QRA STUDY OF AN ACTIVATED CARBON FILTER SAFEGUARD SYSTEM

M. Sam Mannan, Yanjun Wang, and Harry H. West
Mary Kay O'Connor Process Safety Center, Chemical Engineering Department, Texas A&M University System, College Station, Texas 77843-3122, USA (mannan@tamu.edu)

The Mary Kay O'Connor Process Safety Center (MKOPSC) at Texas A&M University conducted a Quantitative Risk Analysis (QRA) for subsystems of the VX neutralization process. The process is conducted in a negative pressure containment system. The very large air handling system also acts to direct any fugitive emissions or small leaks to the carbon adsorption filter systems, the final safeguard in preventing highly toxic chemicals from escaping to the atmosphere.

The activated carbon filter system concentrates the low level fugitive emissions, thereby creating a potential for a more significant catastrophic release if the carbon filter system fails. The risk trade off between capturing low-level fugitive emissions and the potential for a large-scale toxic chemical release must be compared. The fault trees for the air handling system and the carbon filter systems are highlighted. In particular, the uncertainty in the reliability data and their respective impact on the overall failure rate and system availability are emphasized.

The importance of this study was to point out a specific failure mode that was not adequately addressed with safeguards in the original process design, thereby creating an unacceptable risk and requiring additional safeguards. The study also verified that the safeguards in the original design for all other identified failure modes reduced the risks to generally acceptable levels.

KEYWORDS: Process Safety, Quantitative Risk Assessment, Loss Prevention, Fault Tree Analysis, Failure Modes

INTRODUCTION

O-ethyl S-(2-diisopropylaminoethyl) methylphosphonothiolate ($C_{11}H_{26}NO_2PS$) is commonly referred to as VX (Chemical Abstract Service Number 50782-69-9). It is an organophosphorous ester and is a lethal nerve agent. It enters into the body by respiration or skin absorption. It is very persistent and does not evaporate under the normal temperature. VX is generally stored in ton containers. During the VX neutralization process, the ton containers are punched, washed, decontaminated and cut apart in a negative air pressure containment building. The VX agent is collected and then sent to two subsequent reactors. In these reactors, the VX agent reacts with aqueous sodium hydroxide (NaOH) to produce hydrolysate. After the target demilitarization level (330 ppb) is achieved, the hydrolysate product is then sent to a supercritical water oxidation systems for post-treatment to remove the organics.

The US Army System Safety Program Plan defines a risk assessment code (RAC)(Table 3) and three concerned hazard scenarios: VX agent release, personnel injury/illness, and system loss. In this study, the Fault Tree Analysis (FTA) methodology was employed to estimate the risk level of these three major events in the VX neutralization subsystem and the associated support system. Tables 1 and 2 present the hazard severity level definition and frequency level definition for each incident. The RAC matrix (Table 3) is then defined based on the hazard severity level and the hazard frequency level. The defined risk levels range from 1 to 4. Each has a specific acceptability criteria and resolution authority, which is shown below the RAC matrix.

The VX neutralization process is designed to operate in a negative pressure containment system. The very large air handling system is vital for orderly and safe operation. The carbon adsorption filter systems are the final safeguards in preventing highly toxic chemicals from escaping to the atmosphere. The aim of this study is to evaluate the activated carbon filter system from a safety point of view.

METHODOLOGY

In this QRA project, FTA methodology was applied to the VX neutralization processes to obtain the frequency of the major hazard incidents. The hazard frequency level definition (Table 2) was then applied to acquire the corresponding RAC for each scenario. If the calculated RAC code was unacceptable, possible safety mitigations were recommended and compared by revising and reevaluating the fault trees to bring the system to an acceptable risk level.

