View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by UNT Digital Library

This document was prepared in conjunction with work accomplished under Contract No. DE-AC09-96SR18500 with the U.S. Department of Energy.

This work was prepared under an agreement with and funded by the U.S. Government. Neither the U. S. Government or its employees, nor any of its contractors, subcontractors or their employees, makes any express or implied: 1. warranty or assumes any legal liability for the accuracy, completeness, or for the use or results of such use of any information, product, or process disclosed; or 2. representation that such use or results of such use would not infringe privately owned rights; or 3. endorsement or recommendation of any specifically identified commercial product, process, or service. Any views and opinions of authors expressed in this work do not necessarily state or reflect those of the United States Government, or its contractors, or subcontractors.

HAZARD ANALYSIS SOFTWARE

Author: Stephen J. Sommer
Co-authors: Joe Copeland, Bob Lowrie, Tinh Tran, Lynh Nguyen, Matt McCormick
Washington Safety Management Solutions, LLC.
2131 S Centennial Drive
Aiken, SC 29803
Phone: 803-502-9778
Email: steve.sommer@wsms.com

Abstract

Washington Safety Management Solutions, LLC developed web-based software to improve the efficiency and consistency of hazard identification and analysis, control selection and classification, and to standardize analysis reporting at Savannah River Site.

In the new nuclear age, information technology provides methods to improve the efficiency of the documented safety analysis development process which includes hazard analysis activities. This software provides a web interface that interacts with a relational database to support analysis, record data, and to ensure reporting consistency.

A team of subject matter experts participated in a series of meetings to review the associated processes and procedures for requirements and standard practices. Through these meetings, a set of software requirements were developed and compiled into a requirements traceability matrix from which software could be developed. The software was tested to ensure compliance with the requirements. Training was provided to the hazard analysis leads. Hazard analysis teams using the software have verified its operability. The software has been classified as NQA-1, Level D, as it supports the analysis team but does not perform the analysis. The software can be transported to other sites with alternate risk schemes.

The software is being used to support the development of 14 hazard analyses. User responses have been positive with a number of suggestions for improvement which are being incorporated as time permits. The software has enforced a uniform implementation of the site procedures. The software has significantly improved the efficiency and standardization of the hazard analysis process.

INTRODUCTION

Software applications such as Microsoft Word, Microsoft Excel, and Corel Word Perfect are often used to support the documentation of a Hazard Analysis (HA). However, these applications were not developed to support hazard analysis. Therefore, the primary tools used for HA lack the capabilities and features necessary to efficiently produce an HA and ensure its consistency.

Inefficiency occurs when humans manually perform repetitive actions, rely on their memory, and manually extract data from one report to generate another report.

Inconsistencies occur when the same concept is repeated but stated in multiple ways or in activities such as manually recording and maintaining risk rankings (e.g., high frequency with high consequences results in an A1 risk ranking).

HA and Documented Safety Analysis (DSA) data is strongly related. Identification of hazards and their locations is directly related to the identification of events. Data such as causes, locations, Material at Risk (MAR), assumptions, and controls are then related to each event. The events are prevented or mitigated through the application of controls. This information is then discussed in DSA Chapter 3, “Hazard and Accident Analyses,” Chapter 4, “Safety Structures, Systems, and Components,” Chapter 5, “Derivation of Technical Safety Requirements,” and the Technical Safety Requirements (TSRs). While word processors are excellent for writing DSAs and TSRs, a relational database is a better tool for developing the data that will be presented in those documents.

Therefore, Washington Safety Management Solutions (WSMS), LLC, developed software to support HA, DSA and TSR development at Savannah River Site (SRS). This software package has been titled, “electronic Consolidated Hazard Analysis Process,” (eCHAP).

BACKGROUND

WSMS encountered several events which prompted reconsideration of the software used to document our HAs. The process relied on an engineer recording HA data in Microsoft Word tables. While Word and Excel have some powerful features; these features were not developed from the perspective of supporting hazard analysis. Therefore, Word and Excel do not support the efficient use of an engineer’s time.

Consider two (2) cases.

1. Using Word an engineer searches an HA table, either manually or using the Find feature, to find the previous occurrence of a MAR, cause, control, etc. If and when they find it, they copy the information, scroll to their previous location in the table and paste that information into the table. If they don’t find it, they will type in what they remembered which leads to inconsistencies.

2. An engineer is asked to extract information from an HA table to construct another table (e.g., a list of controls and their related events).

Both of these cases require an inefficient use of an engineer's time. In the first case, a short period (seconds to minutes) repeated many times during HA development. In the second case, a significant time period (hours) to find, extract, and reassemble the data. In the second case, if the data in the HA table changes then the second table needs to be manually updated.

In the first case above, the introduction of inconsistencies was mentioned. With a word processor, one is not able to easily view variations from the perspective of "what did the engineer mean." For instance, the following attributes were listed within the same HA:

- Identifies tritium presence inside container
- Identifies tritium quantity inside the container

In this case, a reviewer must determine if these are the same concept (i.e., tritium exists within the container) or there are two concepts (i.e., presence of tritium within the container in the first case and how much tritium is within the container in the second case). If the information were presented in the same location, the analyst could be prompted to consider the potential ambiguity so that the statements may be refined or to replace one statement with the other.

In order to address these types of issues, WSMS assembled a team of experts to assess the SRS HA, DSA, and TSR development processes, identify requirements, and establish design criteria for software development. eCHAP was then developed, tested and deployed and has been in use since the summer of 2007. The primary input source for the eCHAP design was DOE-STD-3009-94, Change Notice No. 3, "Preparation Guide for U.S Department of Energy Nonreactor Nuclear Facility Documented Safety Analyses." Interpretation of this standard was influenced by SRS guidance such as WSRC-SCD-11, Revision 5, "Consolidated Hazard Analysis Process Programs and Methods," and WSRC Manual E7, "Conduct of Engineering and Technical Support Procedure Manual," Procedure 2.25, "Functional Classifications."

DISCUSSION

eCHAP is designed to support the development of DSAs and TSRs beginning with a facility's HA. Within eCHAP there are seven (7) basic steps as follows:

1. Define risk scheme
2. Event identification
3. Standard hazard identification
4. Hazard review
5. Event bounding evaluation
6. Credited control evaluation
7. Credited control specification

Step 1

The first step requires defining the means for categorizing and ranking a facility's hazards. A site or facility will have manuals and/or procedures that define their risk parameters. A Configuration Control Board (CCB) is responsible for interpreting that guidance, preparing and then publishing approved risk schemes within eCHAP.

Within eCHAP, a risk scheme (Figure 1 - Risk Parameters) is required to be defined prior to the start of an analysis. A risk scheme defines the acronyms to be used for frequency (e.g., Anticipated [A], Unlikely [U], Extremely Unlikely [EU], Beyond Extremely Unlikely [BEU]), consequences (e.g., High [H], Moderate [M], Low [L], Negligible [N]), hazard types (e.g., Radiological, Chemical, Physical), receptors (e.g., Immediate Worker [IW], Collocated Worker [CW], Maximally exposed Off-site Individual [MOI]), and risk ranks (e.g., A, B, C, D). These acronyms are used to assemble risk matrices (frequency versus consequence) for each receptor and hazard type (Figure 2 - Risk Matrices). While most of the risk matrices are the same, the software was designed for maximum flexibility in defining risk schemes.

The risk scheme also specifies data such as TSR types (e.g., Limiting Condition for Operation [LCO], Administrative Control [AC], Design Feature [DF]), functional classification (e.g., Safety-Class [SC], Safety-Significant [SS]), and event types (e.g., fire [E-1], explosion [E-2], loss of confinement [E-3]) [Figure 3 - Supporting Details].

Step 2

The second step is event identification which is the core of the hazard analysis. Within this section, the analyst identifies the various event scenarios, estimates unmitigated consequences, identifies defense in depth controls, and then identifies the proposed credited controls (Figure 4 - Hazard Table).

eCHAP provides a generic hazard evaluation table. This table provides the analyst the means to create events and to specify information related to the event itself. Provision is made for replicating events (i.e., making a complete copy of an event for modification), copying events (i.e., copy specific components of one event to another), and searching events for specific information.

Information that is displayed in columns having a yellow background can be directly modified by the analyst. A double-click in the column or clicking its heading opens a screen to permit editing of the information. The analyst can then save the information or cancel the operation and return to the event detail screen.

