KIEM-projecten zijn projecten van minimaal één private partner met één of meer kennisinstellingen gericht op het realiseren van een concrete innovatie. Een KIEM-subsidie kan **niet** gebruikt worden voor:

- Het leveren van uitsluitend goederen;
- Het geven van cursussen;
- Het financieren van studenten of stagevergoedingen.

Please write your application **in English** and make sure that your application is easily readable. We advise a minimum font size of 10pts. Your application should be comprehensive as a separate entity.

Project details

1. Basic details of the project

1a. Title of the proposal An integral SAfety / Security Analysis fraMework
1b. Project acronym SamSam
1c. Project duration: 12 months

2. Details of the project consortium

2a. Contact details of *all* applicants

Main Applicant / Principal Investigator - PI *(from academia)*			
Name, first name, title(s)	Stoelinga, Mariëlle, Dr		female
Date of birth	11.08.1972	Date of PhD	23.04.2002
University	University of Twente		
Department	Computer Science	Section	Formal Methods & Tools
Postal Address	PO Box 217	Zip/city	7500 AE Enschede
Tel / Fax	053-4893773	Email	m.i.a.stoelinga@utwente.nl
Position	*Associate Prof. (UHD)*	End date contract	n/a
Project Manager – PM *(affiliated to a private partner)*			
Name, first name, title(s)	Van Ekris, Jaap, Ir		male
Date of birth	26.03.1972	Date of PhD	n/a
Company	Delta Pi		
Postal Address	Postbus 214	Zip/city	6920 AE Duiven
Tel / Fax	0316-285682	Email	j.vanekris@delta-pi.nl

2b. Past performance of the applicants

Max 1 page per applicant, including a maximum of five relevant items per applicant (academic and private), and a total of not more than 25 items may be listed. Items can be: (scientific) publications, patents, inventions, products successfully introduced to the market, etc.

Dr. Mariëlle Stoelinga is an associate professor in the Formal Methods and Tools (FMT) group at the University of Twente (UT). She is an active and well-established researcher (h-index 24; 2064 citations in total) in the area of risk management for computer systems, and develops quantitative risk assessment methods to model, predict, and improve the risks of complex systems. These methods include fault tree analysis, attack trees, architectural reliability modeling, and model-based testing. Stoelinga has developed compositional methods to simplify and improve (dynamic) fault tree analysis [2], which led to the DFTCalc tool set [12]. Recently [46], this framework has been extended with maintenance, and applied in two large case studies in railway engineering, in collaboration with ProRail and NedTrain. Within the EU project TREsPASS, Stoelinga investigates quantitative cybersecurity. In particular, she has developed various innovative methods for attack tree analysis [18,19,41], and confidentiality [17,38,39].

She (co-)supervised a large number of PhD students and postdocs, and has been invited as a keynote speaker at several venues. She has written over 60 peer-reviewed publications in scientifically renowned venues, two of which obtained best paper awards.

Stoelinga has coordinated several national projects, and a WP in the EU FP7 project Quasimodo, on extra-functional system aspects. At the moment, she is the PI of ArRangeer project, funded by STW and ProRail, to integrate fault tree analysis and maintenance. She also leads the BEAT project, funded by a prestigious NWO-top grant. She is a key participant in the EU FP7 project TREsPASS, on quantitative sociotechnical security analysis. From these funds, Stoelinga has formed a research group consisting of 6 PhD students, a number of MSc students, and visitors.

Key achievements. Stoelinga's key achievements are

- Excellent scientific track record: Google Scholar H-index 24, total number of citations 2064.
- Development of DFTCalc, an analysis tool for dynamic fault trees [2,12,46].
- Project leader of several national research projects, leading role in several EU projects.
- Ample experience with industrial-academic partnerships, eg in the STW/ProRail project.

Ir. Jaap van Ekris is a specialist in Reliability, Availability, Maintainability and Safety (RAMS) of highly critical embedded systems. He has been responsible for the software reliability and safety analysis of a large number of high-profile safety-critical assets, including the nuclear power plant in Borssele, the EuroControl Air Traffic Control Center, the Oosterstelde storm surge barrier, the baggage handling systems of Heathrow T5, and the landing gear of the Boeing 747 airplane. He has a secondary specialisation in IT security, where he was responsible for the integrity of the Dutch passports, the Dutch passport production, the Dutch National Internet voting system, and the security of the primary safety systems of the Schweizerische BundesBahn (SBB).

Currently Van Ekris is the chairman of the TOPAAS workgroup, responsible for the development and maintenance of the TOPAAS software reliability quantification method, used in all large infrastructure works in the Netherlands.

Finally, Jaap van Ekris is a PhD-student at Eindhoven University of Technology, working on customer satisfaction in mission critical environments. He has published several scientific papers [20]-[22].

