ICISSP 2020

A Domain-Specific Modeling Framework for Attack Surface Modeling

Tithnara Nicolas Sun, Bastien Drouot, Joël Champeau, Fahad R. Golra, Sylvain Guérin, Luka Le Roux, Raúl Mazo, Ciprian Teodorov, Lionel Van Aertryck, Bernard L'Hostis

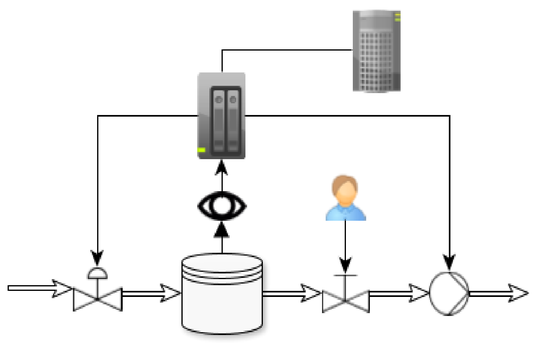
Problem: Cybersecurity of cyber physical systems & internet of things is vital. Security is a **continuous process** that runs throughout and at times even beyond the **life-cycle of a system**. Traditional methods of **security modeling** miss this life-cycle-based dynamicity.

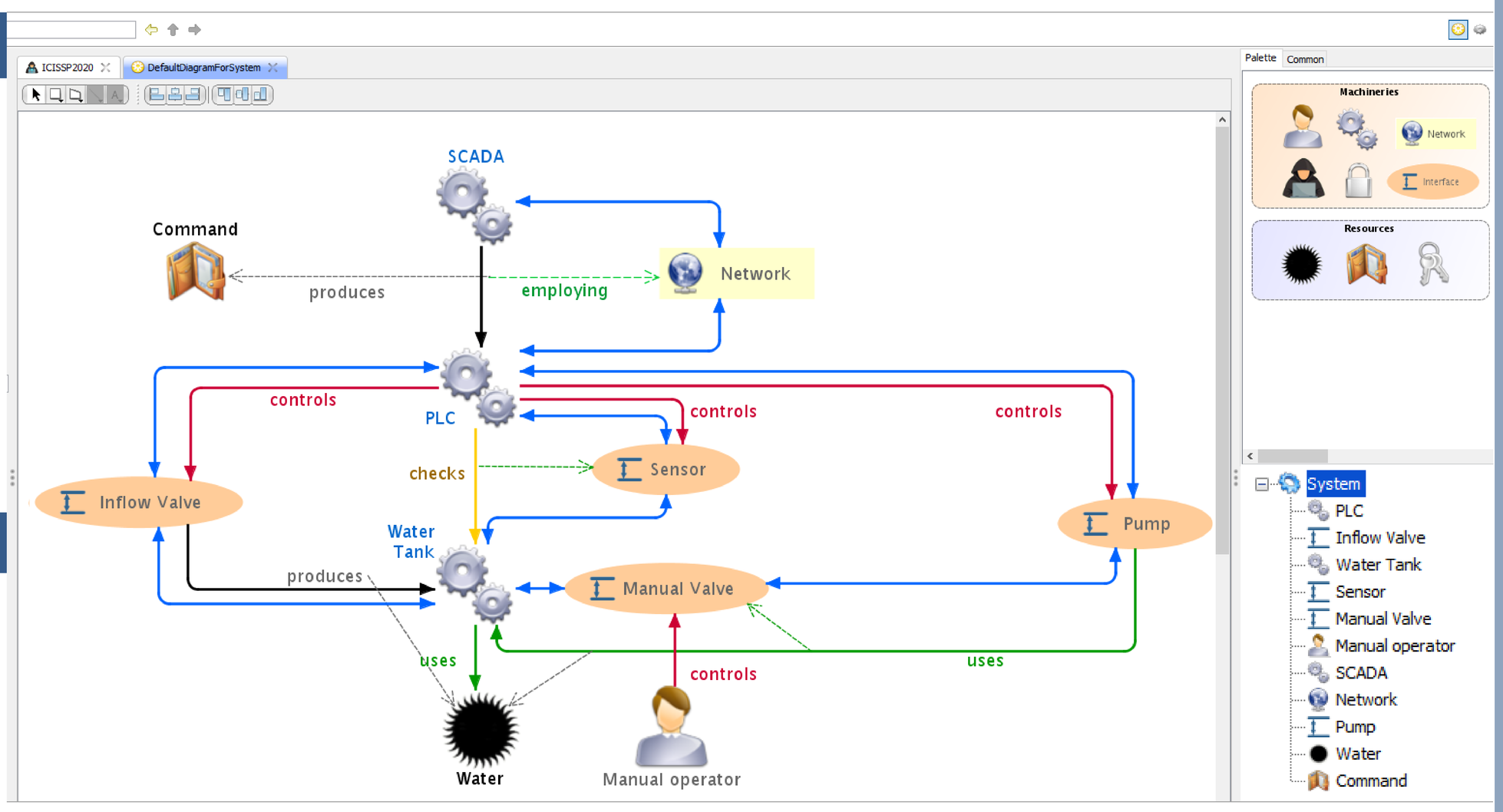
Contribution: We propose an **open-source framework** based on **Pimca**, a domain specific **systems modeling language highlighting the attack surface**[1] during cyber threat analysis[2].

