Towards Provable Security in Industrial Control Systems Via Dynamic Protocol Attestation

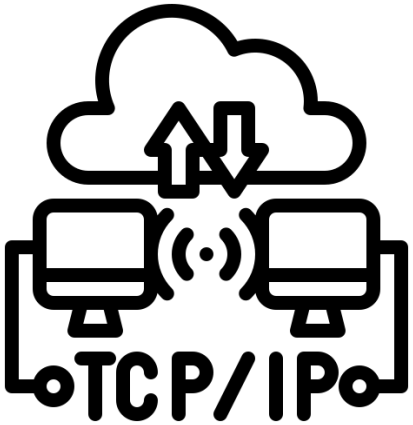
Arthur Amorim, Trevor Kann, Max Taylor, Lance Joneckis

Our methodology retrofits legacy ICS to mitigate real-world safety and security weaknesses with little overhead.

INL Idaho National Laboratory

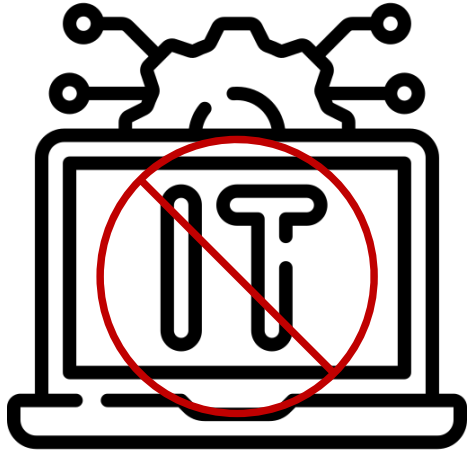
Industry 4.0 has made ICS more interconnected, but also more vulnerable.

Connected to the Internet



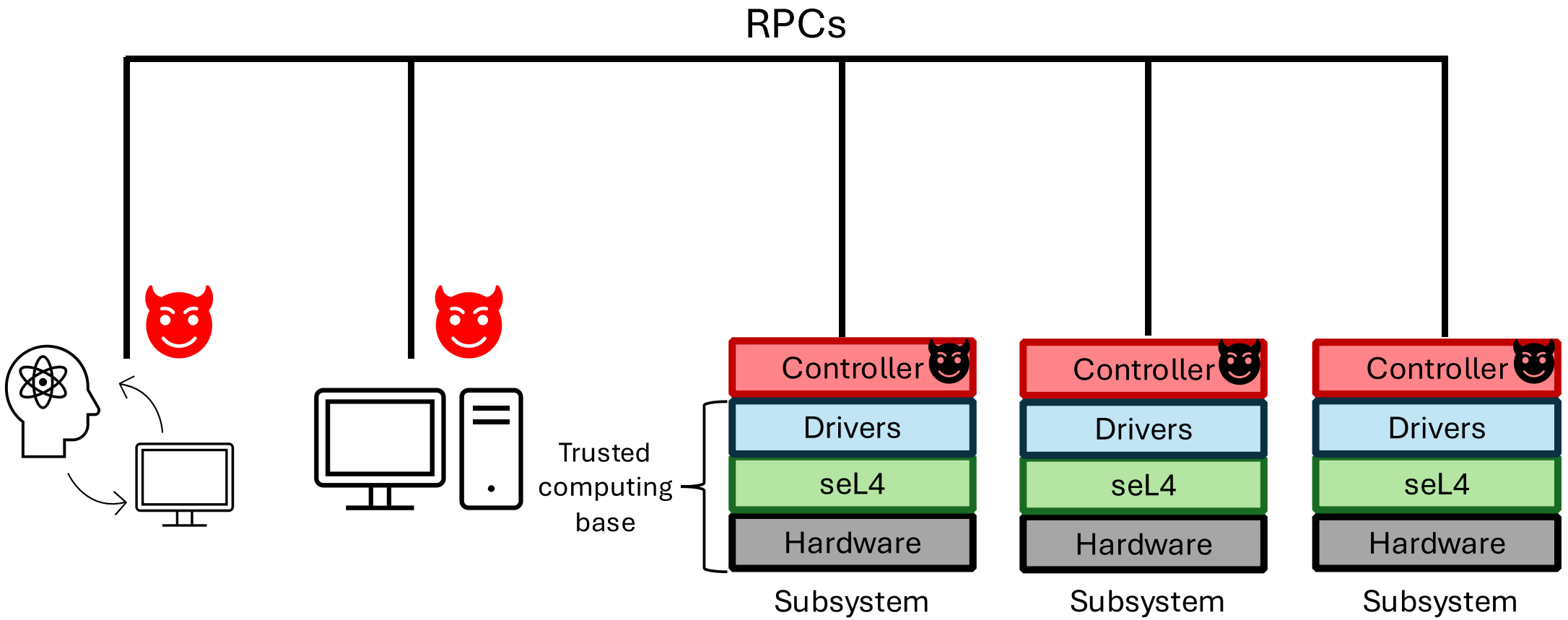
Using protocols with known vulnerabilities

