Session No. 618

Developing and Implementing an Effective System Safety Program for Chemical Weapons Demilitarization

Jeffrey Weldon, BS CSP

Introduction

Implementing an effective process safety management program on a chemical weapons demilitarization facility is challenging. Accomplishing the mission and maintaining effective risk reduction requires a strong commitment to safety, a well-written program, a dedicated and competent team, and proven processes. On U.S. military contracts, MIL STD 882D is implemented as System Safety Engineering and complies with process safety requirements.

This presentation provides an overview of the Blue Grass Chemical Agent Demilitarization Pilot Plant System Safety Program. A brief overview of the chemical weapon demilitarization program and the Blue Grass Facility will be provided followed by a short video of the Rocket Cutting and Rocket Shear Machines.

1. 0 Background

The Chemical Demilitarization Program was established in 1986 by Public Law 99-145 and directed by several succeeding laws. In 1997, Congress established the Assembled Chemical Weapons Alternatives program to safely test and demonstrate at least two alternative technologies to the baseline incineration process for the destruction of the nation's stockpile of assembled chemical weapons. Assembled chemical weapons are configured with fuzes, explosives, propellant, chemical agents, shipping and firing tubes and packaging materials. Congress authorized ACWA to manage the development and pilot-scale testing of these technologies in 1999. A public law signed that year stated that funds would not be allocated for a chemical weapons disposal facility at Blue Grass Army Depot until the Secretary of Defense certified demonstration of six incineration alternatives. After successfully demonstrating three technologies in 1999 and three more in 2000, ACWA determined that four of them were viable for pilot testing. ACWA was assigned responsibility for the destruction of chemical weapons stockpiles in Colorado and Kentucky in October 2002. In 2003, DoD selected neutralization followed by Supercritical Water Oxidation for the destruction of the Kentucky stockpile. Additionally, in November 2007, ACWA was formally activated as the U.S. Army Element, Assembled Chemical Weapons Alternatives. The BGCAPP project was designed to safely destroy the chemical agents [mustard/blister agent (H), and nerve agents /organophosphate

compounds (GB, and VX) in munitions at the Blue Grass Army Depot (BGAD**).** (Exhibit 1 identifies the location of the BGAD).

2.0 System Safety Plan

Experience indicates that the degree of safety achieved in a system is directly dependent upon the emphasis given[1]

This fact is true for all aspects of a safety and health program, but a well-written program plan is fundamental to successfully managing risk. It is essential that sufficient time and effort is taken to develop a plan. This must be developed in concert with the other stakeholders. The goals of the plan are:

1. Safety will be addressed fully in the project's planning and criteria development, and implemented throughout design, equipment procurement, installation, construction, testing, inspection, acceptance, systemization, training, operations, maintenance, and ultimately closure.
2. Hazards associated with each system, subsystem, equipment, or facility will be identified and evaluated. These hazards will be tracked in a formal hazard tracking log, eliminated via design change, or controlled to an acceptable level throughout the entire life of the plant. Field and engineering changes (management of change) will be subjected to safety reviews to identify and minimize potential risk, avoid compromising safety, and help to minimize costly changes and retrofitting actions.
3. Safe and efficient disposal must be included in all operations using or producing hazardous materials.
4. Accidents, injuries, system loss, and near misses will be evaluated for lessons learned and corrective actions to prevent recurrence. Hazard analyses will be updated as required by review of "lessons learned."

There are several templates available to model a plan. At Blue Grass Chemical Agent Destruction Pilot Plant we implemented the Program Manager for Chemical Agent Demilitarization (PMCD) System Safety Management Plan (SSMP) which is based on the Army Safety Program (AR 385-10), System Safety Engineering (DA Pam 385-16), and is based on US Military Standard 882D. BGCAPP produced a flow diagram (See exhibit 2) as the basis of our plan and project procedures. Flow diagrams provide a systematic approach and ensure that each activity is clearly defined and assigned. Section numbers identified in the flow diagram indicate where each is explained within the plan.

System safety applies engineering and management principles, criteria, and techniques to achieve acceptable mishap risk, within the constraints of operational effectiveness, time, and cost, throughout all phases of the system life cycle. It draws upon professional knowledge and specialized skills in the mathematical, physical, and scientific disciplines, together with the principles and methods of engineering design and analysis, to specify and evaluate the environmental, safety, and health mishap risk associated with a system.[2]

How risk will be defined is central to the plan. Many companies utilize a risk matrix. (See exhibit 3 of 882 D's for mishap values and exhibit 4 for risk assessment codes (RAC) and resolution authority). This tool also needs to specify who has the authority to accept the risk at

the various classifications. This should follow some hierarchy. At BGCAPP a residual risk acceptance rating of 4 could be approved by the safety manager. A RAC of 3 by the government project manager, but higher RACs of 2 or 1 scores would require very senior (off project) approval. Thus, significant effort is expended to reduce residual risk to 3 or 4 during design. This keeps the operational risk low and the approval local.