Requirements

- Systems modeling with the intent of **highlighting** the **attack surface**
- Security concerns modeling using a **graphical** language, geared towards **automation**
- **Analysis-agnostic** attack surface modeling

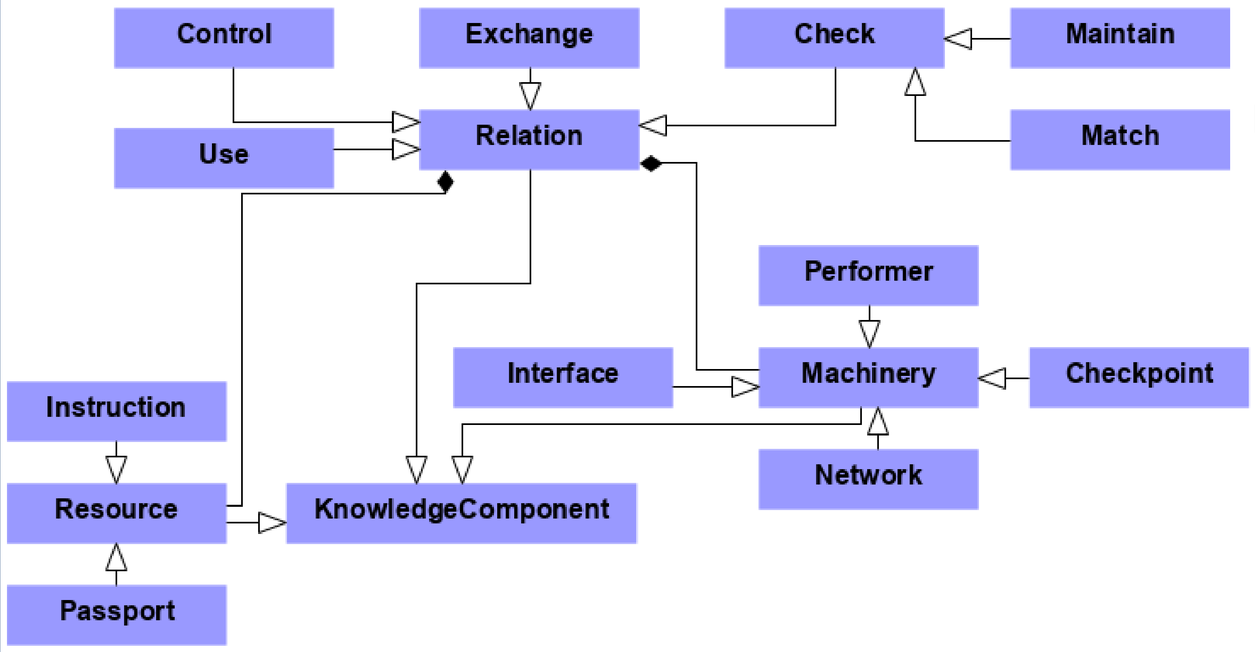
Water pump





Pimca language

- **Expressive relations** modeling complex interactions between components enable deeper security analysis and attack surface reasoning. Well-defined components also expose particular interactions and weaknesses in the attack surface.
- **Coarse-grain security-focused systems modeling** abstracts away internal architectural details and handles heterogeneous systems with ease.



Attack surface inference

1 ***How to reach the target ?***

Target: Water tank

Deducing sub-objectives using relations

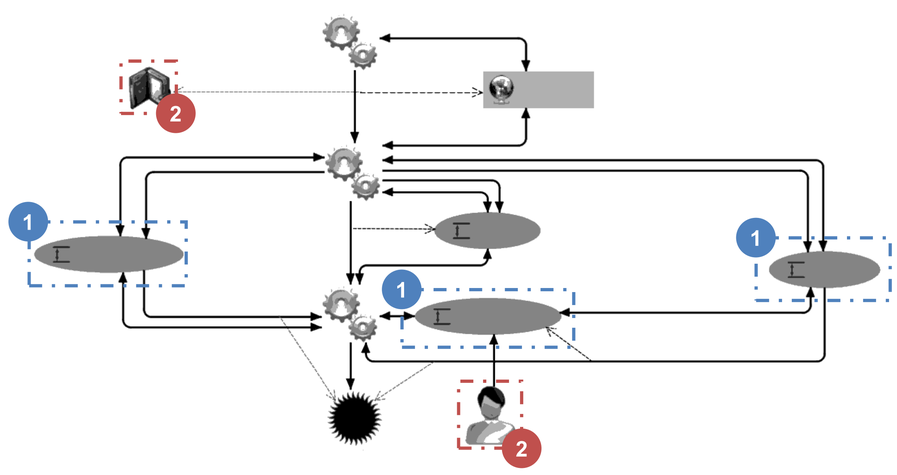
⇨ We can infer **intermediary targets**: Inflow valve, manual valve, pump

2 ***What are the targets available ?***

Capabilities: Social engineering, network access

Deducing reach based on attacker capabilities

⇨ The attack surface **extends** to: Command (through network), manual operator (through social engineering)



Conclusion: Our framework satisfies the intention of **highlighting the attack surfaces** in a system model. Preliminary validation is done on use cases, which emphasized the system modeling along with the **attack surface deduction and refinement** enabled by our framework.

Future Works: We intend to model the systems **dynamic behavior** using a component-by-component basis. We also plan to model an **executable attacker** so that we can **simulate** the system-under-attack behavior.

tithnara.sun@ensta-bretagne.org

We thank the French ministry of the armed forces and the DGA for funding this research

1. Manadhata, P. K. and Wing, J. M. (2011). An attack surface metric. IEEE Transactions on Software Engineering,37(3):371–386.
2. Farrell, M., Bradbury, M., Fisher, M., Dennis, L., Dixon,C., Yuan, H., and Maple, C. (2019). Using Threat Analysis Techniques to Guide Formal Verification: A Case Study of Cooperative Awareness Messages,pages 471–490. Springer.