BAYESIAN NETWORK BASED ANALYSIS OF CYBER SECURITY IMPACT ON SAFETY

Jinugu Ranjith 1, MATOORI KIRAN 2, MEDE CHITTI BABU 3
4.K.VENKATA RAMANA, 5.MD.ANWAR ALI
Assistant Professor, Department of Computer Engineering, Ellenki college of Engineering and Technonlogy, patelguda (vi), near BHEL ameenpur (m), Sangareddy Dist. Telangana 502319.

Abstract

Cyber security gains further importance regarding life cycle risk analysis of technical systems, e.g. Cyber Physical Systems (CPS) or Systems of Systems (SoS) in the context of increasing dependency on networked systems and processes in domains like industry 4.0 or smart home. At the same time, the operation of networked systems in environments critical to safety poses the challenge of analyzing a growing number of potential interactions between safety and security aspects. In industrial environments, the assessment of functional safety is a standard procedure, e.g. using IEC 61508 and domain-specific derivatives, while cyber security in safety relevant domains has only been introduced in the last few years. The assessment of cyber security is a rapidly developing discipline, but until now there have been only few approaches to merge the standardized procedures in safety and security. This paper presents an approach based on Bayesian Networks (BN) that enables to consider the impact of cyber security threats on functional safety considerations. By means of a simplified x-by-wire system, safety and security relations as well as structures are derived and an integrated safety and security BN is established. It is shown that parameter learning in BN can be used to adapt chosen target parameters to a required integrated safety and security level. Thus, it is possible to enhance the system configuration considering new cyber security threats.

Keywords: Safety & Security, Safety & Security Interdependencies, Security, Security Influences, Bayesian Net- works, Cyber Attacks, Cyber Security, Functional Safety, Parameter Learning, Machine Learning

Introduction

Cyber security gains further importance regarding life cycle risk analysis of technical systems, e.g. Cyber Physical Systems (CPS) or Systems of Systems (SoS) in the context of increasing dependency on networked systems and processes in domains like industry 4.0 or smart home. At the same time, the operation of networked systems in environments critical to safety poses the challenge of analyzing a growing number of potential inter- actions between safety and security aspects.

In the industrial field, the assessment of functional safety is a standard procedure, e.g. using IEC 61508 and domain-specific derivatives, while cyber security in safety relevant domains was only introduced in recent years. The assessment of cyber security is a rapidly developing discipline, but until now there have been only few approaches to merge the standardized procedures in safety and security. For example, two introduced approaches

propose a combination of Fault Tree Analysis (FTA) with Attack Tree Analysis (ATA) (Fovino et al., 2009) or Boolean Driven Markov Processes (BDMP) (Kriaa and Bouissou, 2014).

This paper presents an approach based on Bayesian Networks (BN) that enables the consid- eration of the impact of cyber security threats on functional safety considerations. In a first step, safety as well as security structures and their po- tential relations are derived. Then, the BN-based modeling of influences of cyber security on func- tional safety is shown in a simplified example of a safety relevant x-by-wire system that features hot redundancy to ensure reliability. The following reliability analysis reveals the potential impact of security threats in networked environments.

The paper additionally presents a first approach to adapt existing systems facing new security threats. A required integrated safety and security level is defined as a maximum limit value for the system failure rate and target parameters in both domains are chosen. A subsequent adaption to an artificially compiled dataset representing a required safety and security level by parameter learning then delivers new target marginal distribu- tion probabilities (MDP). On this basis, a further optimization of the system considering new cyber security threats is possible. Finally, the approach and further developments in the field of safety and security are discussed.

Background

Recent research shows that safety and especially cyber security share interdependencies in a broad range of products, especially in cyber phyical systems (CPS) (Banerjee et al., 2012). Besides

Security

Security analysis is mostly conducted indepen- dently from safety analysis and industry mostly resorts to using state-of-the-art methods of cyber security testing and vulnerability analysis. This includes for example penetration testing of systems as well as formal code verification (Shebli and Beheshti, 2018).