Key achievements. Van Ekris' key achievements are

- Ample experience with RAMS analyses for critical infrastructures
- Ample experience with cybersecurity analyses
- Driving force behind the TOPAAS method for software reliability
- Publication of several scientific papers [20]-[22]

3. Summaries of the research proposal
3a. Formulation of the main goal(s) of the project

The goal of the SamSam project is to develop an integral model-based analysis framework for Reliability, Availability, Maintainability and Safety (RAMS[1]) and cyber security aspects. Usually, RAMS and security are considered separately, which is inefficient and ineffective, since RAMS and security are tightly connected and often lead to conflicting requirements: measures that increase reliability or safety can be exploited by hackers; measures that increase security often decrease the system safety or availability. The aim of the SamSam project is to integrate two existing, prominent frameworks for RAMS and security analysis, (namely, attack trees and fault trees), and evaluate these via three industrial case studies. Thus, the expected project results are:

- The integration of existing methods for RAMS and security.
- Its evaluation via three industrial case studies.
- An instruction manual for integral RAMS/security analysis, based on our findings in the case study analysis.
- Dissemination of project results via scientific publications, a workshop, and consultancy products.

3b. Popular summary
Please provide in Dutch (for copy/paste purpose):

- *SamSam:* safety en cybersecurity analyseer je samen!
- Dr. M.I.A (Mariëlle) Stoelinga, f, Universiteit Twente, Formele Methoden & Tools.
- Delta Pi.
- A text summarizing the essence of the project in easily accessible language (about 50 words).

In het SamSam-project ontwikkelen we een geïntegreerd afwegingenkader om zowel beschikbaarheid, veiligheid (RAMS), als security in samenhang te analyseren: meestal worden RAMS en security apart van elkaar geanalyseerd. Dit is onwenselijk, aangezien zij elkaar (negatief) kunnen beïnvloeden: Maatregelen die de veiligheid verhogen, kunnen door hackers misbruikt worden; maatregelen die de security verhogen kunnen juist de veiligheid of beschikbaarheid verkleinen. Het SamSam-project integreert bestaande safety- en securityraamwerken, aan de hand van drie industriële cases.

[1] See Section 7c for a glossary of terms.

4. Classification

4a. Field(s) of research

Main research field: 16.10.00 (Computer systems, architectures, networks)
Other relevant research field(s): 16.20.00 (Software, algorithms, control systems)

4b. Suitability with the Call IPPSI and the Roadmap ICT

Indicate why your proposal fits the Call for Proposals *IPPSI – Innovative Public Private Partnership for ICT* and *the Roadmap ICT for the Top Sectors*. Use maximal ½ page.

Our proposal fits in Action Line 1 of the Roadmap ICT: *ICT one can rely.*

Connection to the Roadmap*.* The Roadmap ICT for the top sectors states in Chapter One:

> *"In many parts of society ICT is vital. Healthcare systems, energy, water, and many other aspects of society need ICT systems to function. As a society grows more and more dependent on ICT, it is essential that we invest in the level of trust worthiness of this technology. Trust implies reliable, dependable, safe, and secure systems. Recent events have shown that trust does not come easily but goes quickly. And, trust is not only a technical issue. Reliability and dependability of ICT systems need to be developed further, explicitly modeling risks*.''

This is exactly what we are going to do: model the combination and safety and security risks in critical assets, like healthcare, transportation and energy supply systems. This will provide practitioners the required tooling to assess the necessity and effects of security measures, allowing an integral approach to risk management. In that way, the governing bodies can assess whether or not the RAMS and security goals are met on a continuous basis; or whether additional measures are needed, like more redundancy, different access policies, etc. As expressed in the project goals, we will assess their applicability via three industrial case studies.

Connection to Action Line "ICT ONE CAN RELY ON"*.* The current proposal is clearly related to the Action Line *ICT one can rely on* that focuses on how ICT-services can be provided safely and reliably and can be used with confidence. More specifically, our project matches Action Lines subtheme on *Secure and vital ICT*, where the Roadmap states

> *"Further in the future, the ambitions of the top sectors call […] by developing ICT-technologies for reliability through design for service, continuity and security management."*

Thus, the roadmap often mentions cyber security and RAMS in combination. As stated, current risk analysis methods often focus on only one of these aspects, whereas our project aims at an integral approach, enabling RAMS and security trade offs.

5. Other grant applications N/A

Proposed Project (max. 4 pages in total for section 6)

6. Description of the project

See also the evaluation criteria in section 4.2 of the 'Call for Proposals IPPSI' for more details. The description must clarify the character, approach and capitalize the valorisation of the proposed project. It should illustrate why this project fits the Roadmap ICT for the Top Sectors, i.e. the proposal:

- addresses one or more new issues
- leads to innovation in ICT
- (has the potential to) contribute(s) to industrial innovation.

6a. Project description and Innovative aspects

Context and motivation. Our society critically depends on the correct functioning of infrastructures like energy supply, medical devices, railroads, waterways and flood prevention structures: their disruption may lead to serious economic damage, and the loss of lives. Therefore, these assets have to meet high standards, both in terms of system availability, safety and security, in order to prevent unplanned service disruptions due to component failures or malicious attacks.

