Preprints of the Federated Conference on
Computer Science and Information Systems pp. 1435–1441

Studying Interrelationships of Safety and Security for Software Assurance in Cyber-Physical Systems: Approach Based on Bayesian Belief Networks

Andrew J. Kornecki
Embry Riddle Aero University
600 S. Clyde Morris Blvd
Daytona Beach, Florida, USA
Email: kornecka@erau.edu

Nary Subramanian
The University of Texas at Tyler
3900 University Blvd
Tyler, Texas, USA
Email: nsubramanian@uttyler.edu

Janusz Zalewski
Florida Gulf Coast University
10501 FGCU Blvd
Ft. Myers, Florida, USA
Email: zalewski@fgcu.edu

***Abstract*— The paper discusses mutual relationships of safety and security properties in cyber-physical systems (CPS). Generally, safety impacts the system's environment while environment impacts security of a CPS. Very frequently, safety and security of a CPS interact with each other either synergistically or conflictingly. Therefore, a combined evaluation of safety and security that considers their interrelationships is required for proper assessment of a CPS. Bayesian Belief Networks (BBN) can be used for this evaluation where factors related to safety and security of a CPS are assumed to be randomly distributed. The result of this evaluation is an assessment that is non-deterministic in nature but gives a very good approximation of the actual extent of safety and security in a CPS. Using a case study of a SCADA system in an oil pipeline control, the authors present a BBN approach for assessing mutual impacts of security and safety violations. This approach is compared with the Non-Functional Requirements approach (NFR), used previously, which is largely qualitative in nature. This study demonstrates that the BBN approach can significantly complement other techniques for joint assessment of safety and security in CPS.**

I. Introduction

MODERN industrial computer systems are a complex combination of hardware and software. In addition, with the proliferation of the Internet, they are all becoming interconnected, which gave rise to the term cyber-physical systems (CPS), reflecting the fact that embedded computers are interfaced to physical devices and make them accessible in the cyberspace.

The ease of interconnectivity raises a number of previously unknown issues in the design and operation of safety-critical CPS, which are now exposed to security vulnerabilities and related threats. Thus, relevant problems are being addressed by respective professional communities. For example, recent discussions between aviation professionals engaged in the work of RTCA Special Committee SC205 [1] dedicated to the software aspects of airborne systems certification (safety focus) and SC216 [2] dealing with aviation systems security, brought us an interesting perspective. The two committees came up with two sets of guidelines for industry developing aviation systems discussing these issues somehow independent from each other.

Thus, industry faces enormous challenges when designing and implementing software-intensive safety and security related systems exposed to abundant networking environments. The critical observation of this paper is that some aspects of integration of complementary views existing in specific domains are inadequate and exhibit lack of required system and process thinking.

The paper presents a perspective on joint, integrated treatment of safety and security properties in cyber-physical systems, with a potential for quantitative analysis of their interrelationships to provide software assurance, i.e., to achieve a required level of confidence that software systems and services function in the intended manner, are free from accidental or intentional vulnerabilities, provide security capabilities appropriate to the threat environment, and recover from intrusions and failures [3]. Our conjecture is that security and safety can be addressed jointly to measure their mutual impact on system trustworthiness and on each other.

The rest of the paper is structured as follows. Section 2 outlines some previous studies on joint treatment of safety and security, Section 3 introduces the case study of an oil pipeline control system, Section 4 discusses our approach, based on Bayesian belief networks, and Section 5 derives some conclusions.

II. Safety and Security

A. Common Perspective

From the technical perspective, in cyber-physical systems, critical system properties, such as security, safety, reliability, etc., cannot be treated in isolation from each other. In industrial applications, with a control system in charge of the technological process, typically safety was considered a critical property. Computer systems were

This project has been funded in part by a grant SBAHQ-10-I-0250 from the U.S. Small Business Administration (SBA). SBA's funding should not be construed as an endorsement of any products, opinions, or services. The second and third authors gratefully acknowledge the AFRL 2011 and 2012 Summer Faculty Fellowships, in Rome Labs.

designed such that the behavior of computer software or hardware would not endanger the environment in a sense that equipment's failure would cause death, loss of limbs or large financial losses.

On the other hand, the security of industrial computer control systems was typically limited to the physical plant access and off-line protection of data. With the miniaturization of computing devices, growing sophistication of control, and with the advent of the Internet, multiple functions of industrial control systems have become accessible online, which opened doors to enormous security threats. Thus, to increase trustworthiness of industrial computer systems, security concerns have to be taken into account and the mutual relationships of safety and security have to be studied and reconciled.