Consequence analysis was first employed to determine a hazard severity level of II – Critical. FTA was then used to calculate the occurrence frequency of potential incidents. The first step of FTA is to identify the undesired top events. As mentioned, three major hazards were defined: agent release in-plant, personnel injury, and system loss. In the second step, the backward-reasoning FTA technique is applied to each scenario until external or primary basic events, whose failure rate data are available, are reached. It is essential to include necessary and sufficient events that can contribute to the top event. Using the process information, failure rate data, and human error probability; an estimation of the probability of the identified hazardous incident can be accomplished.

Average failure rate data for process equipment are available in literature in many databases. Data exists on probability of failure on demand for safeguards as well as human errors. In this study, the American Institute of Chemical Engineers (AIChE) Center for Chemical Process Safety (CCPS) publication, "Guidelines for Process Equipment Reliability Data with Data Tables," [1] was the primary source of equipment failure data. Other sources include the offshore reliability data (OREDA) [2], Mechanical Reliability [3], and specific technical articles in the MKOPSC Library that provide special process equipment or process instrumentation failure data. Other equipment failure data can be obtained from the Government Industry Data Exchange Program (GIDEP) [4], IEEE Standard 500-1984 [5], and European Industry Reliability Data Handbook (EIREDA) [6]. Additional equipment reliability and failure rate databases are available for purchase or by a combination of financial support and equipment reliability data sharing. Hartford Steam Boiler and the AIChE special interest group on reliability are examples of groups that have additional data. However, the use of these special-purchase failure rate databases was not appropriate for this study.

In some instances, failure data can be represented by statistical distribution functions, thereby permitting Monte Carlo analysis techniques to predict a distribution of failure estimates. However, the dearth of applicable failure probability distribution data for this new VX neutralization technology does not justify such complex modeling methods.

HVAC SYSTEM DESCRIPTION

The VX neutralization facility was designed to provide agent containment through the use of effective physical separation between the toxic and nontoxic areas and a ventilation system design using progressively negative differential pressures. Areas are categorized according to the potential contamination level. Areas with the higher potential of contamination must be maintained at lower (negative) pressure. Thus air is controlled to flow progressively from the areas of the least probable contamination to the areas of the highest probable contamination. The building's design also facilitates the HVAC design goals with construction to provide appropriate airlocks to minimize air leakage. The process vent streams cannot be discharged directly to the outside because they contain trace amounts of VX agent and volatile organic compounds (VOCs). These vent streams are filtered at the main activated carbon filter units to remove VOCs and agent before transferring into the building's exhaust air streams.

The VX neutralization facility includes a cascade ventilation system that is vital for orderly and safe operations because it provides controlled air temperature, air pressure, and flow to confine the contaminants within special areas. The functions of the cascade HVAC system are:

1. Protect the equipment/building areas and the site's environment.
2. Provide sufficient air volume to remove agent and VOCs from the contaminated areas.
3. Maintain negative room pressure to prevent diffusion or leakage of possible contaminants to the outside.
4. Control and minimize the spread of contamination by maintaining a certain direction of airflow.
5. Receive and filter the process vent stream to minimize discharge to the atmosphere.

The cascade ventilation system was designed to have a total of four supply air handling units and eight exhaust activated carbon filter units. During normal operation, three supply air handling units and six exhaust activated carbon filter units are online. The air handling units supply 100% outside air. The air is then transferred to areas of successively more contamination potential. The pressure in each room is monitored and alarmed if an out-of-range pressure condition occurs. If the pressure between Category C and A/B rooms equalizes, isolation dampers are closed to confine the possible contamination in specific areas. Air entering the supply units passes across an air tempering hot water coil with face and bypass dampers. The air then passes through media particulate filters rated at 30% and 85%. Next, the air is heated by a hot water coil or cooled by chilled water to the desired temperature. Constant-flow, variable-speed centrifugal fans are used to overcome the pressure drops through the coils, filters, and ductwork to move the air to the various Category C areas. Differential pressure gauges are installed to monitor the filter loading and alarm on high-pressure differential.