Difficulty with testing new patches

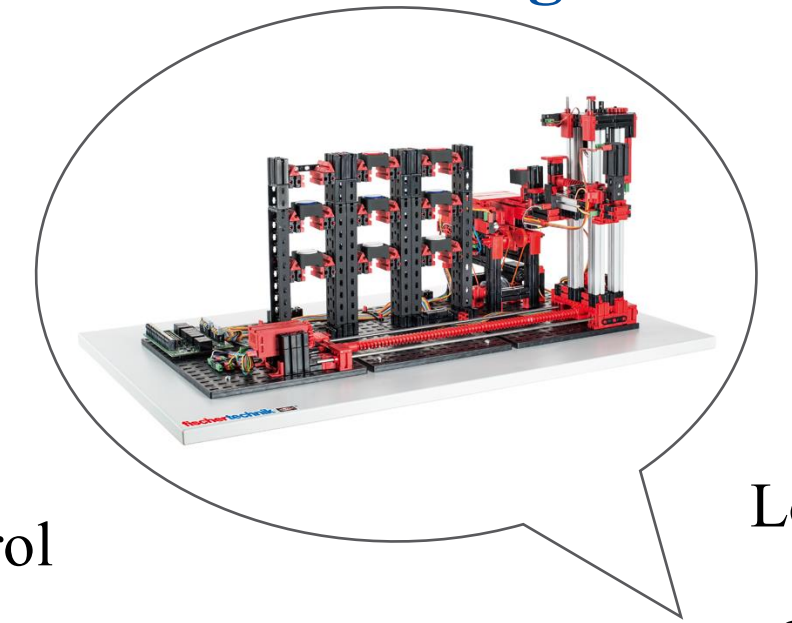


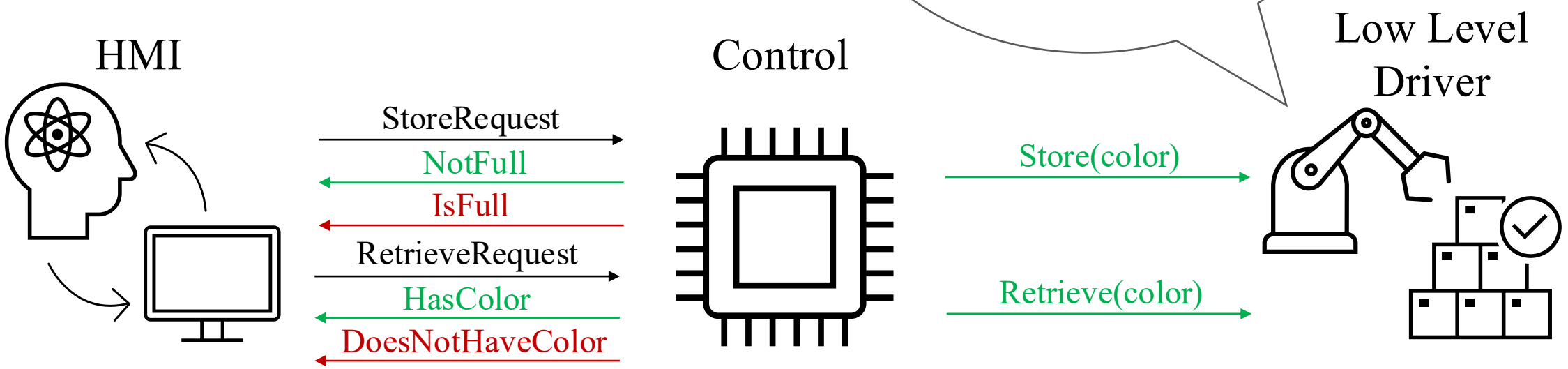
Cannot use IT security approaches

The attacker is assumed to have compromised controllers, being able to execute malicious remote procedure calls over the network.



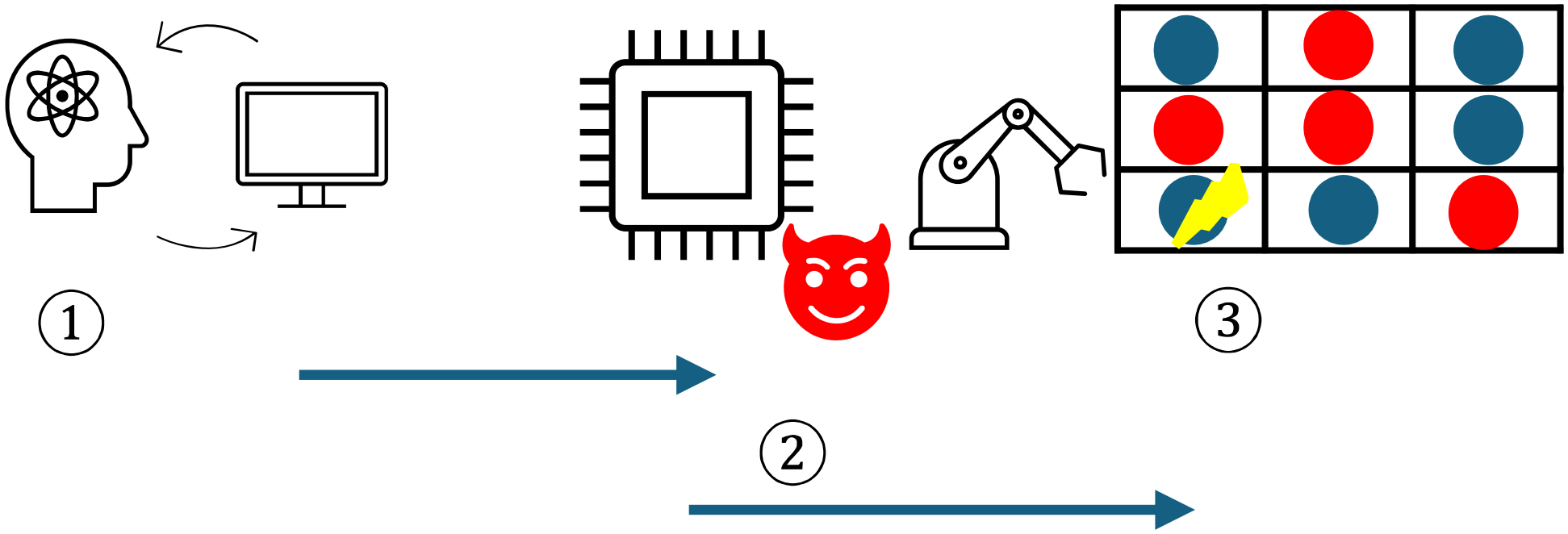
A protocol is a set of rules that dictates what messages can be sent over a network.