Efficiency and consistency is obtained by storing information and making it available to the analyst for reuse. For instance, clicking on the Locations column opens a screen (Figure 5 - Event Type Detail) that shows the locations currently related to the particular event. Icons are provided to permit the user to add new locations and relate them to this event or to link existing (stored) locations to this event (Figure 6 - Location Linking). Currently linked locations are designated with a check and any other previously identified locations are also

listed. The analyst can add or remove links by checking or unchecking the boxes and clicking the save button.

eCHAP

Washington Safety Management Solutions

Current facility: H Canyon | eCHAP Risk Schemes | Current user: steve.sommer [Log Out]

Main Menu \ Risk Scheme List \ Risk Scheme August 2007

View Supporting Details | View Risk Matrix

Frequencies

Acronym	Description	Order
A	Anticipated	1
U	Unlikely	2
EU	Extremely Unlikely	3
BEU	Beyond Extremely Unlikely	4
NC	Not Credible	5

Hazard Types

Acronym	Description	Order
Rad	Radiological	1
Chem	Chemical	2
Phy	Physical	3

Receptors

Acronym	Description	Order
WG1	Hazard Hugger	1
WG2	Uninvolved Worker	2
WG3	Collocated Worker	3
MOI	Maximally Exposed Offsite Individual	4

Risk Ranks

Acronym	Description	Order
A1	High 1	1
A2	High 2	2
C/A3*	High 3	3
B1	Moderate 1	4
C/B1**	Moderate 2	5
B	Low	6
C	Negligible	7
NA	Not Applicable	8

Consequences

Acronym	Description	Order
H	High	1
M	Moderate	2
L	Low	3
N	Negligible	4

Figure 1 - Risk Parameters.

Current facility: H Canyon | **Risk Matrix Details** | Current user: steve.sommer [Log Out]

Main Menu \ Risk Scheme List \ Risk Scheme August 2007 \ Risk Matrix

View Risk Scheme | View Supporting Details

Rad (Radiological) | WG1 (Hazard Hugger)

	NC (Not Credible)	BEU (Beyond Extremely Unlikely)	EU (Extremely Unlikely)	U (Unlikely)	A (Anticipated)
H (High)	NA (Not Applicable)	C/A3* (High 3)	A2 (High 2)	A1 (High 1)	A1 (High 1)
M (Moderate)	NA (Not Applicable)	C/B1** (Moderate 2)	B1 (Moderate 1)	B1 (Moderate 1)	B1 (Moderate 1)
L (Low)	NA (Not Applicable)	C (Negligible)	B (Low)	B (Low)	B (Low)
N (Negligible)	NA (Not Applicable)	C (Negligible)	C (Negligible)	C (Negligible)	C (Negligible)

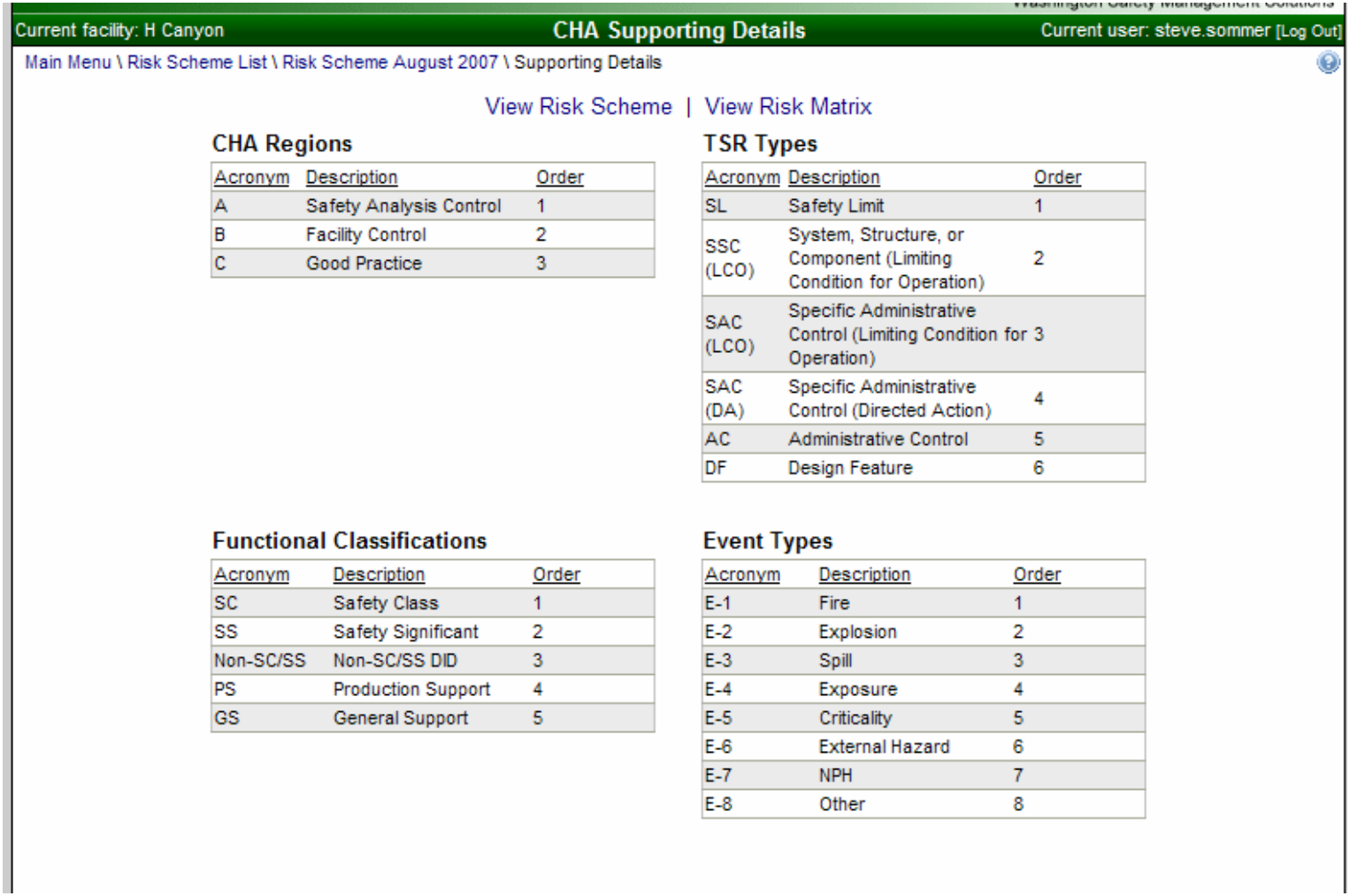
Rad (Radiological) | WG2 (Uninvolved Worker)

	NC (Not Credible)	BEU (Beyond Extremely Unlikely)	EU (Extremely Unlikely)	U (Unlikely)	A (Anticipated)
H (High)	NA (Not Applicable)	C/A3* (High 3)	A2 (High 2)	A1 (High 1)	A1 (High 1)
M (Moderate)	NA (Not Applicable)	C/B1** (Moderate 2)	B1 (Moderate 1)	B1 (Moderate 1)	B1 (Moderate 1)
L (Low)	NA (Not Applicable)	C (Negligible)	B (Low)	B (Low)	B (Low)
N (Negligible)	NA (Not Applicable)	C (Negligible)	C (Negligible)	C (Negligible)	C (Negligible)

Rad (Radiological) | WG3 (Collocated Worker)

	NC (Not Credible)	BEU (Beyond Extremely Unlikely)	EU (Extremely Unlikely)	U (Unlikely)	A (Anticipated)
H (High)	NA (Not Applicable)	C/A3* (High 3)	A2 (High 2)	A1 (High 1)	A1 (High 1)
M (Moderate)	NA (Not Applicable)	C/B1** (Moderate 2)	B1 (Moderate 1)	B1 (Moderate 1)	B1 (Moderate 1)
L (Low)	NA (Not Applicable)	C (Negligible)	B (Low)	B (Low)	B (Low)
N (Negligible)	NA (Not Applicable)	C (Negligible)	C (Negligible)	C (Negligible)	C (Negligible)

Figure 2 - Risk Matrices.



Current facility: H Canyon | CHA Supporting Details | Current user: steve.sommer [Log Out]

Main Menu \ Risk Scheme List \ Risk Scheme August 2007 \ Supporting Details

View Risk Scheme | View Risk Matrix

CHA Regions

Acronym	Description	Order
A	Safety Analysis Control	1
B	Facility Control	2
C	Good Practice	3

TSR Types

Acronym	Description	Order
SL	Safety Limit	1
SSC (LCO)	System, Structure, or Component (Limiting Condition for Operation)	2
SAC (LCO)	Specific Administrative Control (Limiting Condition for Operation)	3
SAC (DA)	Specific Administrative Control (Directed Action)	4
AC	Administrative Control	5
DF	Design Feature	6

Functional Classifications

Acronym	Description	Order
SC	Safety Class	1
SS	Safety Significant	2
Non-SC/SS	Non-SC/SS DID	3
PS	Production Support	4
GS	General Support	5

Event Types

Acronym	Description	Order
E-1	Fire	1
E-2	Explosion	2
E-3	Spill	3
E-4	Exposure	4
E-5	Criticality	5
E-6	External Hazard	6
E-7	NPH	7
E-8	Other	8

Figure 3 - Supporting Details.