Safety and security measures, however, are often conflicting. Measures that increase system safety, decrease security and vice versa: Installing a firewall, for instance, prevents malicious attacks via the internet, but may reject (and has done so in practical cases) non-malicious packages with essential operational information; emergency stop systems increase safety, but can be exploited (and again, have been) by intruders to halt complete installations. Current risk analysis methods for critical infrastructures, however, focus either on safety/availability (FMECA [26], fault tree analysis [4,5]) or on security (structured analysis [47], attack trees [3]) aspects. As a result, suboptimal solutions are implemented, or money is wasted, for instance, because proposed security measures are rejected by the safety standards. Field research has shown that current owners of large infrastructure universally recognize that safety requirements effectively block many security measures, because their effects on safety cannot be predicted.

Delta Pi (Delta Performance Improvement BV) is an innovative SME specialized in risk analysis for critical infrastructures. Delta Pi provides a strategic risk consultancy for organizational processes, as well as technical infrastructure, based on qualitative and quantitative models. Markets targeted are both the public sector (with customers including Rijkswaterstraat, ProRail, the Dutch navy) as well as industry (including Tata Steel, ASML, Siemens, KPN, VolkerWessels). Delta Pi feels the need for integral safety and security analysis daily: not only do customers ask for it; practical analysis shows that good operational performance often requires an integral analysis framework.

State-of-the art in RAMS and cybersecurity analysis. *RAMS analysis* has a long history [24], starting in the late 19^{th} century with mass production systems and statistical quality control, boosting after world war II. Following [27], we categorize RAMS analysis techniques in three groups (1) *structured methods* based on textual descriptions or spreadsheets, such as Failure Model and Criticality Analysis (FMECA, [26]) and HAZard and OPerability study (HAZOP, [28]). (2) *domain-specific languages* such as fault trees (FT, [4,25]), event trees

[39], reliability block diagrams [29], (3) *architectural approaches*, based on AADL [33] and UML/MARTE [25] that augment existing architectural approaches with RAMS aspects.

All these methods allow both quantitative and quantitative analysis [39]. Quantitative analysis, while being more labor intensive than a qualitative approach is often preferred [11], e.g., to prioritize potential measures, and for certification. Quantitative analysis takes as a starting point the failure probabilities for the system components, and derives the failure probabilities for the entire system. In particular, system metrics like the *reliability* (i.e., the probability of failure during the mission time), the *availability* (i.e., the average percentage of time that the system is functional), and *MTTF* (i.e., mean time to failure) are of interest. In practice, FMECAs and fault trees are by far the most popular, being deployed by companies such as NASA, ESA, SpaceX, Airbus, the FAA, Honeywell, Toyota, etc.

Cybersecurity analysis is a more recent field; see [16,34,40] for overviews. Following the same categorization into (1) *structured methods,* (2) *domain-specific languages* and (3) *architectural approaches*, we see that the structured, more informal methods dominate the security field [16]. Examples are the factor analysis method FAIR [47]. Among domain-specific languages, attack trees (AT, [3]), and their variants like attack-defense [10] and attack-countermeasure trees [42], are the most prominent. Architectural security analysis frameworks can further be divided into two groups: Some are more geared towards the technical infrastructure, such as the ADVISE framework [35] and the UML-based CORAS framework [44]. Others take the enterprise architecture as a starting point, such as the Open Group standardized language ArchiMate [48].

Like fault trees, attack trees can be used to compute propagation of risks: if we equip the basic attack steps with probability, then one can compute the probability that successful system attack occurs. However, the risks in attack trees are slightly different from fault trees: whereas fault trees consider the probability that a component or subsystem fails, attack trees often predict the probability that an attack is successful, given that it was attempted.

Combined RAMS/security analysis. There are a few frameworks that combine safety and security analysis: Security HAZOP [36] and FMVEA [43] respectively extend HAZOP and FMECA analysis with security aspects. There are some few promising approaches that combine attack trees and fault trees as well [7, 30,31,32]. However, these are mostly qualitative and/or cannot model defences.

Ongoing research on FTs and ATs aims at making the analysis faster and more versatile. Our earlier work concerns compositional analysis techniques for FTs [2,12,46] and ATs [18,19,41]: we translate each FT or AT element into a stochastic model, i.e., a Markov chain or their variants. By composing (while performing minimization at each step) all individual models together, we obtain a stochastic model for the entire tree, which can then be further analysed with standard stochastic methods. This method is fast and flexible: novel constructs (such as maintenance policies [46]) can be easily integrated by providing their underlying Markov model. As such, these compositional techniques form an excellent starting point for the integration of FTs and ATs.

Challenges and shortcomings of existing approaches. Whereas RAMS and security analysis are well-established, their combination is not so: a rigorous, quantitative framework for combined RAMS and security analysis is lacking.

