Preventing recurrence of industrial control system accident using assurance case

Mirko Napolano[2], Fumio Machida[1], Roberto Pietrantuono[2], Domenico Cotroneo[2]
[1]*Knowledge Discovery Research Laboratories, NEC Corporation, Kawasaki, Japan*
[2]*Dipartimento di Ingegneria Elettrica e delle Tecnologie dell'Informazione (DIETI) - Università degli Studi di Napoli Federico II, Via Claudio 21, 80125, Naples, Italy*

mi.napolano@studenti.unina.it, f-machida@ab.jp.nec.com, {roberto.pietrantuono, cotroneo}@unina.it

***Abstract* – Lessons learned from accident experiences in safety-critical infrastructures are valuable not only for the organizations operating the infrastructures but also for third-party organizations developing or operating similar safety-critical infrastructure systems. While such accident knowledge is often reported after rigorous investigations of the accidents, learning from the knowledge and applying them to improve other systems is not a trivial issue, since the report is not structured for such a purpose. In this paper, we present a method to elucidate the accident knowledge by assurance case consisting of structured arguments and evidence. We introduce a new assurance case pattern and create a post-failure safety case that argues over the avoidance of a similar accident. The effectiveness of the proposed method is evaluated through a case study concerning the PG&E accident in SCADA system.**

***Keywords* – assurance case, assurance case pattern, accident recurrence prevention, event and causal factor analysis, knowledge management.**

I. INTRODUCTION

Critical infrastructure systems, such as power grids, gas pipelines, water supplies, communication and transportation services are essential for human lives and a wide variety of social activities. Such systems are recently getting smarter and more efficient with the aid of software and communication networks. Accordingly, they may confront new types of threats such as the increasing number of software bugs, network disconnections, security attacks, failure propagation to other systems and so on. Although complete avoidance of system failures or accidents in these rapidly-evolving infrastructures is almost impossible to achieve, infrastructure providers should strive to reduce the risk as much as possible during their design and operation. Whenever the provider encounters an undesirable accident, it is crucial to analyze its causes and improve the system design and operations so as to ensure that similar failures will never occur in the future.

Independent public agencies like the National Transportation Safety Board (NTSB), European Aviation Safety Agency (EASA), and Japan Transport Safety Board (JTSB) are in charge of investigating accidents that occur in several industry domains. Such agencies spend many months to reconstruct the events and assess the causes by involving a variety of entities (usually companies, regulators and emergency bodies). At the end of this process, reports are published along with accident narrative, system descriptions, lessons learned, and a list of recommendations for the stakeholders. This source of information, so-called accident knowledge, is useful not only for the concerned system provider, but also for third-party organizations to improve their systems and to potentially avoid similar accidents in the future. Nonetheless, the list of recommendations, which contains very important information, is addressed to the concerned companies and regulators, but it is usually difficult for third-party engineers to use such unstructured information. Moreover, the list of recommendations may not cover all the necessary measures to the identified accident causes and hence engineers need to carefully go through the whole documents that must be a very expensive time-consuming task.

In this paper, we propose a method to analyze the mishaps from the accident reports, extract the causes, and provide a structured way to present the accident knowledge. The elucidation of the accident knowledge is performed through an *accident causation model* and an *assurance case*, which is a structured argumentation supported by a body of evidence. In order to guide the assurance case composition, we propose a new assurance case pattern, which has an analogous structure to the Hazard Avoidance Pattern [5].We discuss the advantages of our approach by comparing its application with the use of the list of recommendations presented in the accident reports. The comparative evaluation is carried out on a case study dealing with a Supervisory Control And Data Acquisition (SCADA) system, which monitors and manages a gas pipeline. The main contributions of this paper are threefold. First, we propose a new approach to structure reusable accident knowledge using assurance cases. Second, in order to guide the composition of assurance case for preventing recurrence of an accident, we define a new assurance case pattern called *Accident Recurrence Prevention Pattern*. Third, we show the advantages of the proposed approach through the real accident case compared to the published accident reports. In particular,

the understandability of the accident knowledge, its reusability and the effectiveness of causations are evaluated.

The rest of the paper is organized as follows. Section II briefly introduces assurance cases. Section III explains the proposed approach to create assurance case for arguing accident recurrence prevention. Section IV presents the case study and shows the instance of accident recurrence prevention case. The advantages of the proposed approach are discussed in Section V. Finally, Section VI gives our conclusion.

II. ASSURANCE CASE

A safety case is a structured argumentation composed by claims and supported by evidence aimed at demonstrating the safety of a system [1]. It is widely used as a way to demonstrate that a system is acceptably safe. The concept of safety case has been generalized and formalized in a detailed and rigorous standard as *assurance case* [2][3]. An assurance case is defined as a structured argument, supported by evidence, intended to justify that a system has specific attributes, such as reliability, availability, or safety. In this way, it is possible to use a method of reasoning and arguments to demonstrate the validity of the top-level claim, whose context is not necessarily related to safety.