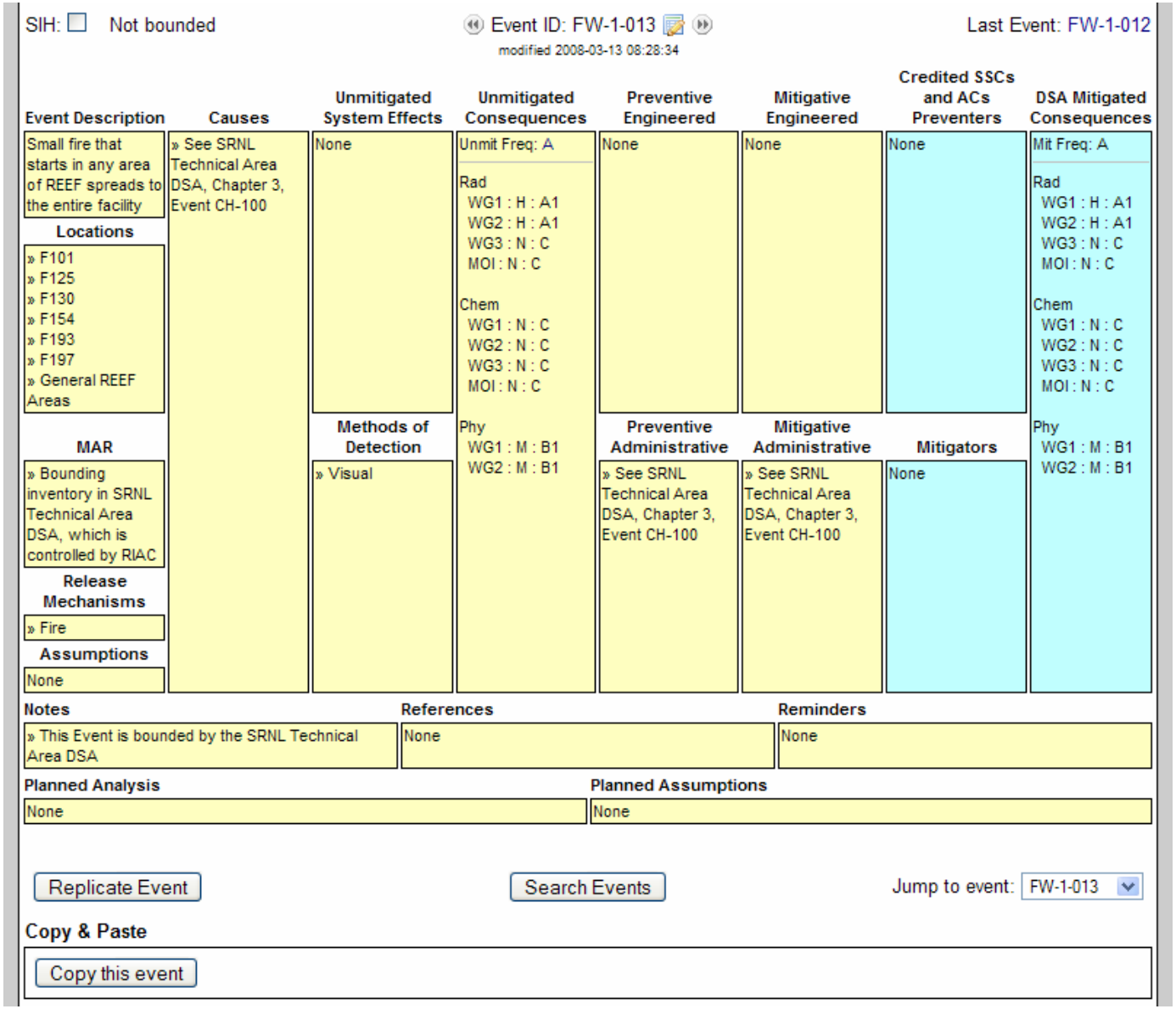


Figure 4 - Hazard Table.

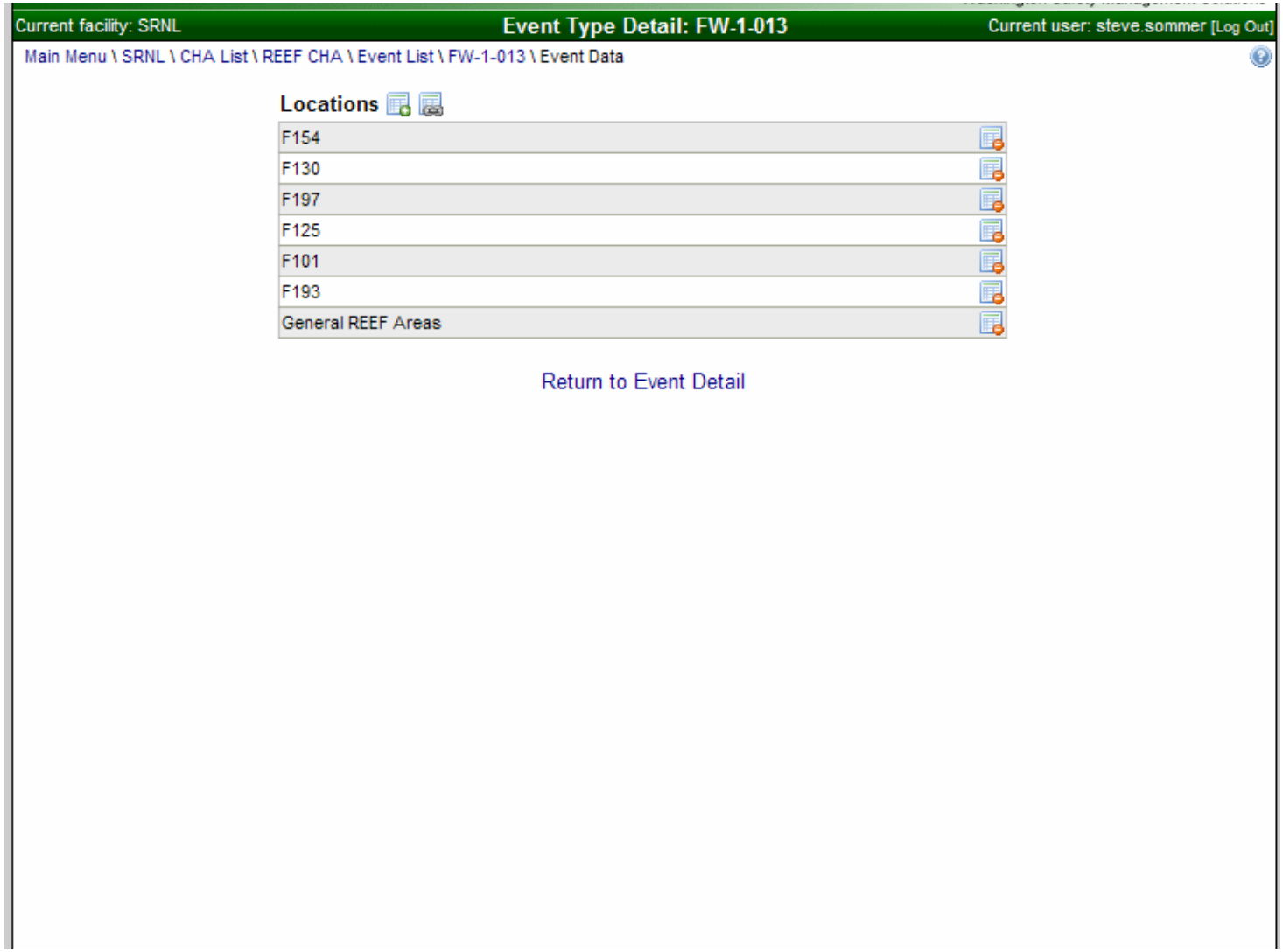


Figure 5 - Event Type Detail.