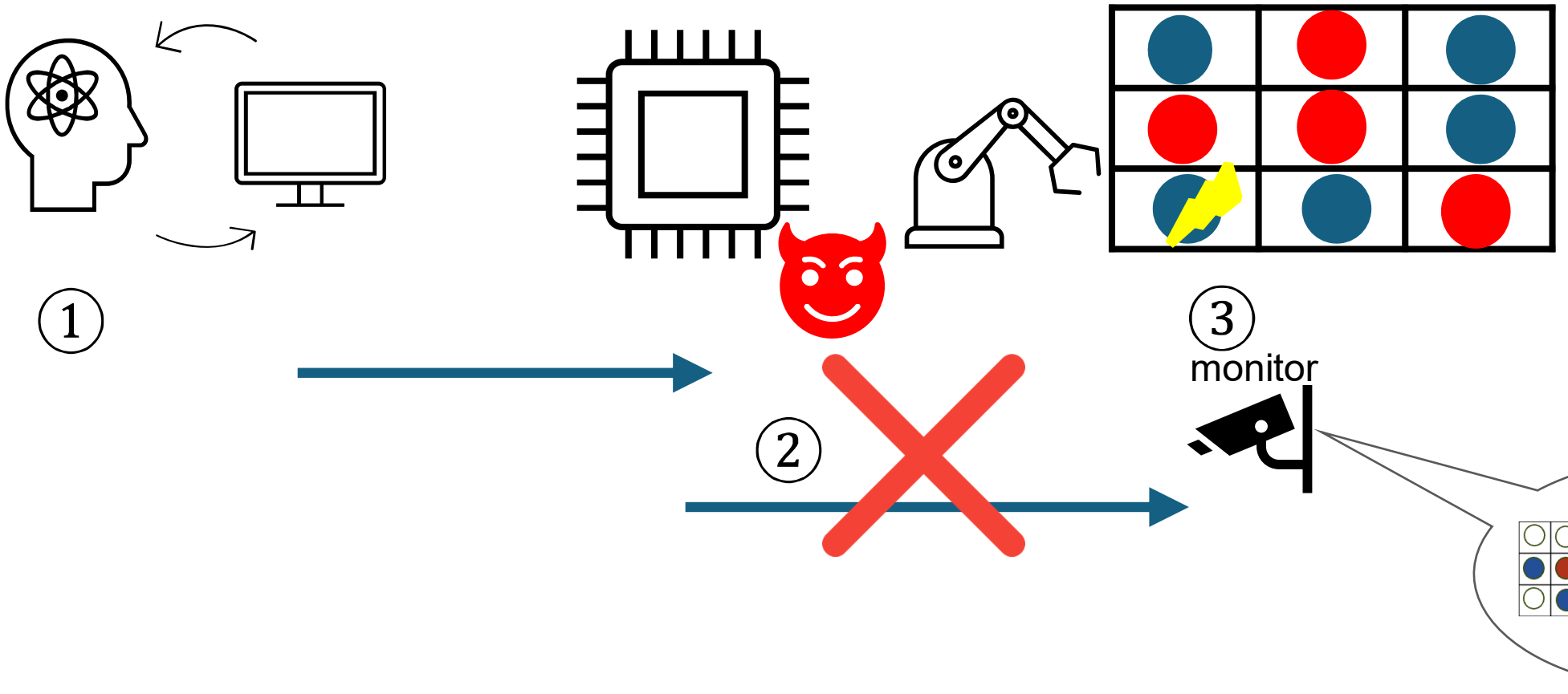


Idaho National Laboratory

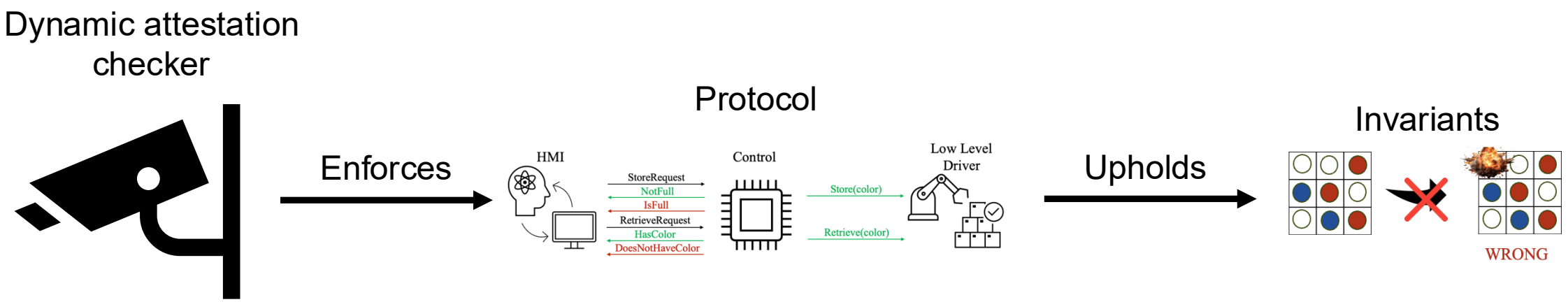
Some sort of dynamic checking is paramount to ensure a protocol is being followed at runtime.



Some sort of dynamic checking is paramount to ensure a protocol is being followed at runtime.

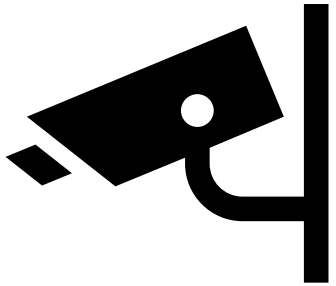


How can we know that our monitor is any good?



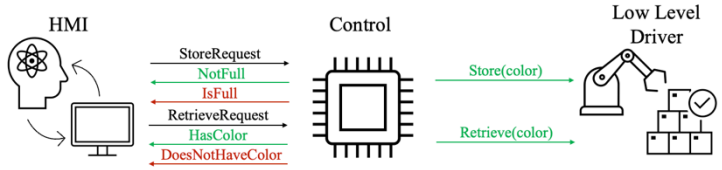
How can we know that our monitor is any good?

