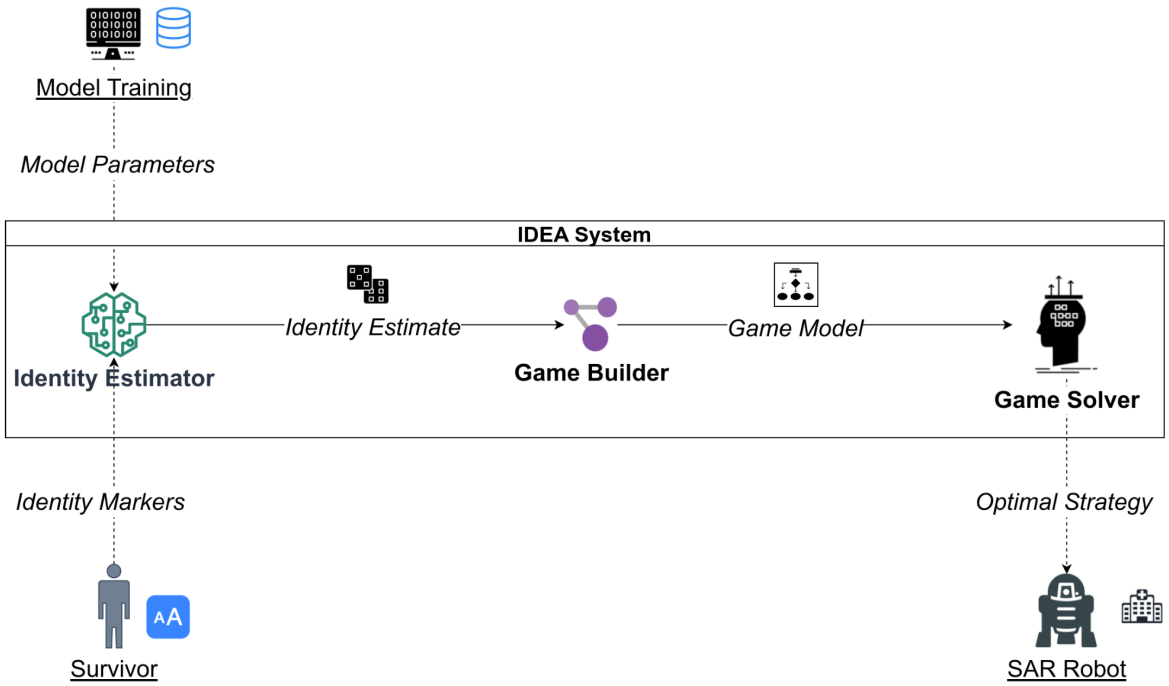
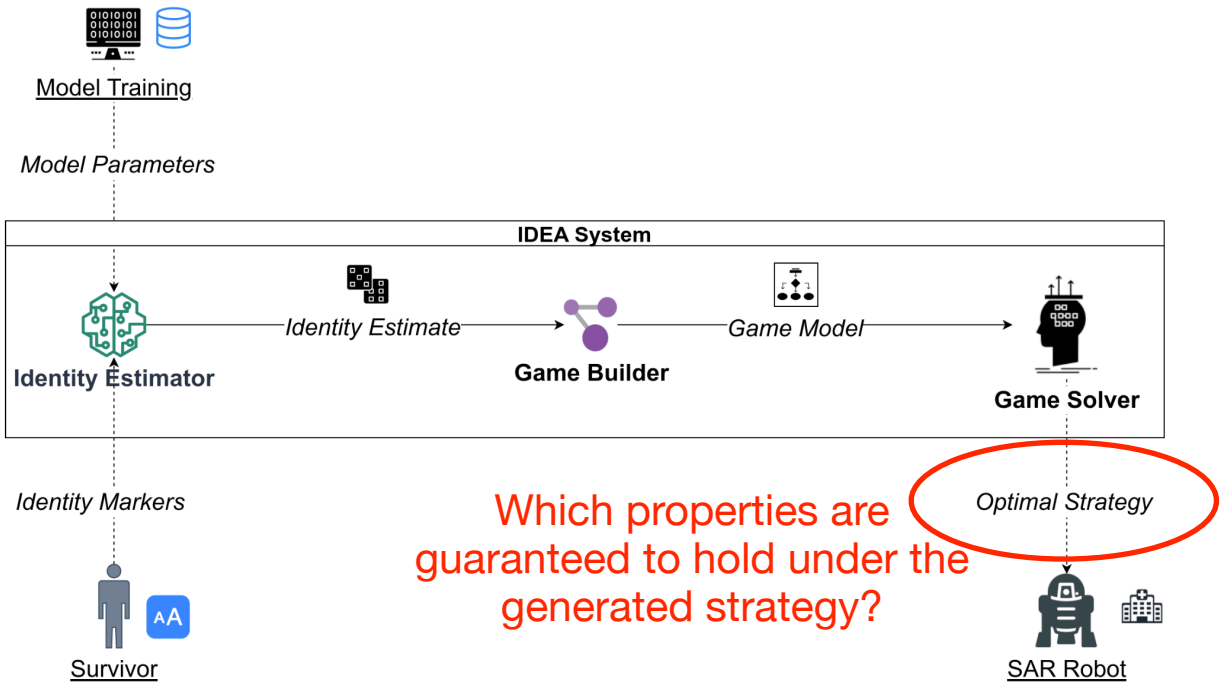
Towards a Formally Verified Identity-Aware Architecture for Autonomous Systems

The IDEA Framework [1]



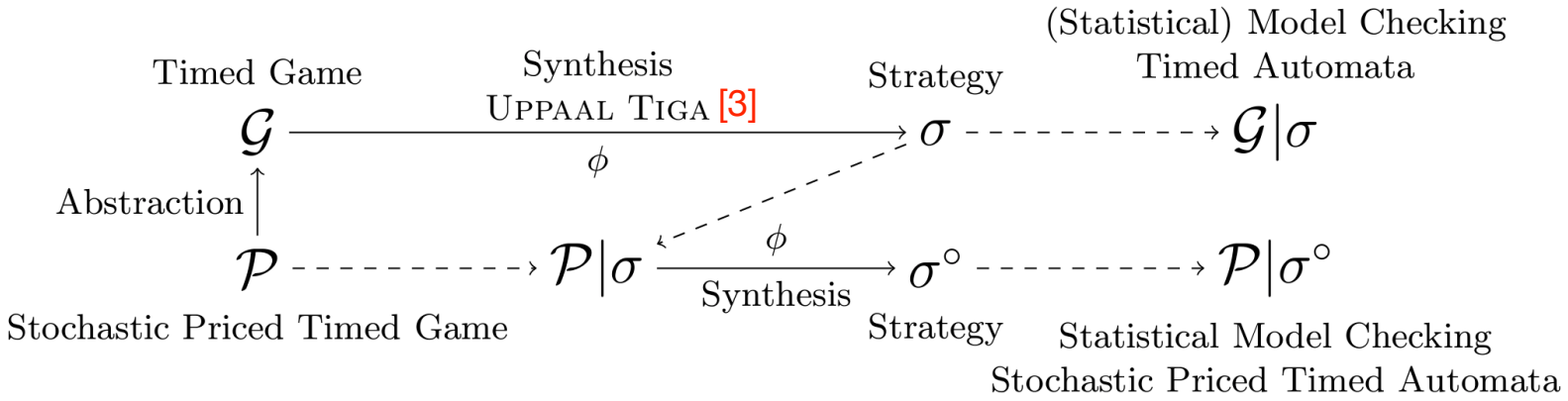
[1] Gavidia-Calderon, C., Kordoni, A., Bennaceur, A., Levine, M., & Nuseibeh, B. The IDEA of Us: An Identity-Aware Architecture for Autonomous Systems. Submitted to TOSEM.