The supply air-handling system is started manually at the main HVAC control panel. Interlock logic prevents more than the prescribed number of units in the system from being operated at a time. In the event of a loss of airflow in an operating supply unit, a low-limit flow transmitter signals an alarm at the main HVAC control panel and resets the interlock logic so that the standby fan can be automatically started.

HIGH-HUMIDITY EXHAUST SCENARIO

Based upon preliminary failure mode analysis studies, a number of scenarios were evaluated. This study describes a particular scenario that has the potential for compromising the carbon filter systems. Other scenarios, such as fire within the carbon bed systems, had adequate safeguards defined in the original design.

The performance of the activated carbon bed filters is critical to successful containment of any agent that might be present in the exhausts. The performance of any activated carbon bed filter is known to degrade when the relative humidity of the exhaust air exceeds 70%. However, experimental measurements or calculations are not available for the efficiency of carbon bed filters under high-humidity conditions. In this case, each exhaust filter contains six carbon beds in series. Agent monitors are located after the first and second beds. However, the conservative assumption of a common mode failure is that VX agent breakthrough on one carbon bed due to high relative humidity will subsequently bypass all remaining carbon beds.

The cascade HVAC system depends on operating system heat loads to increase the air temperature and thereby reduce the relative humidity of the air before it reaches the exhaust activated carbon filters. Incoming air is cooled to 55°F; therefore, the exhaust air would normally be about 55% relative humidity at 72°F in the summer. Lower relative humidity can be expected in the winter.

Furthermore, the HVAC system is designed to remain operational during an emergency, such as a VX leak. However, once a VX leak is known, all other operations will cease, thereby reducing the process heat load. Preliminary analysis of the heat loads suggests that non-process heat loads add about 10ºF of sensible heat to the HVAC exhaust. Hence, humidity control procedure systems are required to ensure activated carbon bed performance. This can be further compounded upon the loss of utility power because only essential power will be online, and sensible heat to the HVAC exhaust will be minimal. No mitigation credit can be taken for process system shutdown upon agent breakthrough on the first carbon bed, because in this scenario, it is already assumed that the process system has been previously shut down because of a large leak event. Depending on the post-release procedures to bring the HVAC system back to operational status, in addition to a potential agent release scenario, the high humidity failure event would also be an HVAC system loss category failure.

A high humidity condition in the exhaust air could also be the result of excess steam during the steam cleaning of the VX containers after the contents have been transferred to the neutralization reactors.

RESULTS & RECOMMENDATIONS

In the original HVAC design, redundant moisture sensor-activated exhaust control system was not included to ensure that the relative humidity of the exhaust manifold upstream of the carbon filter systems is below 70%. RAC hazard Severity Level II (agent release) was assigned to this event because the HVAC carbon filters would be inoperable, hence, any simultaneous VX leak would be outside engineering controls. “Agent release through the HVAC system” events were found to be at RAC 2 (undesirable) prior to implementing recommended changes (as shown in the attached fault tree in Figure 1).

Note that one can calculate the impact of the humidity control interlock system by setting the probability of “supply air heater fails to operate on high humidity” under Gate

158 to 1. Hence the impact of recommended control features on the RAC matrix can be easily evaluated.

An exhaust air humidity control interlock system with redundant humidity sensors is recommended to bring this event to RAC 3 (acceptable with control). In the high humidity scenario, the supply air heaters will be turned on and the supply air chillers turned off until the exhaust air relative humidity is controlled to an acceptable limit. This system will ensure that the relative humidity contacting the activated carbon filters will remain under the design limit of 70% relative humidity. The humidity sensors should be inspected on a 4- to 6-month preventive maintenance schedule. In particular, a 2 out of 3 voting logic control system may be considered to add even higher reliability to the relative humidity safeguard system.

