A semantic approach for identifying assurance deficits in unmanned aerial vehicle software

A. Groza, I. A. Letia, A. Goron, S. Zaporojan

Department of Computer Science - Technical University of Cluj-Napoca

August 13, 2014

Outline

Introduction

- Assuring safety in complex technical systems is a crucial issue in several critical applications like air traffic control or medical devices
- Safety assurance and compliance to safety standards may prove to be a real challenge when we deal with adaptive systems
- Argument-based safety cases offer a plausible alternative basis for certification of critical software

TECHNICAL UNIVERSITY OF CLUJ-NAPOCA ROMANIA

Objectives

- Create a framework for evidential reasoning with visualization support
- Apply an efficient validation method for competing hypotheses

The Challenge

Formalize the GSN graphical notation in DL such as to permit automatic reasoning on each diagram of the safety cases

Limitations:

- Transform GSN notation to DL notation
- Find an appropiate declarative language which allows reasoning

The Approach

- Provide a formal representation of the argumentative-based Goal Structuring Notation (GSN) standard

The Approach

- Provide a formal representation of the argumentative-based Goal Structuring Notation (GSN) standard
- Exploit reasoning in description logic to identify assurance deficits in the GSN model

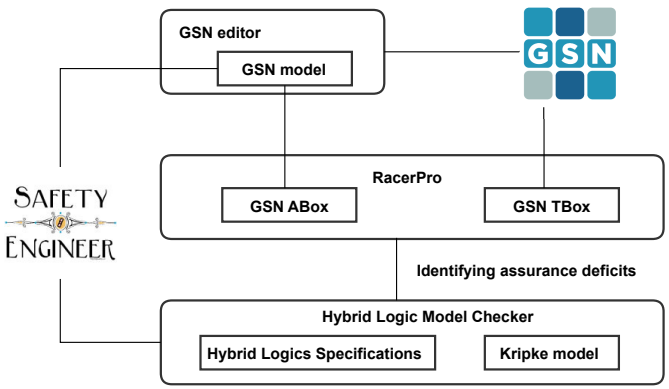
TECHNICAL UNIVERSITY OF CLUJ-NAPOCA ROMANIA

The Approach

- Provide a formal representation of the argumentative-based Goal Structuring Notation (GSN) standard
- Exploit reasoning in description logic to identify assurance deficits in the GSN model
- Flaws are given to a hybrid logic-based model checker to be validated against a Kripke model

TECHNICAL UNIVERSITY OF CLUJ-NAPOCA ROMANIA

System Architecture



The solution is based on three technical instrumentations:

- the $\mathcal{SHI}$ version of DL
- the GSN standard
- hybrid logics (HLs)

TECHNICAL UNIVERSITY OF CLUJ-NAPOCA ROMANIA

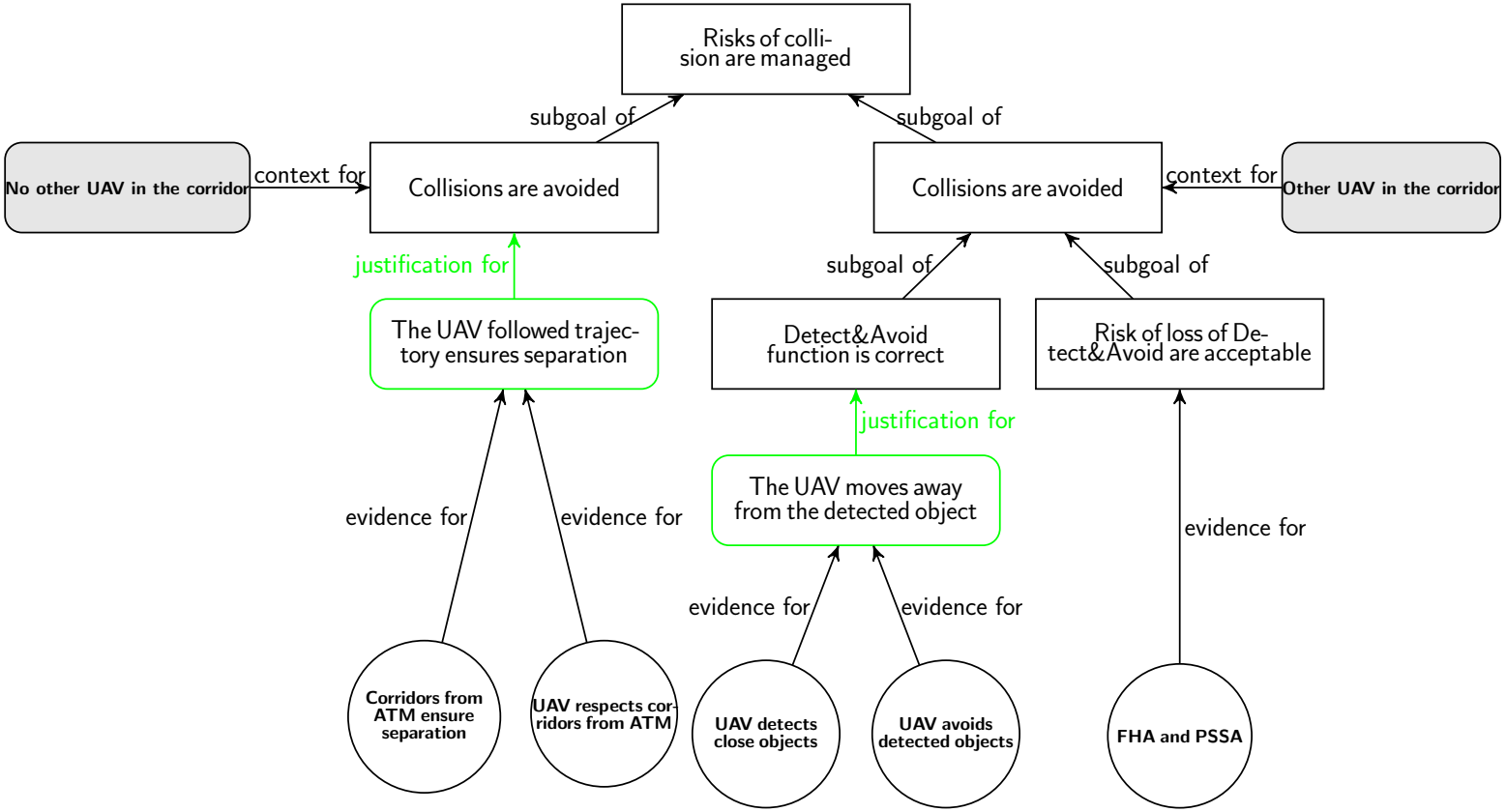
Safe insertion of a UAV into the civil air traffic