B. Background

Several industries have attempted to address related issues, for example, railways [4], chemical [5], off-shore [6], automation [7], nuclear [8], and industrial control [9]. Since the publication of a seminal paper by Burns et al. [10], around three dozen papers have been published discussing jointly safety and security issues, recently summarized in [11]. Since then, a more comprehensive review of related issues has been published [12].

Boyes, based on his 25 years of industry experience, discussed the problems of vulnerability of critical infrastructure due to the increasing interactions with external networks [13]. The question posed is whether or not the safety system built on top of the control system is not only safe but also secure. He identified situations when security violations may lead to safety violation and thus related incidents resulting even in some fatalities. He observed that security issues must be considered in safety implementation in any process plant, just as safety issues must be considered when administering conventional information technology security issues.

However, there seem to be only a few studies that aim at assessing both properties in a comprehensive manner, including an impact, which one might have on another in the same system. For example, the OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) framework [14] provides a checklist-based approach to evaluate safety and security in an organization; however, explicit analysis of tradeoffs between these properties is left to the judgment of evaluators.

Metrics-based approaches can be used to compute safety and security quantitatively: for example, Fenton's [15] causal/explanatory model which uses factors to determine metrics can perhaps be applied in the context of cyber-physical systems as well. Likewise, ATAM, the Attribute Tradeoff and Analysis Method [16], develops a utility tree to capture factors involved in analyzing a design. Again, the tradeoff analysis is mostly implicit. The NFR Approach, where NFR stands for Non-Functional Requirements, allows explicit joint analysis of safety and security properties [17]-[18], by using a goal-orientation. This approach is essential for the current research and described in detail in the next section.

III. NON-FUNCTIONAL REQUIREMENTS APPROACH

The Non-Functional Requirements (NFR) approach is a goal-oriented technique that can be applied to determine the extent to which specific objectives are achieved by a design. The NFR considers properties of a system such as reliability, maintainability, and usability, and could equally well consider functional objectives and constraints for a system. Thus the NFR approach can be applied to evaluate whether a specific design satisfies safety and security requirements for the system.

The NFR approach uses a well-defined ontology that includes softgoals, contributions, and propagation rules [17]. The graph that captures the softgoals, their decompositions, and the contributions is called the Softgoal Interdependency Graph (SIG). The approach relies on a qualitative assessment based on the concept of the contribution "satisficing" positively or negatively the softgoals resulting in determination of the network softgoals to be satisficed or denied.

Subramanian and Zalewski recently applied the NFR [18] to evaluate safety and security of an example cyber-physical system: a typical oil pipeline control SCADA based system (Figure 1) at the Center for Petroleum Security Research (CPSR) [19]. Such system consists of the Master Station and Remote Terminal Units (RTU) connected directly to field instruments measuring pressure and rate of flow of the oil. The field instruments also contain shutoff valves that can change the rate of flow or the pressure. The RTU's communicate with a central master via Ethernet, satellite, cable, cellular phones, or fiber optics.

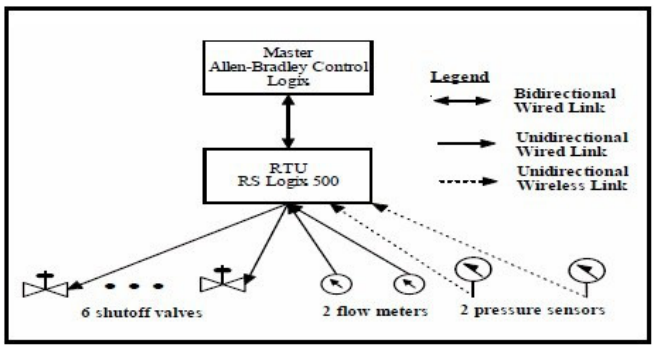


Fig. 1 Example of application (oil pipeline flow control)

In the selected example, safety requirements combine operational and maintenance safety. For operational safety, pressure, structural integrity, and correct distribution are

monitored. For maintenance safety, the flow must be diverted to alternate line, leaving the flow-free portion of the pipeline not monitored for operational safety. Security requires that only authorized personnel are to control the system, all events are logged for audit, and encrypted data are used for wireless transmissions.

The results of the study [18] showed that the NFR approach is effective in joint qualitative assessment of security and safety properties, allowing for simultaneous evaluation of impacts lower level variables might have on these system level properties. In the current project, we are using the same case study and apply the technique known as Bayesian Belief Networks (BBN) to address issues of mutual relationships of safety and security, and their impact on each other.