Performance methodologies and how safety design will be achieved are two other basics issues the plan must address. The three types of methodologies used are:

- Qualitative
- Quantitative
- To an established standard

Hazard and operability analysis is a qualitative method. It can use key word and node analysis. 'What if' and Failure Mode and Effect Analysis (FMEA), are other qualitative methodologies. FMEA being used to assess component reliability and effect on the overall system. Fault Tree, a quantitative methodology, was used for one system when a more in depth analysis of the human causes of non-human element failures was needed.

The plan needs to specify under what parameters each will be used. In complex organizations the plan may not specify the safety designs. These may be contained in other documents, however they need to be clearly cross-referenced and if they are not they need to be addressed in another formal document. These include what standards, specifications, regulations or checklists are used in the design of the system. Exhibit 5 shows an abridged checklist that is used.

Several factors will determine the type of review to be performed. The system's complexity and the potential risks will determine the amount of time to be allocated as well as the preference of the analyst conducting the review. At BGCAPP, Preliminary Hazard Analysis, (PHAs), were based on the process flow diagrams or on preliminary piping and instrumentation drawings (P&IDs) and the operating and design team's knowledge. Failure Mode and Effect Analysis or Hazard and Operability Studies (HAZOPS) were also used at the PHA stage. As the piping and instrumentation drawings were developed, reviews shifted to a combination of FMEA and "What-if"-analysis unless the complexity of the system required a more robust analysis. This was at the intermediate design stage. For critical or higher risk systems (those involving the potential for catastrophic damage or fatalities) we also conducted preliminary Operations Safety and Health Analysis, (OSHAs). These focussed on reviewing operator error and maintenance type activities in conjunction with hardware failures. This proved to be very beneficial for establishing the basic software parameters for the systems and enabled timely cost effective adjustments to overall operating control philosophies.

Another general consideration for the design is the number of failures that will lead to a mishap. Military Standard 882D requires that if the system is not critical two independent failures should be required to result in a mishap and if the system is critical then three independent failures should be required. In contrast to the design failures is the analysis. As an example when postulating events for the 'What If' analysis, will single or multiple failures be considered? At BGCAPP for most events where system damage or delay in operations was the consequence, we only postulated single point failures. If more catastrophic results were likely, we looked at multiple failures recognizing that the frequency of such events is reduced. The higher RAC was assigned based on the combined consequence and frequency. Many times the RAC is the same, lower consequence with occasional frequency as it is for high consequence with a remote frequency.

It must be noted that although it maybe possible to create an exhaustive list of all the hazards of a process, system or piece of equipment, it may not be possible to identify all the risks and in fact some risks may never be known[3]. The cost benefit or "valve added" approach must be used to determine when sufficient risk analysis has been conducted.

Another potentially contentious issue is who has the authority to resolve differences that occur in the risk ranking or risk reduction process. Disagreements may arise between engineering and system safety or operations and system safety on the effectiveness or the need of a safeguard or mitigation measure. The plan needs to specify how these issues will be resolved. These decisions are often characterized as business decisions. The established residual risk acceptance ratings provide parameters that must be followed, however the ALARP principle, As Low As Reasonably Practical, is a business decision not a system analysis function. Another area that can be challenging for the analyst is risk resolution. It is important that this work scope remain with engineering when design related and with operations when procedural. The analyst may be lured or pushed into this role, but design engineering should be left to the designers and operational risk resolution with operations. The system safety analyst role is to manage the risk. This needs to be clearly understood. The program plan must also contain each system safety team position with clearly defined qualifications, functions, and responsibility for integration of activities. This should include a division of responsibility matrix (See exhibit 6).

The use of teams for performing various functions is another consideration. At BGCAPP any hazard analysis that required a team was called a Hazard Event Analysis Review Team (HEART). A hazard analysis may be required at any stage of the operational life of the equipment.

Teams with technically proficient members and when professionally facilitated can achieve more thorough and practical analysis than an individual or even two individuals. The plan must define how and when teams will be utilized. It must also clarify when it is acceptable for the system analyst to perform analysis independently, for although the team approach may achieve a more robust result, they are by nature slow inefficient and expensive. Management of the team and keeping members focused on the identification of risk is a key function of the facilitator. Engineers may want to delve into redesign, operators may want to identify different approaches to "work around" in the event of a failure. While these are important in the long run, they complicate the objective. This is risk identification. The composition of the team and defining the stakeholders of the system safety program must also be addressed.

Budget aspects would not be addressed in the plan, but the plan should provide sufficient detail to establish the budgetary needs for the system safety program. This is why it is imperative that department managers impacted by the plan and the responsible managers sign the plan.