The IDEA Framework [1]



[1] Gavidia-Calderon, C., Kordoni, A., Bennaceur, A., Levine, M., & Nuseibeh, B. The IDEA of Us: An Identity-Aware Architecture for Autonomous Systems. Submitted to TOSEM.

Uppaal Stratego [2]



[2] David, A., Jensen, P. G., Larsen, K. G., Mikučionis, M., & Taankvist, J. H. (2015). Uppaal stratego. In TACAS 2015, Proceedings 21 (pp. 206-211). Springer Berlin Heidelberg.

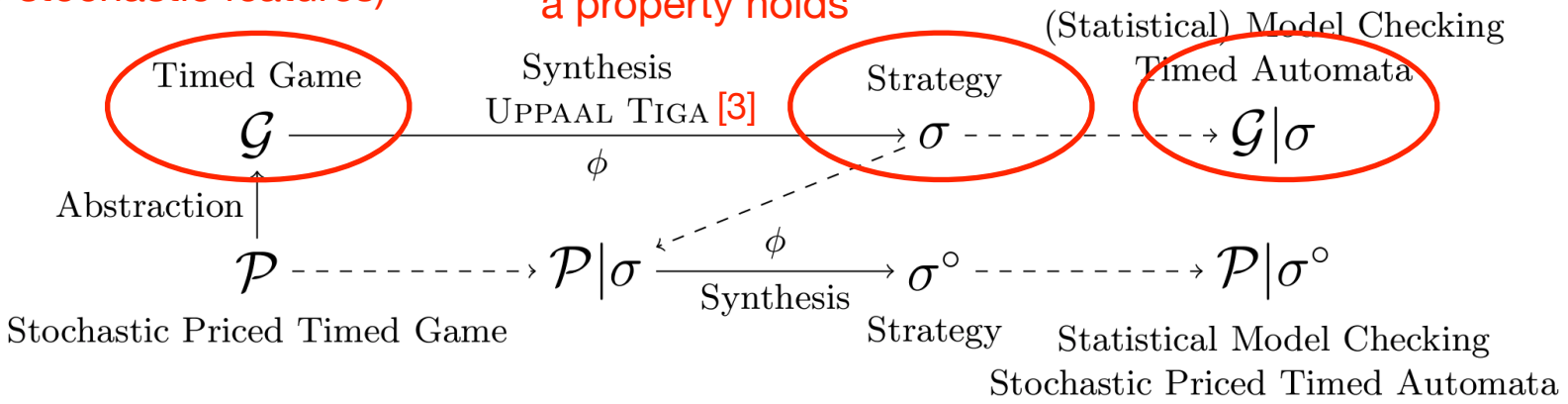
[3] Behrmann, G., Cougnard, A., David, A., Fleury, E., Larsen, K. G., & Lime, D. (2007). UPPAAL-Tiga: Time for Playing Games! (Tool Paper). In CAV 2007. Proceedings 19 (pp. 121-125). Springer Berlin Heidelberg.

Uppaal Stratego [2]

Timed Game Automata (TGA) Network (i.e., no stochastic features)

Strategy guaranteeing that a property holds

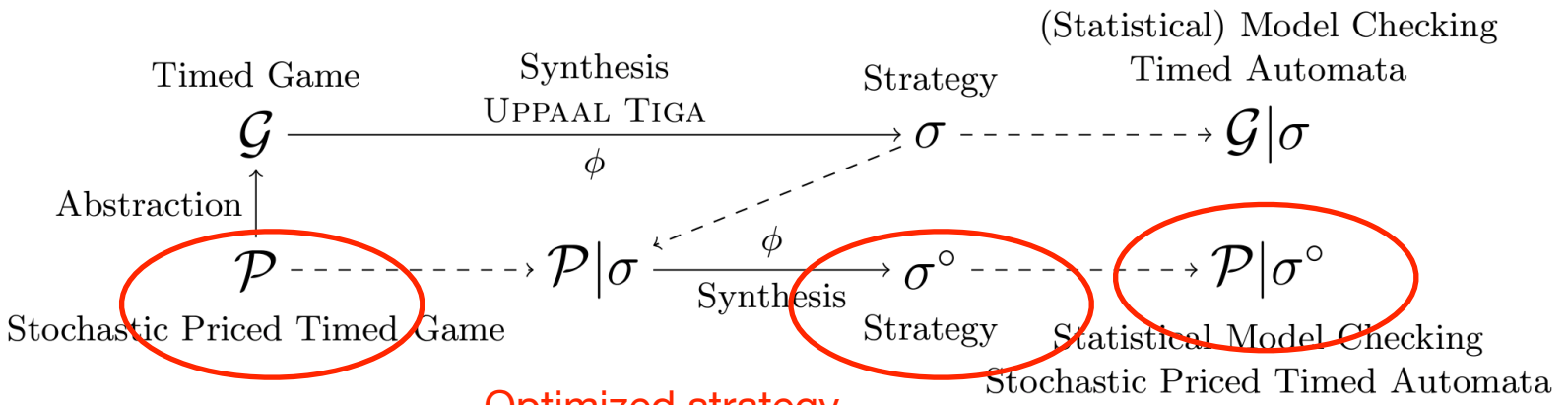
Model Checking under the generated (verified) strategy



[2] David, A., Jensen, P. G., Larsen, K. G., Mikučionis, M., & Taankvist, J. H. (2015). Uppaal stratego. In TACAS 2015, Proceedings 21 (pp. 206-211). Springer Berlin Heidelberg.

[3] Behrmann, G., Cougnard, A., David, A., Fleury, E., Larsen, K. G., & Lime, D. (2007). UPPAAL-Tiga: Time for Playing Games! (Tool Paper). In CAV 2007. Proceedings 19 (pp. 121-125). Springer Berlin Heidelberg.

Uppaal Stratego [2]



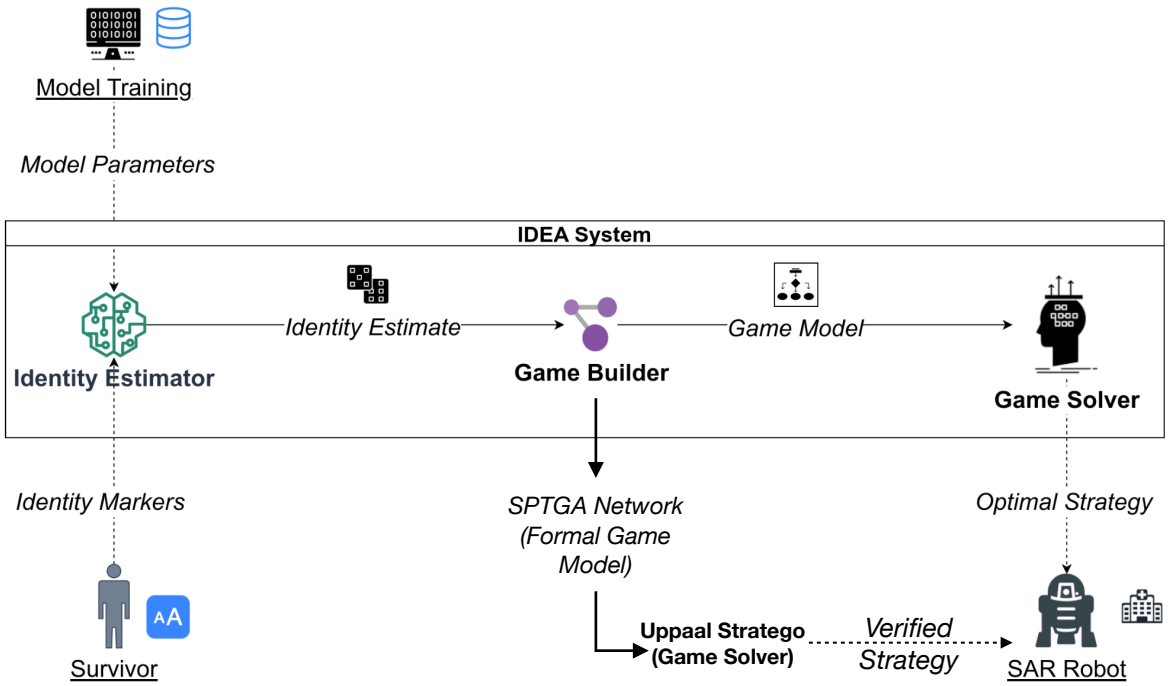
Stochastic Priced Timed Game Automata (SPTGA) Network (i.e., including the stochastic part)