It is usually difficult to follow an argumentation just by reading the textual inferences deriving from claims, arguments, and evidence. In order to clearly explain and describe safety cases and assurance cases, a graphical notation method is commonly used. Goal Structuring Notation (GSN) [4] is one of the commonly accepted notations, where an argument is represented by a directed graph in which each node represents an element of the argumentation and each link represents their relationships. Even resorting to such a helpful notation method, arguing safety and describing the arguments as a safety case are time-consuming complicated tasks, especially when the target system is huge and complex. To assist the argument process, we may use patterns of safety argument which are extracted from past safety arguments. Safety case patterns [5] are introduced as "a means of documenting and reusing successful safety argument structures". The format of the safety case pattern is considered in [6] and the formalization of the pattern is proposed in [7]. In the research area of safety cases, many studies addressed the issue of effective composition of safety cases by reusing or improving previous cases. A strategy to create assurance cases by retrieving and reusing previous similar works is presented in [8]. Safety case lifecycle is discussed in [9][10] in which a pre-failure safety case is revised through a failure analysis to produce an enhanced post-failure safety case.

Safety case were originally developed for assuring plant safety for the chemical industry [11]. The application domains of safety and assurance cases are expanding to railway systems [12][13], defence systems [1], nuclear plants [14], automotive functional safety [15] and medical devices [16]. Safety cases are sometimes required to comply with the safety standards like Def Stan 00-56 [1][17] and Yellow Book [19]. A survey on the use of safety cases in safety-critical industries is provided in [20][21]. Regardless of the application domains, an initial version of safety/assurance case is assumed to be created in the early stages of system development lifecycle. In this paper, we exploit assurance cases for the purpose of assuring accident recurrence prevention, where any earlier assurance cases are not necessary. To the best of our knowledge, this is the first work to present a guide to construct an assurance case aiming at accident recurrence prevention after experiencing an accident.

III. ASSURANCE OF ACCIDENT RECURRENCE PREVENTION

To avoid similar accidents in different periods, both in the concerned infrastructure and also in other organizations, we aim to use assurance cases to describe the accident in a structured manner. The authors in [9] and [10] use both the pre-failure safety case and the information from the accident to perform a failure analysis in order to provide lessons and recommendations, and to build a more accurate post-failure safety case. Our work is based on the different assumption that there is no pre-failure safety case for the target system that experienced an accident. The reasons supporting this assumption are the following: 1) the system could be too old and many upgrades have been applied during its life-cycle, with studies and assessment not well related among them; 2) another company, which has been commissioned to improve the actual system, could not access the previous information for the sake of confidentiality or unavailability of data; 3) the system could be too complex to be completely assured by a safety case in all of its parts or functions. The lack of documented safety arguments in most digital systems is also confirmed in [10] where the author proposes a way to derive them retroactively.

Based on the above assumption, we propose an approach to create a post-failure assurance case which aims to avoid accident recurrence in the future. The overview of the proposed approach is shown in Figure 1.

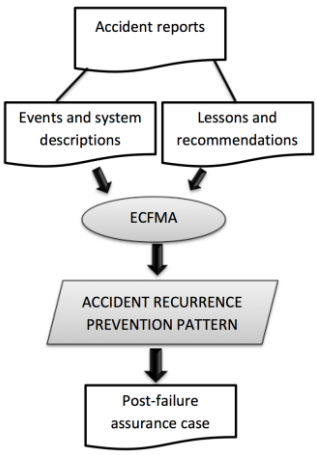

Figure 1. Conceptual schema of the proposed approach

Failure analysis is conducted using the reports published by public investigative agencies. From these documents, not only agencies' lessons and recommendations but also events and system descriptions are used to determine the accident causes. The analysis is performed through two steps. In the first step, Event and Causal Factor Mitigation Analysis (ECFMA) is used

to reconstruct the events, discover the causes and insert possible solutions. In the second step, the results from ECFMA are structured with arguments and claims in an assurance case, which is guided by a new pattern named "Accident Recurrence Prevention Pattern". ECFMA and the new assurance case pattern are detailed in the following subsections.

A) ECFMA

In order to reconstruct events and to determine the causes of a mishap, investigative boards need to use accident causation models. Event and Causal Factor Analysis (ECFA) [22] is one of the most common causation models. This model and analysis method is originally developed by the US Department Of Energy (DOE) and is widely used for describing the events, conditions and identifying accident causes. The first step is to collect information about events and decisions and plot them on a timeline. As the event timeline is established, the related conditions and information are linked to the events and decisions. After this process, investigators need to determine, among the conditions in place, which one has not been adequate for the situation. They should identify the particular condition that originated the unsafe situation. This results to be a hazard in the mishap, namely "causal factor", which either caused the accident (root cause, direct cause) or did not mitigate a hazardous situation (contributory cause). The result of this process is called ECF chart.