Moreover, combined RAMS / security frameworks have hardly been applied and validated in practice. For example, it is not clear how a combined attack-fault tree looks like: do the current modelling constructs from FTs and ATs suffice, or are additional constructs required? What kind of information do the leaves, (which model the components failures or basic attack steps) need to carry?

Goal. The goal of this project is to integrate existing RAMS and security techniques, leading to an integral framework for RAMS and security trade offs, based on scientifically sound methods. We will focus on

1. *The integration of attack trees*[2] *and fault trees,* leading to attack fault trees (AFTs). As stated, we believe that our compositional analysis techniques FTs and ATs provide an excellent starting point for their integration and quantitative analysis methods.
2. *Empirical evaluation.* We plan to investigate, via three existing industrial case studies, whether existing RAMS and security analysis can be combined into an integrated AFT: given an existing fault tree, and a security risk analysis, can we integrate the two into a meaningful AFT?
3. *Documentation.* With a leading role for Delta Pi, we want to develop a manual providing guidance in the construction of AFTs, similar to ProRail's *Leidraad RAMS* [11], NASA's *Fault Tree Handbook* [1,5], and Rijkswaterstaat's *Probabilistisch Beheer & Onderhoud* [23].

Approach. In this project, we take a case study-driven approach. We will analyze three cases, of increasing complexity, and base the methodology (i.e., the conceptual integration of ATs and FTs) on our findings during the case analysis. All cases are in the domain of waterway engineering, keeping focus during the project. The cases will be provided by Delta Pi, in collaboration with Rijkswaterstaat and have been chosen in such a way that (1) RAMS and security aspects play a crucial role (2) both RAMS and security risks analyses have been performed in isolation, and extensive documentation is available about safety (FMECA's, fault trees) and about security (vulnerability / threat analysis) (3) A sense of urgency is felt by the stakeholders for integral RAMS / security analysis.

Case 1: The Oosterscheldekering. The Oosterschelde storm surge barrier is owned by Rijkswaterstaat and is responsible for protecting the Zeeland-province against floods. Delta Pi actively supports Rijkswaterstaat by analysing and improving the RAMS aspects of this storm surge barrier on a structural basis. Given the IT-design of the barrier, the current understanding is that the barrier is not at risk for cybercrime. The main questions concern the re-evaluation of the existing security assessment:

- Have we missed any cybersecurity risks?
- Are these risks worth quantifying and relating to RAMS analysis? (i.e., can cybercrime quantitatively be related to unavailability of the barrier)?
- How to RAMS and security risk compare? What are trade offs?

Case 2: Maeslantkering. The Maeslantkering storm surge barrier is owned by Rijkswaterstaat and protects the port and city of Rotterdam against floods. As

[2] Even though we use the term Attack Tree, we will use variants that include countermeasures, such as attack-defense trees and attack-countermeasure trees.

such, it has extreme high requirements regarding both availability and reliability (RAMS): if the barrier is not available at the right time, then the port and city of Rotterdam will be flooded, with many deaths as a result. If the barrier closes when it should not, the port of Rotterdam will be closed, causing high economic damage. Delta Pi actively supports Rijkswaterstaat by analysing and improving the RAMS aspects of the Maeslandkering. Security introduces a fundamentally new challenge for RAMS-analysis: it is clear that cybercrime has a negative effect on RAMS achievements, but many security measures also have so as well. The main questions aim at introducing security aspects in the existing RAMS analysis:

- What are the vulnerabilities and how can these be exploited?
- How do attacks propagate through the system?
- Which countermeasures are most effective?
- From a quantitative point of view: is the cure worse than the disease?

Case 3: Zeesluis IJmuiden OpenIJ consortium aims to realize the world's largest lock near IJmuiden and will have to realize a highly reliable operation, free from cyber threats. Delta Pi is responsible for managing the RAMS achievements of this lock. Balancing these conflicting demands during design phase is essential for a good design and reliable operation. Apart from the questions posed for Case 2 above, important issues are:

- Does a quantified security approach lend itself as one of the drivers in a reliability-centered design and maintenance approach?
- Recommendations on the design and deployment of the lock.

Expected results. Thus, the expected results of the SamSam project are:

- Insight in the integral modeling and analysis of RAMS and security risks
- Practical evaluation of combined RAMS/security analysis
- A manual describing how to perform integral RAMS/security analysis in practice.

6b. Valorisation potential of the proposed research

Business Innovation. Critical infrastructures are under continuous security threats: cyber attacks are more and more common and their damage can be enormous. Therefore, there is a large market demand for integral safety and security framework: Delta Pi's customers ask for it.

The results of the SamSam project allows Delta Pi to develop new products, which is an absolute must if they want to keep their competitive edge in RAMS consultancy. In particular, the expected project results allow Delta Pi to

1. Implement the project results in their RAMS tools; the implementation itself falls outside the scope of this project
2. Apply the project results in their consultancy products
3. Attract new customers, and extend existing consultancy contracts
4. Develop innovative training products

6c. Ownership and Transfer of knowledge

Briefly describe the IPR agreements within the team and how the project results are disseminated.

