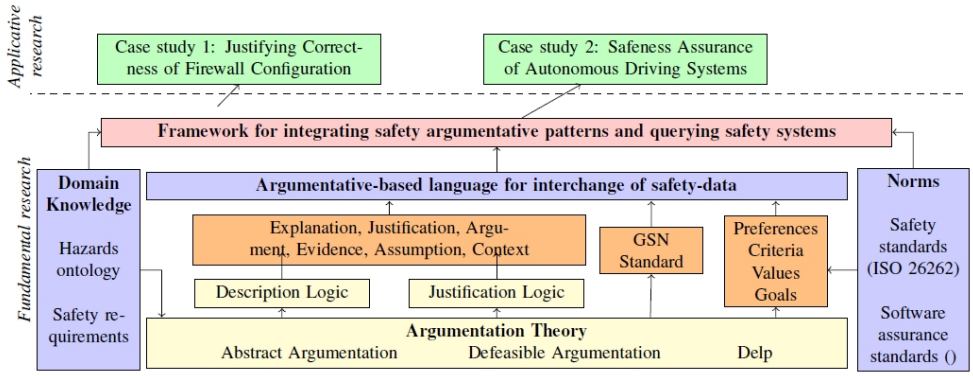
Summary

11 Septembrie 2013 -4 Decembrie 2014
Bilateral Agreement Romania-Argentina
Contract No. 731

Project tile:	ARGSAFE: Using Argumentation for Justifying Safeness of Complex Technical Systems
Romanian partner:	Technical University of Cluj-Napoca
Argentinian partner:	Universidad Nacional del Sur
Duration:	24 months: 11 Septembrie 2013 -11 Septembrie 2015)

Objectives. The top level scientific objective regards safety assurance of software systems by means of argumentation theory.

Date	Objectives	Novelty	Associated Tasks
Jun 2013	O1. Analysis the problem of justifying safeness of complex technical systems.	Identifying the possibilities of integrating argumentation theory, quality standards and ontologies.	Formal analysis of quality standards. Identifying factors affecting confidence in safeness of software systems.
Sep 2013	O2. Developing the assurance model based on argumentation theory.	Justificative reasoning in the context of heterogeneous and contradictory evidence	Developing the defeasible justification logic. Contextualising evidence.
May 2014	O3. Developing the system of justifying safeness of complex technical system.	Automatic identification of inconsistent justifications.	Developing a generic ontology for hazards. Organising the first ARGSAFE workshop.
Sep 2014	O4. Applying the system for safeness assurance of autonomous driving systems.	Organising evidence, building arguments and counter-arguments.	Formalising safeness requirements. Formalising assumptions regarding operating mode and specific hazards.
Dec 2014	O5 Applying the system for verifying correctness of firewall configuration	Presenting arguments for decision support under temporal constraints	Identifying inconsistency in security rule-based systems. Organising the second ARGSAFE workshop.
Mar 2015	O6. Developing a methodology of exploiting structured arguments in safeness assurance	Re-using safety cases. Re-engineering complex software systems based on arguments.	Defining patterns of safety cases. Stating the principle of building arguments when developing complex software systems.



Team:

- Technical University of Cluj-Napoca: Assoc. Prof. dr. .eng.Adrian Groza, Prof. dr. eng. Ioan Alfred Letia, Phd stdeunt Anca Goron.
- Universidad National del Sur: Assoc. Prof. Sergio Alejandro Gomez, Prof. Carlos Ivan Chesnevar

Publications:

1. S. A. Gomez, A. Goron, A. Groza - Assuring Safety in an Air Traffic Control System with Defeasible Logic Programming, Argentine Symposium on Artificial Intelligence (ASAI14), 1-5 September 2014, Buenos Aires, Argentina
2. S.A. Gomez, A. Groza, C.I. Chesnevar - An Argumentative Approach to Assessing Safety in Medical Device Software using Defeasible Logic Programming, International Conference on Advancements of Medicine and Health Care through Technology (MEDITECH2014), Ed. S. Vlad, R. Ciupa, ISBN 978-3-319-07652-2, IFMBE, Vol 44, Springer, pp. 167-172
3. S. Gomez, A. Groza, C Chesnevar, I. A. Letia, A. Goron, M Lucero - ARGSAFE: Usando Argumentacion para Garantizar Seguridad en Sistemas Tecnicos Complejos, WICC, Ushuaia, Tierra del Fuego, Argentina, 7-8 May 2014
4. A. Goron, A. Groza, S. A. Gomez, I. A. Letia - Towards an argumentative approach for repair of hybrid logics models, ARGMAS@AAMAS, Paris, France, 5-9 May 2014

Deliverables:

(D1.1) Web page: http://cs-gw.utcluj.ro/∼adrian/projects/argsafe

(D1.2) Presentation poster (available on the project web page);

(D1.3) Workshop: "Agreement Technologies in Software Engineering": http://cs-gw.utcluj.ro/∼adrian/workshops/ATSE2013.html

(D1.4) Ontology for the Goal Structuring Notation standard (available at project web page);

(D1.6) First year technical report (available at project web page);

(D2.1) EdSafe tool (available on the project web page);

(D2.2) Second year technical report (available on the project web page).

Novelty. We propose an *argumentation approach for hybrid logics model update*. Argumentation theory is used to assist the process of updating the model. We view a Hybrid Kripke model as a description of the world that we are interested in. The update on this Kripke model occurs when the system has to accommodate some newly desired properties or norm constraints. When the model fails to verify a property, a defeasible logic program is used to analyze the current state. Depending on the status of the arguments, the system can warrant four primitive operations on the model: updating state variables, adding a new transition, removing a transition, or adding a new state. A running scenario is presented showing the verification of an unmanned aerial vehicle, by interleaving reasoning in Defeasible Logic Programming and the Hybrid Logic Model Checker.

Assuring safety in complex technical systems is a crucial issue in several critical applications like air traffic control or medical devices. We developed a *framework based on argumentation for assisting flight controllers to reach a decision related to safety constraints* in an ever changing environment in which sensor data is gathered at real time.

Modern health-care technology depends to a large extent on software deployed in medical devices, which brings several well-known benefits but also poses new hazards to patient safety. As a consequence, assessing safety and reliability in software in medical devices turns out to be a critical issue. We developed a *method for safety assessment of medical devices based on Defeasible Logic Programming (DeLP)*, which provides an argumentative framework for reasoning with uncertain and incomplete knowledge. We contend that argumentation theory as defined in DeLP can be used to integrate and contrast different evidences for assessing the approval and commercialization of medical devices, aiming at increasing transparency to all the stakeholders involved in their certification. The outlined framework is validated by modeling the infamous Therac-25 accident.

Economic impact. Increasingly, safety regulatory bodies require the developers of critical software systems to provide explicit safety cases - defined in terms of structured arguments based on objective evidence - in order to prove that the system is acceptable safe. Argumentative-based safety cases are progressively adopted in the defense (UK), automotive, railways, off-shore oil & gas, or medical device domains. Consequently, this research aims i) to identify links between argumentation theory and engineering of safety systems, ii) to develop argumentation methods to transfer confidence in safety-critical software systems. iii) to apply the developed technical instrumentation at two case studies: 1) safeness of autonomous driving software, respectively 2) justifying correctness of firewall configuration. System capabilities include 1) automatic norm checking for compliance, 2) safety reports generation, 3) facilitating understanding and confidence transfer.