Since ECFA is just an accident causation model, it does not help provide countermeasures and solution to the elimination or mitigation of the discovered hazards. Thus, we extend ECFA to associate countermeasures with the corresponding causal factors and name it as Event and Causal Factor Mitigation Analysis (ECFMA). In ECFMA, a countermeasure is represented by a "solution" element. By directly connecting it to the corresponding causal factor in the ECF chart, we can make a basis of causation model with countermeasures, which is used for making arguments on how to avoid this mishap in the next step. An example of the ECFMA is shown in Figure 2.

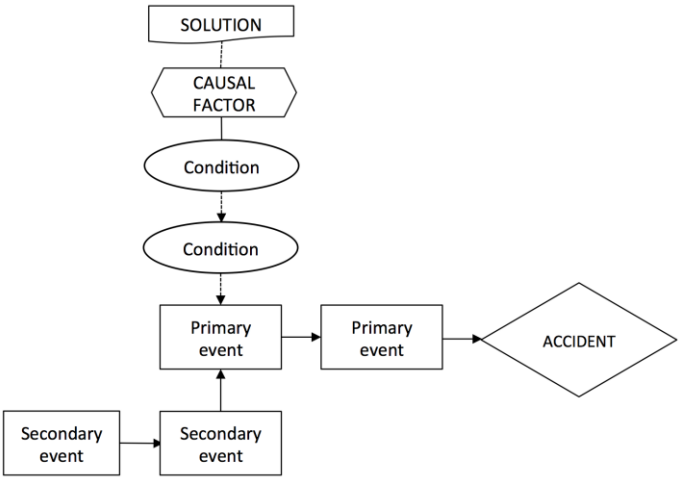

Figure 2. Example of ECFMA

By adding the solution elements to the assessed causal factors, a complete depiction of events, conditions, causes and mitigations is available in the same artifact. This is an intermediate step towards the elucidation of the accident knowledge. In fact, as we will show in the next sections, the instantiation of the assurance case pattern is performed by using causal factors and solution elements.

B) Accident Recurrence Prevention Pattern

The second step of our method is the construction of an assurance case from the results of ECFMA in order to structure the acquired knowledge through an argumentation.

Looking at the pattern catalogue for safety cases [5], the "Hazard Avoidance Pattern" is found as the most suitable pattern for our scope. This pattern aims to argue that the system is safe proving that every identified hazard has been mitigated or eliminated. However, it is too generic to our objective, since it does not provide claims about the solutions to the discovered hazards and it can be used only in the highest level of a safety case. For these reasons, we have built a new assurance case pattern, called "*Accident Recurrence Prevention Pattern*", which is specific for the accident cases.

The pattern is described using GSN as shown in Figure 3. In this pattern, the intent is to argue that a specific accident, which could cause severe consequences if the hazards are not correctly addressed, can never reoccur in the future by showing the addressing of the identified hazards. In order to create a new pattern, we have followed the principle and the format presented in [5] and [6]. For each of the identified hazards, solutions supported by evidence are provided to justify the top-level claim. It can be used either as stand-alone or as a support for a higher-level safety case in which the safety is assured by showing the satisfaction of safety system requirements and/or how different identified accidents can be avoided.

Since our goal is to assure that a similar accident can never happen again in the future, we have chosen, as top-level claim, the statement "*Accident X can never reoccur using system Y*". Context elements about the system operating role and the accident are added to the top-level claim to help focus on the problem. A sub-claim that better clarifies the top-level claim follows: it states that "*All possible hazards in accident Y have been addressed*". The attached context element is used to list all the hazards discovered through the reports and analyses. The assumption "*All possible hazards in accident Y have been identified*" might be supported by evidence like the accident reports published after the rigourous accident investigation.

After this, we need to develop the strategy. In this case, as in the Hazard Avoidance Pattern, the strategy is an "argument over each hazard". So, we need to specify that "*each hazard W has been mitigated or eliminated*". Differently from other patterns, the argumentation continues through the addressing of each hazard by showing the specific proposed solution.

