PESARO 2014

The Fourth International Conference on Performance, Safety and Robustness in Complex Systems and Applications

ISBN: 978-1-61208-321-6

February 23 - 27, 2014

Nice, France

PESARO 2014 Editors

Wolfgang Leister, Norsk Regnesentral (Norwegian Computing Center), Norway

PESARO 2014

Foreword

The Fourth International Conference on Performance, Safety and Robustness in Complex Systems and Applications (PESARO 2014), held between February 23rd-27th, 2014 in Nice, France, continued the inaugural event dedicated to fundamentals, techniques and experiments to specify, design, and deploy systems and applications under given constraints on performance, safety and robustness.

There is a relation between organizational, design and operational complexity of organization and systems and the degree of robustness and safety under given performance metrics. More complex systems and applications might not be necessarily more profitable, but are less robust. There are trade-offs involved in designing and deploying distributed systems. Some designing technologies have a positive influence on safety and robustness, even operational performance is not optimized. Under constantly changing system infrastructure and user behaviors and needs, there is a challenge in designing complex systems and applications with a required level of performance, safety and robustness.

We take here the opportunity to warmly thank all the members of the PESARO 2014 Technical Program Committee. The creation of such a high quality conference program would not have been possible without their involvement. We also kindly thank all the authors who dedicated much of their time and efforts to contribute to PESARO 2014. We truly believe that, thanks to all these efforts, the final conference program consisted of top quality contributions.

Also, this event could not have been a reality without the support of many individuals, organizations, and sponsors. We are grateful to the members of the PESARO 2014 organizing committee for their help in handling the logistics and for their work to make this professional meeting a success.

We hope that PESARO 2014 was a successful international forum for the exchange of ideas and results between academia and industry and for the promotion of progress in the field of performance, safety and robustness in complex systems and applications.

We are convinced that the participants found the event useful and communications very open. We also hope the attendees enjoyed the charm of Nice, France.

PESARO Advisory Committee:

Piotr Zwierzykowski, Poznan University of Technology, Poland
Wolfgang Leister, Norsk Regnesentral (Norwegian Computing Center), Norway
Yulei Wu, Chinese Academy of Sciences, China
Harold Liu, IBM Research, China

PESARO 2014

Committee

PESARO Advisory Committee

Piotr Zwierzykowski, Poznan University of Technology, Poland
Wolfgang Leister, Norsk Regnesentral (Norwegian Computing Center), Norway
Yulei Wu, Chinese Academy of Sciences, China
Harold Liu, IBM Research, China

PESARO 2014 Technical Program Committee

Amr Aissani, USTHB - Algiers, Algeria
Salimur Choudhury, Queen's University - Kingston, Canada
Dieter Claeys, Ghent University, Belgium
Juan Antonio Cordero, École Polytechnique / INRIA, France
Nadir Farhi, IFSTTAR/COSYS/GRETTIA, France
John-Austen Francisco, Rutgers University - Piscataway, USA
Mina Giurguis, Texas State University - San Marcos, USA
Mesut Günes, FU-Berlin, USA
Charles Kamhoua Kenmogne, Air Force Research Laboratory, USA
Daniel Kosiorowski, Cracow University of Economics, Poland
Wolfgang Leister, Norsk Regnesentral (Norwegian Computing Center), Norway
Harold Liu, IBM Research, China
Olaf Maennel, Loughborough University, UK
Kia Makki, Technological University of America (TUA), USA
Stefano Marrone, Seconda Università di Napoli, Italy
Birgit Milius, Institut fuer Eisenbahnwesen und Verkehrssicherung (IfEV) /Technische Universitaet – Braunschweig, Germany
Asoke Nandi, Brunel University, UK
Maciej Piechowiak, Kazimierz Wielki University - Bydgoszcz, Poland
M. Zubair Rafique, KU Leuven, Belgium
Roger S. Rivett, Land Rover - Gaydon, UK
Dhananjay Singh, Electronics and Telecommunications Research Institute (ETRI), South Korea
Mukesh Singhal, University of California, Merced, USA
Young-Joo Suh, Pohang University of Science and Technology (POSTECH), South Korea
Yuejin Tan, National University of Defense and Technology - Changsha, China
Yang Wang, Georgia State University, USA
Yun Wang, Bradley University - Peoria, USA
Jun Wu, National University of Defense and Technology, China
Yanwei Wu, Western Oregon University, USA
Yulei Wu, Chinese Academy of Sciences, China
Gerhard Wunder, Fraunhofer Heinrich Hertz Institut - Technical University Berlin, Germany
Gaoxi Xiao, Nanyang Technological University, Singapore

Copyright Information

For your reference, this is the text governing the copyright release for material published by IARIA.

The copyright release is a transfer of publication rights, which allows IARIA and its partners to drive the dissemination of the published material. This allows IARIA to give articles increased visibility via distribution, inclusion in libraries, and arrangements for submission to indexes.

I, the undersigned, declare that the article is original, and that I represent the authors of this article in the copyright release matters. If this work has been done as work-for-hire, I have obtained all necessary clearances to execute a copyright release. I hereby irrevocably transfer exclusive copyright for this material to IARIA. I give IARIA permission or reproduce the work in any media format such as, but not limited to, print, digital, or electronic. I give IARIA permission to distribute the materials without restriction to any institutions or individuals. I give IARIA permission to submit the work for inclusion in article repositories as IARIA sees fit.

I, the undersigned, declare that to the best of my knowledge, the article is does not contain libelous or otherwise unlawful contents or invading the right of privacy or infringing on a proprietary right.

Following the copyright release, any circulated version of the article must bear the copyright notice and any header and footer information that IARIA applies to the published article.

IARIA grants royalty-free permission to the authors to disseminate the work, under the above provisions, for any academic, commercial, or industrial use. IARIA grants royalty-free permission to any individuals or institutions to make the article available electronically, online, or in print.

IARIA acknowledges that rights to any algorithm, process, procedure, apparatus, or articles of manufacture remain with the authors and their employers.

I, the undersigned, understand that IARIA will not be liable, in contract, tort (including, without limitation, negligence), pre-contract or other representations (other than fraudulent misrepresentations) or otherwise in connection with the publication of my work.

Exception to the above is made for work-for-hire performed while employed by the government. In that case, copyright to the material remains with the said government. The rightful owners (authors and government entity) grant unlimited and unrestricted permission to IARIA, IARIA's contractors, and IARIA's partners to further distribute the work.

Table of Contents

Automatic Decomposition and Allocation of Safety Integrity Level Using System of Linear Equations

Mohamed Slim Dhouibi, Jean-Marc Perquis
Valeo Etudes Electroniques
Creteil, France
Email: {slim.dhouibi, Jean-marc.prequis }@valeo.com

Laurent Saintis, Mihaela Barreau
Université d'Angers
Angers, France
Email: {laurent.saintis, mihaela.barreau}@univ-angers.fr

***Abstract*—In ISO-26262, the Automotive safety integrity level (ASIL) represents the degree of rigour that should be applied in the development, implementation and verification of a requirement in order to reduce and control the risk in the final product. The ASILs are allocated to the safety requirements which are inherited by the subsystems and components in a hierarchical approach. During the allocation process, the safety requirements could be decomposed over redundant elements. It is referred to as ASIL decomposition and is an important feature, as it helps to reduce the complexity and the development cost of the design. The decomposition could lead, however, to different allocations. In this paper, we propose an approach to find all the possible allocations in order to assist the analyst in reaching the optimal allocation.**

***Index Terms*— ASIL decomposition, ISO 26262**

I. Introduction

ISO-26262 [1] is the functional safety standard for electrical and electronic systems in road vehicles. It focuses on the requirements, processes and methods to deal with the effects of systematic failures and unsystematic hardware failures. Published in 2011, this standard is an adaptation of IEC-61508 [2]. It has inherited and adapted different concepts such as the concept of Safety integrity level (SIL) which was redefined as Automotive Safety Integrity Level (ASIL). Henceforth, the safety integrity levels are defined and ordered by criticality as follows: Qm (not safety critical), ASIL A, ASIL B, ASIL C, ASIL D(most stringent).