Optimized strategy guaranteeing that a property holds AND maximizing (minimizing) a certain quantity

Statistical Model Checking under the optimized strategy

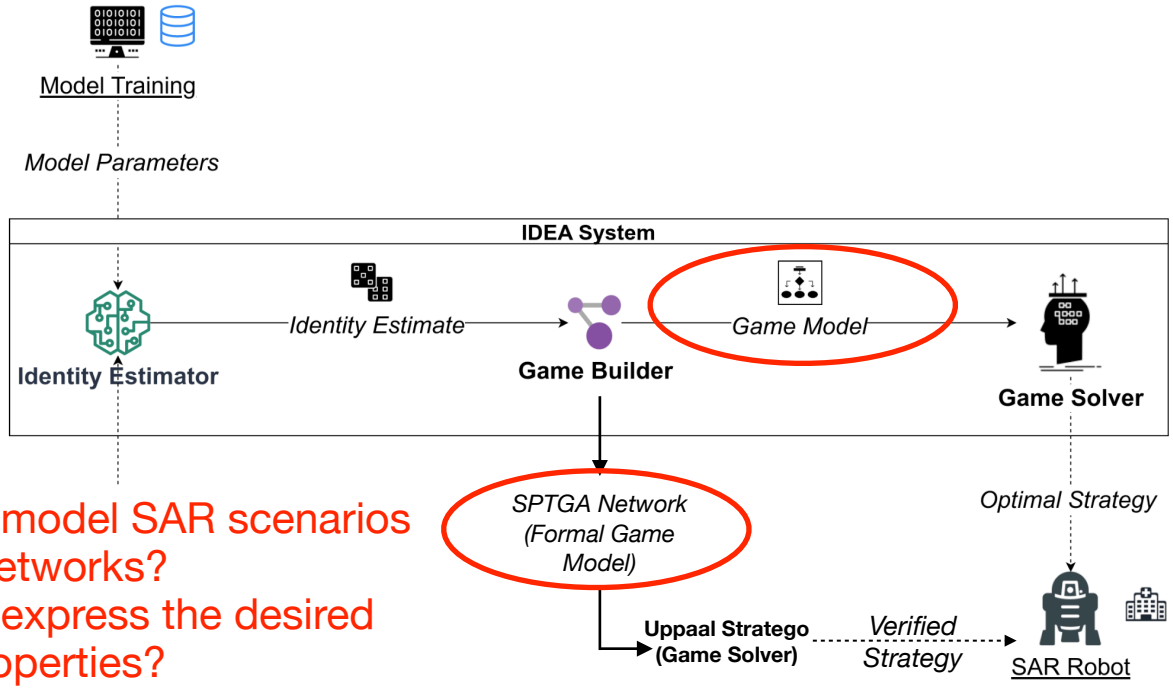
[2] David, A., Jensen, P. G., Larsen, K. G., Mikučionis, M., & Taankvist, J. H. (2015). Uppaal stratego. In TACAS 2015, Proceedings 21 (pp. 206-211). Springer Berlin Heidelberg.

The IDEA Framework [1] + Formal Verification



[1] Gavidia-Calderon, C., Kordoni, A., Bennaceur, A., Levine, M., & Nuseibeh, B. The IDEA of Us: An Identity-Aware Architecture for Autonomous Systems. Submitted to TOSEM.

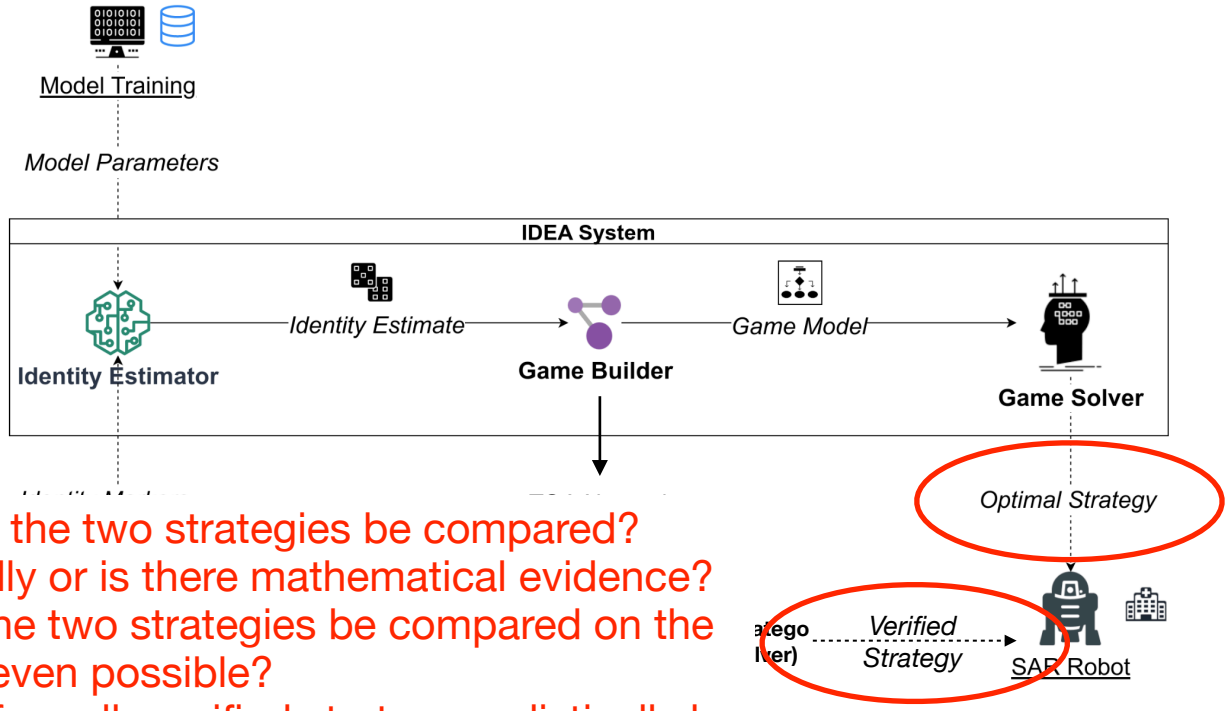
The IDEA Framework [1] + Formal Verification



- How to model SAR scenarios as TGA networks?
- How to express the desired formal properties?
- Are the two models equivalent?

[1] Gavidia-Calderon, C., Kordoni, A., Bennaceur, A., Levine, M., & Nuseibeh, B. The IDEA of Us: An Identity-Aware Architecture for Autonomous Systems. Submitted to TOSEM.