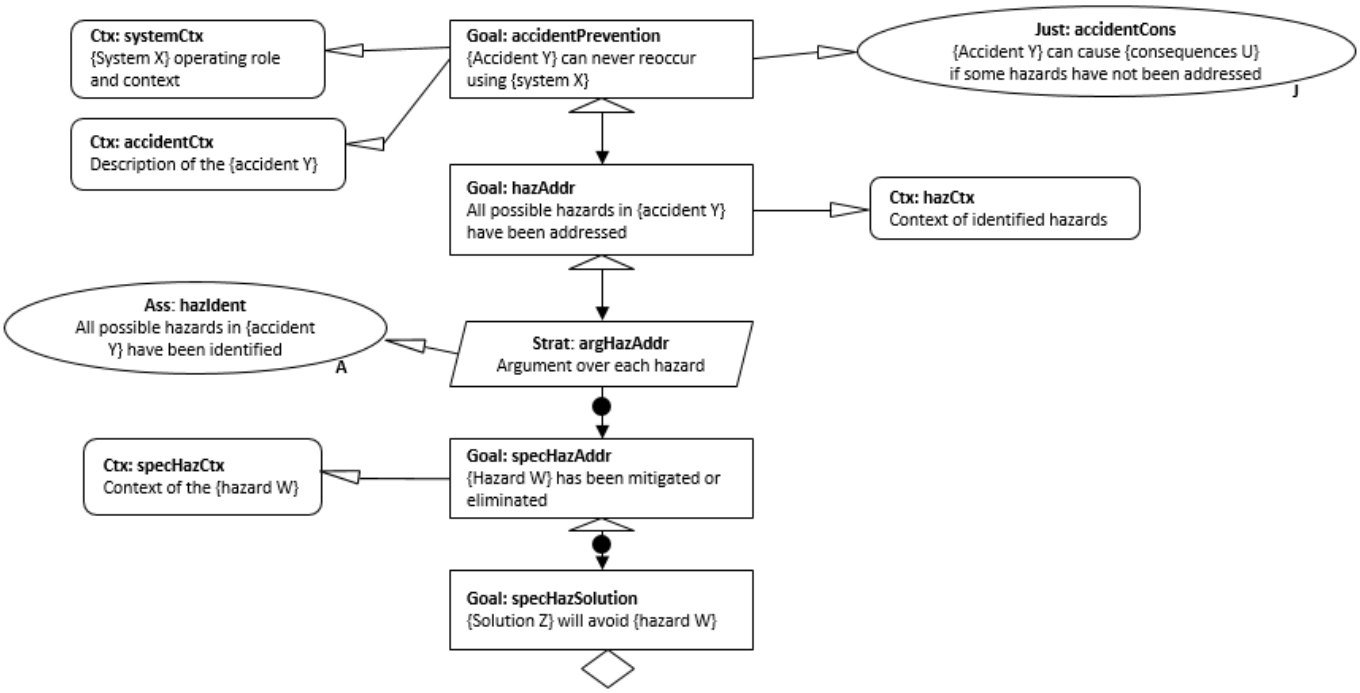

Figure 3. Accident Recurrence Prevention Pattern

In this phase, we can use the results of the ECFMA, where solutions have been already structured and related to the problems. The claim "*Solution Z will avoid hazard W*" is constructed from this information. Once the pattern is instantiated, the evidence need to be provided and attached to prove that the solutions are effective.

C) Post-failure assurance case

Conducting ECFMA followed by Accident Recurrence Prevention Pattern, we can create a post-failure assurance case which argues about the prevention of similar accidents in the future. Indeed, this post-failure assurance case gives reusable accident knowledge in a structured representation. Engineers who are not involved in this accident can also understand the causations of the accident and the corresponding countermeasures more easily than reading thoroughly the published accident reports. Moreover, context elements are introduced to set the place of both the accident occurrence and the system role. In this way, whoever needs to determine whether the accident is relevant for its purpose can easily have a look at the context elements before reusing and applying the provided mitigations.

IV. CASE STUDY

To illustrate how the proposed method works in practise, we apply the method to the PG&E accident in SCADA system.

A) PG&E accident

We reviewed the accident report about the San Bruno PG&E's pipeline explosion (September 9, 2010). In this case, as a result of an electrical maintenance work in a station along the pipeline, an overpressure in the pipeline has been generated causing the rupture of a segment of the pipe. The released natural gas ignited, resulting in an explosion that destroyed 38 homes and damaged 70. Eight people were killed, fifty-eight were injured and many more were evacuated from the area.

Pacific Gas and Electric Company (PG&E) is one of the major providers of natural gas in California. In order to manage a so big and complex gas pipeline, the company uses a SCADA system. Human operators can manage the system to remotely monitor and control the movement of gas through the whole pipeline. Typically, a SCADA system consists of a control center, several field instrumentations and a communication infrastructure. All the data regarding the pipeline are collected by the field equipment and sent to the control center using the communication infrastructure. From the center, operators can monitor parameters such as flow rates, pressure levels, equipment status, control valve positions and alarms indicating abnormal conditions. Along each line of the gas pipeline, three kind of valves are used: regulating control valves, which are electrical actuated and controlled valves whose set point can be programmed remotely by operators; monitor control valves, which are stand-alone pneumatically actuated valves whose set point can be changed only manually; manual valves, which can be used by the technicians on the field.

