condition if the differential pressure across the de-entrainer pads remains low AND the air flow through the instrument sensing lines is in the correct range.

The final elements that must be activated upon a trip of the high level SIS are the same as for the flammable gas SIS, with the following two exceptions:

- Closure of the steam safety shutoff valve is not necessary for the high level SIS.
- A vacuum breaker valve is opened upon activation of the SIS. This is simply an automatic valve that opens and floods the headspace of the C-A-1 vessel with air. By breaking the vacuum in the C-A-1 vessel, foam-over or boil-over of the waste is stopped immediately.

Since the final elements of both SISs have many overlapping features (shut off pumps and open dump valves), all final elements have been combined for both SISs.

Consequences of waste spill over accidents are only to the facility worker, therefore, from Table 3 this SIS was developed at a SIL-1 level. This means that redundant instrumentation and logic solvers was not required for the high level SIS. The functional requirements, control logic, and design analysis for the flammable gas SIS is provided in the "Design Analysis Report for the 242-A Evaporator C-A-1 Vessel Flammable Gas Control System" [5] and for the high level SIS in "Design

Analysis Report for the 242-A Evaporator C-A-1 Vessel High Level Control System" [6].

Operation of Safety Instrumented Systems at the Evaporator and Lessons Learned

Both of the 242-A SISs were developed, designed, and constructed by 2013. In February of 2014, a cold run campaign (evaporator operation with water only) was held with the purpose of testing and commissioning all new safety systems at the facility, including the two new SISs. The first fully operational waste evaporation campaign was held later the same year. Since that time, five successful waste evaporation campaigns were performed with no failure of the SIS systems and a few trips of the SISs. Lessons that have been learned from operation of the facility with active SISs are:

- Operation of the SISs is a background function only. Operators do not need to do anything while running except monitor the SIS parameters. In fact, it is a requirement of ISA-84 that operations cannot defeat the SIS through operational controls or procedures.
- The greatest time associated with operations interface with the SISs is in maintenance and not operation. The maintenance cycle of the SISs is large - the single-most time consuming system in the facility to maintain. Every 182 days, up to 5 or 6 weeks are spent in calibration of SIS associated instruments, and in functional checks of the SIS systems.
- The primary reason for the extensive maintenance cycle of the SISs is the requirement to meet the SIL levels. To obtain the SIL-2 rating of the flammable gas SIS and the SIL-1 rating of the high level SIS, calculations of the failure on demand of each system drove an extensive 6-month maintenance cycle. The primary reason for this was in the use of relay logic instead of the use of a PLC as the logic solver. The failure on demand of the various solid-state relay devices, particularly the time delay relays, drove the reliability of the whole system down and the maintenance frequency up.
- Several trips of the SIS have been experienced. None of the SIS trips were due to the failure of a SIS component. Most trips were caused by the plugging up of the purge airline, at the nozzles inside the C-A-1 vessel which are located just above the waste surface. Plugging is likely due to waste splashing (from boiling) on the nozzles and then drying up and crusting over. A water flush of the purge air system always clears the problem and operations has always been able to resume. This problem has led to an engineering design to add a purge line flush system.

Operations and facility engineering are working together to determine how to minimize operational trips and spurious trips of both SISs. Additionally, engineering is continually looking for more efficient and less time-consuming procedures and methods of performing the preventive maintenance testing and calibrations of both systems.

Looking Forward

Upgrades of the SIS systems at the 242-A facility are in the planning stages, including:

- The SISs are likely to be upgraded to a PLC driven logic solver. It is anticipated that this could reduce the maintenance cycle to annual, with a smaller time required for calibrations and functional testing.
- A seismic SIS is to be developed. At the same time the first two SISs were developed, a push button was provided in three locations inside and outside the facility. These push buttons activated all final elements of the SISs and bring the facility to a safe condition. The buttons are to be pushed in an earthquake and for other emergency conditions. WRPS has been directed to upgrade this manually activated seismic shutdown system into a fully automated SIS, via the use of seismic switches.
- A fire SIS is to be developed. This SIS will trip the same final output (safe condition) as the other SISs, but will be activated by fire and/or heat detectors located in key locations in the facility. The primary purpose of this SIS is to activate the facility safe response before other SIS components are damaged and can no longer provide their safety function.

CONCLUSIONS

The use of ISA-84 safety instrumented systems has filled in a critical gap in the tools available to tank farms nuclear safety and facility engineering personnel to apply controls to facility accidents. Up until the implementation of the two new 242-A evaporator SIS controls, only safety significant mechanical devices, or administrative type controls have been used to control DSA accidents. Now, with the use of ISA-84, tank farms is able to develop instrumented systems and interlocking functions as safety significant controls. The new SIS controls are not without their growing pains, such as high maintenance and spurious trips of the systems. However, engineering and operations are working together to learn how to better use SIS systems to avoid spurious trips and to optimize the SIS maintenance program. Overall, the use of SIS safety systems at tank farms, and particularly in the 242-A evaporator facility, has been beneficial and has improved the safety culture in the tank farms facilities and it workers.

REFERENCES

1. HNF-14755, "242-A Evaporator Documented Safety Analysis", Rev. 06a, Washington River Protection Solutions, Richland, Washington.
2. DOE-STD-3009-94, Change Notice No. 3, "DOE Standard – Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Documented Safety Analyses."

3. ANSI/ISA-84.00.01-2004 Part 2, "Functional Safety: Safety Instrumented Systems for the Process Industry Sector – Part 2: Guidelines for the Application of ANSI/ISA-84.00.01-2004 Part 1."
4. DOE-STD-1195-2011, "Design of Safety Significant Safety Instrumented Systems Used at DOE Nonreactor Nuclear Facilities."
5. RPP-RPT-54583, "Design Analysis Report for the 242-A Evaporator C-A-1 Vessel Flammable Gas Control System", Rev. 06, Washington River Protection Solutions, Richland, Washington.
6. RPP-RPT-54584, "Design Analysis Report for the 242-A Evaporator C-A-1 Vessel High Level Control System", Rev. 05, Washington River Protection Solutions, Richland, Washington.