Dynamic attestation checker



Enforces

Protocol

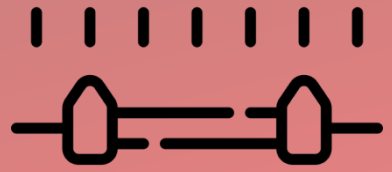


VERY IMPORTANT

Upholds

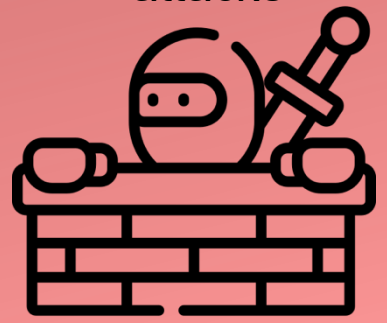
Invariants

Input validation attacks



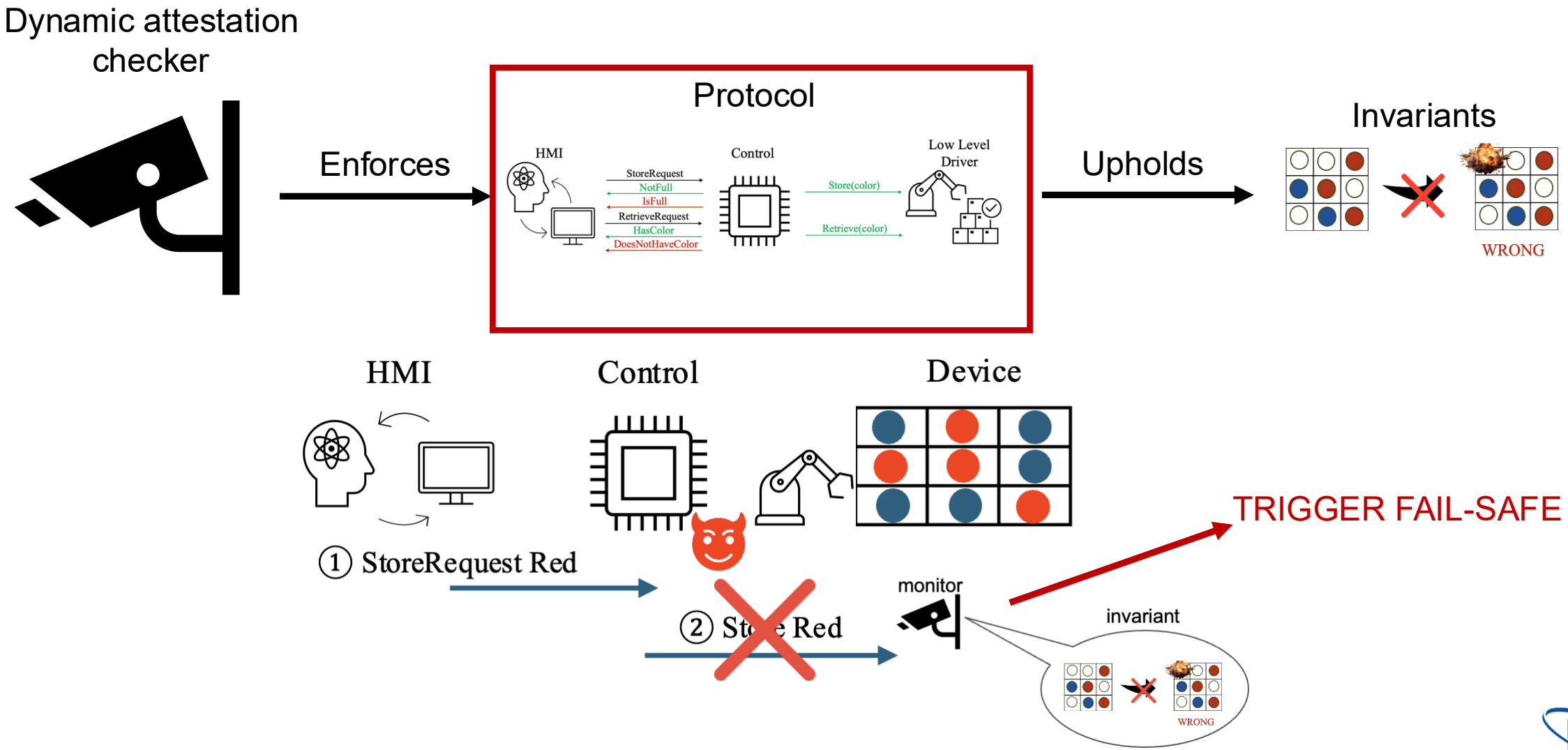