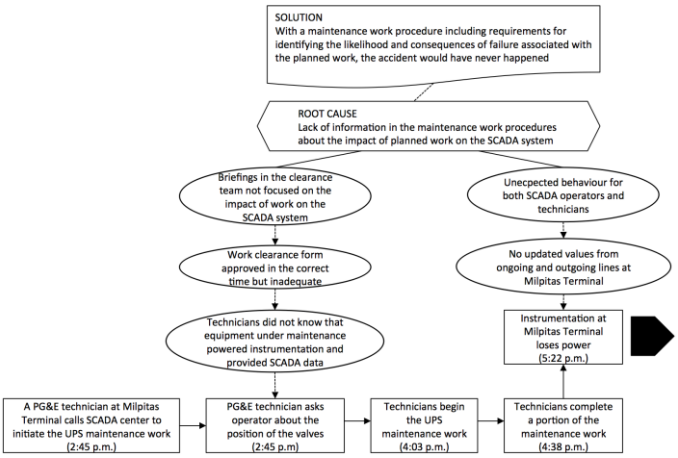

Figure 4. Initial part of the PG&E case's ECFMA

TABLE 1. HAZARDS AND SOLUTIONS IN PG&E CASE

Hazard	Type	Solution
Lack of information in the maintenance work procedure	Root cause	Procedure considering the consequences on SCADA system
Loss of power for regulating valves	Direct cause	Use of separate circuit breakers and new power supplies
Inappropriate fail-safe mode	Contributory cause	Use of close fail-safe mode
Absence of RCV	Contributory cause	Installation of RCV along all the pipeline

We have performed the accident causation analysis using the report issued by the National Transportation Safety Board (NTSB) [23]. Since the resulted ECFMA chart is too big to be completely reported, an excerpt of the results from the ECFMA is shown in Figure 4. Several problems in the SCADA system have been identified using the NTSB report and then, according to our method, organized through the ECFMA. The causes and the proposed mitigations have been summarized in TABLE 1.

The identified root cause has been the lack of information in the maintenance work procedures about the impact of the planned work on the SCADA system. The direct cause of the rupture was the failure of power supplies during the electrical maintenance in a station along the pipeline that triggered an overpressure in the pipeline. Contributory causes in the accident were the inadequate open fail-safe mode, which is activated when a loss of control for the valves occurs, and the absence of Remote Control Valves (RCV), which could have given SCADA operators the ability to mitigate the overpressure by closing the valves. The proposed solutions were, respectively: 1) a maintenance work procedure including requirements for identifying the likelihood and consequences of planned work on SCADA system; 2) the use of separate circuit breakers and new power supplies in the station; 3) the use of close fail-safe mode; 4) the installation of RCVs along all the lines.