The safety requirements are attributed one of these values and are subsequently inherited in a hierarchical approach by the sub-systems and the components. The ASIL determines the qualitative and quantitative levels that the element, implementing the safety requirement, should meet and the necessary safety activities to be conducted during the safety life cycle to ensure that the risk is brought to an acceptable level.

The ASIL allocated to the safety requirements implemented by the subsystems or components heavily impacts the concepts and components choice. In [3], a study on the impact of the ASIL levels on the design is conducted. It gives an overview on the capable architecture concepts to meet each safety level. The redundancies needed to be introduced in the concept to meet the ASIL levels and the corresponding development effort, let us conclude that, often, the overall development cost depends on the requirements safety level. The Higher levels lead to higher costs.

In Part 9 of the standard, an ASIL decomposition approach is introduced allowing to reduce the safety levels by decomposing the safety requirements over redundant and sufficiently independent elements. The decomposition when applied results in safety requirements with lower ASIL allocated to the redundant elements. Since higher ASIL implies higher cost, the ASIL decomposition can help to meet the safety requirements without incurring excessive costs. Its application must though verifies different requirements that are detailed in [4]. The reader can refer to [4] and [5] for examples of application of ASIL decomposition.

The decomposition follows predefined patterns. In Fig 1, we can see the different applicable patterns. For example, an ASIL D could be decomposed in three different ways.

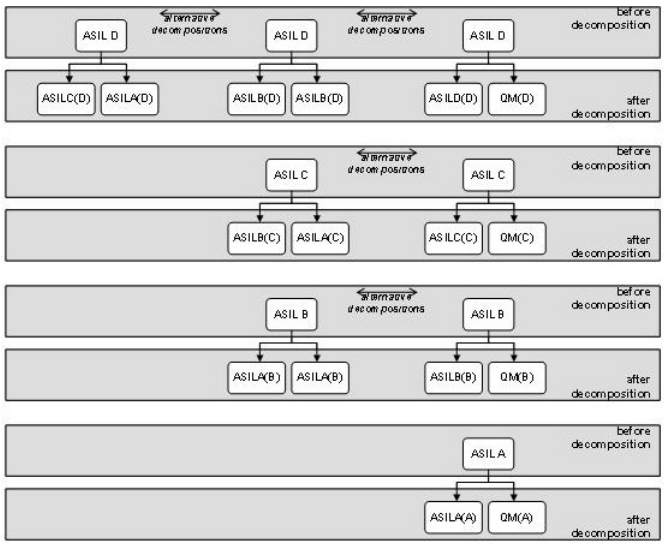

Fig. 1. ASIL Decomposition Patterns

The resulting decomposed requirements could also be decomposed subsequently, since, multilevel decomposition is allowed by the standard. In the design cycle, the designers could resort to ASIL decomposition at different levels : system, subsystems, software and hardware. This results in multiple possible allocations. Finding an effective allocation that answers to the different safety goals without incurring unnecessary development constraints is crucial. Often manually performed,

 ISBN: 978-1-61208-321-6

the complexity of the systems and the multiple failures modes of its sub-systems make it error prone. An automatic approach to allocate the ASIL is indeed needed to ensure the consistency and the optimality of the solution.

In this paper, we propose an approach for an automatic decomposition and allocation of ASILs. It allows finding all the possible allocations not only with respect to the different safety goals but also with respect to the analyst preferences. The approach is based on the minimal cut sets extracted from the fault tree for the considered safety goals. A matrix approach is used to formulate and retrieve the solution set. The paper is organized as follows: In the second section, we review the previous works on the automatic allocation of safety levels. In the third section, we present our approach with a small example to explain the different steps. In the last section, we present the experimental evaluation results on a generic example.

II. Advances on automatic safety levels allocation

The SIL concept was adopted by the standards derived from IEC 61508. The allocation and decomposition process differs though among these standards. For a comparison of the different concepts, the reader may refer to [16]. These differences in the allocation approach makes the works on determination of SILs such as [6],[7] and [8] unapplicable in the ISO 26262 context. The cited works are based on probabilistic approaches to determine the SIL. While, in the ISO 26262, the ASIL determines the quantitative targets concerning the random hardware failures and not the other way around.

In [9], a tool for Development Assurance Level (DAL) allocation, i.e, DALCULATOR is proposed. The allocation and decomposition problem is solved using a Pseudo-Boolean logic. The allocation approach in the ARP-4754, a guideline for development of civil aircraft and systems, seems to present more similarities than the previous works in the fact that it is a qualitative approach. But, such tool can not be used in an automotive context. Unlike the ASIL decomposition, the tool does not aim to a requirement decomposition over the redundant elements. It aims at downgrading the DAL to the really needed level in case of independent elements.

In the ISO 26262 context, [10] proposed an approach to allocate the ASILs to the system components. The allocation process and decomposition algorithm were implemented in HIP-HOPS, a safety analysis and optimization tool [15]. The proposed algorithm exhaustively explores the different possible ASIL allocations and leaves to the analyst the choice of the allocation to be implemented afterwards. This algorithm was enhanced for better performance and presented in [14]. Although the algorithm has the advantage of finding all the possible allocations, it has a main drawback. The processing time could reach dozens of hours for large scale systems.

The approach in [11], on the other hand, avoided the exhaustive search by aiming to find an optimal allocation. In this approach, numerical values are associated to ASILs and are used as a cost indicator. It could be considered as a simple cost model. As for the allocation problem, it is interpreted as a linear program. The set of MCS are interpreted as the constraints. Whereas, the objective function is the cost of the system, considered in this case as the sum of the ASILs allocated to the different components of the system. The main advantages of this approach are the simplicity of implementation and the processing time. The approach takes also into account the preferred ASIL for specific components, which makes it more adapted to industrial cases where the reused components are preferred to be allocated the same ASIL. But, the simple cost model adopted here is the main disadvantage. It suggests in this case that subsystems or components with the same ASIL have the same cost or impact on the solution rating. The result of the optimization could be misleading since subsystems, at the same ASIL, with different complexities or sizes have not necessarily the same cost. A more elaborated cost model is, in this case, necessary for better optimization results.

For large scale systems, [12] and [13] preferred the optimization heuristics as an approach to reach an optimal allocation. The heuristics are known to have better performance in larger problems. The solution is found faster but there is no guarantee that the found solution is a global optimal one. [12] used a penalty based algorithm whereas [13] used a Tabu search algorithm. They tested the approach using different generic simple cost models (linear, logarithmic ...). The results of the runs showed that the obtained solution depends tightly on the used cost model. Though no efficient cost model that would take into account the different parameters were proposed.