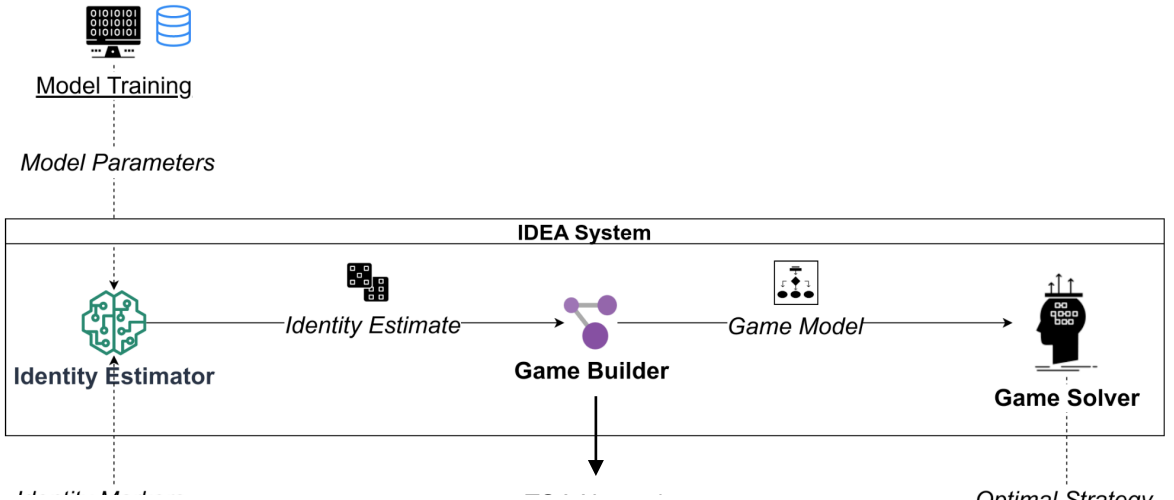
The IDEA Framework [1] + Formal Verification



- How can the two strategies be compared? Empirically or is there mathematical evidence?
- Should the two strategies be compared on the fly? Is it even possible?
- Can the formally verified strategy realistically be computed at runtime?

[1] Gavidia-Calderon, C., Kordoni, A., Bennaceur, A., Levine, M., & Nuseibeh, B. The IDEA of Us: An Identity-Aware Architecture for Autonomous Systems. Submitted to TOSEM.

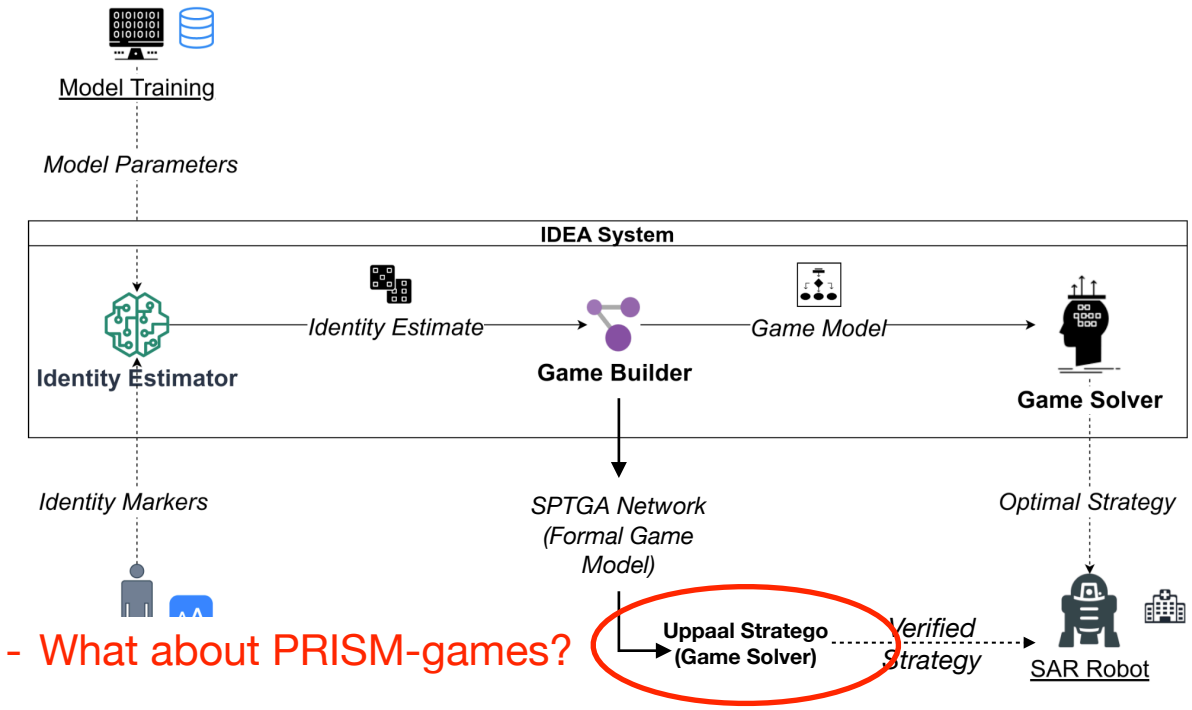
The IDEA Framework [1] + Formal Verification



- Does the robot take into account both strategies?
- Do specific criteria exist to choose when one is preferable over the other? (E.g., the verified strategy overperforms the optimal one if >10 First-responders are in close proximity)

[1] Gavidia-Calderon, C., Kordoni, A., Bennaceur, A., Levine, M., & Nuseibeh, B. The IDEA of Us: An Identity-Aware Architecture for Autonomous Systems. Submitted to TOSEM.

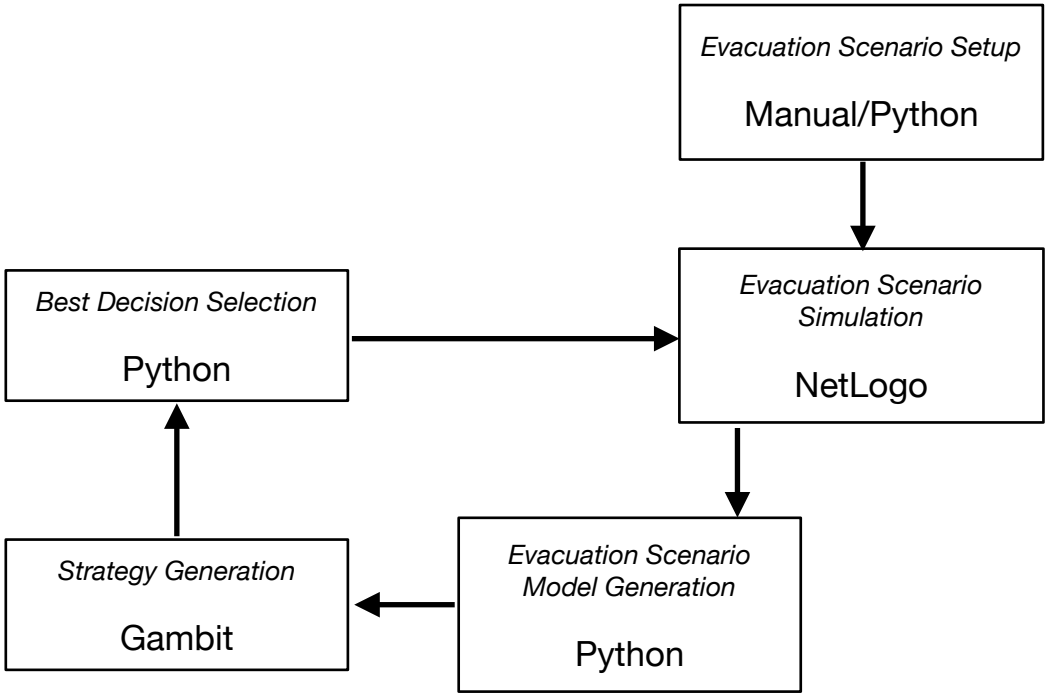
The IDEA Framework [1] + Formal Verification