IV. Bayesian Belief Network Approach

A. Background

A Bayesian Belief Network (BBN) is a graphical model representing the conditional probability distribution of a set of random variables. The technique has been used in the last two decades in multiple industrial applications for decision making under uncertainty, including safety assessment [20]. Since its theoretical background has been well described elsewhere [21], in this paper we provide only a brief overview of BBN principles.

The BBN is based on a formula for belief updating from evidence (E) about a hypothesis (H) using conditional probability measurements of the prior truth of the statement updated by posterior evidence:

$$P(H|E) = (P(E|H) * P(H)) / P(E) \qquad (1)$$

The BBN is described by a directed acyclic graph of nodes and arcs. The nodes can assume specific states with apriori defined likelihood or with a certainty (if there is evidence of their actual state). The arcs represent relations among the variables in terms of likelihood of being in a specific state depending on a state of their ancestors.

An arc from node A to node B means that variable B depends directly on variable A (and A is called a parent of B). If the variable represented by a node has a known state then the node is said to be observed as an evidence node. A node can represent a variable, a measured parameter, or a hypothesis.

A Bayesian network is specified by an expert providing an initial assessment of likelihood that the nodes are in a specific state as well as the likelihood of descendant node being in a specific state, assuming states of its parent nodes. The network is then used to perform inference after some evidence about the state of specific nodes is entered. The predictive mode allows the user to determine likelihood of the outcome, i.e., top-level node being in certain state, assuming specific evidence one may have on its preceding nodes. The network allows also use a diagnostic mode of reasoning. Introducing the evidence of a resulting event leads to estimates regarding the causes of this event.

There are several tools supporting development of BBN with a list compiled in [22]. MSBNx has been used in this project [23].

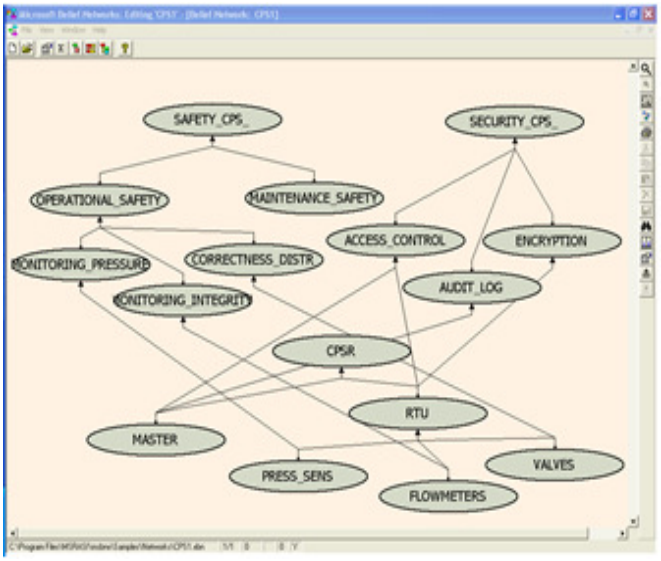


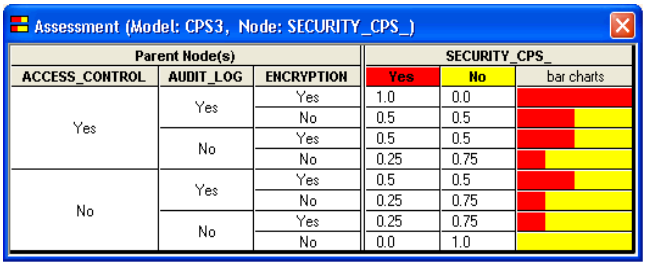
Fig. 2 BBN of the example CPS - oil pipeline control

B. Preliminaries

A BBN model was built for a case study of an oil pipeline control. In reality, safety may be affected by valve fault, pump failure, pressure build-up, leakage, blockage of pipes, and other factors. Security may be affected by lack of authentication and authorization, excessive privileges, wireless transmissions, lack of encryption, connection between the enterprise IT and SCADA networks, lack of audit logs, improper personnel training, poor physical security and the like. However, we consider only a few of these factors to illustrate our ideas. Figure 2 shows a diagram presenting the belief network with safety and security as the top nodes. Here, safety depends on both operational and maintenance safety. Operational safety, in turn, depends on correct monitoring of the pressure (depending on proper work of the pressure sensors) and integrity of the pipeline (depending on correctness of the pressure meters), as well on correctness of flow distribution (proper operation of shutoff valves). Security depends on controlling access, maintaining audit logs, and assuring encryption of transmission. Both Master Controller and RTU's are responsible for access control. Master maintains audit logs while RTU sends data, which may or may not be encrypted. Correct operation of the entire system depends on correctness of the hierarchy of underlying hardware and software.