In the industry, different cost models are used. But, as far we know, no cost model that efficiently take into account the impact of the ASIL on the development cost has been proposed. We think that in this case it would be complicated to use the linear program and heuristics solving approaches. On one hand, their results depend tightly on the used cost model and on the other hand, they limit the analyst/designer to a unique solution. Thus, we propose, here, an alternative approach to find the possible allocations by interpreting the problem as system of linear equations.

III. ASIL allocation as a system of linear equations

The decomposition patterns specified by the standard can be formalized. By assigning numerical values to the ASIL (QM = 0, A = 1, B = 2, C = 3, D = 4), the patterns are verified by the following equation:

$$\sum ASIL_i = ASIL_{SR} \quad (1)$$

The decomposition is in respect with the patterns if the sum of the values of the allocated ASILs are equal to the original ASIL value of the decomposed safety requirement.

The obtained requirement from decomposition are implemented by sufficiently independent redundant elements. These elements ensure, each separately, the non violation of the

 ISBN: 978-1-61208-321-6

safety requirement. Thus, the safety requirement can be decomposed over elements if their loss, only jointly, lead to the violation of the safety requirement. In a functional architecture of the system, these elements are functions.

When an architecture for the system is conceived, safety analysis techniques such as FTA can then lead us to the functions over which an ASIL decomposition could be applied. MCS helps identifying these functions whose loss jointly leads to the violation of the safety requirements. The safety requirement implemented by these functions can then be allocated ASIL values that verifies equation (1).

Let us assume from this point onward that the ASIL allocated to a function in the architecture refers to the ASIL allocated to the safety requirement implemented by this function. In this case, for every MCS leading to violation of a safety requirement, the functions Fi in the architecture verifies the following equation where the coefficient a_i is null if the corresponding function loss is not in the MCS and equal to 1 otherwise

$$\sum a_i \times ASIL_{Fi} = ASIL_{SR} \quad (2)$$

Applied to all the MCS for all the safety requirements (SRi), the allocation problem could be interpreted as a system of linear equations. In a matrix form, a possible allocation should be solution to the equation (3)

$$\begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix} \times \begin{bmatrix} ASIL_{F1} \\ \vdots \\ ASIL_{Fn} \end{bmatrix} = \begin{bmatrix} ASIL_{SR1} \\ \vdots \\ ASIL_{SRn} \end{bmatrix} \quad (3)$$

During this phase, the analyst could prefer a function to be at a specified ASIL. In other cases, he could specify if two functions are not sufficiently independent. It is possible to retrieve the solutions that match these preferences. An extra constraint could be added to the system in the form of an equation. To avoid increasing the size of the system and the resolution time, we take these constraints into account by adapting the original system. To fix a variable at the preferred ASIL, we withdraw its corresponding column from the system after extracting it from the left part of the equation (3). In order to take into account the non dependency of two variables, we merge their corresponding columns using logic 'OR' operation.

Once obtained, the augmented matrix form of the system taking into account all the constraints, we proceed to solving it. Different solving approaches could be used to solve the linear systems. The allocation problem, though, admits often multiple solutions. Thus, many of these approaches could not be applied since the obtained system's matrix is not always square. The simplest approach, in this case, would be to iterate through all the possible values of the variables. Instead we propose to use a classical approach using the Row Reduced Echelon Form (RREF) of the system.

The RREF is generally computed using Gauss-Jordan elimination. It allows to identify the basic and the free variables which corresponds to the columns with no leading entry. In order to find the solutions, we proceed into allocating to these variables a value in the the range of ASILs numerical values, $\{0,..,4\}$, and deduce the rest of the variables accordingly.

The echelon form could also be used to test the solvability of the system. If equations of the form $0 = Cst$, where Cst is non null, exist, we may deduce that no possible allocation can be found. In this case, the analyst could proceed into ignoring the preferred ASIL or review the system.

The major steps of the solving approach are described as follows:

Algorithm 1 ASIL Allocation Solving approach

Input: Mat(m,n+1): the system augmented matrix form
m : number of MCS
n : number of FM
dependent-var : list of dependent variables
preferred-asil : list of functions and their preferred ASIL
Output: Set of possible allocations
Algorithm:

```
initialization;
Mat ← Merge-dependent (Mat,dependent-var)
Mat ← Fix-value(Mat,preferred-asil)
Mat ← RREF(Mat)
List-free-var ← find-free-var (Mat)
Iterate through the possible values of the free variables
{
Fix-value(Mat, List-free-var)
if solve(Mat) in {0,..,4} then
   Solution = Solution ∪ solve(Mat)
end if
}
```

The RREF and solve functions allows respectively, to calculate the row reduced echelon form and to solve the system. The Fix-value function, on the other hand, allows to fix the value of the variables in the systems. It consists of extracting a new system from the original one by eliminating the fixed variables. The merge-dependent function allows to merge the columns corresponding to dependent variables.

IV. Experimental evaluation

A. Example

Next is an illustrative example for the decomposition. We consider a system with two safety requirements (SR1 and SR2) rated ASIL D and ASIL C respectively. The functional elements F1 ... F5 implement these safety requirements. The Fault Tree in Fig.2 describes how the loss of these functions could lead to the violation of the safety requirements. SR1 and SR2 can be decomposed over the element whose failure lead to the violation of the requirement. For example, SR1 can be decomposed over F2, F3 and F4. In order to find the different possible ASIL combinations that could be allocated to these elements, we use the approach presented in the previous section.

 ISBN: 978-1-61208-321-6

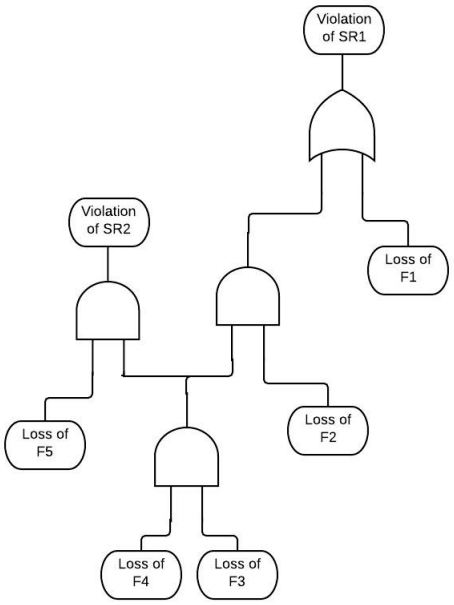

Fig. 2. FT example

We apply the algorithm described above to explain step by step how it works.

From this FT, three MCS lead to the violation of the SRs.

- (Loss of F1) : ASIL D
- (Loss of F2, Loss of F3, Loss of F4) : ASIL D
- (Loss of F3, Loss of F4, Loss of F5) : ASIL C

We suppose that the functions F1 to F5 are sufficiently independent, as required to apply the decomposition. The ASILs allocated to these functions should verify then :

$$ASIL(F1) = 4 \tag{4}$$

$$ASIL(F2) + ASIL(F3) + ASIL(F4) = 4 \tag{5}$$

$$ASIL(F3) + ASIL(F4) + ASIL(F5) = 3 \tag{6}$$

The possible allocations are thus solutions to the following equation :

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix} \times \begin{pmatrix} ASIL(F1) \\ \vdots \\ ASIL(F5) \end{pmatrix} = \begin{matrix} 4 \\ 4 \\ 3 \end{matrix} \tag{7}$$

At this level, it is possible to take into account the preferred ASILs for a specific event.