IPR agreements. Delta Pi's overall business strategy is to actively transfer knowledge to its customers. Then, it is important to be able to use, without limitations, the same methods and tooling for all customers. Especially when it comes to the analysis methods, such as TOPAAS and the SamSam-analysis

framework (which should ideally become mandatory in project tenders) then it is impossible to intellectually protect such methods by IP. Just like the TOPAAS method that was co-developed by Delta Pi, the SamSam analysis framework will be released into the public domain, and Delta Pi will earn its revenues by selling its expertise in the applying these methods.

Whereas the SamSam analysis methodology will be open, the particular models, data, and results concerning the case studies will be proprietary.

Dissemination of results. Our dissemination plan comprises four activities:

- *Scientific publications,* targeting internationally outstanding venues.
- *Publications in professional magazines,* such as Ingenieur, Technisch Weekblad, and Tijdschrift van de Nederlandse Vereniging voor Nederlandse voor Risicoanalyse en Bedrijfszekerheid.
- *Professional training,* which will be commercialized by Delta Pi.
- *Organization of a workshop,* which presents the final project results and that brings together RAMS/security professionals, as well as researchers.

7. Description of the proposed work plan

7a Proposed work plan

Please indicate as concretely as possible (e.g. by a Gantt chart) how the entire project is to be phased, in periods. More specifically, indicate which activities are likely to be carried out. Indicate which tasks will be undertaken by which members of the research team, **including the in kind efforts by the private partners**. If possible specify milestones and deliverables throughout the duration of the project. The project duration should not exceed one year.

		M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12
WP1	Case 1												
	Case 2												
	Case 3												
WP2	Manual												
WP3	Integration												

Workpackages. We plan to organize the project in three workpackages:

- Workpackage 1 (Leader: the postdoc) concerns the modelling, analysis and evaluation of the 3 case studies.
- Workpackage 2 (Leader: Stoelinga) concerns the methodological aspects of the project, namely the conceptual and mathematical integration of attack trees and fault trees.
- Workpackage 3 (Leader: Van Ekris) concerns the writing of the manual for construct AFTs in practice, especially useful for Delta Pi's innovation.

Tasks. Given our case study driven approach, we arrange the tasks based on the cases. Each case study (WP1) consists of the following steps:

1. *Modeling*
    - Based on the system documentation and interaction with experts, we will identify the potential system failures and attacks, and the way they propagate through the system.
    - Then, we will model these attacks as a combined fault/attack tree.
    - Finally, we will collect quantitative data for the component failures and the basic attack steps. That is, we will equip the leaves of the AFT with quantities.

2. *Analysis*
    - Using our tool set [12,46], we will analyze the AFT for various RAMS and security metrics, such as the failure and attack probabilities, reliability, MTTF.
    - Determine the most severe attacks and system failures.
3. *Taking countermeasures*
    - Model the potential countermeasures for the most severe security attacks.
    - Analyze the effects of the counter measure on the system reliability, availability and attack probability and model trade offs, eg via Pareto curves.
4. *Evaluation*
    - We will evaluate both the process and the analytical outcomes the three steps above, via discussions and interviews with experts.

Parallel to the steps above, we will carry out the tasks in WP2 and WP3:

5. *Integration of ATs and FTs (WP2).*
    - Focus is on the methodological integration of ATs and FTs, their semantics, and analysis algorithms.
6. *Documentation (WP3).*
    - Based on the modeling phase in WP1, we will prepare a manual with guidelines for the construction of AFTs.

Moreover, all WPs will be involved in the dissemination of the results.

7b. Description of the consortium

Describe in what manner will be cooperated between the partners in the consortium. Also include possible secondment of requested personnel in the project.

	Contribution	**Affiliation**	**Expertise**
Mariëlle Stoelinga	0.1 FTE	University of Twente	Fault tree analysis, attack tree analysis, stochastic analysis
Postdoc	1.0 FTE	University of Twente	Security and RAMS
Jaap van Ekris	60 hours	Delta Pi	RAMS, fault tree analysis, quantitative risk analysis
Joris ter Heijne	60 hours	Delta Pi	RAMS, cybersecurity

The project will be carried out in close collaboration between the University of Twente and Delta Pi.

Mariëlle Stoelinga is the principal investigator of this project. She will be responsible for the daily supervision of the postdoc, the scientific quality and relevance, and the alignment of scientific and business perspectives of the project.

Jaap van Ekris is the project manager. He will be responsible for overall project progress and the business value of the project results.

Postdoc. We will employ one postdoc in this project, to be employed at the University of Twente. We are looking for someone with a solid background in modelling and analysis of either security of RAMS, and preferably both.