The software for performing the reviews and then capturing the salient aspects of the reviews in a database is also critical to the overall effectiveness and efficiency of the system safety program. There are many commercial programs available, but, BGCAPP elected to develop its own after starting with a commercial product that did not provide all the features needed to track safeguards, mitigation, etc. The transition from a commercial product was problematic; however, it proved to be an extremely effective and improved the program's efficiencies significantly when we transitioned to a web-based platform. Some of our realized benefits were:

1. Immediate access by stakeholders;

2. The iterative process between design and the analyst on risk and resolution could occur remotely;
3. Significantly reduced the need to generate hard copy reports;
4. The software retained all the historical information. This latter point was very beneficial for new stakeholders to understand the system's evolution over time and facilitates change reviews.
5. As systems were physically constructed, access was easy for stakeholders to identify safeguards and mitigation measures for validation.
6. The iterative process between operations and the analyst on risk and resolution could occur remotely. This included the development of the administrative controls for procedures and limiting conditions of operation. These could be validated and recorded into the hazard-tracking log (HTL).
7. Flow down of requirements for vendors was also more manageable. In summary the plan needs to include the software or at a minimum the task analysis indicating what the software needs to accomplish.

Change is inevitable at all phases, so how change will be identified, reported, managed and approved during each phase requires clarity in the plan. A management of change process is essential to maintain the safety basis.

As an example, when the FOAK was approved, the risk associated with the FOAK was also base lined. In other words the level of residual risk was established and accepted for the test. Specific controls and mitigation measures became requirements. Changes are inevitable; the process of how the changes are evaluated and approved in relation to the safety basis must be established and included in the plan. The majority of changes will not affect the safety basis, but may affect the documentation. Relabelling equipment or tag numbers is a good example. The HTL needs to be kept current to facilitate searching of the database. However, changes may remove safeguards, add or eliminate hazards. These impacts will require analysis. The plan needs to establish some criteria to determine the rigor of the analysis. Can it be done independently by an analyst or is a team review necessary? Analysts as well as designers are not infallible, so at a minimum there needs to be check. At BGCAPP both the engineering and system safety reviews had multiple checks. Another aspect as with most design processes there will be a monetary threshold that requires business decisions to authorize changes. The plan needs to address how the system analysis interfaces with this review process. The plan also needs to address vendors and or subcontracts. How will requirements be detailed in contracts and purchase orders? Explicit language for hazard analyses and risk mitigation for both commercial and military specific equipment needs to be developed and included.

Of particular concern is if the supplied part's failure could propagate energy to an adjacent system or accumulate energy. Limits and safety factors need to be specified. Software interface is an obvious aspect, but also consider how positive alerts or threatening conditions will be reported. Understanding how the supplier institutes positive error prevention when an error could result in a loss maybe a consideration

3.0 Design

The majority of the work for the system safety team occurred during design. It is an iterative process between operations, engineering and the system safety team. As design progresses hazards are more clearly understood and controls or mitigation s can be refined. Again it needs to be emphasized that the analyst role is not to design or solve issues to reduce risk. This responsibility principally resides with the design team. Operations and the system team may provide input based on experience.

Formal reviews started with the process flow diagrams. For large complex projects, such as designing a chemical weapons demilitarization plant system boundaries and scope were clearly defined. Ultimately at Blue Grass there would be approximately (513) subsystems. Defining and then grouping these into manageable, yet comprehensive work packages was another responsibility for the analyst. At Blue grass we ultimately ended with (18 packages?).

The preliminary hazard analysis, PHAs, provided the initial assessment of the risk associated with the process or equipment or multiple processes and multiple pieces of equipment as was the case at Blue Grass. Thorough hazard identification and characterization; postulating events from the identified hazards; working closely with the engineering and operation teams; issuing comprehensive reports; as well as maintaining the hazard tracking logs defined the PHA work process. The final objective was to establish a base line that had reduced the risk to as low as reasonably practical.

Our PHA review process eliminated or reduce hazards initially by design, including material selection or substitution. As an example for the Energetics Batch Hydrolyzer, EBH PHA, the postulated event, improper drum rotational direction control failure, could result in unhydrolyzed energetics being removed from the EBH. The event had a RAC value of 3 (severity II and frequency B) the safeguard was the use of a closed caption television (CCTV). A drum discharge switch was added and an interlock to reduce the RAC to a value of 4 (Severity IV frequency C).

As design progresses, details are added and the risk profile must be updated. P&ID drawings are developed and revised. At a stage determined by design and operations a final design was achieved and the subsystem hazard analysis SSHA, is completed. These review and confirm the majority of designed safeguards and mitigation measures. These included fundamental design considerations such as blast and chemical agent containment and isolation for pressure and chemical agent hazards as well as typical industrial hazard such as noise, vibration and thermal hazards. Typical mitigation measures are also identified fail-safe design, system protection and fire suppression to name a few. Because the review changes design, it also results in a change to the risk basis. During the SSHA for example and event was postulated that the chute damper could close on the robotic arm and cause damage RAC 2 (severity II frequency C). The existing safeguard was a programmed permissive to prevent closure if the robot arm was present. An additional proximity switch was added because this was single point failure RAC 3. (severity II frequency E).