Example

- An Unmanned Aircraft System consists of:
- UAV itself: equipped with an autonomous control system
- ground station
- Air Traffic Management: provides the required coordinates for the UAV
- **Goal: prove that an UAV can complete safely its mission and that all the major implied risks are mitigated**

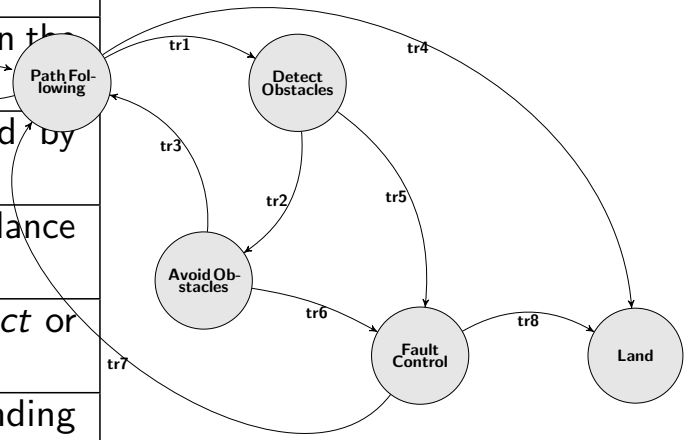
TECHNICAL UNIVERSITY OF CLUJ-NAPOCA ROMANIA

Goal Structuring Notation - UAV Model



Kripke Structure of the UAV

State	Parameters	Specification
PathFollowing	$\neg obs$	UAV follows the path on the given corridor
DetectObstacles	obs	Obstacles are signaled by sensors
AvoidObstacles	$obs \wedge d$	UAV performs an avoidance maneuver
FaultControl	$errObs \vee errAvoid$	Error signaled by *Detect* or *Avoid*
Land	$\neg obs \vee errObs \vee errAvoid$	UAV performs the landing procedure



Modeling the Goal Structuring Notation in DL

Retrieving information about the GSN model

Query	RacerPro query	RacerPro answer
Top level goal	$(concept - instances\ TopLevelGoal)$	g_1
Support goals	$(concept - instances\ SupportGoal)$	g_2, g_3, g_4, g_5
Evidence supporting goal g_1	$(individual - fillers\ g_1\ hasEvidence)$	e_1, e_2
Evidence verified against the model m_1	$(individual - fillers\ m_1)$ $(inverse\ hasModel))$	e_1, e_2, e_3, e_4, e_5
Evidence not verified	$(concept - instances(and\ Evidence$ $(some\ hasTestResult\ False))$	e_1, e_2, e_3, e_4, e_5
Goals supported by not verified evidence	$(concept - instances\ NotVerifiedGoals)$	g_1, g_2, g_3, g_4, g_5

Interleaving reasoning with HL and DL for identifying assurance deficits

Our method interleaves two steps:

- Check with hybrid logic if the evidence nodes from the GSN representation have their corresponding formulas validated against the Kripke model.
- By reasoning in DL, we identify which goals in the GSN model are not supported by verified evidence.