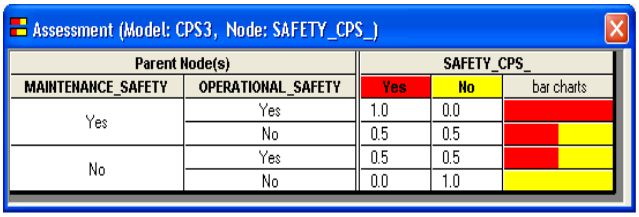
The computation is initialized with the likelihoods reflecting the probability of correct (State 0-YES) or incorrect (State 1-NO) operation. The dependency relations have been also initialized by assuming that incorrect operation of the parent node impacts the descendant node. Two cases were analyzed: all components operated with a specified likelihood of correctness: 90% and 99%.

The example dependency relationships for top-level safety and security nodes are shown in Figures 3 and 4. Likelihood level of the system security and safety properties are determined by dependency relationships based on the specific evidence of the state of the events affecting these properties.



Parent Node(s)			SECURITY_CPS_		
ACCESS_CONTROL	AUDIT_LOG	ENCRYPTION	Yes	No	bar charts
Yes	Yes	Yes	1.0	0.0	
		No	0.5	0.5	
	No	Yes	0.5	0.5	
		No	0.25	0.75	
No	Yes	Yes	0.5	0.5	
		No	0.25	0.75	
	No	Yes	0.25	0.75	
		No	0.0	1.0	

Fig. 3 Dependency relations for Security node



Parent Node(s)		SAFETY_CPS_		
MAINTENANCE_SAFETY	OPERATIONAL_SAFETY	Yes	No	bar charts
Yes	Yes	1.0	0.0	
	No	0.5	0.5	
No	Yes	0.5	0.5	
	No	0.0	1.0	

Fig. 4 Dependency relations for Safety node

Figures 5 and 6 present the example results of inference in a nominal state i.e., assuming the case that the likelihood of correct operation of all base nodes (master controller, flow and pressure sensors, and shutoff valves) is 90%.

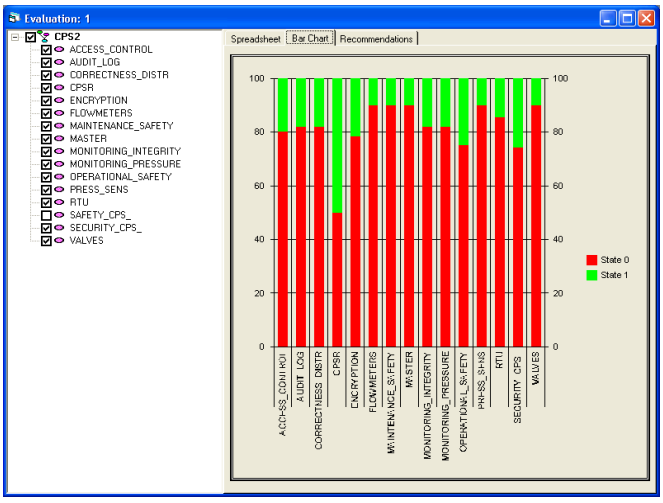
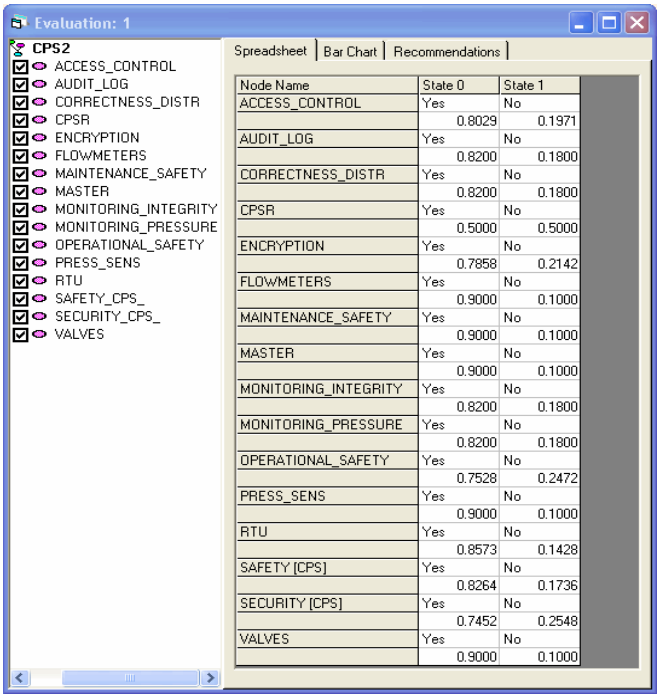