For example, if we would like the 'F3' to be allocated an ASIL C. The system could be modified to take this information into account by withdrawing the corresponding variable from the system :

Using the augmented matrix:

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 4 \\ 0 & 1 & 1 & 1 & 0 & 4 \\ 0 & 0 & 1 & 1 & 1 & 3 \end{bmatrix}$$

we extract from the last column the third column C_3 multiplied by the numerical value associated to ASIL C $C_6 \leftarrow C_6 - (3 \times C_3)$. C_3 is then removed and the system matrix becomes as follows :

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 4 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix}$$

The next step is to reduce the matrix to its row echelon form. It shows that the variables 'x4' and 'x5', corresponding to the fourth and fifth column in the matrix, are the only free variables (in the case with no preferred ASIL).

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 4 \\ 0 & 1 & 0 & 0 & -1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 3 \end{bmatrix}$$

In this case, we will have 25 iterations as these variables take the values from 0 to 4. We will limit here to the two first iteration where ($x4 = 0$, $x5 = 0$) and ($x4 = 0$, $x5 = 1$) . 1st iteration : The system to solve becomes

$$\begin{bmatrix} 1 & 0 & 0 & 4 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 3 \end{bmatrix}$$

A first allocation could be than deduced where: ASIL(F1)=4; ASIL(F2)=1; ASIL(F3)=3; ASIL(F4)=0; ASIL(F5)=0;

2nd iteration : The system to solve becomes

$$\begin{bmatrix} 1 & 0 & 0 & 4 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 2 \end{bmatrix}$$

A second allocation could be than deduced where: ASIL(F1)=4; ASIL(F2)=2; ASIL(F3)=2; ASIL(F4)=0; ASIL(F5)=1;

Continuing the next iterations will allow us to find the rest of the possible solutions.

B. Results

Applied on the example, it was possible to retrieve all the possible allocations, 10 in total. The processing time was very small, less than a second. We applied it also on different generic examples along with the algorithm proposed in [14] (Algorithm 2) to compare the results and the processing time. The examples are inspired from VALEO project examples in their size and the FT structure. The tests were carried out on a machine equipped with an Intel I5 processor and 4 GB of RAM.

Example Size	Nbr possible allocations	Alg 1	Alg 2
5 Functions, 3 MCS	10	0,01	0,1
10 Functions, 19 MCS	1	0,09	356,16
24 Functions, 30 MCS	3	0,04	0,34
48 Functions, 44 MCS	75	0,76	1,4

TABLE I
TESTS PROCESSING TIME

 ISBN: 978-1-61208-321-6

Both algorithms succeeded in finding all the possible allocations. The processing time logically increased with the size of the problem. But, the algorithms were impacted differently. The algorithm 2 is more sensitive to the length of MCS because of its resolution approach which is based on iterations over the possible allocations for each MCS. With an example where the mean length of the MCS is a little higher, a gap appears between the performances of the two algorithm. Our approach seems, on the other hand, less impacted by this issue. Our approach takes also into account the independence parameter into account, an important factor that can influence the allocations which is not taken into account in the algorithm 2. It has also the advantage of taking into account the preferred ASIL and the possibility of avoiding unnecessary resolution effort if no solution exists.

V. Conclusion and Future Works

In the automotive industry, the safety requirements have a considerable impact on the safety critical systems architecture and cost. The allocation and decomposition of ASILs in the ISO-26262 context is crucial to reach an optimal design whether in complexity or in development cost. Yet the size and complexity of the architectures make the allocation process difficult and error prone if done manually. Several works proposed approaches to automate the process. These approaches provide often a unique optimal solution whereas multiple alternatives are often possible. The objective of these approaches being to assist the analyst or designer, reducing the choice to a unique solution is limiting. Thus, we proposed in this article an approach to interpret and solve the ASIL decomposition problem. It is capable of providing multiple solutions with acceptable processing time for small and medium size cases. Interpreting the decomposition problem as a system of linear equations allowed not only to find all the possible allocations but also to take into account the preferences of the analyst and the dependency between the functions. Whereas in this paper we focused on exploring the different possible allocations, we think that in order to reach an optimal design, it is necessary to investigate the allocation problem with more constraints. Our future works will focus on the automatic allocation at a functional level where more parameters should be taken into account, such as the hardware allocation of the functions. Often physical architecture may impose more constraints on the safety level some functions can guarantee. It could also fail to guarantee the independence requirements which lead to developing some functionalities at higher level than previewed.

References

[1] ISO 26262: Road Vehicles - Functional safety, International Organization for Standardization (2011)

[2] IEC 61508: International Electrotechnical Commission. Functional Safety of Electrical /Electronic /Programmable Electronic Safety-Related Systems. Parts 1 to 7, 1998

[3] D. Liaigre. "ISO 26262 impact on the state of the art of actual automotive safety concepts", 19, (2008)

[4] D. D. Ward, and S. E. Crozier. "The uses and abuses of ASIL decomposition in ISO 26262." System Safety, incorporating the Cyber Security Conference 2012, 7th IET International Conference on. IET, 2012: 1-6.

[5] V. Izosimov, U. Ingelsson, and A. Wallin. "Requirement decomposition and testability in development of safety-critical automotive components." Computer Safety, Reliability, and Security. Springer Berlin Heidelberg, 2012. 74-86.

[6] M. Sallak, C. Simon, and J-F. Aubry. "A fuzzy probabilistic approach for determining safety integrity level." Fuzzy Systems, IEEE Transactions on 16.1 (2008): 239-248.

[7] J. Beugin, D. Renaux, and L. Cauffriez. "A SIL quantification approach based on an operating situation model for safety evaluation in complex guided transportation systems." Reliability Engineering and System Safety 92.12 (2007): 1686-1700.

[8] Y. Lee, J. Kim, and I. Moon. "A verification of fault tree for safety integrity level evaluation." ICCAS-SICE, 2009. IEEE, 2009: 5548-5551.

[9] P. Bieber, R. Delmas, and C. Seguin. "DALculusTheory and Tool for Development Assurance Level Allocation." Computer Safety, Reliability, and Security. Springer Berlin Heidelberg, 2011. 43-56.

[10] Y. Papadopoulos et al. "Automatic allocation of safety integrity levels." Proceedings of the 1st workshop on critical automotive applications: robustness and safety. ACM, 2010.

[11] R. Mader, E. Armengaud, A. Leitner, and C. Steger. "Automatic and optimal allocation of safety integrity levels." Reliability and Maintainability Symposium (RAMS), 2012 Proceedings-Annual. IEEE, 2012: 1-6.

[12] D. Parker, M. Walker, L. Azevedoet, Y. Papadopoulos and R. Araujo. "Automatic Decomposition and Allocation of Safety Integrity Levels Using a Penalty-Based Genetic Algorithm." Recent Trends in Applied Artificial Intelligence. Springer Berlin Heidelberg, 2013. 449-459.

[13] L. Azevedo, D.Parker, M. Walker, Y. Papadopoulos, and R. Araujo. "Automatic Decomposition of Safety Integrity Levels: Optimization by Tabu Search." Proceedings of Workshop CARS (2nd Workshop on Critical Automotive applications: Robustness and Safety) of the 32nd International Conference on Computer Safety, Reliability and Security. 2013.

[14] Maenad. (2012). Model-based Analysis and Engineering of Novel Architectures Dependable Electric Vehicles.