The heat loads created by cleanup or repair crews during a maintenance period are not known. Hence, the complete reliance on space temperature in neutralization cubicles to activate a high relative humidity safeguard system was not considered appropriate in this study. This space temperature automated system is somewhat similar to the dual exhaust air humidity sensors systems recommended in the base case hereunder, but relies on an indirect measurement of the relative humidity at the exhaust air carbon filters.

Another alternative strategy of using operating procedures for the operator to respond to a high humidity alarm was considered and rejected because the human error failure rates are not sufficiently reliable enough to achieve failure frequencies consistent with RAC 3.

CONCLUSIONS

The HVAC system maintains an environment of progressively negative differential pressures to control and minimize possible contamination. The performance of the activated carbon filter systems is critical to capturing the agent and VOCs that might be present in the process exhaust. High humidity is a common cause failure of the series activated carbon filters. The original design without the exhaust moisture control system was found to be unacceptable according to RAC matrix. The results of this study indicate the humidity safeguards of the activated carbon filters will bring it to “Acceptable with controls”. The study also verified that many other identified failure modes, such as carbon filter fires and errors during unloading/reloading carbon were adequately protected by safeguards.

REFERENCES

1. Guidelines for Process Equipment Reliability Data with Data Tables, Center for Chemical Process Safety AICHE, *American Institute for Chemical Engineers*, 1989.
2. Offshore Reliability Data Handbook, OREDA-84, P.O. Box 370, N-1322, HOVIK, Norway, 1984. Distributed by *Pennwell Publishing Company*, Tulsa, OK.
3. Moss, T.R. (editor), “Mechanical Reliability”, IPC Science & Technology, Guiford, U.K., 1980.
4. The Government Industry Data Exchange Program (GIDEP), http://www.gidep.corona.navy.mil/
5. IEEE Standard 500-1984 Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for

Nuclear-Power Generating Stations, *The Institute of Electrical and Electronics Engineers*, New York, NY, 1983.
6. European Industry Reliability Data Handbook (EIREDA), EUORSTAT, Paris, 1991.

ACKNOWLEDGEMENTS

This research was funded by the Mary Kay O'Connor Process Safety Center of the Department of Chemical Engineering at Texas A&M University.

Table 1. Hazard severity level definition

Severity level	Agent release in-plant	Personnel injury/illness	System loss
I—Catastrophic	> IDLH outside engineering controls	Illness, death, or injury involving permanent total disability	> 25% and/or >1 month to repair
II—Critical	≥ AEL outside of engineering controls	Injury involving permanent partial disability	10% to 25% and/or 1 week to 1 month to repair
III—Marginal	≥ AEL inside nonagent areas	Injury involving temporary total disability	< 10% and/or 1 day to 1 week to repair
IV—Negligible	< AEL nonagent areas	Injury involving only first aid or minor supportive treatment	No system loss downtime, or repairs completed within 1 day

AEL = airborne exposure level (VX = 0.00001 mg/m^3)
IDLH = immediately dangerous to life and health (VX = 0.02 mg/m^3)

Table 2. Hazard frequency level definition (event/year)

Qualitative frequency	Agent release in-plant	Personnel injury/illness	System loss
A — frequent	A ≥ 1E–01	A ≥ 10.0	A ≥ 1.0
B — probable	1E–01 > B ≥ 1E–02	10.0 > B ≥ 1.0	1.0 > B ≥ 1E–01
C — occasional	1E–02 > C ≥ 1E–03	1.0 > C ≥ 1E–02	1E–01 > C ≥ 1E–02
D — remote	1E–03 > D ≥ 1E–04	1E–02 > D ≥ 1E–04	1E–02 > D ≥ 1E–03
E — improbable	1E–04 > E ≥ 1E–06	1E–04 > E ≥ 1E–06	1E–03 > E ≥ 1E–06
F — rare	1E–06 > F	1E–06 > F	1E–06 > F