Policy violation attacks

Stealthy attacks



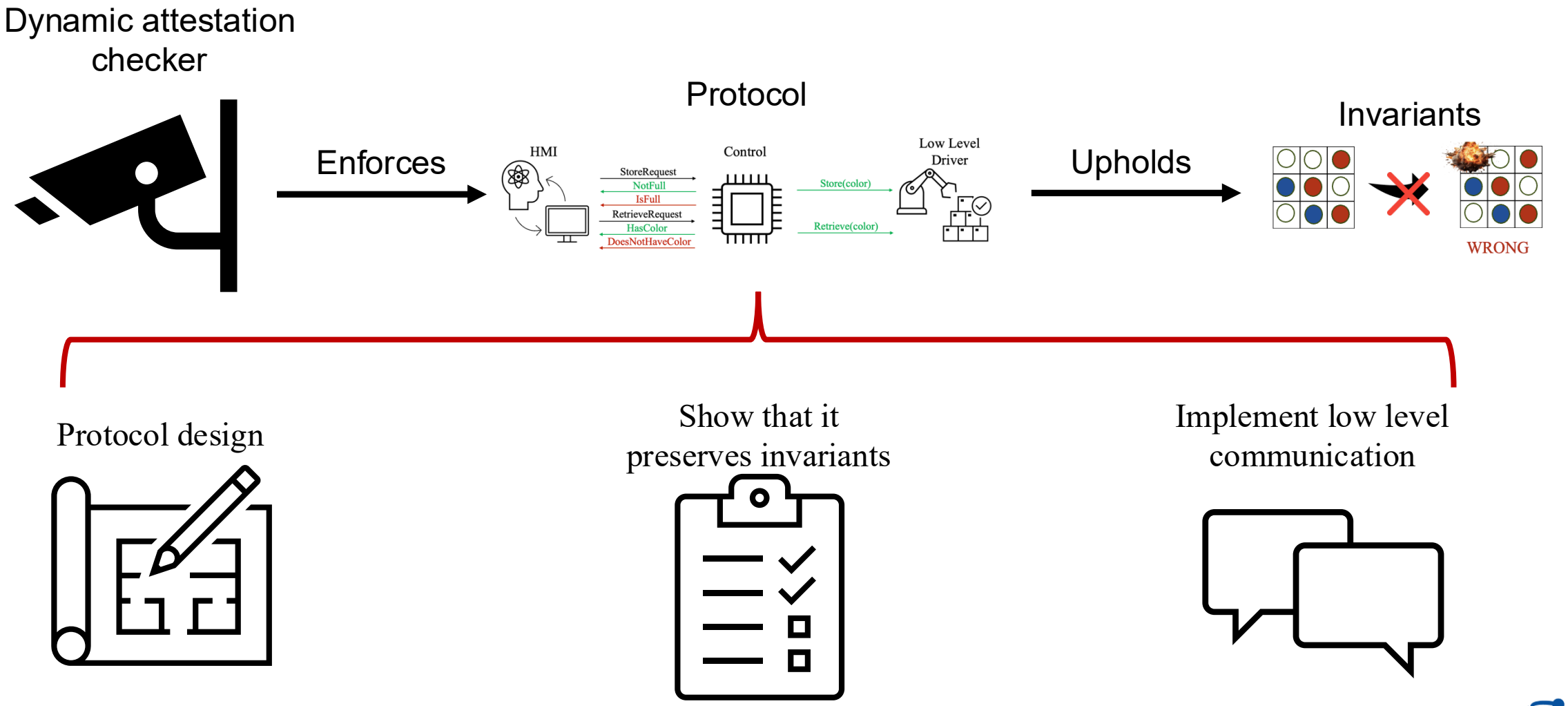
Idaho National Laboratory

A protocol shown to preserve safety invariants can be used with dynamic monitoring to prevent the effects of attacks.