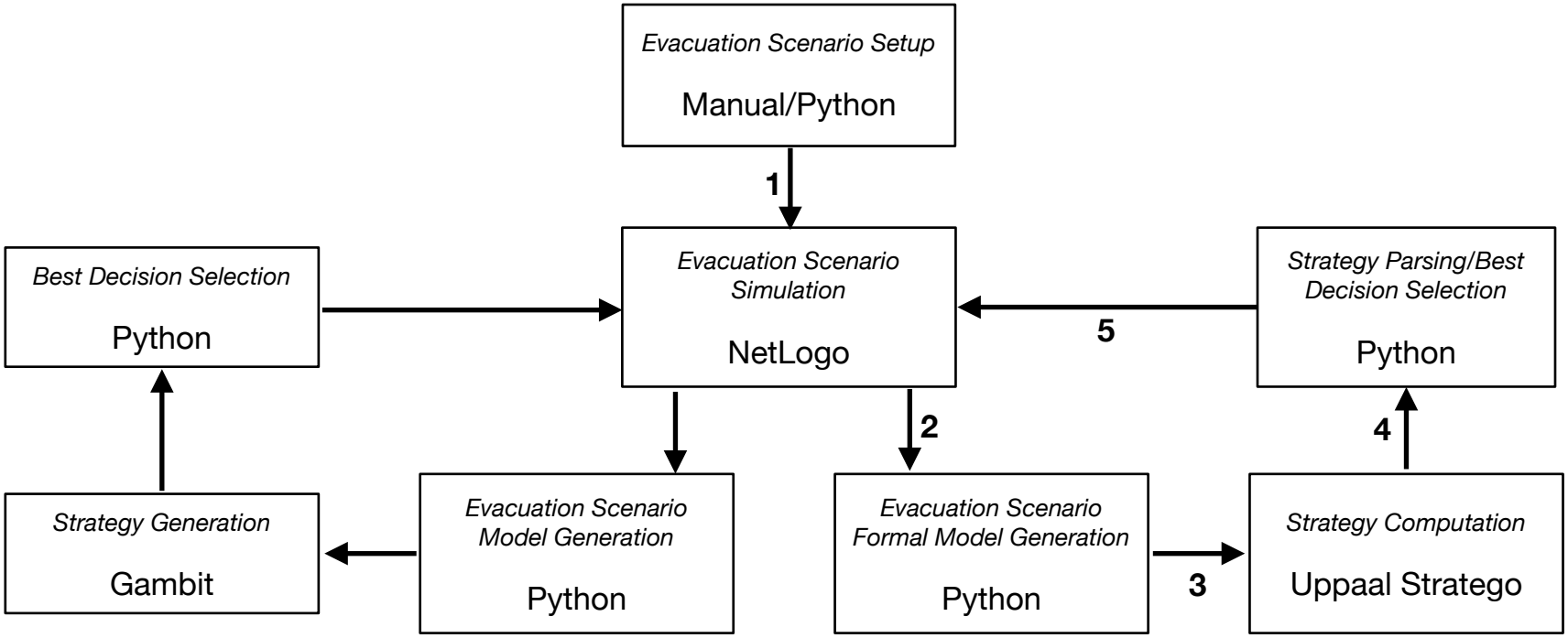
[1] Gavidia-Calderon, C., Kordoni, A., Bennaceur, A., Levine, M., & Nuseibeh, B. The IDEA of Us: An Identity-Aware Architecture for Autonomous Systems. Submitted to TOSEM.