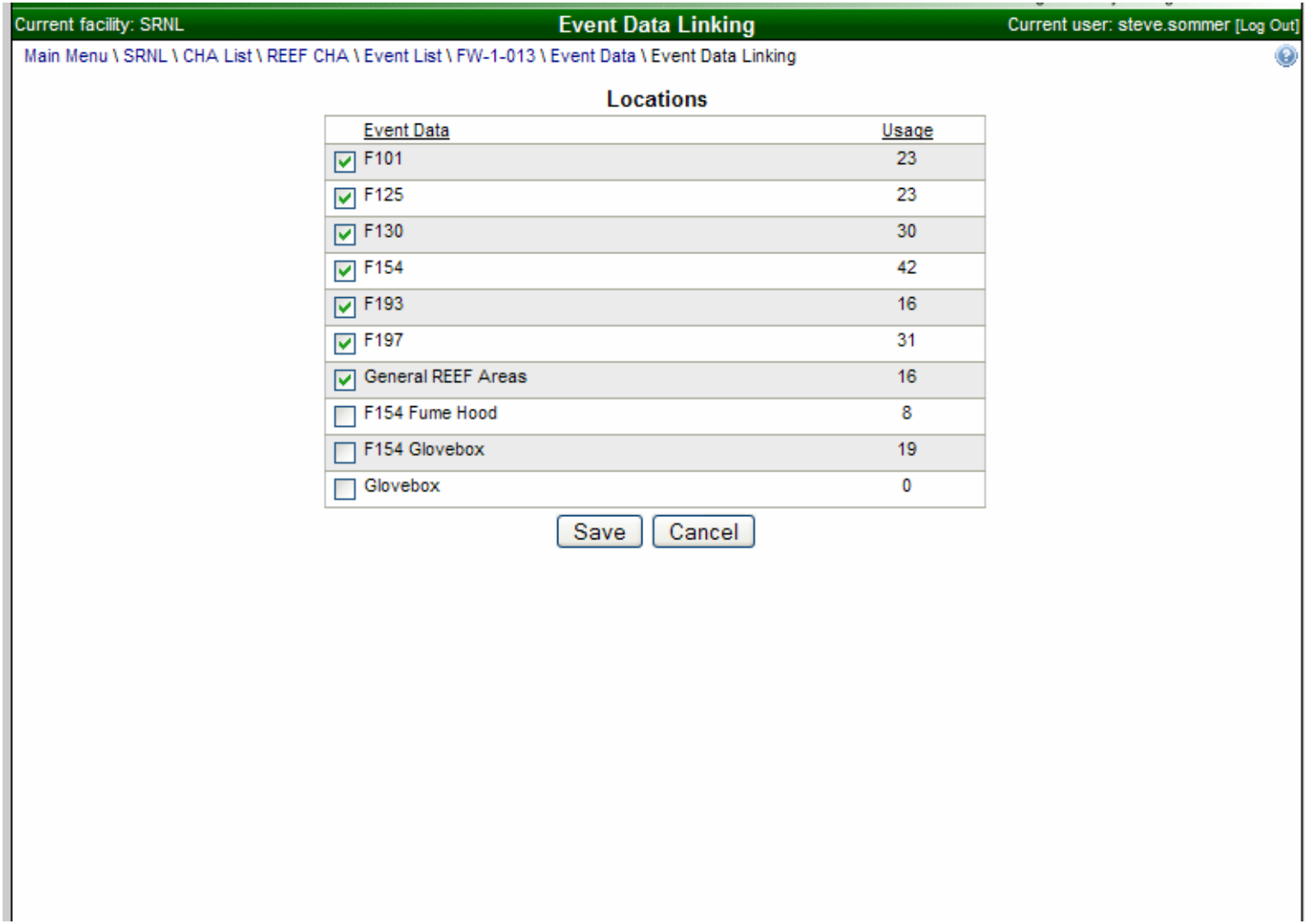


Figure 6 - Location Linking.

This storage and linking capability helps both the efficiency and consistency of HAs. Any previously stored data is available for reuse without the need to "search the table" for the desired information. Additionally, once the information is stored, then the analyst can relate that information to one or more events and the information is always stated the same. This same capability is available for most of the data such as MAR, causes, release mechanisms, references, and assumptions.

Unmitigated frequency and consequences (Figure 7 - Event Evaluation Detail) must be specified by the analyst. The frequency and consequence acronyms identified in the risk scheme are available for the analyst's selection. eCHAP uses the analyst's selections to determine the risk ranking for each specific hazard type and receptor in accordance with the risk matrices that were established in the risk scheme. Therefore, if a frequency or consequence is changed at a later date then the applicable risk ranking is automatically updated to reflect the user's changes.

Returning to Figure 4 - Hazard Table, this screen also provides the analyst the means to identify new controls or to select previously stored controls. Two stacked columns are provided to display the preventive engineered and administrative controls and another two stacked columns are provided to display the mitigative preventive and administrative controls.

eCHAP provides the analyst the means to add and remove controls from the event and to further specify their application (Figure 8 - Edit CHA Event Related Control). New controls are stored for linking to other events. The specific details of a control may vary with the event to which it is applied so eCHAP provides this capability. For instance, a control may be identified as safety-significant for one event because of that event's consequences. For an event with low or negligible consequences that same control could be linked without the safety-significant designation.

The first blue background column displays any controls that the analyst selects as safety-class or safety-significant controls for this event. A second blue background column displays the resulting mitigated consequences for this event. The data in these two blue columns is affected by analyst selections in the yellow background columns (i.e., unmitigated frequency, consequences, and controls).

Step 3

The third step, as currently configured in eCHAP, is hazard identification. Here the analyst relates each MAR and cause identified to a standard hazards list (Figure 9 - Hazard Identification). This configuration will be modified in the future such that hazard identification is a precursor to HA. The purpose here is to relate each cause or MAR to one or more standard hazards. Step 4 will use this information to ensure that the complete spectrum of events has been analyzed.

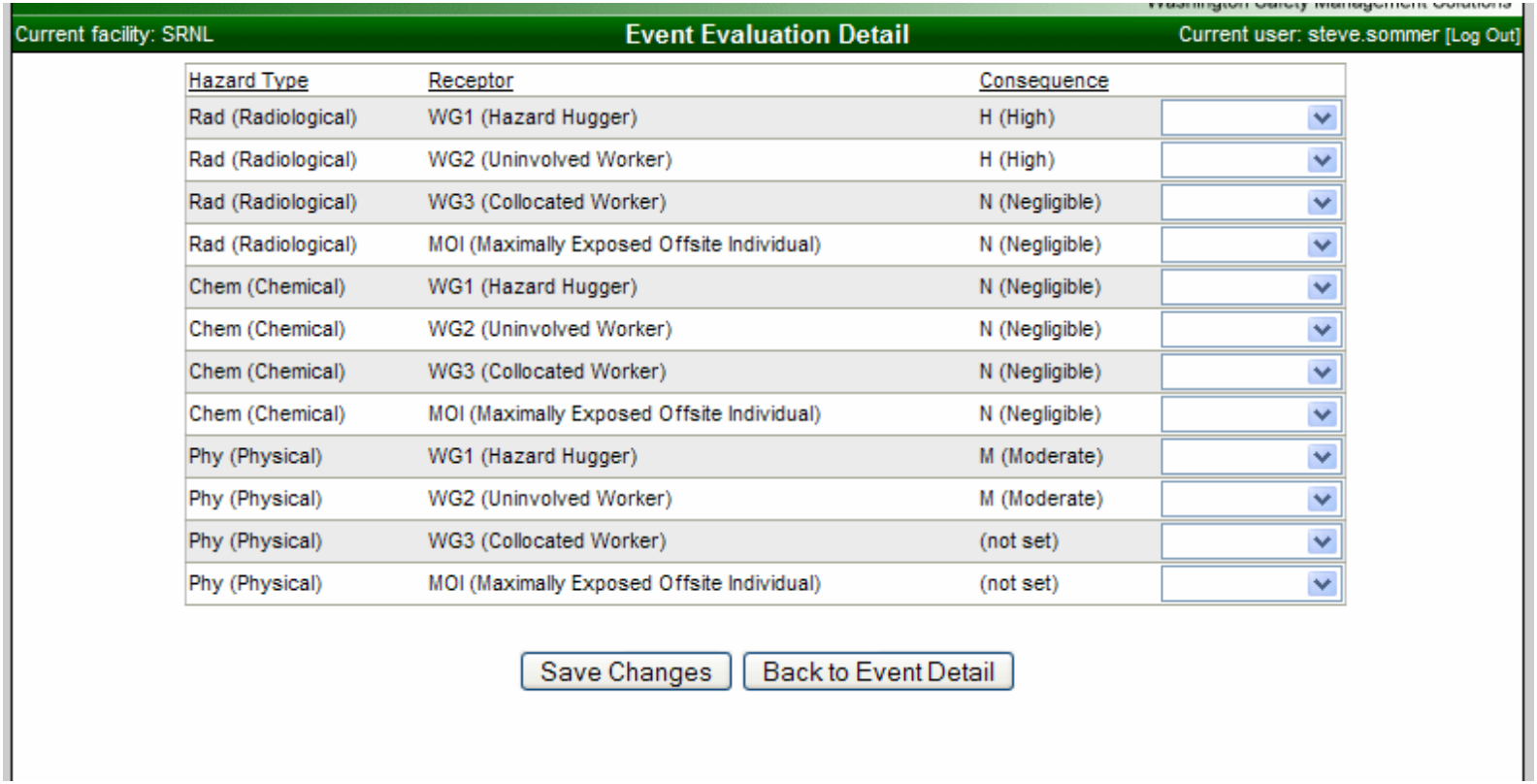


Figure 7 - Event Evaluation Detail.