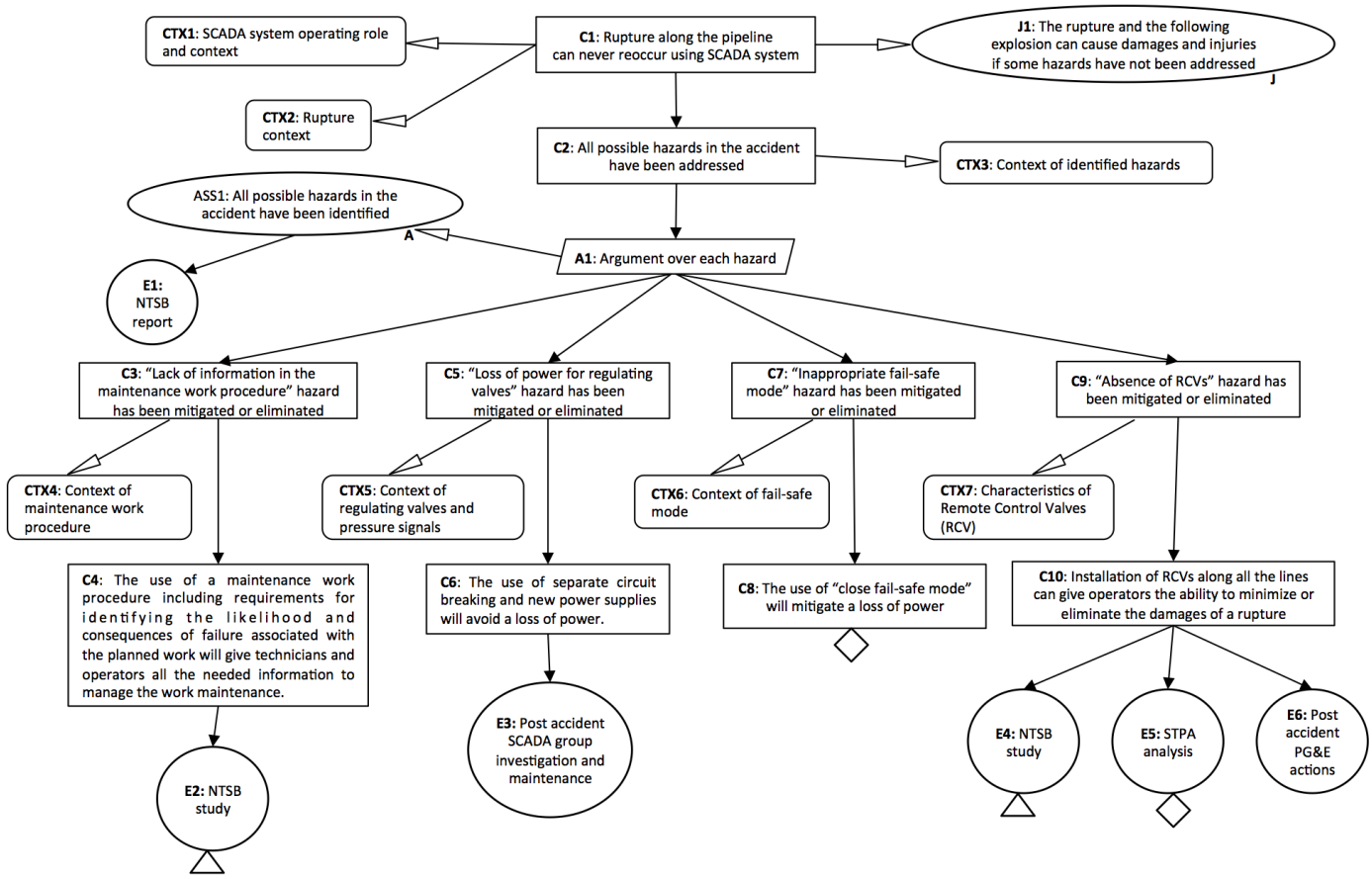

Figure 5. PG&E accident assurance case

The bird's view of the instantiated assurance case is shown in Figure 5. The instantiation of the assurance case pattern is performed using problems and solutions identified during the previous ECFMA analysis. Using "the solution" element in the enhanced chart, we are able to relate them to the problems so as to ease the instantiation of the assurance case pattern. In fact, once all the causal factors and the solutions are assessed, we just replace the elements "hazard" and "solutions" in the pattern with the discovered causal factors and solutions. As evidence, both qualitative and quantitative elements are provided to support the argumentation. Since we do not have the capability to perform a thorough and full analysis on a real system, we attach possible evidence that engineers can use to prove the proposed solutions. This is a common practise when, at a certain stage of safety case development, some elements remain uninstantiated or undeveloped [24]. In some cases, we provide, as evidence, studies that had not been implemented by the concerned company (i.e. NTSB study on RCVs).

V. EVALUATION

In this section we summarize the advantages of our approach using the results from PG&E case study. We compare the assurance case for accident recurrence prevention with the original recommendation report. First, we investigate some quantitative measures of the assurance case and the recommendation report. Due to the structual difference, the assurance case and the recommendation report are not directly comparable by these metrics, but they may provide some implications for clarifying the difference.

To characterize the complexity of the descriptions in the recommendation reports, readability should be considered as a measure. In terms of text readability, the most used metrics are the scores obtained through the Flesch-Kincaid Readability Tests [25] which measure the difficulty to read a text in English by taking into account the number of words, sentences and syllables. The formula for the Flesch Reading Ease Score (FRES) is defined as below:

$$FRES = 206.835 - 1.015\left(\frac{total\ words}{total\ sentences}\right) - 84.6\left(\frac{total\ syllables}{total\ words}\right)$$

The resulting value ranges from 0 to 100: the higher the score, the better the readability.

We calculate the FRES from the report published by NTSB. In the PG&E case the score is 26 The result indicates that the report is not easy to read compared with common text. Since the primary objective of these recommendation reports is to clearly report the accident event and specify the recommendations, they do not care the readability so much. However, in order to extract the knowledge from the reports and apply them for other cases, the understandability of the knowledge is highly influenced by the readability as well.

Instead of solely relying on text, assurance cases can be represented by graphical compact notation by GSN. The basic characteristics of the assurance case can be computed by the number of nodes representing claims, assumptions, justification, arguments and evidence, and the number of links. The number of nodes and links in the accident recurrence prevention case for PG&E accident are 26 and 25, respectively. They are not directly comparable with the size of the recommendation report, but, considering the pages of the recommendation report, searching the information from the assurance case could be easier than retrieving the same information from the entire reports. TABLE 2 summarizes those quantitative measures for the recommendation report and the assurance case.

TABLE 2. QUANTITATIVE MEASURES OF RECOMMENDATION REPORT AND ASSURANCE CASE

		PG&E accident
Recommendation report	Pages	153
	Sections	96
	Levels of sections	4
	Words	61603
	Sentences	2197
	Flesch Reading Ease Score (FRES)	26
Assurance case	Nodes	26
	Links	25

In order to quantitatively compare our approach with the use of recommendations, we introduce some metrics by considering the structure of the reports and assurance case. The recommendation reports are organized in tree structure, since the documents are divided into sections, subsections and paragraphs. The assurance case has also a tree structure as it is composed by nodes at different levels. Starting from this point, we have introduced some metrics to evaluate understandability, reusability and effectiveness.