The resulting security assessment aggregates the findings in qualitative security models like Attack Tree Analysis (Mauw and Oostdijk, 2006) and quantitative enhancements (Kordy and Wide, 2018) additionally involving defensive measures. The results are also used for certification purposes according to standards, e.g. IEC 62443-3-3 (2008). Here, similarly to ISO 61508 in safety, security integrity levels are defined in a qualitative manner. More recently, cyber risk analysis was further developed by implementing game theory in the process of analysis. This lead to the approach of adversarial risk analysis (ARA), e.g. described in Cox (2009) and Insua et al. (2009). ARA is able to take strategies and measures of the de- fender as well as potential attackers into account (Cox, 2009).

Additionally, a few approaches emerged that describe the structure of security systems and measures in BN, e.g. Gribaudo et al. (2015), Fakhravar et al. (2017) and Lichte and

Wolf (2018).

Security in safety analysis Overall, safety and security analysis are both usu- ally conducted at least in safety sensitive or crit- ical sectors. Nevertheless, both processes com- monly lack to analyze the impact of security risks on safety. Simultaneously, the consideration of security as an important precondition for safety critical systems has developed only in the last few years. Therefore, only a few integrated ap- proaches to analyze safety and security risks have been developed. Practically this means that al- though security analysis is implemented in the overall design process, it is usually not integrated into the safety analysis process (Kornecki et al., 2013).

ISSN (PRINT): 2393-8374, (ONLINE): 2394-0697, VOLUME-4, ISSUE-1, 2017
DOI: 10.21276/ijcesr.2017.4.1.5

Recently introduced approaches realized the importance of integrated safety and security analysis and therefore aim at integrating both into a joint methodological process. Two relevant approaches that describe the merging of security into safety analysis propose a combination of Fault Tree Analysis (FTA) with Attack Tree Analysis (ATA) (Fovino et al., 2009) or Boolean Driven Markov Processes (BDMP) (Kriaa and Bouissou, 2014). Other introduced approaches either com- bine methods of Safety and Security, e.g. ATA and bowtie analysis (Abdo et al., 2018), or inte- grate both fields. Here, approaches based on BN are proposed, e.g. Kornecki et al. (2013). Both approaches are rather general regarding systemic interaction of safety and security.

Bayesian networks and parameter learning

Bayesian Networks (BN) are based on Bayesian probabilistics, interpreting probability as a degree of belief. Bayesian probabilistics are less strict regarding evidence than mostly used frequentist probability approaches. BN represent a combi- nation of probability and graph theory. A BN therefore quantifies dependencies between various data, information or knowledge considering uncer- tainties (Jensen and Nielsen, 2007).

Therefore BN on the one hand allow to adapt structures of various data, knowledge and functional relationships as well as methods. Therefore FT or AT can be transferred to BN (see Section 2.1 and 2.2). On the other hand, the structure of BN allows to conduct the widely used inference for further analysis. Especially in the context of Machine Learning (ML), structure learning as well as parameter learning (PL) (Heckerman et al., 1995) are both methods to estimate and analyze unknown structures or parameters with respect to given evidence and constrained or incomplete data sets (Liao and Ji, 2009). The inference problem for parameter learning is typically solved approx- imately. Here, either the expectation maximiza- tion algorithm (Friedman, 1998) or a variational approach, e.g. in Blei et al. (2017) are used.

Especially parameter optimization and balancing is an important problem when considering safety and security interrelationships that may be tackled by methods based on BN. A general ap- proach is given in Pelikan et al. (2002). How- ever, in existing integrated safety and security ap- proaches these enhanced possibilities of analysis are not considered.

2. Approach

The subsequently presented approach is applied to a simplified x-by-wire CPS without loss of generality for arbitrary application. Hereby, the four main steps of the analyzing and optimizing procedure are explained.

In a first step, the considered system is defined and its relevant safety and security structures are analyzed.

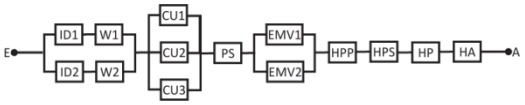

Fig. 1. Block Diagram of X-by-wire CPS

is designed as a homogeneous redundant n + 1 system. Herein, components are considered as an interface device (ID) for command input and the electric wiring connecting the ID to the command unit. The command unit consists of a position sensor (PS), a homogeneous n + 1 redundancy of electro-magnetic valves (EMV) and three hetero- geneous redundant n + 2 control units (CU). To realize the input commands, a hydraulic system is used that comprises a hydraulic power pump (HPP), a pressure sensor (HPS), the pipeline sys- tem (HP) and the hydraulic actors (HA).