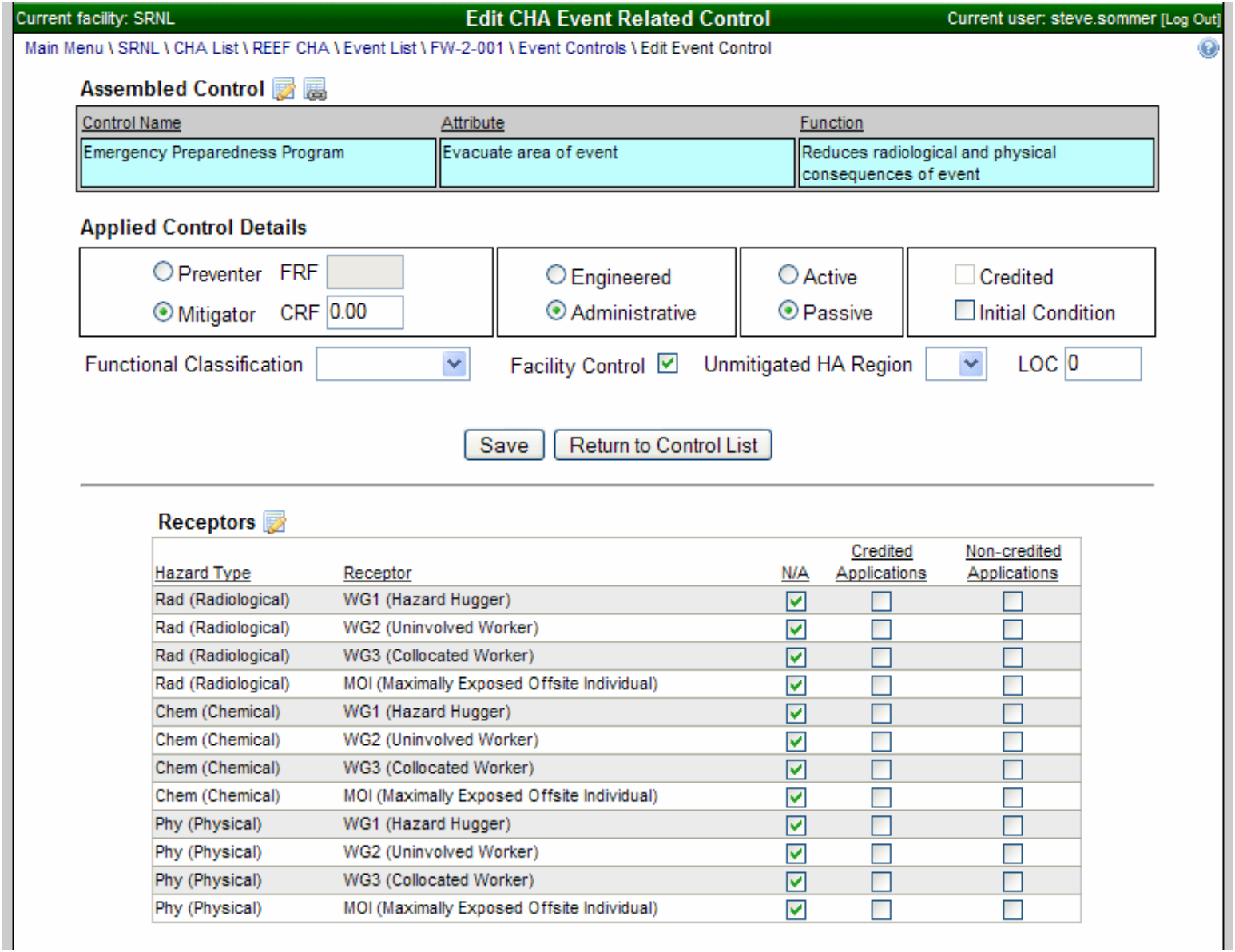


Figure 8 - Edit CHA Event Related Control.

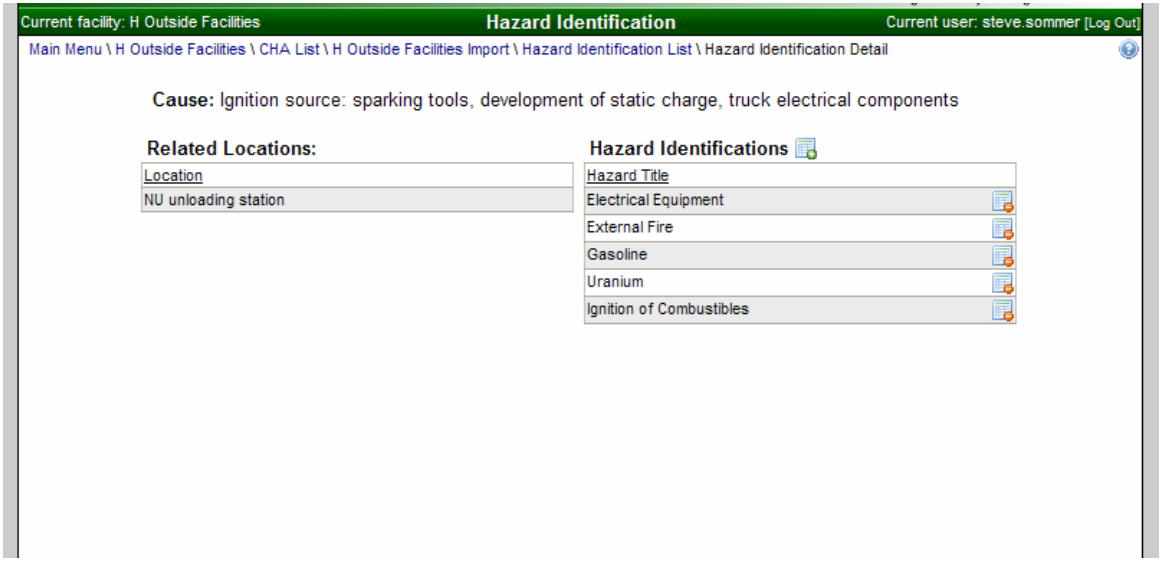


Figure 9 - Hazard Identification.

Step 4

The fourth step is hazard review. Here the analyst can review the data assembled during Step 3 above to verify that the entire spectrum of events has been addressed. This screen (Figure 10 – Hazard) will indicate all the hazards that have been developed into at least one event and will also indicate the hazards that have not been developed (Figure 11 - Hazards without Related Events). The hazards which have not been related can be reviewed for applicability, standard industrial hazard, or the need to develop an event to address the hazard.

Step 5

The fifth step is event bounding evaluation (Figure 12 - Event Bounding Evaluation). Using this screen, the analyst can review all the events of a specific event type (e.g., fire, explosion) against all the other events of the same type. The analyst can determine if the event of interest, event in top portion of screen, is “bounded” by any of the events in the lower portion of the screen. The analyst must consider both the consequences and the control sets of both events. If the analyst determines that the event of interest is “bounded” by the other event, the analyst sets the “Bounded By” drop-down to the other event and documents their decision. The analyst completes this exercise for each event.