Livia Lestingi
DEIB, DeepSE Group
https://www.deepse.deib.polimi.it

The IDEA Framework

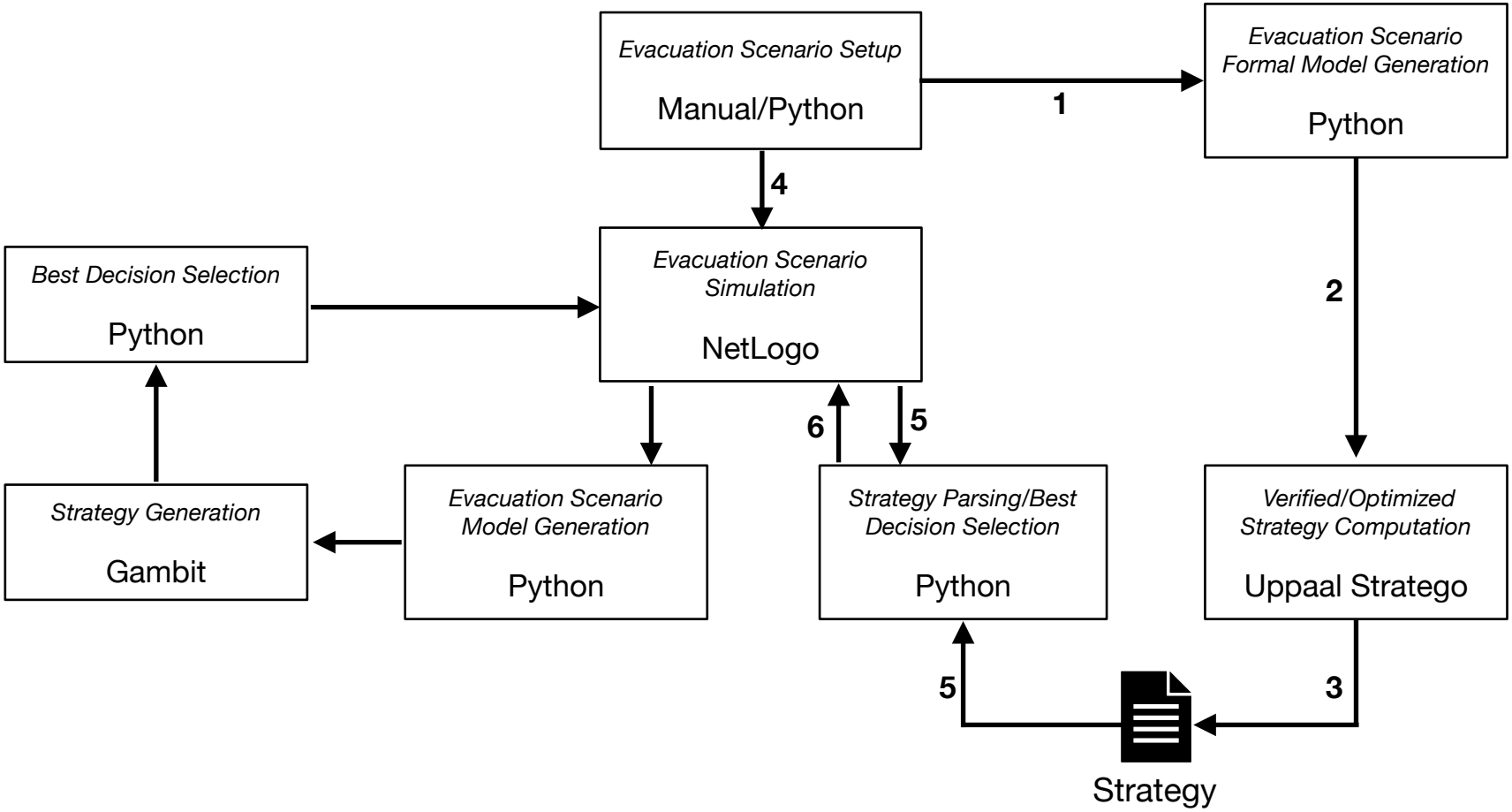


The IDEA Framework + Formal Verification: Option 1



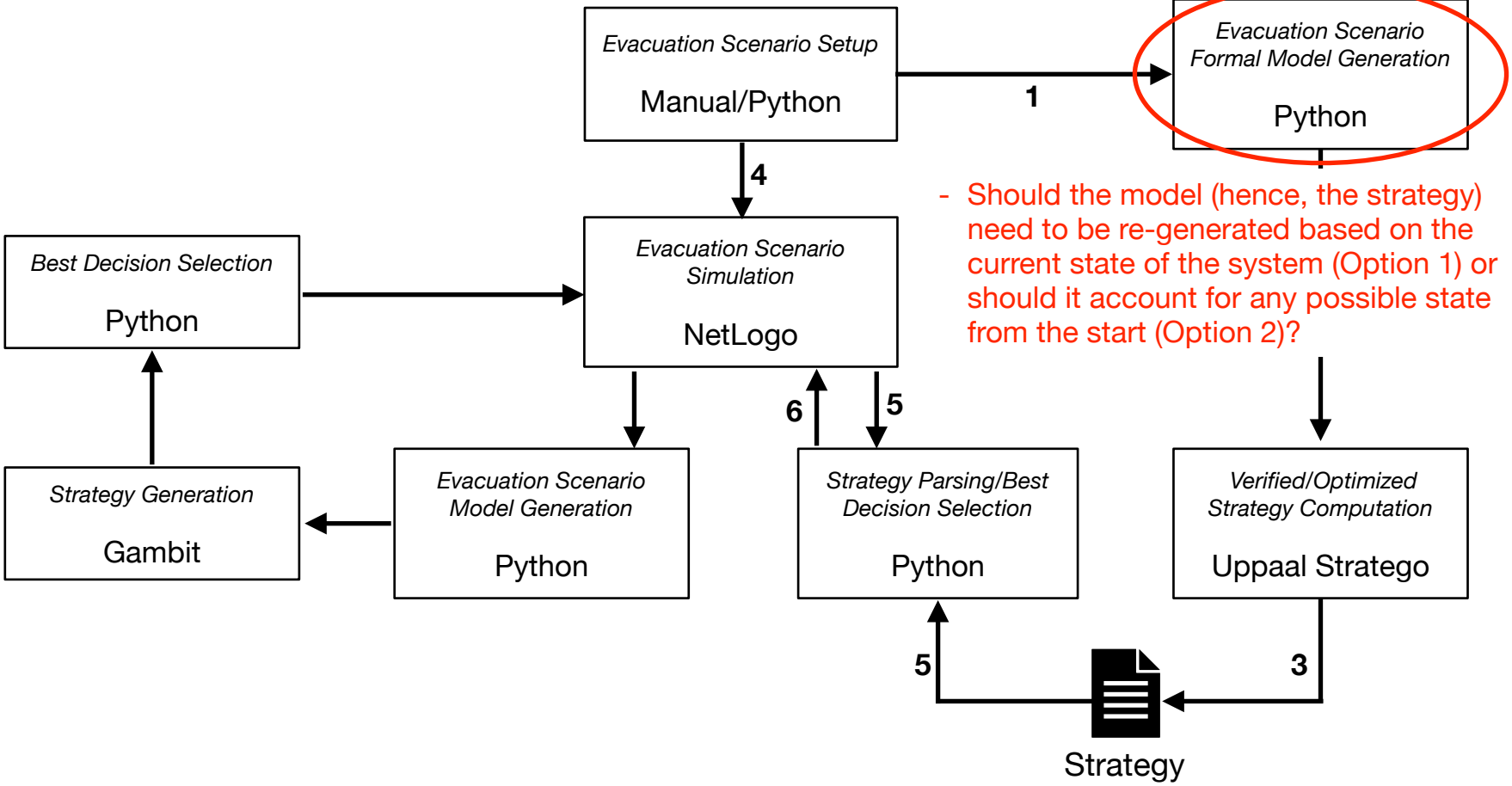
Livia Lestingi
DEIB, DeepSE Group
https://www.deepse.deib.polimi.it

The IDEA Framework + Formal Verification: Option 2



Livia Lestingi
DEIB, DeepSE Group
https://www.deepse.deib.polimi.it

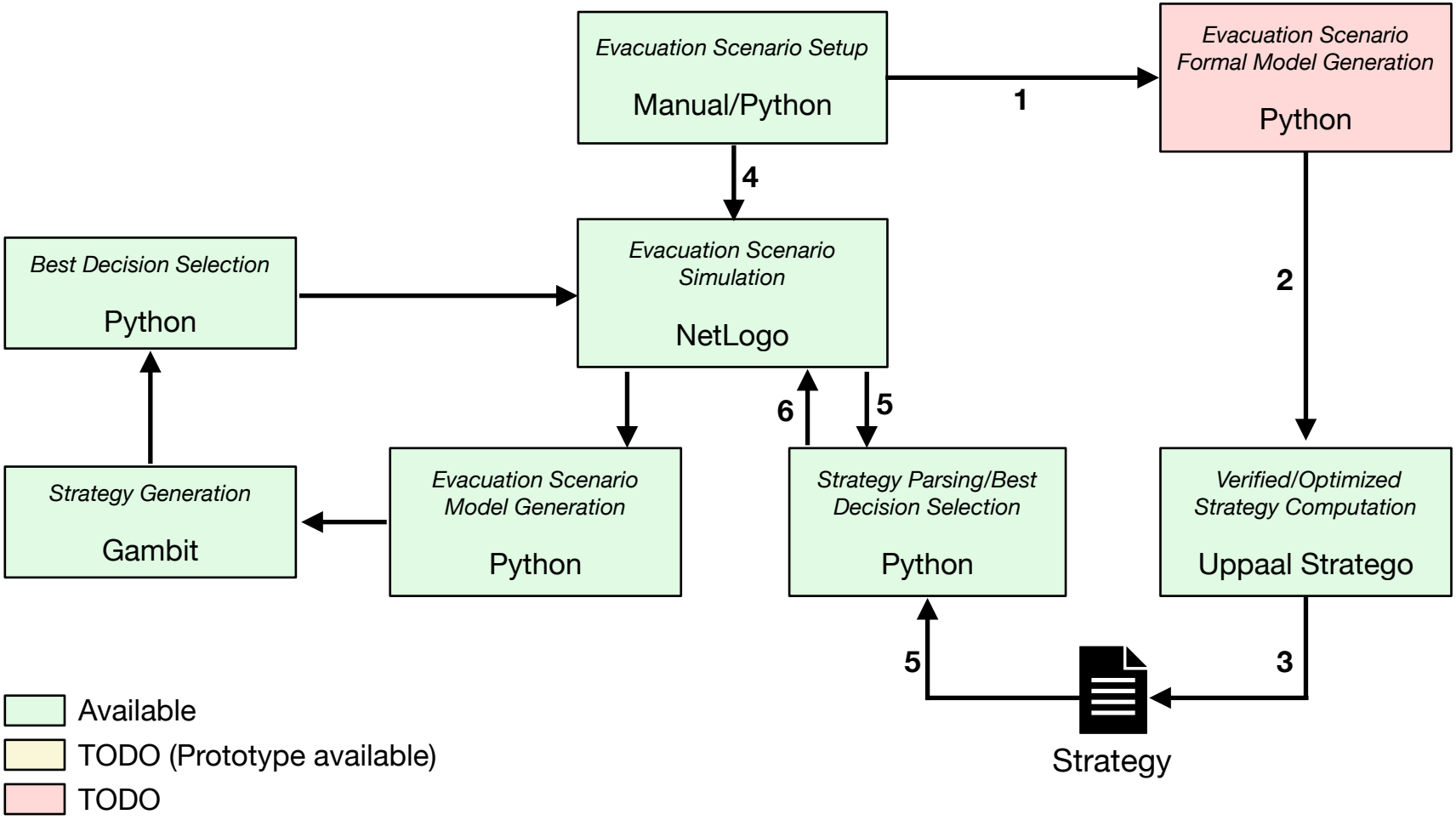
The IDEA Framework + Formal Verification: Option 2



- Should the model (hence, the strategy) need to be re-generated based on the current state of the system (Option 1) or should it account for any possible state from the start (Option 2)?