Fig. 5: A nominal state of the system in a bar-chart format

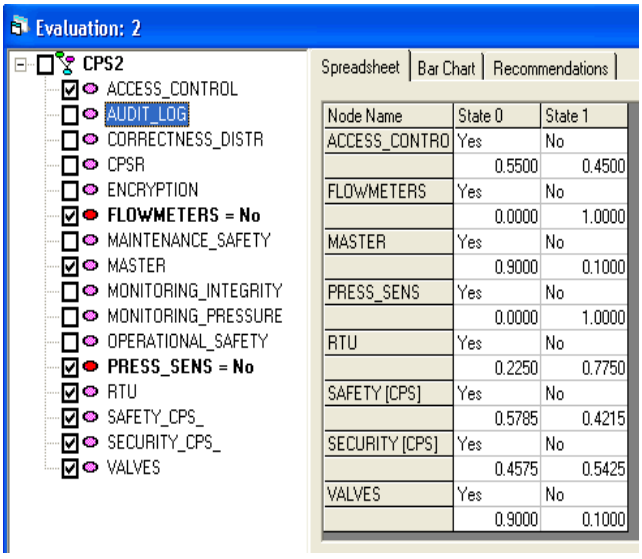


Node Name	State 0	State 1
ACCESS_CONTROL	Yes	No
	0.8029	0.1971
AUDIT_LOG	Yes	No
	0.8200	0.1800
CORRECTNESS_DISTR	Yes	No
	0.8200	0.1800
CPSR	Yes	No
	0.5000	0.5000
ENCRYPTION	Yes	No
	0.7858	0.2142
FLOWMETERS	Yes	No
	0.9000	0.1000
MAINTENANCE_SAFETY	Yes	No
	0.9000	0.1000
MASTER	Yes	No
	0.9000	0.1000
MONITORING_INTEGRITY	Yes	No
	0.8200	0.1800
MONITORING_PRESSURE	Yes	No
	0.8200	0.1800
OPERATIONAL_SAFETY	Yes	No
	0.7528	0.2472
PRESS_SENS	Yes	No
	0.9000	0.1000
RTU	Yes	No
	0.8573	0.1428
SAFETY [CPS]	Yes	No
	0.8264	0.1736
SECURITY [CPS]	Yes	No
	0.7452	0.2548
VALVES	Yes	No
	0.9000	0.1000

Fig. 6: A nominal state of the system in a tabular format (Table 1, case #1, 90% likelihood)

C. Modeling

Several experiments were conducted to assess the impact of specific base elements evidence on the likelihood of the system safety and security represented by top nodes. The results of selected experiments are depicted in Figures 7-9. These three examples show the BBN results when there is failure evidence of elements impacting safety (sensors), impacting security (audit log and encryption), and impacting both (valves and encryption) – all under assumption that likelihood of all other elements being operational is 90%.



Node Name	State 0	State 1
ACCESS_CONTRO	Yes	No
	0.5500	0.4500
FLOWMETERS	Yes	No
	0.0000	1.0000
MASTER	Yes	No
	0.9000	0.1000
PRESS_SENS	Yes	No
	0.0000	1.0000
RTU	Yes	No
	0.2250	0.7750
SAFETY [CPS]	Yes	No
	0.5785	0.4215
SECURITY [CPS]	Yes	No
	0.4575	0.5425
VALVES	Yes	No
	0.9000	0.1000

Fig. 7: An example scenario - safety impact: pressure and flow sensors not working (Table 1, case #3, 90% likelihood).

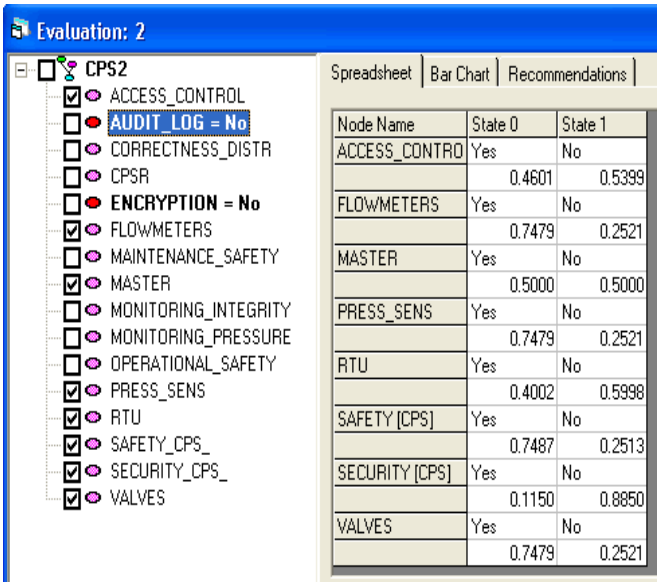


Fig. 8: An example scenario - security impact: audit log and encryption not operational (Table 1, case #8, 90% likelihood)