Joris ter Heijne is a risk management specialist at Delta Pi. He is responsible for RAMS-analyses of the Oosterschelde storm surge barrier and the Haringvliet

barrier, safety analysis for TATA-steel and ProRail. Recently he has finished the training DHM Security Management and currently is being trained as a specialist in the area of cyberrisks and information security.

7c. Glossary of terms

AT	Attack Tree
AFT	Attack Fault Tree
FMECA	Failure Mode Effect and Criticality Analysis
FT	Fault Tree
MTTF	Mean Time To Failure
RAMS	Reliability, Availability, Maintenance, Safety

8. Literature references

Please refer to the 'open' literature only.

[1] Fault tree analysis (FTA). Norm IEC 60050:2006, 2007.

[2] H. Boudali, P. Crouzen, and M.I.A. Stoelinga. Dynamic fault tree analysis using input/output interactive Markov chains. In *The 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pages 708–717. IEEE Computer Society, 2007.

[3] B. Schneier. Attack trees: Modeling security threats. Dr. Dobb's journal, 24(12), Dec 1999.

[4] M. Stamatelatos, W. Vesely, J. B. Dugan, J. Fragola, J. Minarick, and J. Railsback. Fault Tree Handbook with Aerospace Applications. Office of safety and mission assurance NASA headquarters, 2002.

[5] W. E. Vesely, F. F. Goldberg, N. H. Roberts, and D. F. Haasl. Fault Tree Handbook. Office of Nuclear Regulatory Reasearch, U.S. Nuclear Regulatory Commision, 1981.

[6] John B. Bowles and William Hanczaryk. Threat effects analysis: Applying FMEA to model computer system threats. In 2008 Annual Reliability and Maintainability Symposium, pages 463–468. IEEE, January 2008.

[7] P. J. Brooke and R. F. Paige. Fault trees for security system design and analysis. Computers & Security, 22(3):256 – 264, 2003.

[8] U. Franke, R. Sommestad, M. Ekstedt, and P. Johnson. Defense graphs and enterprise architecture for information assurance analysis. In Proceedings of the 26th Army Science Conference, 2008.

[9] IsoGraph AttackTree+. http://www.isograph.com/software/attacktree/diagram-construction/.

[10] B. Kordy, Piotr Kordy, Sjouke Mauw, and Patrick Schweitzer. AD- Tool: Security analysis with attack-defense trees. In 10th International Conference on Quantitative Evaluation of Systems, pages 173–176. Springer, 2013.

[11] ProRail. Leidraad voor RAMSHE – LMC-studie, 2010. (in Dutch). Avaialble via http://www.leidraadse.nl/assets/files/downloads/Publicaties/leidraad_rams_-_sturen_op_prestaties_van_systemen.pdf

[12] F. Arnold, A. Belinfante, F. van der Berg, and M.I.A. Stoelinga. DFTCalc: A tool for efficient fault tree analysis. In Proc. 32nd Int. Conf. Computer Safety, Reliability and Security (SAFECOMP), LNCS, pages 293–301. Springer, 2013.

[13] E.J.J. Ruijters, M.I.A. Stoelinga: Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools. Computer Science Review 15: 29-62, 2015.

[14] V. Novák, I. Perfilieva, and J. Močkoř, (1999) *Mathematical principles of fuzzy logic*, Kluwer Academic.

[15] M. Hazewinkel, ed. (2001), Bayesian approach to statistical problems, Encyclopedia of Mathematics, Springer.

[16] D. Ionita, Current Established Risk Assessment Methodologies and Tools. MSc thesis, University of Twente, June 2013.

[17] F. Arnold, W. Pieterse, M.I.A. Stoelinga: Quantitative penetration testing with item response theory. 9th International Conference on Information Assurance and Security 2013: 49-54

[18] F. Arnold, H. Hermanns, R. Pulungan, M.I.A. Stoelinga: Time-Dependent Analysis of Attacks. Third International Conference on Principles of Security and Trust (POST'14), LNCS, p285-305, 2014.

[19] R. Kumar, E.J.J. Ruijters and Mariëlle Stoelinga *Quantitative Attack Tree Analysis via Priced Timed Automata.* 15th International Conference on Formal Modeling and Analysis of Timed Systems (FORMATS), LNCS, Springer, 2015.

[20] Van Ekris. TOPAAS: An alternative approach to software reliability quantification, Quality and Reliability Engineering International Factors in Project Management Influencing Repeat Business, Proceedings of the 2009 IASTED on Software Engineering, 2009

[21] Van Ekris. Customer Perception of Delivery Quality: A Necessary Area for Attention for Project Managers, Proceedings of the 2008 IASTED on Software Engineering, pp 268-274, 2008.

[22] Van Ekris. Towards business oriented questionnaires for the specification of software product quality, "Project Control for 2000 and Beyond", Conference proceedings of ESCOM – ENCRESS '98, Rome, 1998.