After the SSHA, an initial Operability Safety and Health Analysis (OS&HA) was conducted. The intent is to closely evaluate the human failure component of the process. There is sufficient detail available about how the operators and maintenance workers will interact with the system but most importantly is the controlling operator's interaction with the system. Limits and operating boundaries can be established in the control logic for both operational and maintenance modes. This needs to include local control systems. This analysis requires robust event postulation and significant support from the operating team. It is at this stage that the software control logic is refined. These controls include soft and hard interlocks, redundancy, warning systems for temperature, pressure or other impending mishaps. Also health hazards can be assessed, protective clothing proposed, issues that must be specified in the procedures, and other administrative controls documents will initially be addressed during this OS&HA. The hazard analysis can then be a tool for development of procedures. The HTL will also provide rational and support for the use of warnings, cautions, and notes.

How equipment is to be positioned is assessed. Access during operations especially where fully encapsulated level 'A' suits are required is critical. Servicing, maintenance, repair, or adjustment exposes operators to sources of hazards such as: high pressures, high temperatures, high voltage, hazardous chemicals, cutting edges, sharp points, noise etc. The OS&HA also helps determine administrative controls or mitigation measures. These include process monitoring (e.g., for chemical agent, temperature, and air/liquid flow) in the design to provide warnings of impending mishap conditions or to aid in timely response to minimize consequences of mishaps or near misses.

Interface analysis can also be completed if design has progressed on adjacent systems, utilities, input or output processes. The FOAK will have operational limits and requirements. These need to be reviewed to establish controls to regulate, monitor or limit inputs that could result in a mishap. Upset conditions or failures in these adjacent or utility systems must also be reviewed for consequences on the FOAK. As an example, if the discharge volume for the ventilation system was reduced by 50% because of an event in an adjacent area how would this impact the EBH, what monitoring would alert the EBH operators and what measures would need to be taken? Should this be an automated response or manual?

As design progresses there will be change and these will be managed in accordance to the plan. As was noted earlier the HTL has an historical aspect. This feature proved to be very valuable. From inception to completion design may take years. Stakeholder composition will change and with them ideas or challenges to the design may arise. Being able to provide the iteration and evolution of the current state, the changes and the rational for those changes lessons the potential impact particularly with time, these new stakeholders may impose.

The final challenge for the team is to establish when management of change processes will be implemented. At Blue Grass this was determined to be when the design was issued for construction. As indicated earlier in the system plan section, criteria is critical to define what change thresholds must be reached to result in the type and rigor of review.

4.0 First of a Kind Equipment

First of A Kind, FOAK, presents additional challenges to the system safety program. FOAK becomes necessary when there is need to accomplish a specific unique process. Equipment may or may not exist. If it does exist in the commercial sector it most certainly has not been used in

the configuration or application needed. As BGCAPP was the last facility to be designed, it also benefitted from valuable lessons learned from other facilities and from similar equipment previously designed.

The role of the safety analyst is to present the risks of each technology proposed. It is therefore imperative that the system analyst be thorough in the review to provide the information necessary to support the decision of technology acceptability. Typically in the early stages of assessing alternative technologies only basic information may be available, however, hazards can be identified and when coupled with operating concepts events can be postulated. These can then be assigned risk assessment codes. There will also be unknown aspects and assumptions may be necessary to further understand the risk. In simplistic terms the more hazards that are associated with the technology the more potential event scenarios the higher the cumulative risk. Comparison must be consistent. A thorough analysis of one system with a cursory analysis of a second may make one appear to have more hazards when it fact it had a more comprehensive review. Each technology's overall risk can then be compiled and compared with any assumptions being noted. Safety was a significant aspect of the decision at BGCAPP. There are many tools available to analyze and compare technologies. Simple weighted matrices and parato analysis are two tools.

The final technology decision may also be influenced by prior experience and capability to control the hazard or mitigate its consequence. As an example if this same hazard is being managed in another process it may impose less of a burden on resources than a new hazard that has not been managed. Training, or the current facility may have excess capacity in ventilation systems or fire suppression are a few examples. This will influence the factors that will ultimately be the basis for the selected technology provided the systems are equally effective.

5.0 Fabrication and assembly

Who, how and where equipment will be fabricated may or may not have significant relevance on how the unit is produced and the risk. The key at Blue Grass was to validate the specifications captured the controls and mitigations identified during all the risk reviews. This responsibility resided with the engineering team. Engineering determined how the proposal incorporated the system safety deliverables. The P&IDs will contain the specifics and fabrication hold points. With vendors change management needs to be clearly documented.

6.0 Testing

The design basis is often determined with laboratory and bench scale testing. Additional testing is then done to validate the design basis once the equipment is fabricate at plant scale. For vendor-supplied equipment, who and how the acceptance testing will be performed is another issue that needs to be addressed. Commonly referred to as the FAT the Factory Acceptance Test requires input from the system safety team. All those events postulated that could result in damage to the EBH from infrastructure or temporary utilities or the test itself need to be addressed. As an example, the steam jacket for the EBH was designed for and operating range of 60 to 80 pounds of steam pressure with a limit of 120. There are two regulators in the steam supply system to prevent over pressurization. For the FAT a temporary steam generator must be used. This generator must also have two regulators if it has the potential to deliver steam that would exceed these limits.