[15] Y. Papadopoulos et al. "Engineering failure analysis and design optimisation with HiP-HOPS." Engineering Failure Analysis 18.2 (2011): 590-608.

[16] J. Blanquart et al. "Criticality categories across safety standards in different domains." ERTS-2012, Toulouse (2012): 1-3.

 ISBN: 978-1-61208-321-6

An Evaluation Scenario for Adaptive Security in eHealth

Wolfgang Leister
Norsk Regnesentral
Oslo, Norway
wolfgang.leister@nr.no

Mohamed Hamdi
School of Communication Engineering
Tunisia
mmh@supcom.rnu.tn

Habtamu Abie
Norsk Regnesentral
Oslo, Norway
habtamu.abie@nr.no

Stefan Poslad
Queen Mary University
London, UK
stefan.poslad@qmul.ac.uk

***Abstract*—We present a scenario and storyline that are part of a framework to evaluate adaptive security in the Internet of Things, also denoted as the IoT. The successful deployment of the IoT depends on ensuring security and privacy, which need to adapt to the processing capabilities and resource use of the IoT. We develop a scenario for the assessment and validation of context-aware adaptive security solutions for the IoT in eHealth. We first present the properties to be fulfilled by a scenario to assess the adaptive security solutions for eHealth. We then develop a home scenario for patients with chronic diseases using biomedical sensors. This scenario is then used to create a storyline for a chronic patient living at home.**

Keywords*—*Internet of Things; assessment scenarios; eHealth systems; adaptive security.

I. Introduction

Wireless Body Sensor Networks (WBSNs) improve the efficiency of eHealth applications by monitoring vital signs of a patient using low-rate communication media and constitute an important part of the Internet of Things (IoT) by bringing humans into the IoT. However, the successful deployment of the IoT depends on ensuring security and privacy, which need to adapt to the processing capabilities and resource use of the IoT. The "Adaptive Security for Smart Internet of Things in eHealth" (ASSET) project researches and develops risk-based adaptive security methods and mechanisms for IoT that will estimate and predict risk and future benefits using game theory and context awareness by Abie and Balasingham [1]. The security methods and mechanisms will adapt their security decisions based upon those estimates and predictions.

The main application area of ASSET is health and welfare. Health organisations may deploy IoT-based services to enhance traditional medical services and reduce delay for treatment of critical patients. A case study will evaluate the developed technologies for adaptive security using both simulation and implementation in a testbed based upon realistic cases. Blood pressure, electrocardiogram (ECG) and heart rate values will be gathered from patients and made anonymous. The sensor data will be stored in different biomedical sensor nodes that are capable of communicating with any of the following connectivity options available: ZigBee, Wi-Fi, 3G, GPRS, Bluetooth, and 802.15.4. For instance, a smartphone with a suitable transceiver could act as an access point between sensor nodes and a medical centre. For the evaluation in the case study, we developed a set of scenarios to assess the adaptive security models, techniques, and prototypes that will be introduced in ASSET. These scenarios describe the foreseeable interactions between the various actors and the patient monitoring system based on IoT.

In computing, a scenario is a narrative: it most commonly describes foreseeable interactions of user roles and the technical system, which usually includes computer hardware and software. A scenario has a goal, a time-frame, and scope. Alexander and Maiden [2] describe several types of scenarios, such as stories, situations (alternative worlds), simulations, story boards, sequences, and structures. Scenarios have interaction points and decision points where the technology under consideration can interact with the scenario. This means that the scenarios developed for a particular situation have to take into consideration the technologies used by the different actors. The importance of scenarios in the assessment of security solutions has been discussed in the literature [3], [4]. This work focuses on the development of scenarios that support the evaluation of adaptive security techniques for the IoT in eHealth.

In this paper, we develop a framework for the assessment of adaptive security solutions. For this, we study a scenario for the home environment, where different Quality of Service (QoS) requirements, contexts and adaptive security methods and mechanisms are analysed. We first define the properties that must be fulfilled by a scenario to assess adaptive security schemes for eHealth. We show the interaction between the scenarios, the threats, and the countermeasures in a global assessment framework for the ASSET project. Second, the scenarios that have been proposed by Leister et al. [5] are reviewed and their adequacy to the evaluation of adaptive security techniques for the IoT is analysed. Finally, we propose a storyline that can support requirements analysis, as well as adaptive security design, implementation, evaluation, and testing.

The rest of the paper is organised as follows: Section II specifies the requirements of adaptive security for the scenario. In Section III, we describe the extension of a previously developed generic system model, which is used for the structure of the scenario in Section IV. In Section V, we present a storyline for our home scenario. Finally, Section VI offers concluding remarks and future prospects.

II. Adaptive security requirements

Designing the scenarios is of central significance for the ASSET project. They depict the operation of systems, here applied to IoT-based eHealth systems, in the form of actions and event sequences. In addition, scenarios facilitate the detection

 ISBN: 978-1-61208-321-6

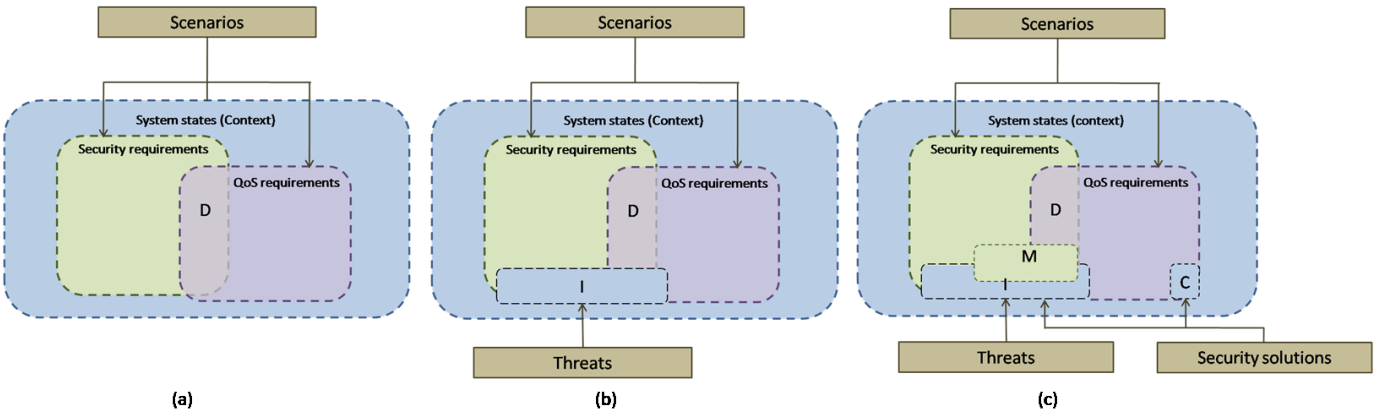

Fig. 1. The ASSET assessment framework.