[23] Rijkswaterstaat, Probabilistisch beheer en onderhoud. http://www.rijkswaterstaat.nl/images/Onderhoudsoptimalisatie_tcm174-331347.pdf

[24] Saleh, J.H. and Marais, Ken, "Highlights from the Early (and pre-) History of Reliability Engineering", Reliability Engineering and System Safety, Volume 91, Issue 2, February 2006, Pages 249-256

[25] A. Bondavalli, I. Majzik, I. Mura, Automatic dependability analysis for supporting design decisions in UML, in: Proc. 4th Int. Symp. High Assurance Systems Engineering, HASE, 1999, pp. 64–71.

[26] Carl Carlson. Effective FMEAs: Achieving Safe, Reliable, and Economical Products and Processes using Failure Mode and Effects Analysis, Wiley, 2012.

[27] Tyler, Brian, Crawley, Frank & Preston, Malcolm (2008). *HAZOP: Guide to Best Practice* (2nd Edition ed.). IChemE, Rugby.

[28] S. Bernardi, S. Donatelli, J. Merseguer, From UML sequence diagrams and statecharts to analysable Petri net models, in: Proc. 3rd Int. Workshop on Software and Performance, WOSP, 2002, pp. 35–45.

[29] S. Distefano, A. Puliafito, Dynamic reliability block diagrams: Overview of a methodology, in: Proc. European Safety and Reliability Conf., ESREL, Vol. 7, 2007, pp. 1059–1068.

[30] N. Fovino, M. Masera, A.D. Cian, Integrating cyber attacks within fault trees, Reliability Engineering & System Safety 94 (9) (2009) 1394–1402.

[31] Max Steiner, Peter Liggesmeyer. Combination of Safety and Security Analysis - Finding Security Problems That Threaten The Safety of a System. Matthieu ROY. Workshop on Dependable Embedded and Cyberphysical Systems, 2013.

[32] G. Sabaliauskaite, A. P. Mathur. Aligning Cyber-Physical System Safety and Security, Complex Systems Design & Management Asia, Springer, 2015.

[33] M. Bozzano, A. Cimatti, J.-P. Katoen, V.Y. Nguyen, T. Noll, M. Roveri. Safety, dependability and performance analysis of extended AADL models, Comput. J. 54 (2011) 754–775.

[34] D.M. Nicol, W.H. Sanders, K.S. Trivedi. Model-based evaluation: from dependability to security. IEEE Transactions on Dependable and Secure Computing, 2004.

[35] Elizabeth LeMay, Michael D. Ford, Ken Keefe, and William H. Sanders. Model-based security metrics using ADversary VIew Security Evaluation (ADVISE). In 2011 Eigth International Conference on Quantitative Evaluation of Systems (QEST). IEEE, 2011.

[36] R. Winther, O.-A. Johnsen, and B. A. Gran. Security assessments of safety critical systems using HAZOPs. In Computer Safety, Reliability and Security, volume 2187 of Lecture Notes in Computer Science, pages 14 – 24. Springer International Publishing, 2001.

[37] T. Minh Ngo, M.I.A Stoelinga, M. Huisman. Effective verification of confidentiality for multi-threaded programs. Journal of Computer Security 22(2): 269-300 (2014)

[38] T. Minh Ngo, M.I.A Stoelinga, M. Huisman. Confidentiality for Probabilistic Multi-threaded Programs and Its Verification. ESSoS 2013: 107-122, 2013.

[39] M. Rausand, A. Høyland: System Reliability Theory: Models, Statistical Methods, and Applications, Wiley, 2006.

[40] M. Felderer, B. Katt, P. Kalb, J. Jürjens, M. Ochoa, F. Paci, L. M. Sang Tran, T. Than Tun, K. Yskout, R. Scandariato, F. Piessens, D. Vanoverberghe, E. Fourneret, M. Gander, B. Solhaug, R. Breu. Evolution of Security Engineering Artifacts: A State of the Art Survey. IJSSE 5(4): 48-98, 2014.

[41] F. Arnold, D. Guck, R. Kumar, and M.I.A. Stoelinga. Sequential and Parallel

Attack Tree Modelling with Markov Automata. Proc. of the 2nd International workshop on the Integration of Safety and Security Engineering, 2015. Accepted for publication.

[42] A. Roy, D. S. Kim, and K.S. Trivedi. Cyber security analysis using attack countermeasure trees. In Proceedings of the 6th Cyber Security and Information Intelligence Research Workshop, 2010.

[43] C. Schmittner, T. Gruber, P. Puschner, and E. Schoitsch. Security application of failure mode and effect analysis (FMVEA). In Computer Safety, Reliability, and Security, volume 8666 of Lecture Notes in Computer Science, pages 310–325, 2014.

[44] M. Soldal Lund, B. Solhaug, K. Stølen: Model-Driven Risk Analysis - The CORAS Approach. Springer 2011.