TECHNICAL UNIVERSITY OF CLUJ-NAPOCA ROMANIA

Validating Evidence with Model Checking

The verification uses the following parameters:

- the minimum distance d_{min} allowed between the UAV and another object without risk of collision;
- the reported coordinates c_{uav} by the UAV; and
- the given coordinates c_{ATM} by the ATM.
- the reported distance d_{obs} between the UAV and another approaching UAV
- the minimum distance d_{min} allowed without any risk of collision

Validating Evidence with Model Checking

For evidence e_1:

$$f_1 =\downarrow i(c_{ATM}) \rightarrow_i [F](c_{ATM} > d_{min}) \quad (1)$$

For evidence e_2:

$$f_2 =\downarrow i(c_{ATM}) \rightarrow @t_i[Next](c_{uav} = c_{ATM}) \quad (2)$$

The justification j_2 of the sub-goal g_2 supported by e_1 and e_2 is expressed as:

$$j_2 =\downarrow i(c_{uav} = c_{ATM}) \rightarrow @_i[F](c_{uav} > d_{min}) \quad (3)$$

The justification j_4 for the sub-goal g_4 is formalized as:

$$j_4 =\downarrow i(d_{obs} < d_{min}) \rightarrow @_i[F]((d_{obs} \neq 0)U(d_{obs} > d_{min})) \quad (4)$$

Evidence e_3 is formally expressed as:

$$f_3 =\downarrow i(d_{obs}) \wedge @_i(d_{obs} < d_{min}) \rightarrow\downarrow i(obs) \quad (5)$$

Evidence e_4 is formally expressed as:

$$f_4 =\downarrow i(obs) \rightarrow @_i((d_{obs} \neq 0)U(d_{obs} > d_{min})) \quad (6)$$

Evidences e_3 and e_4 are used to validate the sub-goal g_4

If the ATM starts transmitting coordinates at a state i, then for all future states the coordinates will be transmitted such that to ensure that the min safe distance is preserved

If the ATM starts transmitting coordinates at a state i, then in the next state the UAV should report the exact coordinates

The implication $f_1 \wedge f_2 \rightarrow j_2$ is true (the following of the coordinates from the ATM ensures the required min safe distance) .

If we bind to i the state in which the reported distance between the UAV and another approaching UAV is less than the min one then for all future states the reported distance must be kept higher then 0

If in the current state i, the distance to a possible obstacle is less than the min allowed one, the presence of an obstacle is reported by the sensors signaling a risk for collision

If we bind to nominal i the state in which an obstacle is signaled by the sensors, then the reported distance to the obstacle must be maintained different than 0 until it becomes higher then the min established threshold

To complete the validation of g_4, we have to prove the formula $f_3 \wedge f_4 \rightarrow j_4$, which is true (the presence of an obstacle indicated by an observed distance, which is less than the min accepted one will entail an avoidance maneuver)

TECHNICAL UNIVERSITY OF CLUJ-NAPOCA ROMANIA

Updating the Abox for the GSN model

Updating the Abox for the GSN model with the newly validated evidences:

$(e_1, f_1) : hasFormula$, $(e_1, "true") : hasTestResult$
$(e_2, f_2) : hasFormula$, $(e_2, "true") : hasTestResult$
$(g_2, j_2) : hasJustification$, $(f - g_2, "true") : hasTestResult$
$(e_3, f_3) : hasFormula$, $(e_3, "true") : hasTestResult$
$(e_4, f_4) : hasFormula$, $(e_4, "true") : hasTestResult$
$(g_4, j_4) : hasJustification$, $(f - g_4, "true") : hasTestResult$

TECHNICAL UNIVERSITY OF CLUJ-NAPOCA ROMANIA

Conclusions

- Combining argumentation and model checking might bring about additional advantages such as preliminary validation of argumentation schemes constructed to support safety cases,
- Ensures that the stability of the system will not be affected by the available choices
- Foresees possible impediments in selecting one option over another
- Abstractization was used to complement the more visually used GSN standard with a formalized model
- This joint approach will increase the degree of trust in certifying the correct functioning of critical safety systems.

TECHNICAL UNIVERSITY OF CLUJ-NAPOCA ROMANIA

Contributions:

- Integrate hybrid logic with argumentation theory
- Provide a formal model of the GSN standard in description logic
- GSN structures safety cases, HL is able to validate evidence nodes
- DL provides a middleware language to integrate GSN and model checking
- DL was used to analyze the status of the arguments and their supporting evidence
- A step towards a formal model for the GSN standard
- Current work is focused on investigating the feasibility of the solution against large-scale safety cases

TECHNICAL UNIVERSITY OF CLUJ-NAPOCA ROMANIA

Thank you!

TECHNICAL UNIVERSITY OF CLUJ-NAPOCA ROMANIA