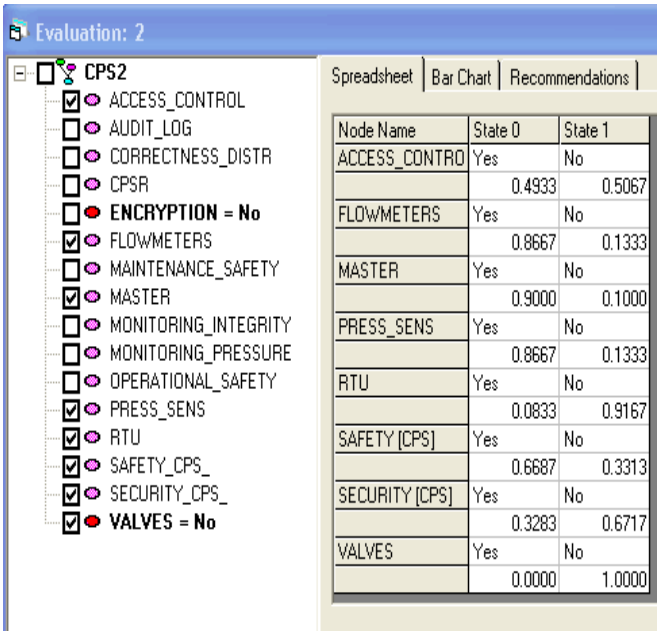


Fig. 9: An example scenario - combined impact valves and encryption not operational (Table 1, case #9, 90% likelihood).

Table 1 illustrates a subset of experiments. After capturing a nominal case (#1), evidence of failing the system components as well as evidence of not operational encryption and audit logs is introduced. Additionally, as presented in the last two rows, the impact of having evidence of a complete failure of safety on security, and vice versa, is analyzed.

Row 1 in Table 1 presents probability levels of safety and security assuming "nominal" values of likelihood of all base events, i.e., when there is no specific evidence and they are defined only by their original probabilities (two scenarios are considered, assuming either 90% or 99% likelihood of correct operations). Consecutive rows present results of deviation from the nominal state and the effect of evidence of these deviations on safety and security. It can be observed that with an evidence of failures or malfunction the probability of a safe/secure operation of the system deteriorates often two-fold.

Using Table 1 one can also compute likelihood of extended scenarios. As an example of a scenario where loss of security negatively impacts safety, consider the case where the RTU in the field was physically tampered which leads to the failure of valve control and thereby permits higher than normal amount of fluid to accumulate in the pipeline. The probability of such compound event can be evaluated from Table 1 as follows:

P(safety violation physical tampering with valve control) = P(safety impact due to security failure)* P(valve failure)

The computation results in probability of safety violation due to a physical tampering destroying the valve control: 0.4668 (0.6907*0.6759) or 0.5811 (0.8357*0.6954), for 90% and 99% scenarios respectively. It is assumed that other evidence is unknown, i.e., the likelihood of correct operation of all remaining components is as specified by the scenario.

TABLE 1: RESULTS OF HYPOTHETICAL SCENARIOS FOR TWO CASES OF THE BASE COMPONENTS OPERATIONAL LIKELIHOOD.

	90% likelihood		*99% likelihood*	
CASE	***Safety***	***Security***	***Safety***	***Security***
#1. nominal	0.8264	0.7452	0.8732	0.8455
#2. valve fails	0.6759	0.5599	0.6954	0.6155
#3. flowmeter & valve fail	0.5785	0.4575	0.5876	0.4993
#4. flowmeter, valve & pressure sensor fail	0.4876	0.3552	0.4876	0.3831
#5. master controller fails	0.8264	0.3552	0.8732	0.3816
#6. encryption fails	0.7487	0.3600	0.8543	0.4350
#7. audit log not operational	0.8264	0.3572	0.8732	0.4372
#8. audit log & encryption fails	0.7487	0.1150	0.8543	0.2047
#9. valve fails & encryption fails	0.6687	0.3283	0.6946	0.3568
Impact				
Safety violation	0	0.6907	0	0.8357
Security violation	0.7893	0	0.8652	0

Additionally, conditional probabilities may also be deduced from Table I. For example, for the scenario where

the valve fails and a security violation occurred, one would wish to deduce the probability that the valve failed due to such security incident. Then:

P(valve failed | security violation) =
P(valve failed and security violation)/P(security violation)

Assuming unknown evidence with 90% scenario, the computation results in the conditional probability 0.7094 (0.5599/0.7893). With 99% scenario, the conditional probability is 0.7114 (0.6155/0.8652).