Prior to conducting the test an operational readiness review is performed. This has three aspects. The first is to require a test plan. These plans typically focus on equipment operations, functionality and through put performance requirements. From an operational safety perspective this has obvious implications and it is an opportunity to supplement the preliminary OSHA. A Job Hazard Analysis (JHA) with event postulation and RAC codes was specified for the EBH.

The second is to physically verify that the safe guards and mitigation measures specified in the safety basis are in place and operational. This is not a safety function, but the documentation should be verified and some field sampling can be accomplished during the Start Up and Safety Inspection, (SUSI), to further validate. A benefit of the testing is that should a safeguard not function as intended, the HTL can be updated to better assign the risk. Additional recommendations can be made for the operational unit if the risk is adversely affected.

Prior to performing the FAT a SUSI is required. (See exhibit 7 for a sample form) This includes a physical inspection of the FOAK and test environment. The objectives of the SUSI are two fold. One is to protect the FOAK as at this juncture damage or replacement would have significant schedule/cost impacts. The other is to protect the operators and facility. Procedures for the test are validated. (See block flow diagram exhibit 8. These include mitigation measures should there be a mishap.

7.0 HEART REVIEWS

HEART reviews have been completed to support the majority of the design phase. Reviews done as a result of change management are categorized based on the complexity of the change. The system safety analyst can conduct a review based on the documents used to define the impact of the change. Or if beyond the analysts experience level, a desk side review can be conducted where an engineering representative, an operations person, and others provide information to the analyst so that he/she can assess the change. For major changes, the HEART can be formal and include a variety of disciplines similar to that done during development of PHAs.

As the program phases change from predominantly design to systemization, the hazard analysis change from design related reviews to operations related. Procedures are reviewed and Job Hazard Analyses, Health Hazard Assessments, etc. are done. These reviews will comprise the formal OSH&As and are also tracked in the project HTL. While the focus changes to human related events, the system safety analyst (and HEART) does not have to limit recommendations to only procedural controls. As with other hazard related recommendations, the risk acceptance authority decides how many resources to allocate to control of postulated events.

8.0 Conclusion

This article provided a step-by-step process for Developing and implementing an effective system safety program for chemical weapons demilitarization. The objective for our program was to reduce risk to level a low as reasonably achievable, (ALARA) at the Blue Grass Chemical Agent Pilot Plant. The importance of a well-written system safety plan and other fundamental aspects of the system safety program were provided and supported with examples.

Endnotes

1. Air Force Safety Agency: Air Force System Safety Workbook, Kirtland AFB NM87117-5670 July 2000
2. Department of Defence: Standard Practice For System Safety, Mil-STD-882D 10 Feb. 2000
3. IBID1: Air Force Safety Agency: Air Force System Safety Workbook, Kirtland AFB NM87117-5670 July 2000