Table 3. RAC matrix

Qualitative frequency	Severity level I (catastrophic)	 II (critical)	 III (marginal)	 IV (negligible)
A — frequent	1	1	1	3
B — probable	1	1	2	3
C — occasional	1	2	3	4
D — remote	2	2	3	4
E — improbable	3	3	3	4
F — rare	4	4	4	4

Acceptability criteria:

RAC	Description	Resolution authority
1	Unacceptable	Assistant secretary of the army
2	Undesirable	Product manager
3	Acceptable with controls	Program manager-safety
4	Acceptable	

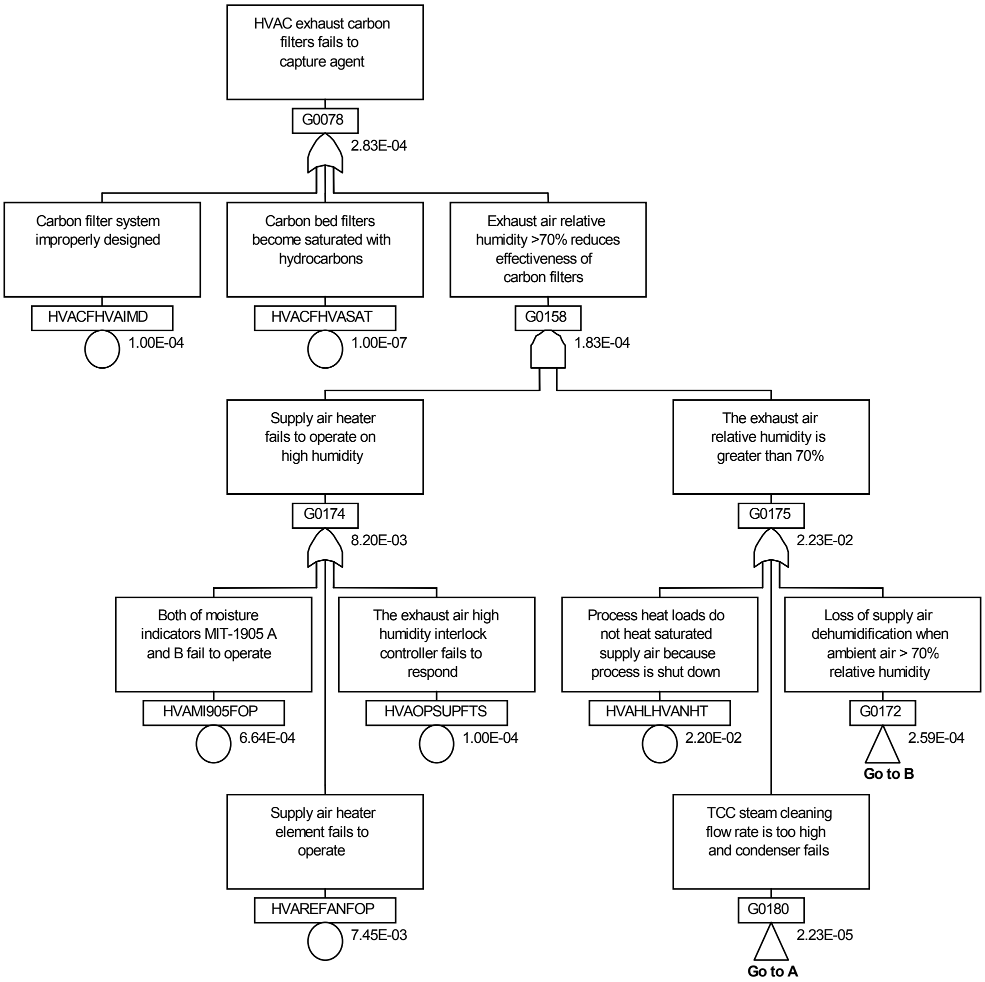
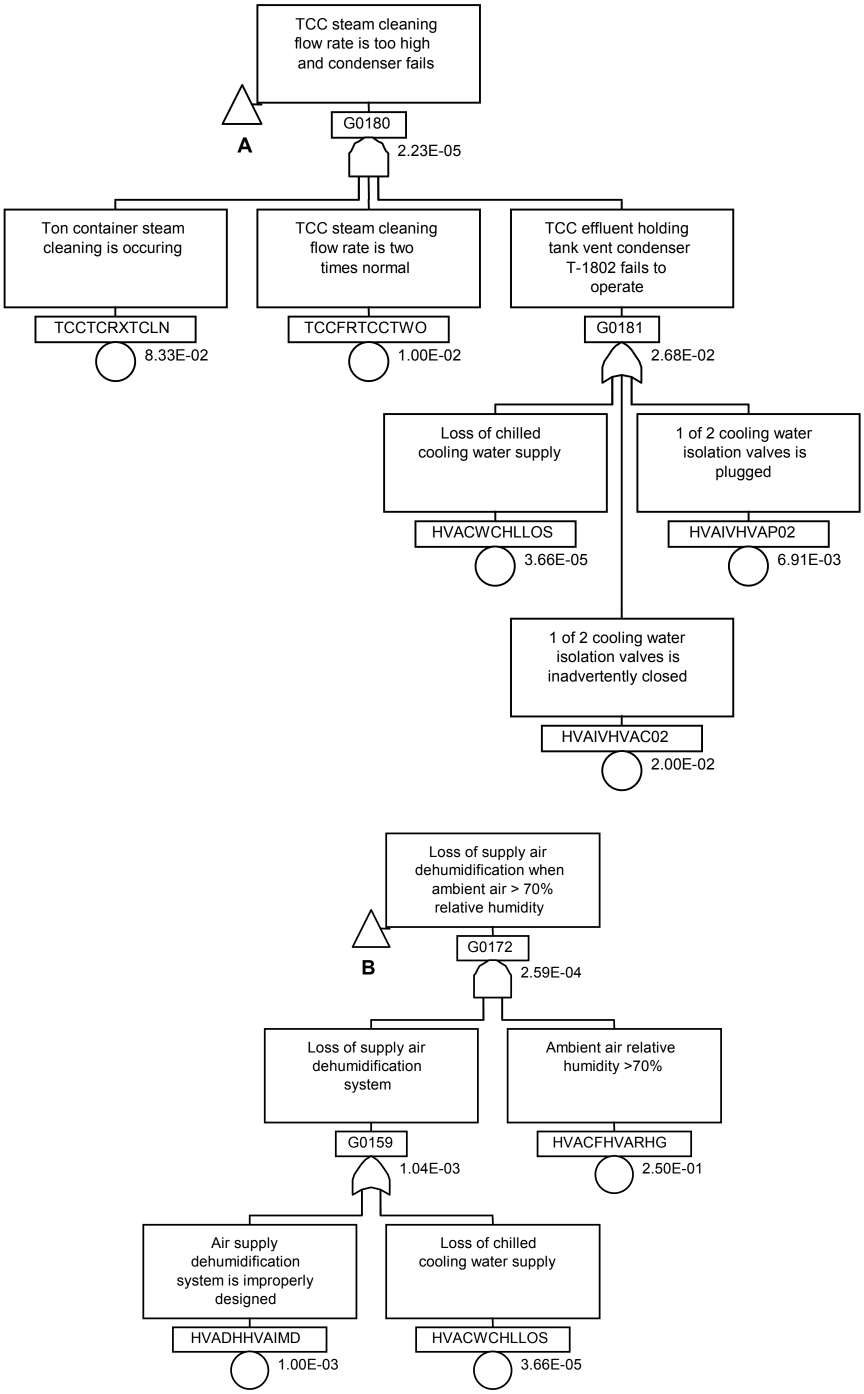


Figure 1. Fault tree for an activated carbon filter safeguard system



Note: The probability shown is based on 16-month.

Figure 1 (continued). Fault tree for an activated carbon filter safeguard system