[45] A. Roy, D.S. Kim, K. S. Trivedi: Attack countermeasure trees (ACT): towards unifying the constructs of attack and defense trees. Security and Communication Networks 5(8): 929-943, 2012.

[46] D. Guck, J. Spel, and M.I.A. Stoelinga. Sequential and Parallel Attack Tree Modelling with Markov Automata. DFTCalc: Reliability centered maintenance via fault tree analysis (tool paper), 17th International Conference on Formal Engineering Methods, ICFEM 2015. Accepted for publication.

[47] J. A. Jones, An Introduction to Factor Analysis of Information Risk (FAIR), Risk Management Insight, 2005.

[48] Marc Lankhorst. Enterprise Architecture at Work - Modelling, Communication and Analysis. Berlin: Springer-Verlag, 2005.

Budget

9. Summary of total project budget

Please refer to sections 3.5 and 6.2 of the Call for Proposals for IPPSI for specific rules and regulations regarding (in cash and in kind) contribution of private partners and eligible costs.

Please complete the tables below.

Contributions Private Partners (in €)	**cash**	**in kind**	**Total**
Delta Pi	8.000	8.000	16000
	..	..	..
…	..	..	..
Total contributions partners	**8.000**	**8.000**	**16.000**
Total Contribution NWO (in €)	**63.723**		**63.723**
Total Contributions (partners + NWO)	**71.723**	**8.000**	**79.723**

Expenses

Detailed overview of cash expenses (in €)	
Postdoc	66.223
Benchfee	3.000
Workshop organization	2.500
Total cash expenses	**71.723**

Detailed overview of in kind contributions (in €)		
Hours to be worked within the scope of the project	120 hours x 79.16 (max € 100/hr)	8.000
Materials and resources		..
Use of equipment		..
Total in kind contributions		**8.000**

We ask for funds to appoint a postdoc on this project. Additional travel budget cover expenses to visit one international conference, and visits within the Netherlands; we foresee regular visits to Delta Pi, and Rijkswaterstaat.

Data management

10. Data management

Responsible data management is part of good research. Therefore in 2015, NWO is starting a pilot in data management.
For the collection/generation of data and the analysis of this data timely measures need to be taken to ensure the storage and later reuse of the data. This means that prior to the start of the research project researchers must ascertain a) if the project can make use of available data from third parties, b) which data can be relevant for reuse and c) how these data can be stored so that they are suitable for reuse. After a proposal has been awarded funding the researcher will draw up a detailed data management plan.

See the explanatory note as well.

a. *Will data be collected or generated that are suitable for reuse?*

We will both collect and generate data. In particular, we will create combined safety and security models for the three case studies mentioned, which are provided by third parties. These models concern the internal workings of the assets, and are proprietary of the three parties, and will not be public. An NDA will be signed between the University of Twente and Delta Pi; legislators of the UT will monitor the quality of the NDA.

We will however publish abstract versions of the models and our results that do not harm the interest of all parties involved. These will be public.

b. *Where will the data be stored during the research?*

Raw data will be stored at Delta Pi and its customers, and if needed, at the UT under an NDA.

The abstract versions of the models and our results will be stored at the University of Twente, and will be available upon request. We will store the data in a secure data repository (with daily back ups) at the FMT group. The University of Twente has recently established a standardized procedure, as well as enhanced (easier to use, more capacity) data storage facilities.

c. *After the project has been completed, how will the data be stored for the long-term and made available for the use by third parties? To whom will the data be accessible?*

The raw data will be stored at Delta Pi and its customers, according to their business needs. The abstract versions will remain at University of Twente's data repositories.

d. Which facilities (ICT, (secure) archive, refrigerators or legal expertise) do you expect will be needed for the storage of data during the research and after the research? Are these available?[3]

We need standard legal expertise, and standard storage facilities. These are available.

Statement

[3] ICT facilities for data storage are considered to be issues such as data storage capacity, bandwidth for data transport and calculating power for data processing.

11. Statement by the PI

☒ By submitting this form through Iris, I declare that I have completed this form truthfully and I declare that I have informed the correct official(s) of my employing institute of this submission (e.g. the scientific director or dean).

☒ By submitting this form I declare that I satisfy the nationally and internationally accepted standards for scientific conduct as stated in the Netherlands Code of Conduct for Scientific Practice 2012 (Association of Universities in the Netherlands).

Name: Dr Marielle Stoelinga

Place: Enschede

Date: July 27, 2015

Letter(s) of commitment

Please enclose the letter of the main applicant on the matching and for each private partner in this project consortium a letter of commitment as separate pdf file to this proposal (*compulsory*). A compulsory format of the letters can be found at the NWO website: www.nwo.nl/RoadmapICT.

Please submit the application to NWO in electronic form (pdf format is required!) using the Iris system, which can be accessed via the NWO website (www.iris.nwo.nl). The application must be submitted from the account of the main applicant. For any technical questions regarding submission, please contact the IRIS helpdesk (iris@nwo.nl).