Illustrations

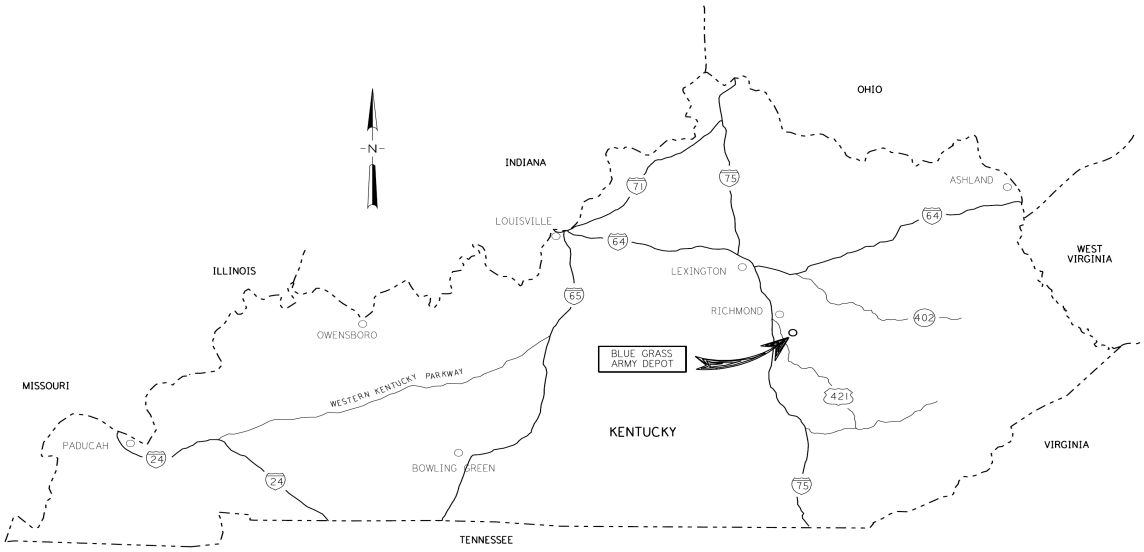

Exhibit 1. BGAD Kentucky Map

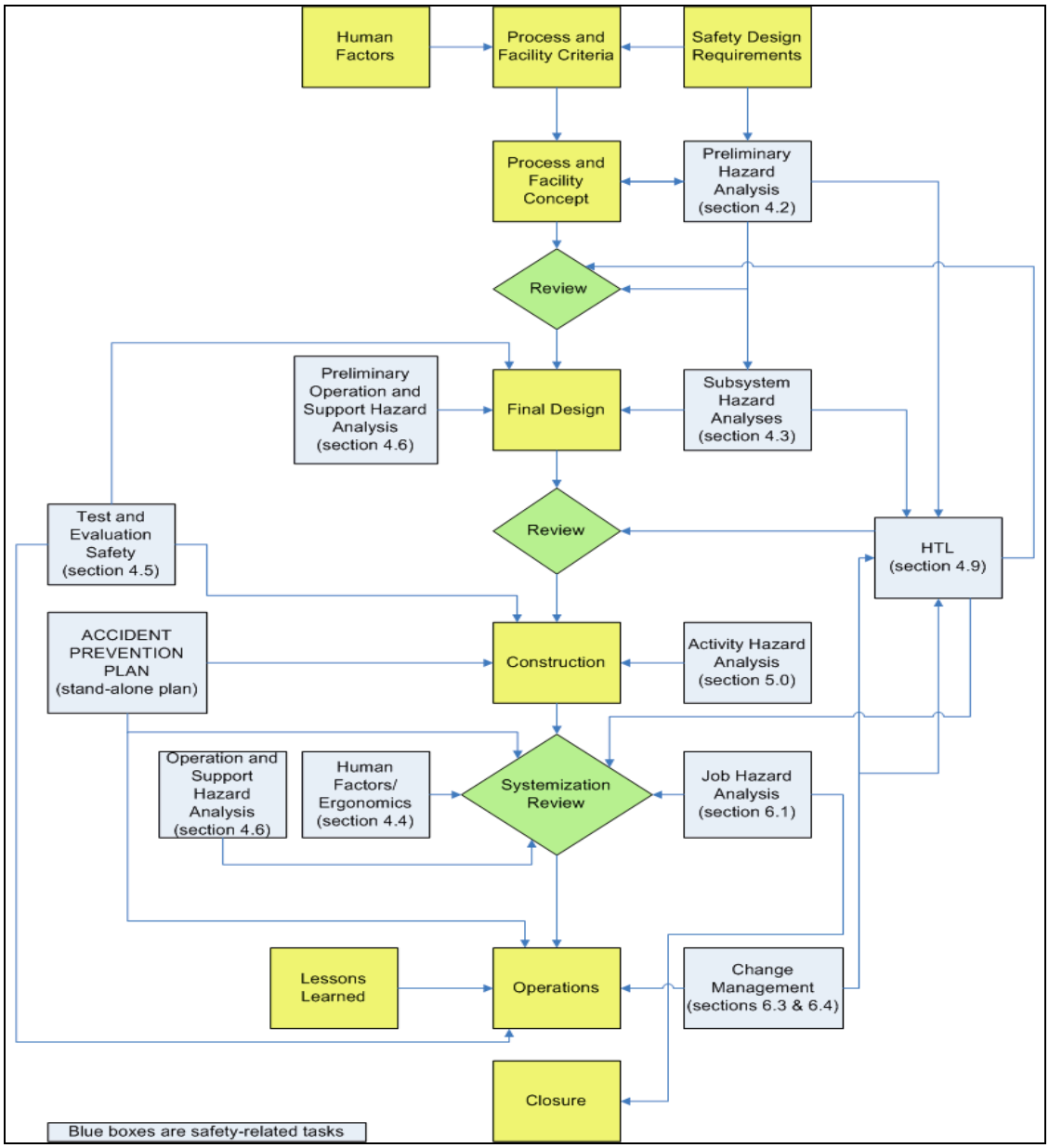

Exhibit 2. System Safety Flow Diagram

SEVERITY PROBABILITY	Catastrophic	Critical	Marginal	Negligible
Frequent	1	3	7	13
Probable	2	5	9	16
Occasional	4	6	11	18
Remote	8	10	14	19
Improbable	12	15	17	20

Exhibit 3. Example Mishap Risk Assessment Values

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

[a]Acceptability criteria:

RAC	Description	Resolution Authority
1	Unacceptable	Assistant Secretary of the Army
2	Undesirable	PM ACWA
3	Acceptable with controls	PM ACWA Site Manager
4	Acceptable	BGCAPP Safety Manager

Exhibit 4. Risk Assessment and Resolution Authority

b. Hazardous substances, components, and operations are isolated from other activities, areas, personnel, and incompatible materials.

c. Equipment is located so that access during operations, servicing, repair, or adjustment minimizes personnel exposure to hazards (e.g., hazardous substances, high voltage, electromagnetic radiation, and cutting and puncturing surfaces).