As shown, BBN's can be used for estimating probabilities of unknown events based on probabilities of known events. As can be expected, the better the data used for modeling BBN, the more trustworthy the computed probabilities. This in turn requires a more accurate modeling of factors affecting both security and safety, which form the basis for BBN's.

The proposed approach allows not only to specify numerical values for safety and security (in terms of their likelihoods), but also allows for quantitative assessment of a relationship between safety and security as well as that of an impact of the status of the system components on safety and security.

An obvious challenge is to identify not only the likelihoods of events at specific nodes representing the system components but also the initial likelihoods of dependency relations between them. These can be derived from failure rates of equipment available, for example, from the military handbook [24] or from industry studies such as [25]. Likelihood estimates can also be obtained from incident rates related to safety and security such as rates of deliberate acts of sabotage and vandalism or the rates of deliberate software attacks [26]. Additionally, the proposed analysis could be conducted, expo facto on a system in which a failure has already occurred to provide some validation evidence and means for calibrating the data.

V. Conclusion

The driving force behind the presented research is that security and safety properties in cyber-physical systems are mutually dependent and influence each other. It is, therefore, natural to seek methods of measuring their mutual impact and assessing their susceptibility to related events and changes in values of basic variables.

In this paper we studied the relationship of safety and security using Bayesian Belief Networks. For a case study of an oil pipeline SCADA based control system, the BBN technique was applied to determine the impact of failures in low-level equipment on the overall security and safety of the entire system and evaluate safety and security in case of equipment or software failures. It turns out that the method proves useful for applied purposes and is comparable to the NFR approach applied previously.

The NFR is a qualitative approach evaluating the safety and security of a cyber-physical system given known factors of a system's configuration (including components and connections). It applies propagation rules to assess NFRs such as safety and security. In contrast, the BBN uses likelihood estimates of a system's configuration to evaluate quantitatively the achievement or denial of safety and security of cyber-physical systems; likelihood estimates can include failure rates of system components and connections or could be likelihood of incidents impacting safety and security. It needs to be noted that [18] describes a qualitative technique to evaluate safety and security. As a result of this evaluation we can conclude to what extent (good or bad) safety and security have simultaneously been achieved in the system. In this paper we have attempted quantitative evaluation of achievement of safety and security in a system using probabilistic computations from BBN.

Therefore, evaluations of safety and security obtained from BBN are rooted in data collected in the field and can be used for both predictive and diagnostic purposes. These data can be used for re-evaluation of contributions in the NFR approach and vice versa, assessments from NFR can be used to re-evaluate critical aspects using the BBN approach. Thus, both these techniques can be used in a complementary manner to iteratively reassess safety and security of cyber-physical systems.

In future work, it would be interesting to include in this study the Safety Case approach [27]. It is based on a graphical Goal Structuring Notation (GSN), similar to NFR, to represent entities and relationships used in the safety argument. Such GSN may be another base to model with BBN's.

References

[1] DO-178C. *Software Considerations in Airborne Systems and Equipment Certification*, RTCA 12-13-11, SC-205, 2011.

[2] DO-326. *Airworthiness Security Process Specification*, RTCA 12-08-10, SC-216, 2010.

[3] N. Mead, J. Allen, M. Ardis, T. Hilburn, A. Kornecki, R. Linger, J. McDonald, *Software Assurance Curriculum Project*, Vol. I, Report CMU/SEI-2010-TR-005, Software Engineering Institute, Pittsburgh, Penn., August 2010

[4] J. Smith, S. Russell, M. Looi. Security as a Safety Issue in Rail Communications, *Proc. SCS 2003, 8th Australian Workshop on Safety Critical Systems and Software*, Canberra, October 9-10, 2003, pp. 79-88.

[5] J. Hahn, D.P. Guillen, T. Anderson. Process Control Systems in the Chemical Industry: Safety vs. Security, *Proc. 20th CCPS, Int'l Conference of the Center of Chemical Process Safety*, Atlanta, Georgia, April 11-13, 2005. Report INL/CON-05-00001.

[6] M.G. Jaatun, T.O. Grotan, M.B. Line. Secure Safety: Secure Remote Access to Critical Safety Systems in Offshore Installations, *Proc. ATC 2008, 5th Intern. Conf. on Autonomic and Trusted Computing*, Oslo, Norway, June 23-25, 2008, pp. 121-133.

[7] T. Novak, A. Treytl. Functional Safety and System Security in Automation. *Proc. ETFA'08, 13th IEEE Conf. on Emerging Technologies and Factory Automation*, Hamburg, Germany, September 15-18, 2008, pp. 311-318.