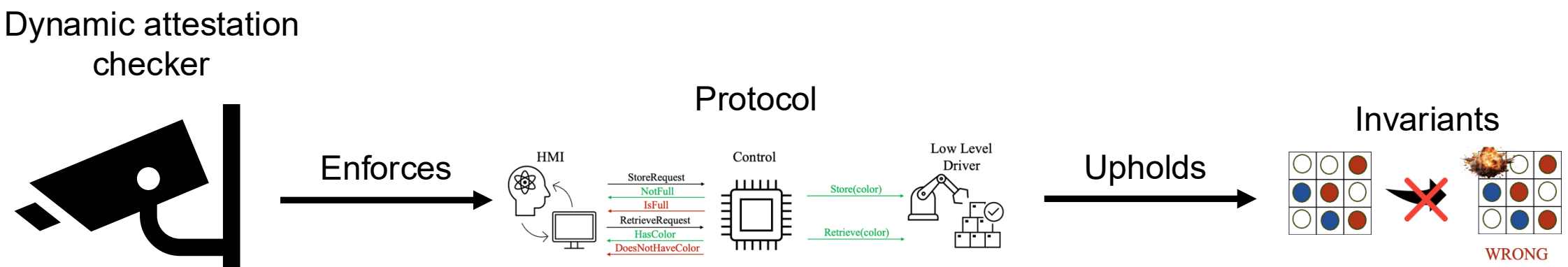


Idaho National Laboratory

A protocol shown to preserve safety invariants can be used with dynamic monitoring to prevent the effects of attacks.

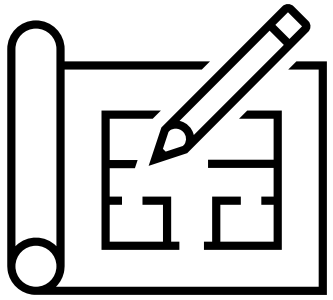


A protocol shown to preserve safety invariants can be used with dynamic monitoring to prevent the effects of attacks.

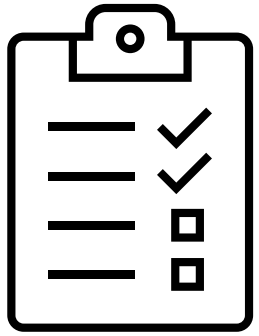


FORMAL METHODS

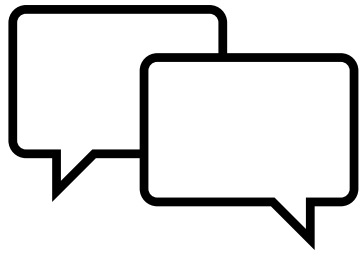
SPECIFICATION



VERIFICATION



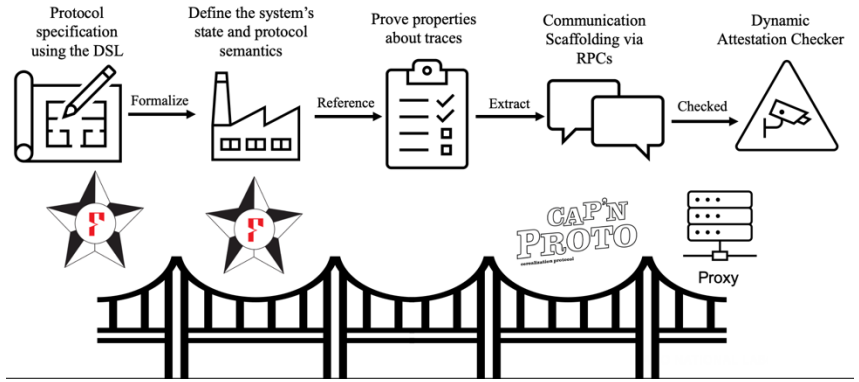
IMPLEMENTATION



Idaho National Laboratory

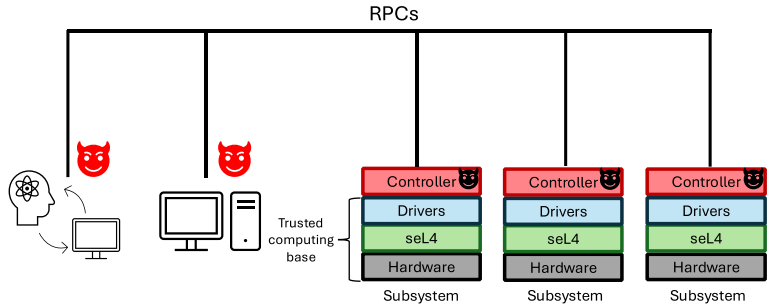
By using our methodology, you can:

Specify and verify protocols.

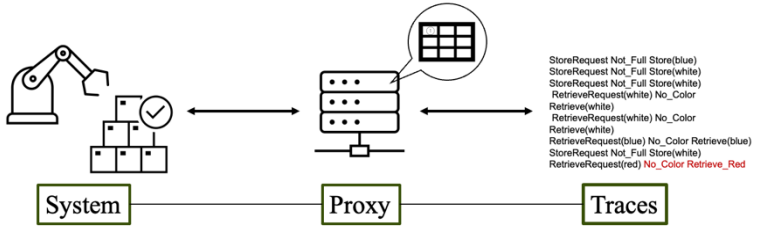


Bridge the gap between design and implementation with relatively low overhead.

Reduce the verification burden by eliminating the need to prove entire systems.