d. Protect power sources, controls, and critical components of redundant subsystems by physical separation or shielding, or by other acceptable methods.

f. Consider safety devices that will minimize mishap risk (e.g., interlocks, redundancy, fail safe design, system protection, fire suppression, and protective measures such as clothing, equipment, devices, and procedures) for hazards that cannot be eliminated. Make provisions for periodic functional checks of safety devices when applicable.

g. System disposal (including explosive ordnance disposal) and demilitarization are considered in the design.

h. Implement warning signals to minimize the probability of incorrect personnel reaction to those signals, and standardize within like types of systems.

i. Provide warning and cautionary notes in assembly, operation, and maintenance instructions; and provide distinctive markings on hazardous components, equipment, and facilities to ensure personnel and equipment protection when no alternate design approach can eliminate a hazard. Use standard warning and cautionary notations where multiple applications occur. Standardize notations in accordance with commonly accepted commercial practice or, if none exists, normal military procedures. Do not use warning, caution, or other written advisory as the only risk reduction method for hazards assigned to Catastrophic or Critical mishap severity categories.

j. Safety critical tasks may require personnel proficiency; if so, the developer should propose a proficiency certification process to be used.

k. Severity of injury or damage to equipment or the environment as a result of a mishap is minimized.

l. Inadequate or overly restrictive requirements regarding safety are not included in the system specification.

m. Acceptable risk is achieved in implementing new technology, materials, or designs in an item's production, test, and operation. Changes to design, configuration, production, or mission requirements (including any resulting system modifications and upgrades, retrofits, insertions of new technologies or materials, or use of new production or test techniques) are accomplished in a manner that maintains an acceptable level of mishap risk. Changes to the environment in which the system operates are analyzed to identify and mitigate any resulting hazards or changes in mishap risk.

Exhibit 5. MIL-STD-882D APPENDIX A13 Basic system safety design checklist

Task	General Safety	System Safety	Medical/Health	Engineering	Operations	Testing Org	Environmental	QA	Construction	Government Team
Schedule HEART		S		P	S		S			
Prepare/Facilitate HEART		P		S	S					
Select Attendees		E		E	E		E			E
Document Hazard Review		P								
Review & Approve Hazard Reports	E			E	E*					
Maintain HTL		P								
Assign responsibility for resolution				E	E					
Propose design resolution for HTL events	S			P	S					
Propose admin resolution for HTL events			S	S	P					
Accept/reject/clarify proposed resolutions Assign Final RAC	S	P								
Request Acceptance of residual risk		P								
Accept Risk	E									E
Test & Evaluation Risk		S	S	S	S	P				
Health Hazard Assessment		S	P		S					
Job Hazard Analyses		P	S		S		S			
Job Safety Analyses		S	S		P					
O&SHA		P	S	S	S		S			
Identify Safety Related Design Requirements including electrical and explosive safety	S		S	P						
Incorporate HA safeguards into specifications				P						
Configuration control of design documents				P						
Review of changes for impact to HA		P								
Review of changes for safety impacts	P			P						
Review of changes for code compliance										
Review changes for compliance with program								P		
Pre-systemization turn over	S		S	S	S				P	
Prepare SUSI	P	S	S	S	S				S	
Site Plan Safety Submission	S			P	S					
Determine safe failure positions for hardware	S	S	S	P	S		S			
Verify logic diagrams accomplish design and operational intent, verify interlocks used as safeguards in HA		S		P	S					
Oversee development of design to ensure compliance with safety programs	P							S		

P = primary/lead
S = supporting
E = equal/shared
* = during subsequent phases

Exhibit 6. Sample Division of Responsibility, DOR, matrix

Bechtel-Parson Blue Grass
Startup and Safety Inspection Checklist

Facility/Building/Utility:	***Safety Lead:***
Reference Documents:	

This form shall be completed prior to use, unless waived in writing by the signatures.
This form shall be used in conjunction with SWPP 4MP-T81-01602.
The responsible Systemization, Operations, Construction, Engineering, and Safety and Health representatives will sign and date this form prior to occupancy or use of the facility, building, or utility.

ITEM	QUESTION	ANSWER	COMMENTS/REFERENCE INFORMATION
1	Are there incomplete items or is a punchlist being worked? (See instruction sheet.)	☐ No ☐ N/A	
2	Has a Life Safety Inspection been completed?	☐ Yes ☐ No	
3	Has a hazard analysis been performed for the facility?	☐ Yes ☐ No	
a)	Has an SSHA been done for this facility or area? List Reference number.	☐ Yes ☐ No	
b)	Has an HHA been completed? List Reference number.	☐ Yes ☐ No	
c)	Has an O&SHA been completed? List Reference number.	☐ Yes ☐ No	
4	Has a physical walk down inspection been completed?	☐ Yes ☐ No	
5	Is an HA required based on facility use?	☐ Yes ☐ No	
6	Type of Assessment for Temporary Use or Systemization	☐ JSA ☐ HA	
7	Have all formal HA events been entered into the project HTL?	☐ Yes ☐ No	
a)	Have all the design safeguards been verified?	☐ Yes ☐ No	
b)	Have all administrative safeguards been verified?	☐ Yes ☐ No	
c)	Are all applicable HTL items closed or have alternative mitigators/safeguards been identified?	☐ Yes ☐ No	
d)	Are there FCS/FPS safeguards?	☐ Yes ☐ No	
e)	Have any applicable FCS/FPS safeguards been verified?	☐ Yes ☐ No ☐ N/A	
f)	Has residual risk been accepted?	☐ Yes ☐ No	
8	Has boundary tag/lock been established?	☐ Yes ☐ No ☐ N/A	

We recommend the facility be approved for use.