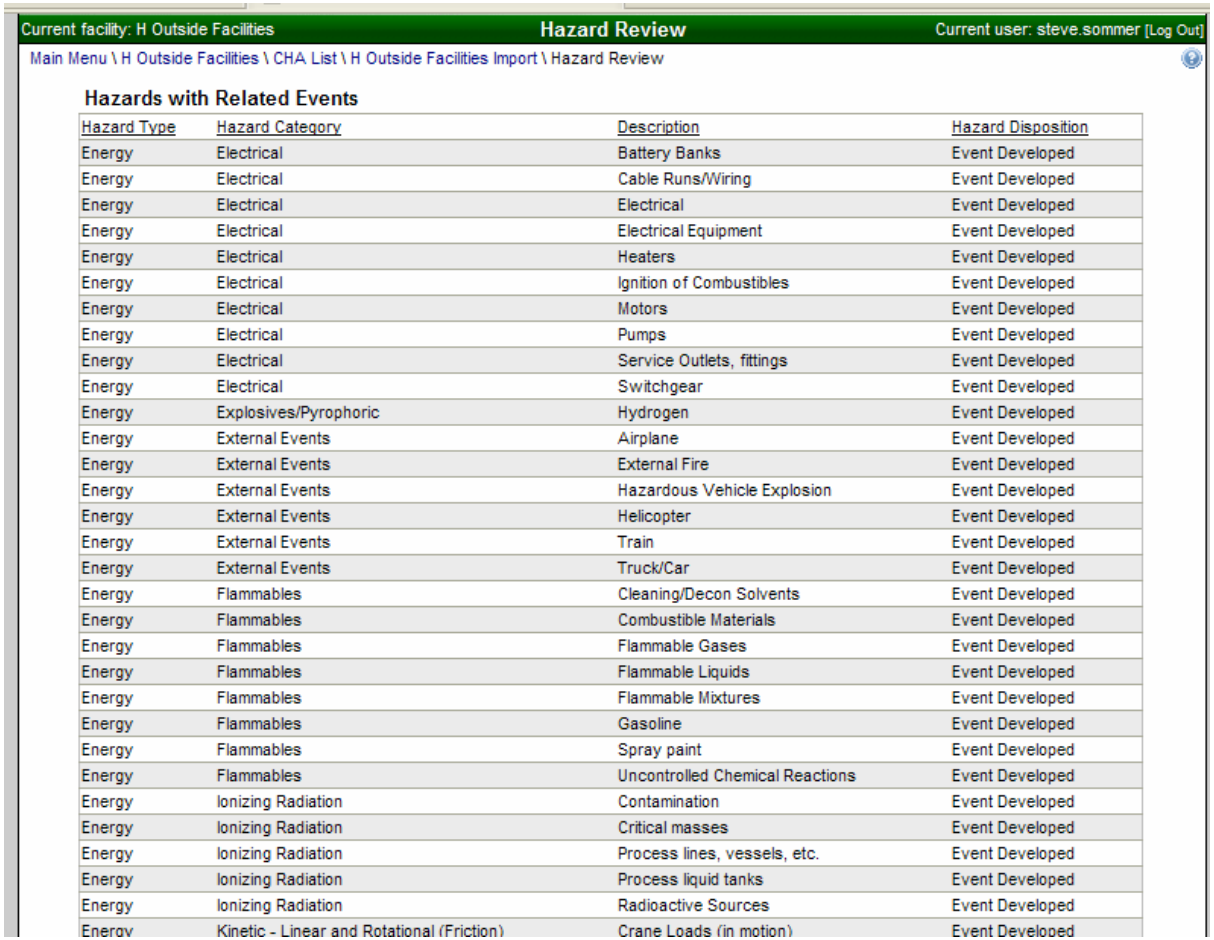
The consequences of the “bounding” event should bind the consequences of the events which it bounds. However, the control sets may not be the same. Therefore, the control sets should be reviewed to ensure that the bounding event control set binds the control sets of the bounded events. If the control set is not bounded, then the event is not bounded.

Step 6

The sixth step is credited control evaluation (Figure 13 - Credited Control Specification). The purpose of this exercise is to examine the credited controls for their susceptibility to failure. Controls that are susceptible to failure may need to be replaced with a less susceptible control or the control may need one or more other controls to lessen the susceptibility of the control. For instance, a tank may be credited for containing waste material. If the tank is considered to be susceptible to failure, then an additional tank inspection program may be appropriate. The software would provide the means to quickly add the inspection program to the overall control set.

Step 7

The seventh step is credited control specification (Figure 14 - Credited Control Specification). The purpose here is to review the controls that have been selected in order to identify where and how the controls will be discussed in the DSA and the TSRs. A basic outline of these chapters, or sections thereof, can be generated from this data. Each outline would be provided to the DSA and TSR writers for preparation of their documents.



Current facility: H Outside Facilities | Hazard Review | Current user: steve.sommer [Log Out]

Main Menu \ H Outside Facilities \ CHA List \ H Outside Facilities Import \ Hazard Review

Hazards with Related Events

Hazard Type	Hazard Category	Description	Hazard Disposition
Energy	Electrical	Battery Banks	Event Developed
Energy	Electrical	Cable Runs/Wiring	Event Developed
Energy	Electrical	Electrical	Event Developed
Energy	Electrical	Electrical Equipment	Event Developed
Energy	Electrical	Heaters	Event Developed
Energy	Electrical	Ignition of Combustibles	Event Developed
Energy	Electrical	Motors	Event Developed
Energy	Electrical	Pumps	Event Developed
Energy	Electrical	Service Outlets, fittings	Event Developed
Energy	Electrical	Switchgear	Event Developed
Energy	Explosives/Pyrophoric	Hydrogen	Event Developed
Energy	External Events	Airplane	Event Developed
Energy	External Events	External Fire	Event Developed
Energy	External Events	Hazardous Vehicle Explosion	Event Developed
Energy	External Events	Helicopter	Event Developed
Energy	External Events	Train	Event Developed
Energy	External Events	Truck/Car	Event Developed
Energy	Flammables	Cleaning/Decon Solvents	Event Developed
Energy	Flammables	Combustible Materials	Event Developed
Energy	Flammables	Flammable Gases	Event Developed
Energy	Flammables	Flammable Liquids	Event Developed
Energy	Flammables	Flammable Mixtures	Event Developed
Energy	Flammables	Gasoline	Event Developed
Energy	Flammables	Spray paint	Event Developed
Energy	Flammables	Uncontrolled Chemical Reactions	Event Developed
Energy	Ionizing Radiation	Contamination	Event Developed
Energy	Ionizing Radiation	Critical masses	Event Developed
Energy	Ionizing Radiation	Process lines, vessels, etc.	Event Developed
Energy	Ionizing Radiation	Process liquid tanks	Event Developed
Energy	Ionizing Radiation	Radioactive Sources	Event Developed
Energy	Kinetic - Linear and Rotational (Friction)	Crane Loads (in motion)	Event Developed

Figure 10 – Hazards with Related Events.

Hazard Review

Hazard Type	Hazard Category	Description	Disposition	
Energy	Electrical	Diesel Generators	(Not Set)	
Energy	Electrical	High Voltage	(Not Set)	
Energy	Electrical	Locomotive, electrical	(Not Set)	
Energy	Electrical	Loss of Facility Power	(Not Set)	
Energy	Electrical	Other	(Not Set)	
Energy	Electrical	Power Tools	(Not Set)	
Energy	Electrical	Shock	(Not Set)	
Energy	Electrical	Transformers	(Not Set)	
Energy	Electrical	Transmission Lines	(Not Set)	
Energy	Electrical	Underground Wiring	(Not Set)	
Energy	Explosives/Pyrophoric	Caps	(Not Set)	
Energy	Explosives/Pyrophoric	Dusts	(Not Set)	
Energy	Explosives/Pyrophoric	Dynamite	(Not Set)	
Energy	Explosives/Pyrophoric	Electric Squibs	(Not Set)	
Energy	Explosives/Pyrophoric	Explosive Chemicals	(Not Set)	
Energy	Explosives/Pyrophoric	Explosive Gas	(Not Set)	
Energy	Explosives/Pyrophoric	Liquid Oxygen	(Not Set)	
Energy	Explosives/Pyrophoric	Nitrates	(Not Set)	
Energy	Explosives/Pyrophoric	Other	(Not Set)	
Energy	Explosives/Pyrophoric	Peroxides	(Not Set)	
Energy	Explosives/Pyrophoric	Potassium	(Not Set)	
Energy	Explosives/Pyrophoric	Primer Cord	(Not Set)	
Energy	Explosives/Pyrophoric	Propane	(Not Set)	
Energy	Explosives/Pyrophoric	Pyrophoric	(Not Set)	
Energy	Explosives/Pyrophoric	Sodium	(Not Set)	
Energy	Explosives/Pyrophoric	Super oxides	(Not Set)	

Figure 11 - Hazards without Related Events.