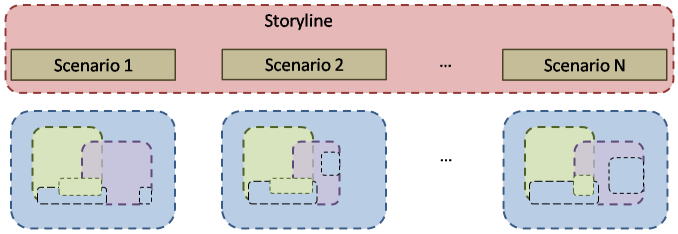

Fig. 2. Illustration of context changes during the execution of a storyline.

of threat occurrences and the identification of the solutions to cope with these threats. In a scenario-based assessment, a set of scenarios is developed to convey the design requirements. With regard to the specific objectives of IoT-based systems, the scenarios should capture two types of requirements:

1) *Security requirements:* Novel adaptive security and privacy mechanisms and methods are required that adapt to the dynamic context of the IoTs and changing threats to them. Thus, the scenarios should be generic enough to capture the security needs for the data processed and exchanged within a patient monitoring system. This is particularly challenging because this system encompasses multiple networking technologies, data, users, and applications, addressing varying processing capabilities and resource use.
2) *Quality of service requirements:* Unlike traditional applications and services relying on communication networks, eHealth applications have stringent QoS requirements. Items such as the communication delay, the quality of the communication channels, and the lifetime of the self-powered sensor nodes are crucial context parameters that have significant impact on the safety of the patient. The scenarios should highlight the needs in terms of QoS and illustrate the dynamic interplay between these needs and the security requirements.

The ASSET scenarios appear as a component of an assessment framework that will serve to improve the applicability of the security techniques proposed in the frame of the project. The other components of the assessment framework are (*i*) a set of threats describing the actions that violate the security requirements, (*ii*) a set of security solutions that mitigate the aforementioned threats, and (*iii*) a set of system states representing the dynamic context in which the patient monitoring system operates. Fig. 1 illustrates the ASSET assessment framework. The security and QoS requirements are the output of the scenario design activity. In other terms, the scenarios should give information about the set of reliable states from the security requirements and the set of states where the QoS is acceptable. The intersection of these sets is the set of desirable states, denoted in Fig. 1(a) by D (Desirable), where the security and QoS requirements are balanced.

One of the intrinsic features of the ASSET scenarios is that the sets of security requirements and QoS requirements could vary in time and space. This will make the threats and the security solutions also vary in time and space. Threats are viewed as actions that generate insecure system states while countermeasures are assumed to thwart the effects of these threats. A threat reduces the set of secure states generated by the scenario of interest and affects the QoS requirements. This is represented by the region I (Impact) in Fig. 1(b). This region represents a set of states that do not fulfil the security or QoS requirements. The countermeasures reduce the size of the set of insecure states generated by the threats. Fig. 1(c) illustrates the effect of the security solutions through the region M (Mitigate). This region extends the set of secure states. Nonetheless, the security solutions can have a negative effect on the QoS, represented by the region C (Cost), consisting of power, processing, memory, and communication overhead.

The elements of this representation will be used in the scenarios during the assessment of adaptive security schemes. The scenarios allow evaluating the potential brought by the security techniques to minimise the effect of the attacks on the context.

For adaptive security solutions, the proposed protection techniques will vary in time and space according to the context. This is not conveyed by the scenario representation of Fig. 1. To overcome this issue, we derive a set of storylines

 ISBN: 978-1-61208-321-6

from the ASSET scenarios. These can be viewed as a sequential application of the scenarios in a way that the selection of the appropriate countermeasures must take into consideration:

- *The space transition between scenarios.* Space encompasses much useful information that affect the security decision-making process. For instance, the location of the WBSN might increase/decrease its vulnerability to threats. Moreover, mobility introduces significant challenges including horizontal and vertical handover management.
- *The time transitions between scenarios (with its implications on the context).* The time interplay between the potential threats and countermeasures has a substantial and dynamic impact on the environment where the patient monitoring system is deployed. The amount of energy, memory, and processing resources are crucial parameters from the QoS perspective and the security solutions have to adapt accordingly. In addition, the state of the communication channel and the proper temporal interplay in all these contexts are important in the selection of the appropriate security decisions.

Fig. 2 illustrates the evolution of the storyline and the underlying impact on the context. Of course, the sequence of scenarios forming a storyline should be consistent so that it translates a real-case situation.

For the assessment of adaptive security protocols and algorithms we can employ multiple tools such as implementation in a lab [6], simulation, and formal reasoning [7]. Here, the scenarios can be connected to the arrangements, which are sets of configuration settings that influences how the formal model operates. Moreover, the properties of a model checker can directly be extracted from the requirements generated from the scenarios.

In the following sections, we develop the scenarios of the ASSET project and show how storylines can be extracted. We also underline the role of the storyline in the assessment of adaptive security techniques for eHealth. Before delving into the details of scenario and storyline engineering, we highlight the major properties that a scenario should have in order to be useful for adaptive security.

III. Extended Generic Model for eHealth Scenarios

Patient monitoring systems are a major data source in healthcare environments. During the last decade, the development of pervasive computing architectures based on the IoT has consistently improved the efficiency of such monitoring systems thereby introducing new use cases and requirements. It is important that these monitoring systems maintain a certain level of availability, QoS, and that they are secure and protect the privacy of the patient. Previously, we have analysed the security and privacy for patient monitoring systems with an emphasis on wireless sensor networks [8] and suggested a framework for providing privacy, security, adaptation, and QoS in patient monitoring systems [9]. We divided patient monitoring systems into four Generic Levels (GLs): (0) the patient; (I) the personal sensor network; (II) devices in the closer environment following several scenarios; and (III) the healthcare information system.

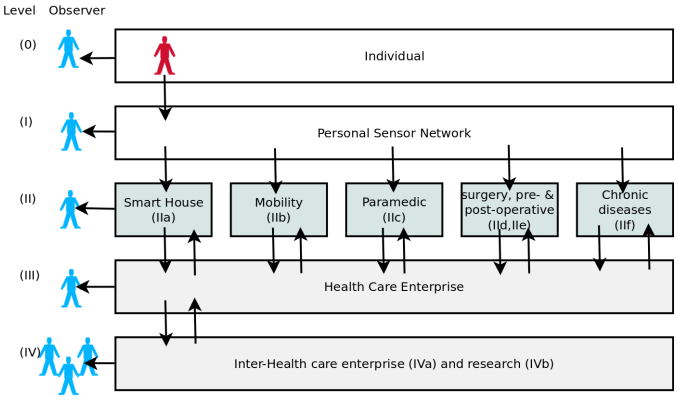

Fig. 3. Generic eHealth framework indicating the use cases in five levels (Extended from [8]).

In this work, we extend the generic model presented by Leister et al. [9] by the definition of three new levels related to the monitoring of chronic diseases, the communication between multiple healthcare providers, and the communication between healthcare providers and medical research institutions, respectively. Consequently, the extended generic model is composed of five levels numbered from (0) to (IV) depending on the logical distance to the patient to whom Level (0) is assigned. Multiple types are considered at Level (II). Note that only one of these types applies at a time. However, it must be possible to switch between the types in Level (II) depending on the activity of the patient. To this purpose, the communication between Levels (II) and (III) is two-way. The key levels of our extended generic model are as follows, as shown in Fig. 3:

(0) **Patient.** This is the actual patient.

(I) **Personal sensor network.** The personal sensor network denotes the patient and the sensors measuring the medical data. These sensors are connected to each other in a WBSN. While this sensor network can be connected randomly, in most cases one special WBSN node is appointed to be a Personal Cluster Head (PCH), which forwards the collected data outside the range of the WBSN.

(IIa) **Paramedic.** The WBSN is connected to the medical devices of an ambulance (car, plane, and helicopter) via the PCH. The devices of the ambulance can work autonomously, showing the patient status locally. Alternatively, the devices of the ambulance can communicate with an external healthcare infrastructure, e.g., at a hospital.