	Print Name	Sign Name	Date
Facility Manager (e.g., Systemization or Office Services Representative)			
Office Representative			
Engineering Representative			
Safety & Health Representative			

Form BG-000-4MP-T81-03711.01, Revised 25 FEB 2010

Exhibit 7. Start – up and Safety Inspection Form

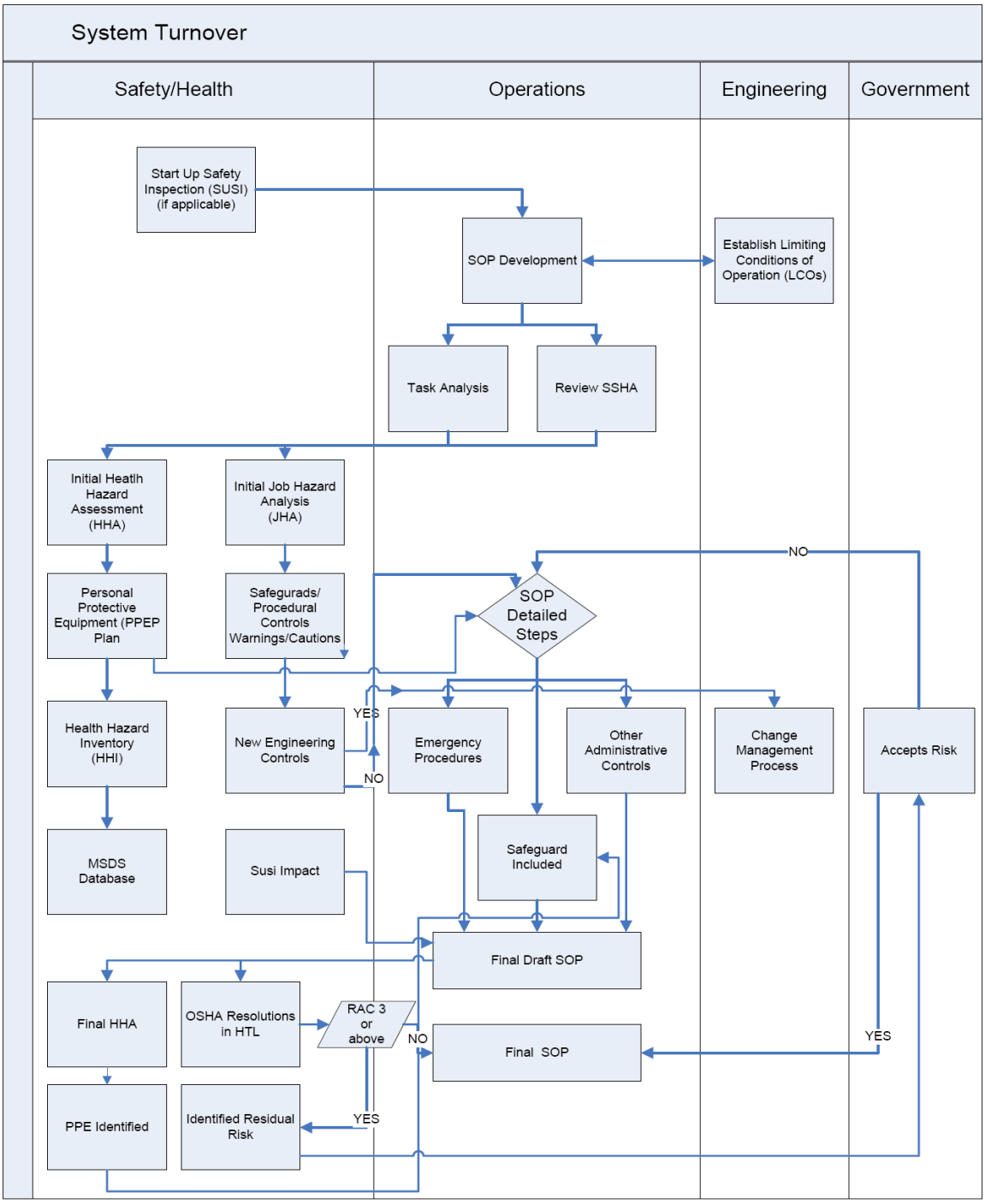

Exhibit 8. Block Flow Diagram for the development of procedures