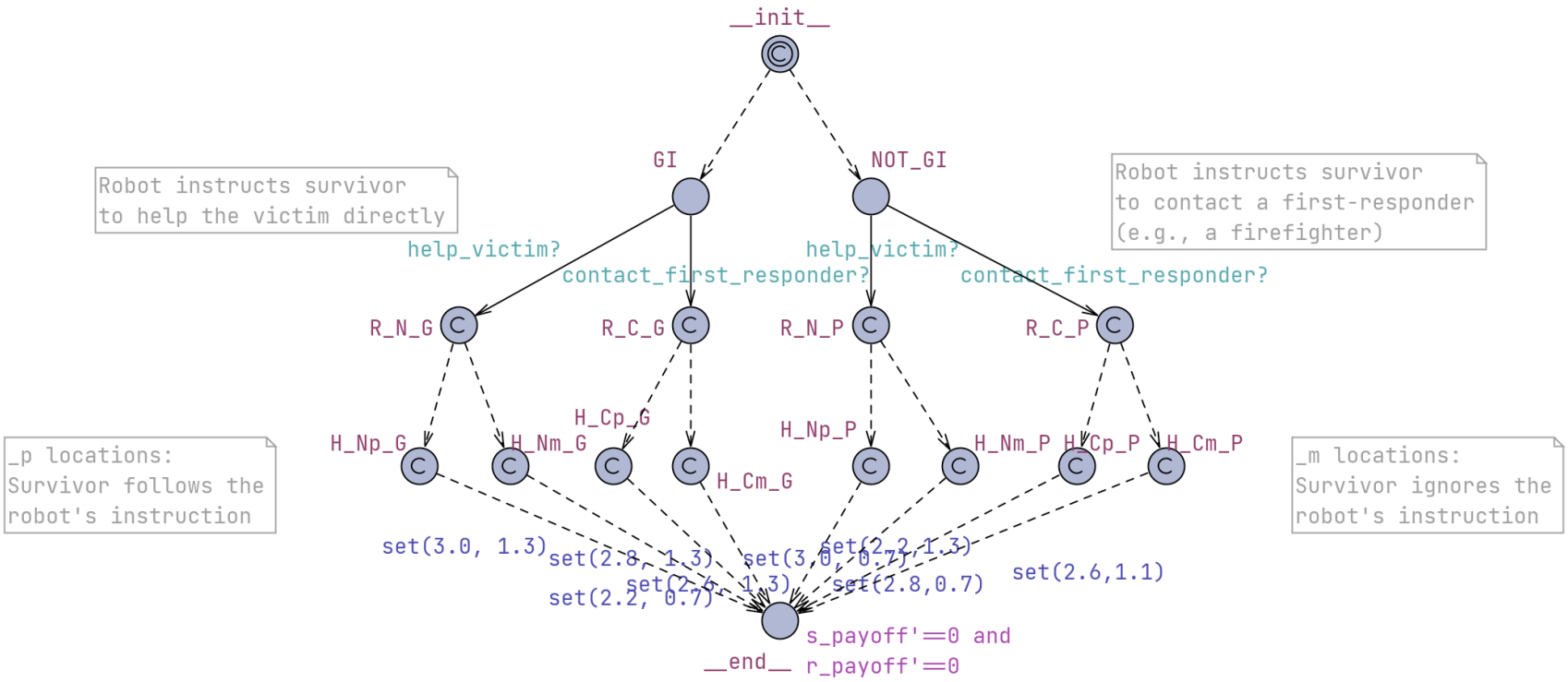
Livia Lestingi
DEIB, DeepSE Group
https://www.deepse.deib.polimi.it

The IDEA Framework + Formal Verification: Current state



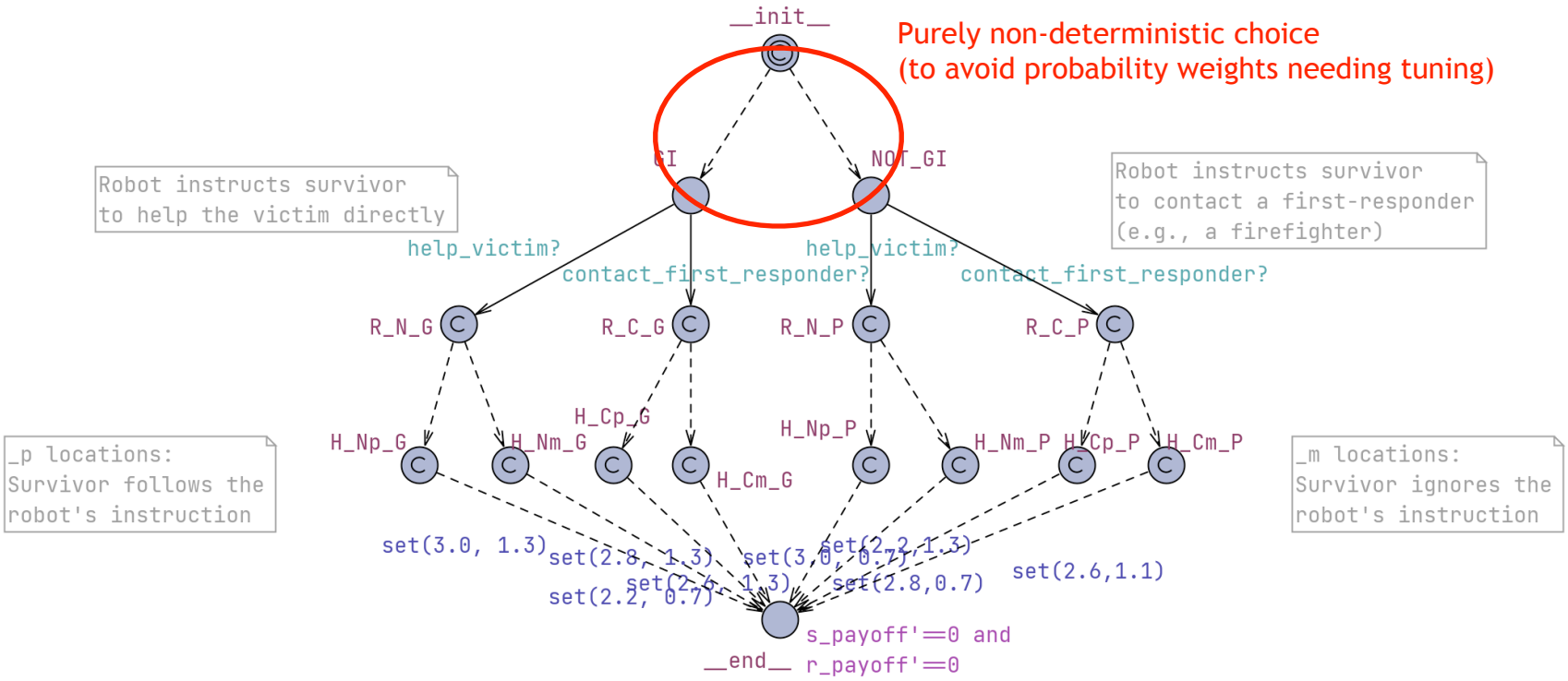
Livia Lestingi
DEIB, DeepSE Group
https://www.deepse.deib.polimi.it