[8] J. Jalouneix, P. Cousinou, J. Couturier, D. Winter. *A Comparative Approach to Nuclear Safety and Nuclear Security*, Tech. Rep. IRSN 2009/117, Institut de Radioprotection et de Sûreté Nucléaire, Fontenay-aux-Roses, France, 2009.

[9] A. Kornecki, J. Zalewski. Safety and Security in Industrial Control, *Proc. CSIIRW 2010, 6th Annual Workshop on Cyber Security and Information Intelligence Research*, Oak Ridge, Tenn., April 21-23, 2010.

[10] A. Burns, J. McDermid, J. Dobson. On the Meaning of Safety and Security, *The Computer Journal*, Vol. 35, No. 1, pp. 3-15, 1992.

[11] J. Zalewski, S. Drager, W. McKeever, A. Kornecki. Towards Experimental Assessment of Security Threats in Protecting the Critical Infrastructure. *Proc. ENASE 2012, International Conf. on Evaluation of Novel Software Approaches to Software Engineering*, Wroclaw, Poland, June 29-30, 2012, pp. 207-212.

[12] L. Pièrre-Cambacédès, M. Bouissou. Cross-fertilization between Safety and Security Engineering, *Reliability Engineering and System Safety*, Vol. 110, pp. 110-126, 2013.

[13] W. Boyes, Safety, Security and Complex Systems in Critical Infrastructure Protection, Invited Talk. *SAFECOMP 2009, 28th International Conference on Computer Safety, Reliability and Security*, Hamburg, Germany, September 15-18, 2009. Available at: http://www.controlglobal.com/articles/2009/CriticalInfrastructure0909.html

[14] OCTAVE, Operationally Critical Threat, Asset, and Vulnerability Evaluation, CERT, Software Engineering Institute, Pittsburgh, Penn., 2008. Available from: http://www.cert.org/octave/

[15] N.E. Fenton, M. Neil. Software Metrics: Roadmap. *Proc. ICSE'00, International Conference on the Future of Software Engineering*, Limerick, Ireland, June 4-10, 2000, pp. 357-370.

[16] R. Kazman, M. Klein, P. Clement. *ATAM: Method for Architecture Evaluation*. Technical Report CMU/SEI-2000-TR-004, Software Engineering Institute, Pittsburgh, Penn., August 2000.

[17] L. Chung, B.A. Nixon, E. Yu, J. Mylopoulos. *Non-Functional Requirements in Software Engineering*, Kluwer Academic Publishers, Boston, 2000.

[18] System Architectures for Cyberphysical Systems, *Proc. SysCon 2013, IEEE Intern. Systems Conference*, Orlando, FL, April 15-18, 2013, pp. 634-641.

[19] Center for Petroleum Security Research, University of Texas at Tyler, 2013. Available from: http://www2.uttyler.edu/cpsr/facilities.php

[20] N.E. Fenton, M. Neil. *The Use of Bayes and Causal Modelling in Decision Making, Uncertainty and Risk*. Agena Risk White Paper. Agena, Cambridge, UK, June 2011. Available from: http://www.agenarisk.com/resources/white_papers/fenton_neil_white_paper2011.pdf

[21] F.V. Jensen, T.D. Nielsen. *Bayesian Networks and Decision Graphs*. 2nd Edition, Springer-Verlag, Berlin, 2007.

[22] K. Murphy. *Software Packages for Graphical Models*, University of British Columbia, Vancouver, Canada, February 12, 2013, Available from: http://www.cs.ubc.ca/~murphyk/Software/bnsoft.html

[23] *MSBNx: Bayesian Network Editor and Tool Kit*, Microsoft Research, Redmond, Calif., 2013. URL: http://research.microsoft.com/en-us/um/redmond/groups/adapt/msbnx/

[24] Military Handbook: Reliability Prediction of Electronic Equipment. Notice 2. MIL-HDBK-217F, 1995.

[25] R. Chalupa. *Failure Modes, Effects and Diagnostics Analysis*. Report No. 06-11-25-R001, Rosemount Corp., Eden Prairie, Minn., 2007.

[26] M.E. Whitman, H.J. Mattord. *Management of Information Security*. 3rd Edition, Cengage Learning, Independence, Kentucky, 2010, pp. 288-291.

[27] T.P. Kelly, I J Bate, J A McDermid, A Burns. Building a Preliminary Safety Case: An Example from Aerospace. *Proc. 1997 Australian Workshop on Industrial Experience with Safety Critical Systems and Software*, Sydney, Australia, October 3, 1997.