A) Understandability

Understandability can be qualitatively defined as "the quality of information which makes it understandable by people with reasonable background knowledge of business and technical activities". We measure the understandability of both report and assurance case by focusing on the references to the mitigations and the distance between hazards and the provided mitigations. Two metrics can be characterized:

1. The number of direct links from the description about hazard to the description about the corresponding mitigation
2. The average number of hops over the tree structure from the description about hazard to the description about the corresponding mitigation

TABLE 3. UNDERSTANDABILITY QUANTIFICATION

		PG&E accident
#1: Direct links from hazard to mitigation	***Recommendation report***	0/4
	Assurance case	4/4
#2: Average hops from hazard to mitigation	***Recommendation report***	24.5
	Assurance case	1

TABLE 3 summarizes the computed understandabilities. Regarding metric #1, for each hazard we have analyzed the references to the solution inserted in the investigative

documents. In the report, hazards are described in a specific paragraph, while solutions for the mitigation or elimination of the hazard are usually provided in other parts of the report itself. In many cases there are no references to the paragraph describing the hazard. On the other hand, in our assurance case pattern, identified hazards have direct relationship with the corresponding mitigations by link from claim "specHazAddr" to the claim "specHazSolution".

Concerning metric #2, for each hazard we have measured the hops from the paragraph describing the hazard to the paragraph showing the corresponding mitigation by counting the number of paragraphs. In PG&E report the average number of hops from hazard to mitigation is 24.5, However, in our assurance case pattern, the argumentation over how each hazard can be mitigated or eliminated is developed through just one hop, which makes the argument easier to follow.

B) Reusability

Reusability is the ability of an item to be used repeatedly. In order to reuse the identified hazard in the safety analysis for another system, the context information of the hazard is very important so that engineer can judge whether the hazard is applicable to the target system. We have quantified this property in a way similar to the understandability assessment, by focusing on the references to the context. Again, two metrics can be defined:

1. The number of direct links from the description for recommendation to the description about the corresponding hazard
2. The number of hops from the description for recommendation to the description about the corresponding hazard context

TABLE 4 summarizes these reusability metrics. For metric #1, we have analyzed the recommendations to search for references to the context. Recommendations do not provide any references or pointers to the corresponding scenario or context. In fact, recommendations are typically described in a general form such that descriptions about real accident including context and causes are omitted or abstracted. They are useful for summary, but are too abstract for engineers who try to learn and reuse the hazards and the mitigations. On the other hand, assurance case provides a structured body in which general hazard is associated with the concrete problem encountered in the accident by the link between "specHazCtx" and "specHazAddr". This greatly helps decision of hazard reuse.

TABLE 4. REUSABILITY QUANTIFICATION

		PG&E accident
#1: Links from recommendations to hazard context	***Recommendation report***	0/4
	Assurance case	4/4
#2: Hops from mitigation to hazard context	***Recommendation report***	31.25
	Assurance case	2

For metric #2, similarly to the understandability study, we have counted the hops from the paragraph describing the mitigation to the paragraph describing the hazard. In PG&E report the average number of hops is 31.25, In our assurance case pattern, starting from "specHazSol", which describes the general mitigation, it is possible to contextualize the solution by "jumping back" to the "specHazCtx" within two hops. In this way, the time spent for contextualizing the hazard can be reduced by using the references included in the context element.

C) Effectiveness

We have evaluated the effectiveness of our method by comparing the problems solved by the recommendations and the problems worked out by our approach. As indicated in the NTSB Investigative process, which is one of the most important investigative board in the world, safety recommendations "are based on the findings of investigation, and may address deficiencies which do not pertain directly to what is ultimately determined to be the cause of the accident" [26]. It means that they address mainly underlying problems and organizational deficiencies. TABLE 5 summarizes the number of mitigated hazards by recommendation reports and our approach.

TABLE 5. EFFECTIVENESS RESULTS

		PG&E accident
Number of mitigated hazards	***Recommendation reports***	2
	ECFMA+AC	4

In the PG&E case, two identified hazards have been addressed in the final recommendations, namely the lack of information in the maintenance work procedure and the absence of RCVs. On the other hand, our approach provides two more hazard mitigations which are presented in the reports but not in the recommendation list.

With these two case studies, we have shown that the list of recommendations is not enough to cover all the causes and avoid a similar accident. It means that third-party engineers using directly the final list of recommendations would not be aware of the other hazards and problems, even if they are described in other parts along the report. Instead, our approach aims to work out all the causes analyzing all the knowledge provided by the reports (events narrative, system descriptions and analyses, recommendations). In this way, we can eliminate both organizational deficiencies and technical problems, so as to avoid both specific problems experienced in the accident and potential hazards that have not turned up in the episode.

VI. CONCLUSION

Accident knowledge is valuable for infrastructure providers who need to improve the design and operations of their mission-critical infrastructures. Structuring the knowledge extracted from the accidents or failures are practically important to effectively apply the knowledge to prevent similar accidents in the same and even in different

organizations. In this paper, we presented a method for reusing and elucidating the accident knowledge gained from safety-critical infrastructure systems by using assurance case.. Through the PG&E case study, we showed the effectiveness of the presented approach and compared the understandability and reusability with the original recommendation reports.

In our case study we considered the instantiation of the Accident Recurrence Prevention Pattern without claiming about any system's property like safety. The pattern can be used to instantiate a sub-part of a higher-level assurance case, which may demonstrate the fulfillment of a property (i.e. safety, reliability, etc.) by arguing over both the addressing of system requirements and the non-recurrence of common accidents. Besides, evaluating the performance while applying the approach to further real cases would allow the validation of the efficiency of our approach. For instance, by measuring the time spent for retrieving the knowledge and reusing it to other system, we can further investigate the efficiency. These aspects can be incorporated in the future work.