Use formal methods to retrofits legacy ICS to mitigate real-world safety and security weaknesses.

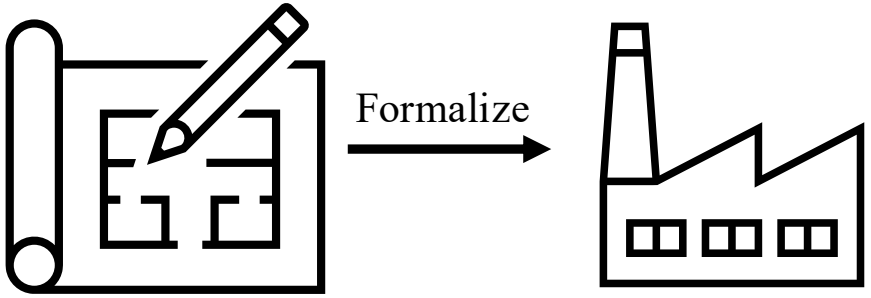


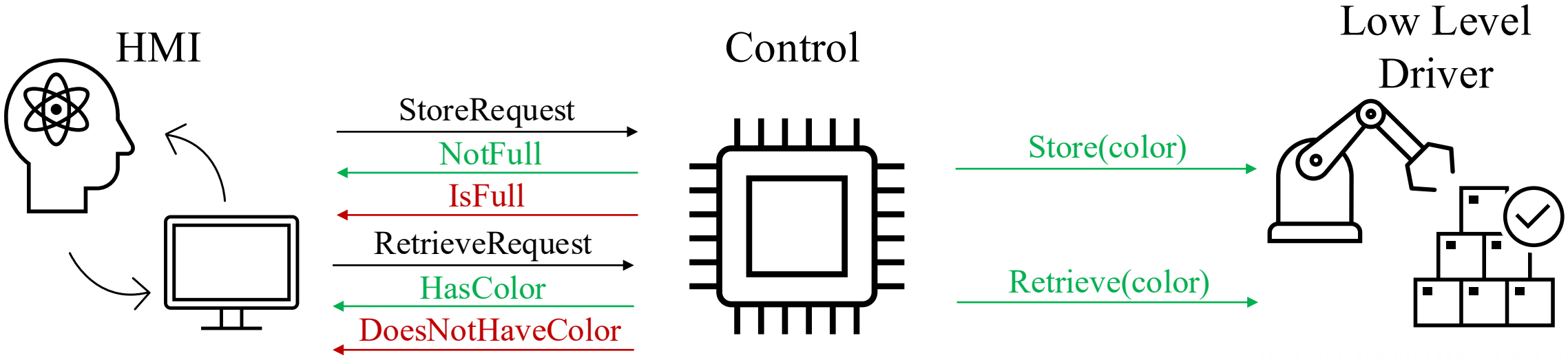
Idaho National Laboratory

The protocol semantics reflect how each executing an RPC changes the state.

Protocol design using the DSL

Define the system's state and protocol semantics

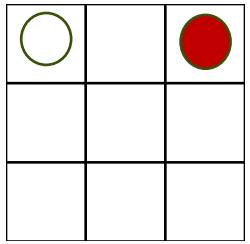


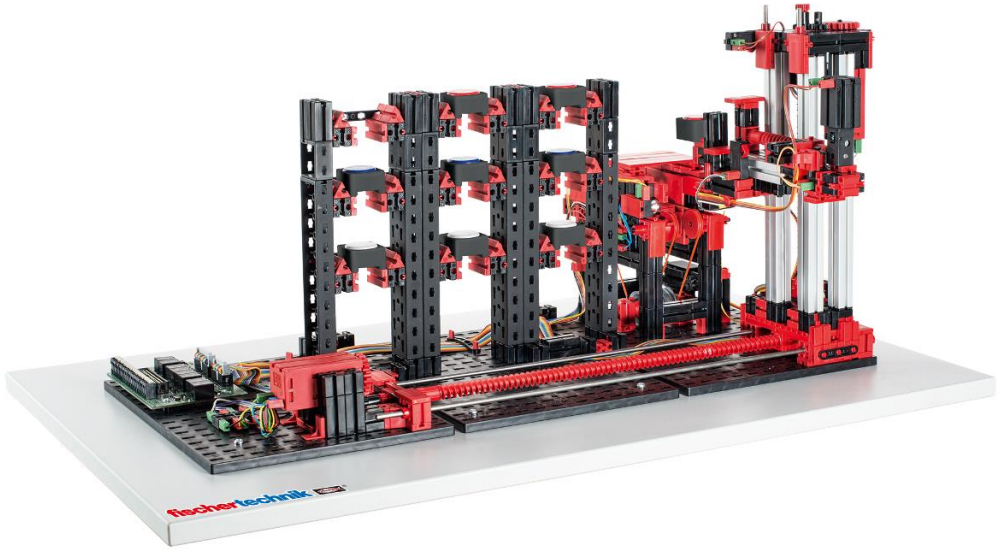


Semantics are used to identify “bad” Message x State pairs.