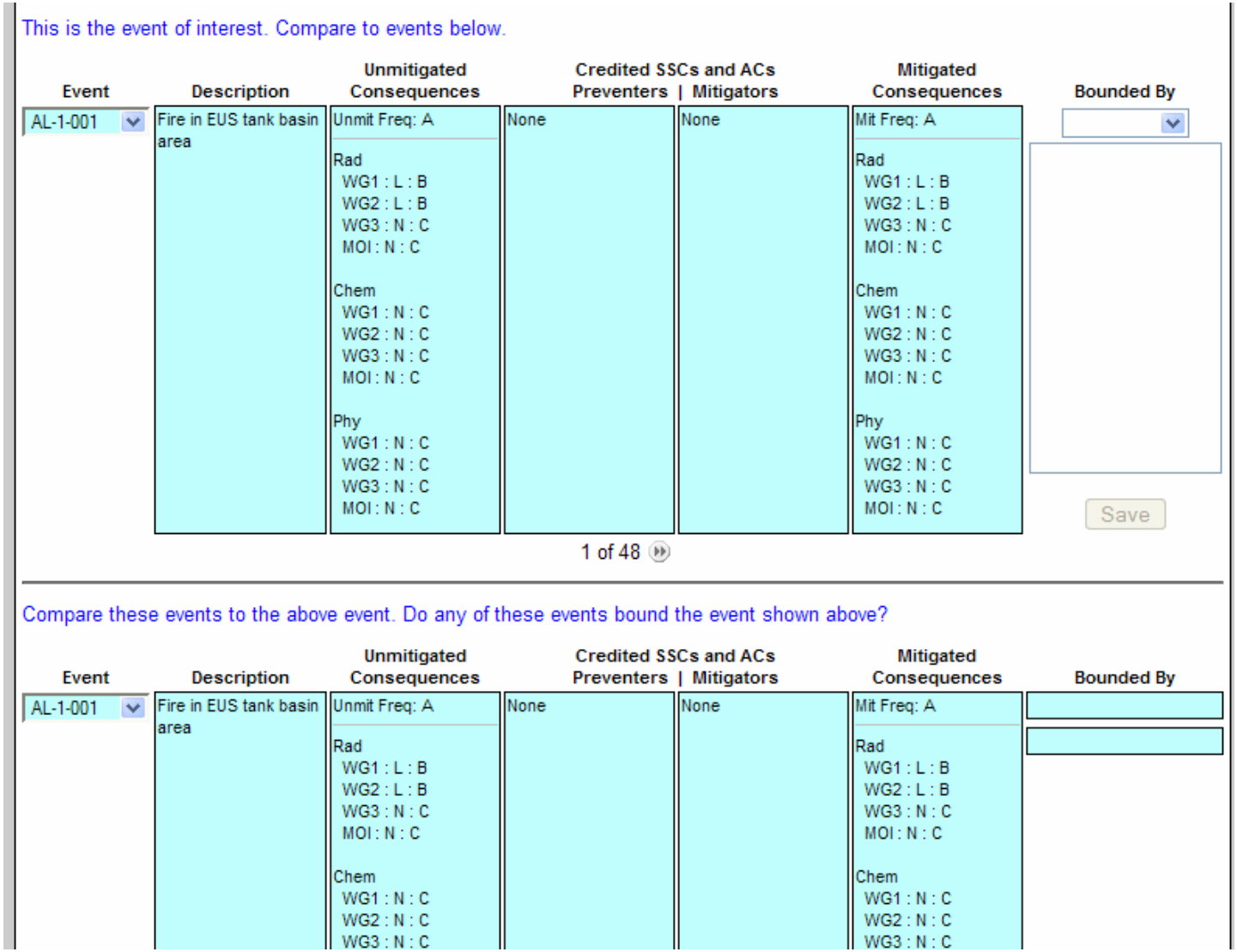


Figure 12 - Event Bounding Evaluation.

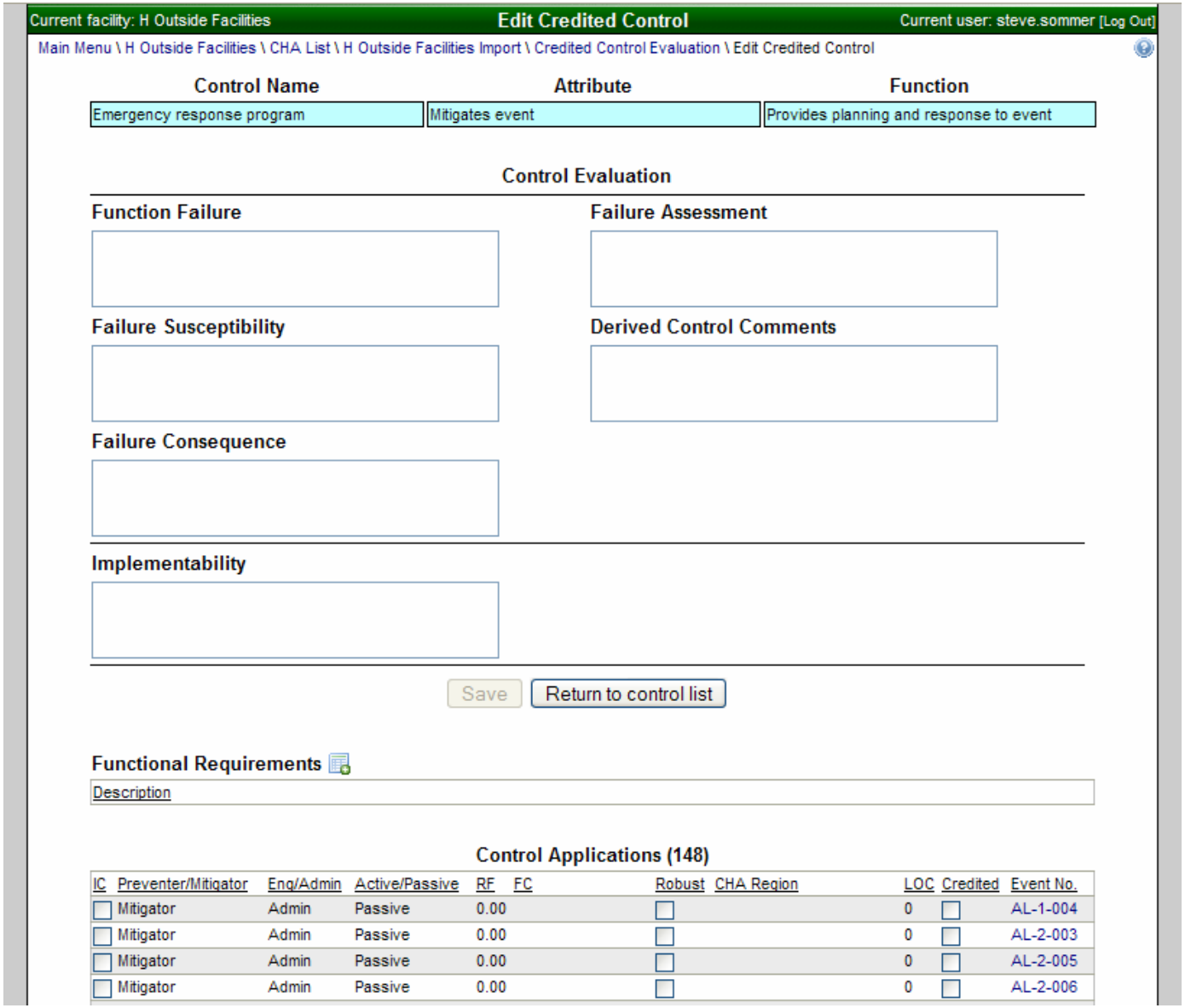


Figure 13 - Credited Control Specification.