REFERENCES

[1] "Ministry of Defence, Defence Standard 00-56 Issue 4 : Safety Management Requirements for Defence Systems - Part 1: Requirements", June 2007

[2] "IEEE Standard Adoption of ISO/IEC 15026-1 - Systems and Software Engineering - Systems and Software Assurance - Part 1: Concepts and Vocabulary", November 2014

[3] "IEEE Standard Adoption of ISO/IEC 15026-2:2011 - Systems and Software Engineering - Systems and Software Assurance - Part 2: Assurance Case", September 2011

[4] "GSN Community Standard Version 1", November 2011, http://www.goalstructuringnotation.info

[5] Timothy Kelly, "Arguing Safety: A Systematic Approach to Managing Safety Cases", Ph.D. thesis, University of York, 1998

[6] Timothy Kelly, John A. McDermid, "Safety Case Construction and Reuse Using Patterns", in proceedings of *16th Intemational Conference on Computer Safety and Reliability (SAFECOMP97)*, Springer, 1997

[7] Ewen Denney, Ganesh Pai, "A Formal Basis for Safety Case Patterns", in proceedings of *32nd International Conference on Computer Safety, Reliability and Security (SAFECOMP 2013)*, LNCS 8153, pp. 21-32, September 2013

[8] Alejandra Ruiz, Ibrahim Habli, Huàscar Espinoza, "Towards a Case-Based Reasoning Approach for Safety Assurance Reuse", in proceedings of *Next Generation of System Assurance Approaches for Safety-Critical Systems Workshop (SASSUR 2012)*

[9] William S.Greenwell, Elisabeth A.Strunk, John C.Knight, "Failure Analysis and the Safety-Case Lifecycle", 2004

[10] William S.Greenwell, "Pandora: An Approach to Analyzing Safety-Related Digital-System Failures", Ph.D. thesis, University of Virginia, 2007

[11] "The Offshore Installations (Safety Case) Regulations 1992 (S.I. 1992/2885)", January 1992

[12] UK Health and Safety Executive (HSE), "Railways (Safety Case) Regulations 1994 (HSI 1994/237H)", March 1994

[13] UK Health and Safety Executive (HSE), "Railways (Safety Case) Regulations 2000 (SI 2000/2688)", 31 December 2000

[14] UK Health and Safety Executive (HSE), "Safety Assessment Principles for Nuclear Facilities", December 2006, http://www.hse.gov.uk/nuclear/SAPs/SAPs2006.pdf

[15] International Organization for Standardization (ISO), "ISO 26262: Road vehicles – Functional safety, DIS 2010-07-09", 2010

[16] U.S. Food and Drug Administration (FDA), "Infusion Pumps Total Product Life Cycle – Guidance for Industry and FDA Staff", Issue December 2, 2014, http://www.fda.gov/ucm/groups/fdagov-public/@fdagov-meddev-gen/documents/document/ucm209337.pdf

[17] Ministry of Defence, Defence Standard 00-56 Issue 2: "Safety Management Requirements for Defence Systems", December 1996.

[18] MoD, Defence Standard 00-56: Safety Management Requirements for Defence Systems, Ministry of Defence, Defence Standard, Issue 2, December 1996.

[19] Rail Safety and Standards Board, "Engineering Safety Management: the Yellow Book – Volumes 1 and 2: Fundamentals and Guidance", Issue 4, 2007

[20] The Health Foundation, "Evidence: Using safety cases in industry and healthcare", December 2012

[21] The Health Foundation, "Supplements to Evidence: Using safety cases in industry and healthcare", December 2012

[22] "U.S. Department Of Energy (DOE) Handbook – Accident and Operational Safety Analysis, Volume 1: Accident Analysis Techniques", July 2012, http://energy.gov/sites/prod/files/2013/09/f2/DOE-HDBK-1208-2012_VOL1_update_1.pdf

[23] "Pacific Gas and Electric Company Natural Gas Transmission Pipeline Rupture and Fire: NTSB Pipeline Accident Report", August 30, 2011

[24] S. Nair, J.L. de la Vara, M. Sabetzadeh, L.C. Briand, "An extended systematic literature review on provision of evidence for safety certification", Information and Software Technology Volume 56, Issue 7, July 2014

[25] Kincaid, J.P., Fishburne, R.P., Rogers, R.L., & Chissom, B.S. "Derivation of New Readability Formulas (Automated Readability Index, Fog Count, and Flesch Reading Ease formula) for Navy Enlisted Personnel", Research Branch Report 8-75. Chief of Naval Technical Training: Naval Air Station Memphis, 1975

[26] U.S. National Transportation Safety Board (NTSB), "The Investigative Process", http://www.ntsb.gov/investigations/process/Pages/default.aspx