In order to enable a simplified calculation of the system's failure rate, the failure rates of the components listed in Table 1 were determined.

Component Failurerateλ

ID1, ID2	$1{\cdot}10^{-5}$
W1,W2	$1{\cdot}10^{-3}$
EMV1,EMV2	$1{\cdot}10^{-6}$
PS	$1{\cdot}10^{-6}$
CU1	$1.5{\cdot}10^{-4}$
CU2	$2{\cdot}10^{-4}$
CU3	$1{\cdot}10^{-4}$
HPP	$1{\cdot}10^{-6}$
HA	$1{\cdot}10^{-6}$
HPS	$1{\cdot}10^{-6}$
HP	$3.5{\cdot}10^{-5}$

Given the basic functional structure and neces- sary failure rates we can now further analyze the system in the next section.

System analysis

The first main step of the approach is to further investigate the safety and security related structure of the system. In order to analyze safety rele- vant structures, we conduct a fault tree analysis (FTA) to understand the relationship between the system's components. Therefore, we use the block diagram (see Figure 1) that describes the reliabil- ity relevant functional structure

The structure is then transferred to the FT de- picted in Figure 2. Following, the security re- lated characteristics of the system are investigated. Here, different important characteristics of possi- ble security incidents are identified to be used later in the BN:

- feasible attack targets and the likelihood of attacks
- affected system components
- assumed defensive security measures and the global efficiency in attack preven- tion
- estimated local efficiency of security measures

However, this process is not further described in this paper. As a result of analysis, the likelihood of an attack (LOA) within an observation period of t = 1y is set to:

$$LOA(t{=}1){=}1{-}e^{-\lambda_{LOA}}{=}0.9 \qquad (1)$$

$$\text{Theresultingattackrate}\lambda_{LOA}\text{isthen}$$

$$\lambda_{LOA}{=}2.3026 \qquad (2)$$

The results of the investigation of feasible attack targets and their likelihood of being the target in case of a cyber attack are summarized in Table 2. The attack targets are chosen

Table 2. Feasible Attack Modes and Likelihoods for

t = 1y

AttackTargets	Likelihood(MDP)
SensorDatabases	0.2
ActuatorCommands	0.1
ControlValues	0.1
ControlSetPointVariables	0.1
ControlUnitSystem	0.5

In the last step, we use the derived model to reach a required combined safety and security failure rate λSecSaf,Req. For this purpose, target values are derived to enhance either cyber security effi- ciency, safety measures or both. The derivation is done by using the set-up BN for learning the marginal distribution probabilities (MDP) of the chosen input parameters (see above) conducting Bayesian inference. Thus, we get updated MDP for the nodes of these parameters that can serve for further practical considerations to optimize the

References

Abdo, H., M. Kaouk, J.-M. Flaus, and F. Masse (2018). A safety/security risk analysis approach of industrial control systems: A cyber bowtie

– combining new version of attack tree with bowtie analysis. Computers & Security 72, 175

– 195.

Banerjee,

A., K. K. Venkatasubramanian, T. Mukherjee, and S. K. S. Gupta (2012). Ensuring safety, security, and sustainability of mission-critical cyber–physical systems. In Proceedings of the IEEE, Volume 100, pp. 283–299.

Bieber, P., C. Castel, and C. Seguin (2002). Combination of fault tree analysis and model check- ing for safety assessment of complex system. In A. Bondavalli and P. Thevenod-Fosse (Eds.), Dependable Computing EDCC-4, Berlin, Hei- delberg, pp. 19–31. Springer Berlin Heidelberg. Blei, D. M., A. Kucukelbir, and J. D. McAuliffe (2017). Variational inference: A review for statisticians. Journal of the American Statistical

Association 112(518), 859–877.

Bobbio, A., L. Portinale, M. Minichino, and

E. Ciancamerla (2001). Improving the analysis of dependable systems by mapping fault trees into bayesian networks. Reliability Engineering & System Safety 71(3), 249 – 260.