Formal Model



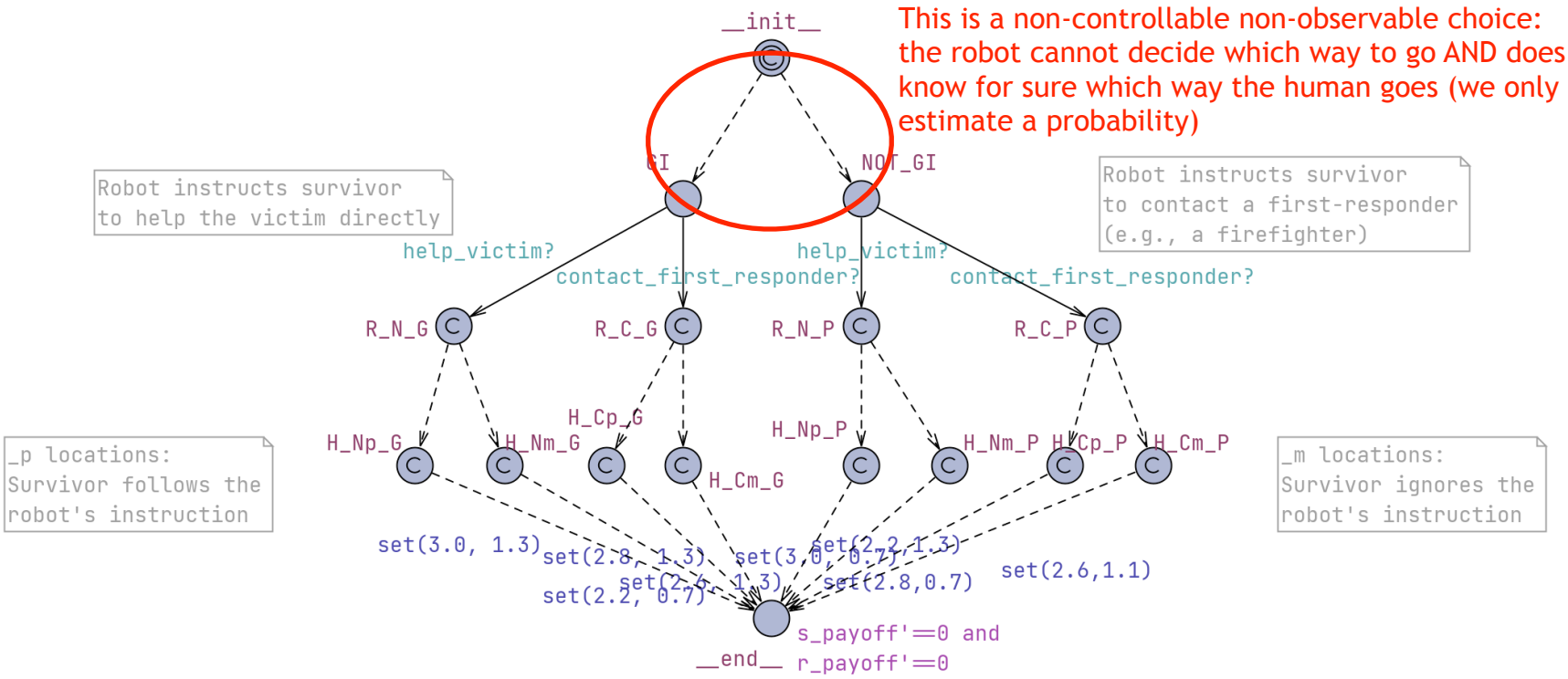
Livia Lestingi
DEIB, DeepSE Group
https://www.deepse.deib.polimi.it

Formal Model



Livia Lestingi
DEIB, DeepSE Group
https://www.deepse.deib.polimi.it

Formal Model



This is a non-controllable non-observable choice: the robot cannot decide which way to go AND does not know for sure which way the human goes (we only estimate a probability)

Formal Model: How to deal with uncontrollable unobservable actions?

Re-calibrate the expected payoff value to account for the probability to reach the corresponding state (where act is either call-staff or do-help):

$$U(\langle \mathsf{GI}, \mathsf{act} \rangle) \rightarrow U(\langle \mathsf{GI}, \mathsf{act} \rangle) \times P(\mathsf{GI})$$

$$U(\langle \mathsf{NOT\_GI}, \mathsf{act} \rangle) \rightarrow U(\langle \mathsf{NOT\_GI}, \mathsf{act} \rangle) \times (1 - P(\mathsf{GI}))$$

Formal Model: How to deal with uncontrollable unobservable actions?

Re-calibrate the expected payoff value to account for the probability to reach the corresponding state (where act is either call-staff or do-help):

$$U(\langle \mathsf{GI}, \mathsf{act} \rangle) \rightarrow U(\langle \mathsf{GI}, \mathsf{act} \rangle) \times P(\mathsf{GI})$$

$$U(\langle \mathsf{NOT\_GI}, \mathsf{act} \rangle) \rightarrow U(\langle \mathsf{NOT\_GI}, \mathsf{act} \rangle) \times (1 - P(\mathsf{GI}))$$

Extracted from Uppaal strategy

Estimated (at runtime) by NN

Formal Model: How to deal with uncontrollable unobservable actions?

Re-calibrate the expected payoff value to account for the probability to reach the corresponding state (where act is either call-staff or do-help):

$$U(\langle \mathsf{GI}, \mathsf{act} \rangle) \rightarrow U(\langle \mathsf{GI}, \mathsf{act} \rangle) \times P(\mathsf{GI})$$

$$U(\langle \mathsf{NOT\_GI}, \mathsf{act} \rangle) \rightarrow U(\langle \mathsf{NOT\_GI}, \mathsf{act} \rangle) \times (1 - P(\mathsf{GI}))$$

	contact-staff	do-help
GI	1.3	0.77
NOT_GI	0.85	1.28

Formal Model: How to deal with uncontrollable unobservable actions?

Re-calibrate the expected payoff value to account for the probability to reach the corresponding state (where act is either call-staff or do-help):

$$U(\langle \mathsf{GI}, \mathsf{act} \rangle) \rightarrow U(\langle \mathsf{GI}, \mathsf{act} \rangle) \times P(\mathsf{GI})$$

$$U(\langle \mathsf{NOT\_GI}, \mathsf{act} \rangle) \rightarrow U(\langle \mathsf{NOT\_GI}, \mathsf{act} \rangle) \times (1 - P(\mathsf{GI}))$$

P(GI) = 0.8	contact-staff	do-help
GI	1.3*0.8=1.04	0.77*0.8=0.62
NOT_GI	0.85*0.2=0.17	1.28*0.2=0.26

Formal Model: How to deal with uncontrollable unobservable actions?

Re-calibrate the expected payoff value to account for the probability to reach the corresponding state (where act is either call-staff or do-help):

$$U(\langle \mathsf{GI}, \mathsf{act} \rangle) \rightarrow U(\langle \mathsf{GI}, \mathsf{act} \rangle) \times P(\mathsf{GI})$$

$$U(\langle \mathsf{NOT\_GI}, \mathsf{act} \rangle) \rightarrow U(\langle \mathsf{NOT\_GI}, \mathsf{act} \rangle) \times (1 - P(\mathsf{GI}))$$

P(GI) = 0.8	contact-staff	do-help
GI	1.3*0.8=1.04	0.77*0.8=0.62
NOT_GI	0.85*0.2=0.17	1.28*0.2=0.26

1.21 > 0.88

(contact-staff is preferable)

Livia Lestingi
DEIB, DeepSE Group
https://www.deepse.deib.polimi.it

Formal Model: How to deal with uncontrollable unobservable actions?

Re-calibrate the expected payoff value to account for the probability to reach the corresponding state (where act is either call-staff or do-help):

$$U(\langle \mathsf{GI}, \mathsf{act} \rangle) \rightarrow U(\langle \mathsf{GI}, \mathsf{act} \rangle) \times P(\mathsf{GI})$$

$$U(\langle \mathsf{NOT\_GI}, \mathsf{act} \rangle) \rightarrow U(\langle \mathsf{NOT\_GI}, \mathsf{act} \rangle) \times (1 - P(\mathsf{GI}))$$

P(GI) = 0.12	contact-staff	do-help
GI	1.3*0.12=0.156	0.77*0.12=0.09
NOT_GI	0.85*0.88=0.75	1.28*0.88=1.12

Formal Model: How to deal with uncontrollable unobservable actions?

Re-calibrate the expected payoff value to account for the probability to reach the corresponding state (where act is either call-staff or do-help):

$$U(\langle \mathsf{GI}, \mathsf{act} \rangle) \rightarrow U(\langle \mathsf{GI}, \mathsf{act} \rangle) \times P(\mathsf{GI})$$

$$U(\langle \mathsf{NOT\_GI}, \mathsf{act} \rangle) \rightarrow U(\langle \mathsf{NOT\_GI}, \mathsf{act} \rangle) \times (1 - P(\mathsf{GI}))$$

P(GI) = 0.12	contact-staff	do-help
GI	1.3*0.12=0.156	0.77*0.12=0.09
NOT_GI	0.85*0.88=0.75	1.28*0.88=1.12

0.9 < 1.21

(do-help is preferable)

Livia Lestingi
DEIB, DeepSE Group
https://www.deepse.deib.polimi.it

Experimental Results

Experimental results?