(IIb) **Smart home.** The patient is in a smart-home environment where the personal sensor network interacts with various networks and applications within this environment. The smart home infrastructure might be connected to a healthcare enterprise infrastructure

 ISBN: 978-1-61208-321-6

using long-distance data communication.

(IIc) **Mobility.** The patient is mobile, e.g., using public or personal transportation facilities. The personal sensor network of the patient is connected to the infrastructure of a healthcare enterprise via a mobile device, e.g., a mobile Internet connection.

(IId) **Intensive care/surgery.** During an operation the sensor data are transferred to the PCH or directly to the hospital infrastructure over a relatively short distance. The sensors are in a very controlled environment, but some sensors might be very resource limited due to their size, so extra transport nodes close to the sensors might be needed.

(IIe) **Pre- and postoperative.** During pre- and postoperative phases of a treatment, and for use in hospital bedrooms, the sensor data are transferred from the sensor network to the PCH and then to the healthcare information system.

(IIf) **Chronic disease treatment.** The WBSN data are used by healthcare personnel in non-emergency treatment of individual patients with a chronic disease.

(III) **Healthcare information system.** This is considered a trusted environment. It consists of the hospital network, the computing facilities, databases, and access terminals in the hospital.

(IVa) **Inter-healthcare provider.** Information is shared between different healthcare providers concerning medical information of an individual patient.

(IVb) **Healthcare provider and research.** Information is shared between healthcare providers and medical research organisations for the purposes of research, new solutions development, etc.

Through the potential interactions between these levels, notice that the model can support the elaboration of multiple scenarios where the actors interact by switching from a level to another. The scenarios in healthcare using biomedical sensor networks are quite complex. Therefore, they need to be efficiently structured. We consider two main scenarios (hereafter denoted as *overall scenarios*) and we decompose them into sub-scenarios (hereafter denoted as *core scenarios*). A particular interest is given to the transitions between the core scenarios since these transitions constitute substantial sources of threats. For ASSET, we consider a home scenario (A) and a hospital scenario (B).

Each of these overall scenarios contain a set of core scenarios which are denoted by the scenario identifier A or B, followed by a dash and the core scenario numbering in roman numbers. The transitions between these core scenarios model the interaction between the various components of the patient monitoring system. In this paper, we focus on the Home Scenario (A) where the patient is supposed to be monitored outside a hospital performing normal daily actions. However, to extract useful technical cases for the evaluation phase we need to structure the scenario according to the patient's actions and situation.

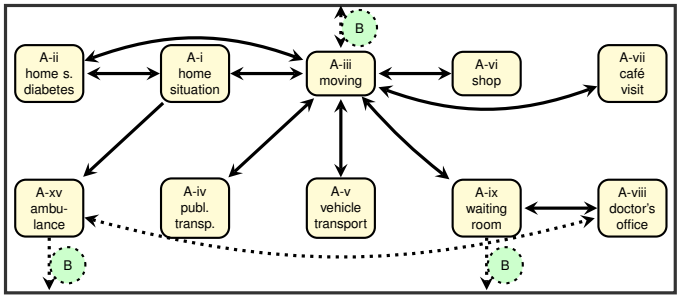

Fig. 4. The Home Scenario with the underlying core scenarios and their transitions.

IV. The Structure of the Home Scenario

Home Scenario (A) envisages that the monitored patient can be in various contexts performing normal daily actions. For example, for a patient with diabetes the following core scenarios can apply:

- The patient is at home or a nursing home using monitoring equipment.
- The patient uses sensors and communicates electronically with the doctor's office.
- The patient uses specific monitoring equipment for diabetes.
- The patient visits the doctor's office regularly and uses public transport or a car to get there;
- At the waiting room the patient can communicate data to the health care infrastructure of the doctor's office.
- The patient regularly takes walking or jogging trips.
- The patient regularly visits a café with friends; this includes walking or commuting with public transport.
- In case of an emergency or planned surgery, the patient may be sent to a hospital with an ambulance.

This list of situations is not yet a useful narrative. It needs to be structured and enriched with, such as the specific context information, the necessary devices of the IoT, the communication channels, and actions of the involved actors. This is done in the core scenarios that describe a specific part of an overall scenario; e.g., a situation a patient experiences. Each core scenarios can be part of several overall scenarios.

1) Home Situation (monitored at home) (A-i): Biomedical sensors are employed in an environment where the patient is at home or in a nursing home. The patient is monitored by a WBSN, and the sensor data and alarms can be transmitted to medical centres and emergency dispatch units.

Here, the sensors might not be monitoring or transmitting the physiological patient data continuously in order to reduce battery power consumption. Depending on a predefined algorithm, abnormal sensor data from certain sensors may be used to activate other sensors autonomously before an alarm is triggered, and sent to a central monitoring unit. In this scenario, the following characteristics are given:

1) Ease of use and non-intrusiveness are important issues.
2) Very low power consumption, enabling a long life span of the batteries, is required.

 ISBN: 978-1-61208-321-6

3) A network infrastructure is available, such as access to the Internet via LAN, WLAN, or mobile networks.
4) Limited mobility, handoff is possible, but infrequent.

Core Scenario A-i could be split up into several sub-scenarios, if necessary, depending on the patient's activities, time of the day, etc. These sub-scenarios may include sleeping, watching TV, kitchen work, or other household activities.

We created a specialised scenario for patients living at home with diabetes monitoring (A-ii). The patient uses a smartphone with a health-diary software that also implements personal health records (PHR) and stores measurements. The measurements are performed using special devices that communicate with the smartphone using Bluetooth. Note that such specialisations also could be described as a part of the storyline of a separate core scenario.

On a regular basis, the patient transmits measurements to the doctor's office, thus synchronising the PHR with the hospital information system; the patient also has an audio-/video-conversation where medical questions are discussed. During these sessions the patient might take pictures with the smart phone camera or perform other measurements.

2) Moving (Walking and Jogging) Scenario (A-iii): The patient does daily training, i.e., jogs in the nearby park, or does shorter walks from the home to the public transport, to the café, shop, or doctor's office. A common feature in these situations is that the patient needs to use a smartphone as a device that collects sensor data, using the mobile networks to transmit the data. When walking or jogging in the park many other people and their devices might interfere with the communication of the smartphone.

When walking in the woods, there might be several spots which are not covered by a mobile network. In this case, the signal is so weak that only an emergency calls from another provider can be done. While data traffic is not possible, SMS messages can be used to send data with very low bandwidth, possibly after several retries. For an average walking trip, this outage may last for some minutes.

3) Transport Scenarios: Core Scenario A-iv presents a situation where a patient commutes to a doctor's office or to a café using public transport. Here, the patient needs to use a smartphone as a device that collects sensor data, using the mobile networks to transmit the data. Blind spots without connectivity to a mobile network, roaming, varying data transmission quality, etc., are parts of this scenario. This scenario can be applied to long-distance trains, planes, etc.

Core Scenario A-v represents the scenario where a patient uses his own or another's (private) car to commute to a shop, a café, or the doctor's office. Here, the patient needs to use a smartphone as a device that collects sensor data, using the mobile networks or networks installed or used in the car to transmit the data. Blind spots without connectivity to a mobile network, roaming, varying data transmission quality, etc., are parts of this scenario.