Cox, L. A. (2009). Game theory and risk analysis.

Risk Analysis 29(8), 1062–1068.

Fakhravar, D., V. Cozzani, N. Khakzad, and G. Re- niers (2017). Security vulnerability assessment of gas pipelines using bayesian network. In 27th European Safety and Reliability Confer- ence ESREL 2017.

Fovino, L. N., M. Masera, and A. De Cian (2009). Integrating cyber attacks within fault trees. Re- liability Engineering & System Safety 94-9, 1394–1402.

Friedman, N. (1998). The bayesian structural em algorithm. In Proceedings of the Fourteenth Conference on Uncertainty in Artificial Intel- ligence, UAI'98, pp. 129–138. Morgan Kauf- mann Publishers Inc.

Gribaudo, M., M. Lacono, and M. S. (2015). Exploiting bayesian networks for the analysis of combined attack trees. Electronic Notes in Theoretical Computer Science 310, 91 – 111.

Heckerman, D., D. Geiger, and D. M. Chickering (1995, Sep). Learning bayesian networks: The combination of knowledge and statistical data. Machine Learning 20(3), 197–243.

IEC 61508 (2010). Functional safety of electri- cal/electronic/programmable electronic safety- related systems (e/e/pe, or e/e/pes). IEC 61508:2010.

IEC 61513 (2011). Nuclear power plants - in- strumentation and control important to safety

- general requirements for systems. IEC 61513:2011.

IEC 62278 (2002). Railway applications - com- munication, signalling and processing systems

- software for railway control and protection systems. IEC 62278:2002.

IEC 62443-3-3 (2008). Industrial communication networks – network and system security – part 3-3: System security requirements and security levels. IEC 62443-3-3:2008.

Insua, D. R., J. Rios, and D. Banks (2009). Ad- versarial risk analysis. Journal of the American Statistical Association 104(486), 841–854.

ISO 26262 (2011). Road vehicles – functional safety. ISO 26262:2011.

Jensen, F. and T. Nielsen (2007). Bayesian Net- works and Decision Graphs. Springer Berlin.

John, A., Z. Yang, R. Riahi, and J. Wang (2016). A risk assessment approach to improve the resilience of a seaport system using bayesian networks. Ocean Engineering 111, 136 – 147.

Johnson, R. E. (2010). Survey of scada security challenges and potential attack vectors. In 2010 International Conference for Internet Technology and Secured Transactions, pp. 1–5. IEEE.

Khakzad, N., F. Khan, and P. Amyotte (2011). Safety analysis in process facilities: Comparison of fault tree and bayesian network approaches. Reliability Engineering & System Safety 96(8), 925 – 932.

Kordy, B. and W. Wide (2018). On quantitative analysis of attack-defense trees with repeated labels. In L. Bauer and R. Ku¨sters (Eds.), Principles of Security and Trust, Cham, pp. 325–

346. Springer International Publishing.

Kornecki, A. J., N. Subramanian, and J. Zalewski (2013). Studying interrelationships of safety and security for software assurance in cyber- physical systems: Approach based on bayesian belief networks. In 2013 Federated Conference on Computer Science and Information Systems, pp. 1393–1399. IEEE.

Kriaa, S. and M. Bouissou (2014). Model- ing safety and security interdependencies with bdmp (boolean logic driven markov processes). In A. Bondavalli, A. Ceccarelli, and F. Ortmeier (Eds.), SAFECOMP 2014. Springer, Cham.

Liao, W. and Q. Ji (2009). Learning bayesian net- work parameters under incomplete data with do- main knowledge. Pattern Recognition 42(11), 3046 – 3056.

Lichte, D. and K.-D. Wolf (2018). Approach to a bayesian decision model for cost-benefit analysis in security risk management. In 28th European Safety and Reliability Conference ES- REL 2018.

Mauw, S. and M. Oostdijk (2006). Foundations of attack trees. In D. H. Won and S. Kim (Eds.), Information Security and Cryptology - ICISC 2005, Berlin, Heidelberg, pp. 186–198. Springer Berlin Heidelberg.

Noel, S. and S. Jajodia (2014). Metrics suite