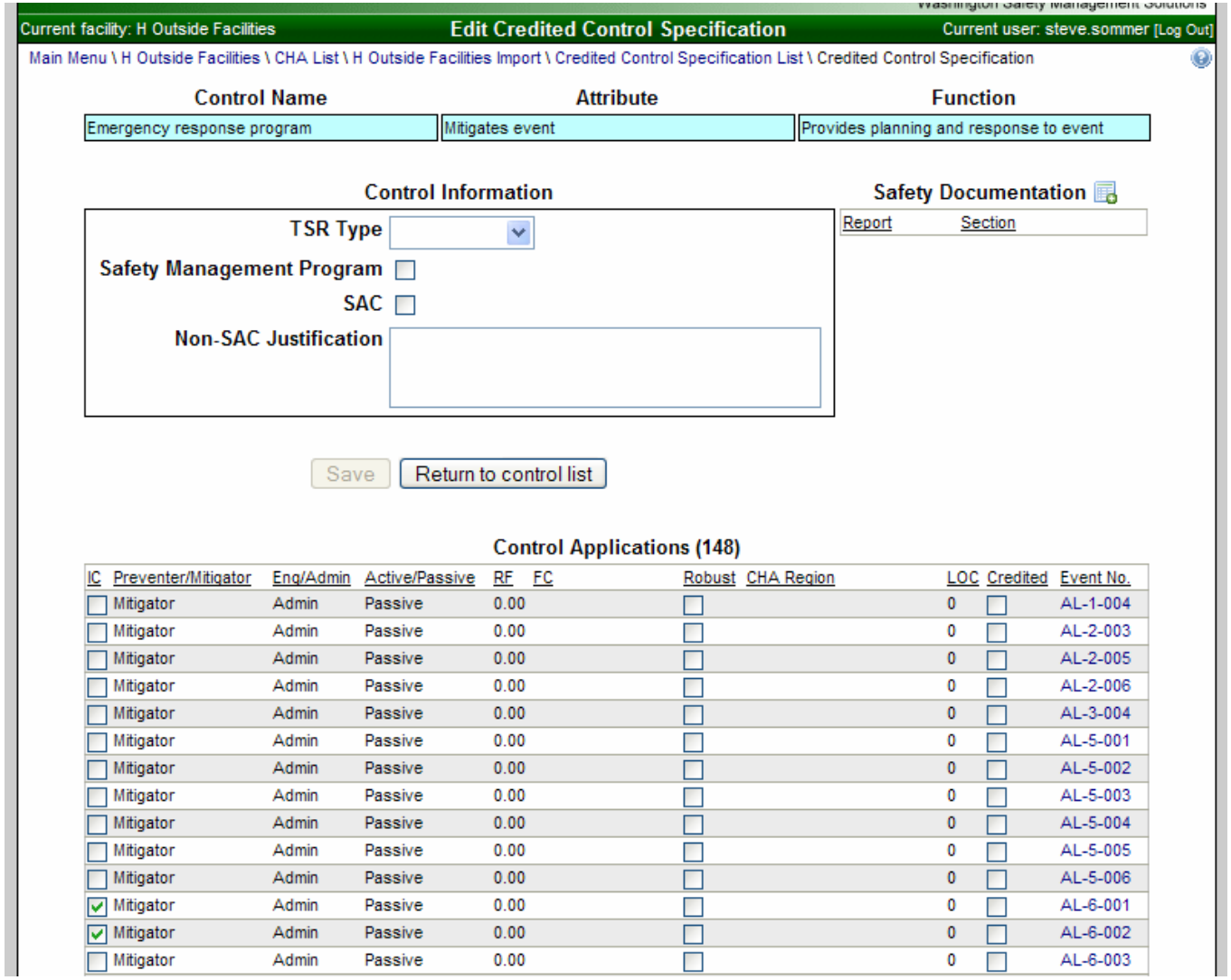


Figure 14 - Credited Control Specification.

Since data is stored during the entire development process then the analyst can "review" specific sets of data and remove any identified inconsistencies. The Event Data Cleanup screen (Figure 15 - Event Data Cleanup) provides the means to do this. In this example, a portion of the various identified causes are listed. The analyst can review these causes and replace duplicates or similar causes with one cause of the analyst's choosing. The analyst can then remove the unused causes from the file.

This process improves the consistency of the document and the method improves the efficiency of finding and correcting these inconsistencies. eCHAP was designed with the intent of being adaptable to various risk schemes such that the same software could handle performance of HAs at multiple DOE sites. In addition, minimal effort would be required to set up another DOE site with eCHAP that would interact with their computer servers.

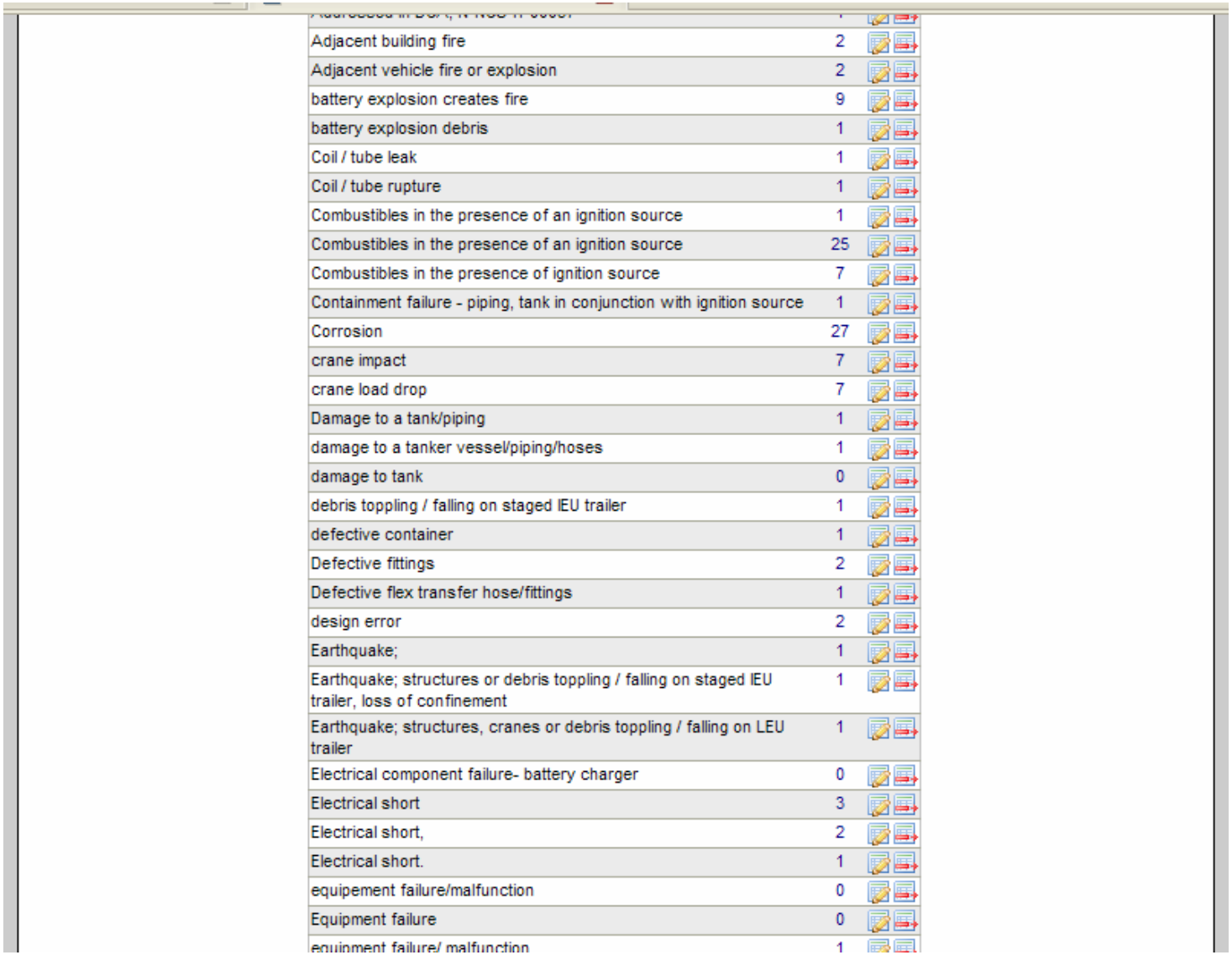
eCHAP provides a tool for recording the data derived during the HA process and does not perform any calculations on that data. Similar to a Microsoft Word or Excel table, the analyst is responsible for the data reported from the software. Therefore, eCHAP has been designated as NQA-1, Level D.

eCHAP is web-based and therefore, information security was considered in its development. The eCHAP database is maintained on a secure server and is user name and password protected.

Multiple users can simultaneously access eCHAP. The web-site provides simple access and use of HA data from multiple secure locations. User feedback is captured in the database which is then used to enhance the product over time.

CONCLUSION

The HA process and the incorporation of that data into DSAs and TSRs has been an inefficient process that contains inconsistencies in large respect due to the tools (i.e., Microsoft Word or Excel) being used. In addition, without a standard platform for performing HAs, analysts tend to develop unique patterns and characteristics in the performance and documentation of their work. To alleviate these issues, a team of experts was selected to review the various criteria and established requirements. Software was developed in accordance with these requirements, tested, and released for use at SRS. While various issues are being worked, eCHAP has received praise and recognition for improving the HA process.



Adjacent building fire	2
Adjacent vehicle fire or explosion	2
battery explosion creates fire	9
battery explosion debris	1
Coil / tube leak	1
Coil / tube rupture	1
Combustibles in the presence of an ignition source	1
Combustibles in the presence of an ignition source	25
Combustibles in the presence of ignition source	7
Containment failure - piping, tank in conjunction with ignition source	1
Corrosion	27
crane impact	7
crane load drop	7
Damage to a tank/piping	1
damage to a tanker vessel/piping/hoses	1
damage to tank	0
debris toppling / falling on staged IEU trailer	1
defective container	1
Defective fittings	2
Defective flex transfer hose/fittings	1
design error	2
Earthquake;	1
Earthquake; structures or debris toppling / falling on staged IEU trailer, loss of confinement	1
Earthquake; structures, cranes or debris toppling / falling on LEU trailer	1
Electrical component failure- battery charger	0
Electrical short	3
Electrical short,	2
Electrical short.	1
equipement failure/malfunction	0
Equipment failure	0
equipment failure/ malfunction	1

Figure 15 - Event Data Cleanup.