4) Café Scenario (A-vii): The patient visits a café. Here, the patient needs to use a smartphone as a device that collects sensor data, using mobile networks or café's WLAN zone for data transfer. Switching between the WLAN and mobile networks may occur, the WLAN might be of varying quality, many other café visitors may interfere, or the WLAN might not actually be connected to the Internet.

5) Doctor's Office Scenario (A-viii): The patient is in the doctor's office, usually after some time in a waiting room (A-ix). Here, the patient can have extra sensors attached. These extra sensors, as well as the existing sensors, can communicate with the doctor's infrastructure either through the smartphone of the patient, or directly, depending on the needs. A doctor can change a sensor's characteristics, which requires the possibility to re-program the sensor devices.

6) Waiting Room Scenario (A-ix): The patient is in a waiting room at a doctor's office or a hospital. Patients that are known to the healthcare system can be connected from their smartphone to the healthcare network; here, specific actions for collecting data from the device or other preparations can be performed. Once the patient is in the range of the waiting room, the smartphone can transfer large amounts of stored patient data directly to the infrastructure of the medical centre via short-range communication, instead of using long-range mobile communication.

7) Other scenarios: In ASSET other scenarios have been developed which are omitted here. Most of these are specific to the hospital scenario B. For completeness, we mention a scenario where patients are brought to a hospital in an ambulance (B-xv).

V. Storyline for the home scenario

We developed the storyline for the home scenario as follows: Petra has both a heart condition and diabetes. In a hospital, she had two sensors placed in her body: one heart sensor and one blood sugar sensor. In addition, she uses external sensors to measure blood pressure, heart beat, inertial sensors, etc., as well as a camera. Petra is living in her home that has been prepared for the monitoring system and is commissioned with the necessary data connections so that her vital signs can be periodically reported to the healthcare personnel in levels (II) (nurse or doctor) or (III) (patient records) as introduced in Fig. 3; several technologies can be applied to achieve this.

The patient monitoring system is set up so that the sensor data are transmitted wirelessly (several transmission technologies are possible) to a smartphone that acts as PCH. The PCH communicates with the hospital infrastructure (Level (III)).

1. Petra is now being monitored at home but data is acquired remotely (A-i); the following requirements are important:
   a. Petra wants her data to remain confidential from neighbours, i.e., people close-by, but outside her home;
   b. Petra wants her data to remain confidential from visitors, i.e., people inside her home.
2. Petra takes a bath in her home (planned sensor acquisition disruption; A-i);
   a. the sensors are water-proof; the PCH is close enough to receive signals;
   b. the sensors need to be removed;

 ISBN: 978-1-61208-321-6

   i. a change in the values implicitly indicates the sensor removal; or
   ii. patient must notify the PCH about the sensors going off-line;
3. Petra is sleeping and sensors fall off (unplanned sensor acquisition disruption; A-i).
4. Petra leaves her home for training outdoors or a stroll in the park nearby (A-iii).
5. Petra leaves her home to visit her friends in a café (A-vii, A-iii, A-iv, A-v).
6. Petra visits her regular doctor for a check-up; the doctor's office is in walking distance from her home (A-iii, A-viii, A-ix).
7. Petra becomes ill and is transported by an emergency ambulance to the hospital (B-xv); transition to the Overall Hospital Scenario B.

To conduct an efficient threat analysis of this storyline, we apply security objectives introduced by Savola and Abie [10] and Savola et al. [11], who stated that adaptive security decision-making should adapt requirements for privacy and data confidentiality based on the data processing needs, roles of stakeholders, regulations and legislation, and the privacy level of data indicated by privacy metrics. For example, the security requirement pointed out in Step 1.a of the storyline is related to confidentiality and privacy, which are often emphasised in healthcare. Strong confidentiality algorithms, key distribution, associated processes, and compliance to appropriate privacy legislation and regulations are crucial.

VI. Conclusions

We highlighted the role of the scenarios in the assessment framework for IoT-based adaptive security solutions in eHealth. This is based on a generic system model, the requirements for eHealth applications, and a generic assessment framework. The Home Scenario of the ASSET project covers multiple core scenarios representing various situations. These address specific requirements related to the context, the data-communication, the devices, and the actions of the involved actors. The core scenarios are specific to the eHealth case, and make it possible to identify relevant cases that need to be evaluated, such as situations where IoT devices need to be removed or disconnected, the use ample communication channels, or the impact of mobility.

A storyline for a home patient with chronic diseases has been described and analysed. In the future, the overall scenarios, as well as the underlying core scenarios and storylines will be used in the ASSET project to evaluate the developed algorithms within adaptive security.

VII. Acknowledgments

The work presented here has been carried out in the project ASSET – Adaptive Security for Smart Internet of Things in eHealth (2012–2015) funded by the Research Council of Norway in the VERDIKT programme. We wish to thank our colleagues involved in this project for helpful discussions that made this study possible.

References

[1] H. Abie and I. Balasingham, "Risk-based adaptive security for smart IoT in eHealth," in BODYNETS 2012 – 7th International Conference on Body Area Networks. ACM, 2012.

[2] I. F. Alexander and N. Maiden, Eds., "Scenarios, Stories, Use Cases: Through the Systems Development Life-Cycle". John Wiley & Sons, 2004.

[3] S. Faily and I. Flechais, "A meta-model for usable secure requirements engineering," in SESS – ICSE Workshop on Software Engineering for Secure Systems. Association for Computing Machinery (ACM), 2010.

[4] H. Mouratidis and P. Giorgini, "Security attack testing (SAT)–testing the security of information systems at design time," Information Systems, vol. 32, no. 1, Jan. 2007, pp. 1166–1183.

[5] W. Leister, H. Abie, and S. Poslad, "Defining the ASSET scenarios," Norsk Regnesentral, NR Note DART/17/2012, Dec. 2012.

[6] Y. B. Woldegeorgis, H. Abie, and M. Hamdi, "A testbed for adaptive security for IoT in eHealth," in ASPI 2013 – International Workshop on Adaptive Security & Privacy management for the Internet of Things. ACM, 2013.

[7] W. Leister, J. Bjørk, R. Schlatte, E. B. Johnsen, and A. Griesmayer, "Exploiting model variability in ABS to verify distributed algorithms," International Journal On Advances in Telecommunications, vol. 5, no. 1&2, 2012, pp. 55–68. [Online]. Available: http://www.iariajournals.org/telecommunications/ [Accessed: 1. Dec 2013].

[8] W. Leister, T. Fretland, and I. Balasingham, "Security and authentication architecture using MPEG-21 for wireless patient monitoring systems," International Journal on Advances in Security, vol. 2, no. 1, 2009, pp. 16–29. [Online]. Available: http://www.iariajournals.org/security/ [Accessed: 1. Dec 2013].

[9] W. Leister, T. Schulz, A. Lie, K. H. Grythe, and I. Balasingham, "Quality of service, adaptation, and security provisioning in wireless patient monitoring systems," in Biomedical Engineering Trends in electronics, communications and software. INTECH, 2011, pp. 711–736.

[10] R. Savola and H. Abie, "Metrics-driven security objective decomposition for an e-health application with adaptive security management," in ASPI 2013 – International Workshop on Adaptive Security & Privacy management for the Internet of Things. ACM, 2013.

[11] R. Savola, H. Abie, and M. Sihvonen, "Towards metrics-driven adaptive security management in e-health IoT applications," in BODYNETS 2012 – 7th International Conference on Body Area Networks. ACM, 2012.

 ISBN: 978-1-61208-321-6