Store Blue

+

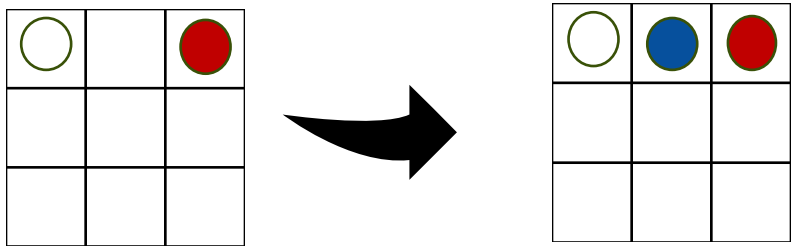


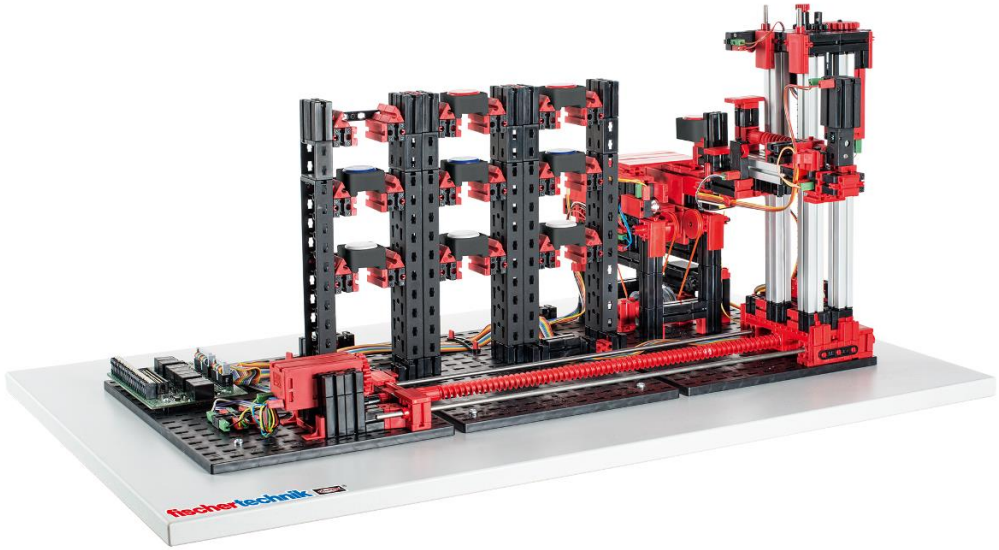


Semantics are used to identify “bad” Message x State pairs.

Store Blue

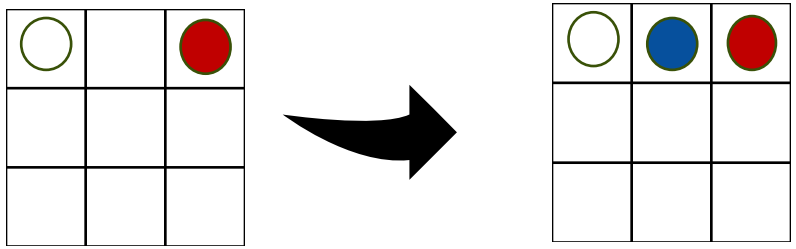
+



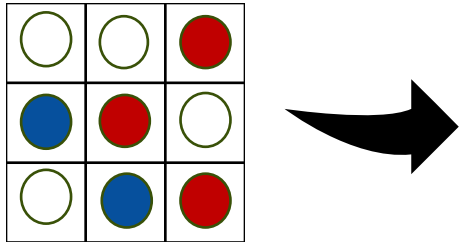


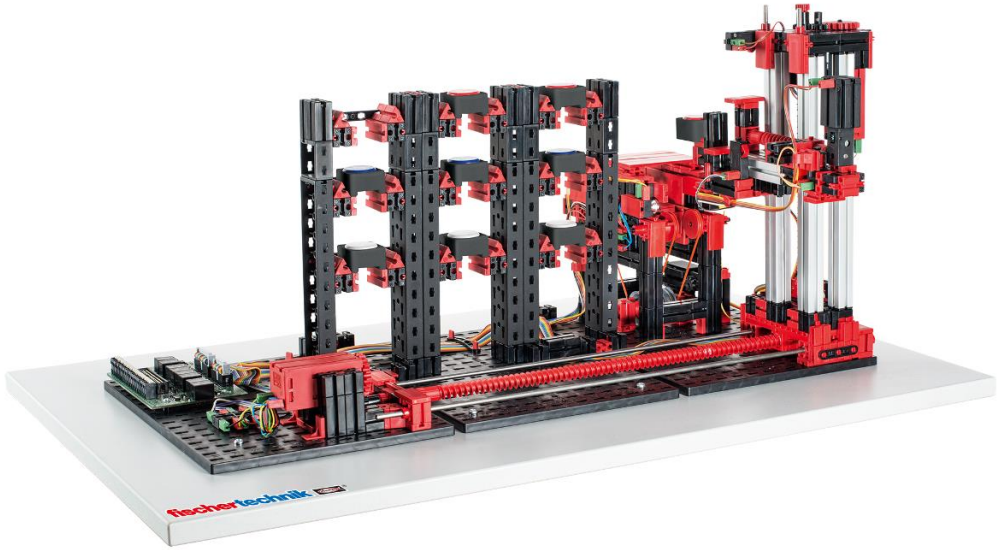
Semantics are used to identify “bad” Message x State pairs.

Store Blue +



Store Blue +

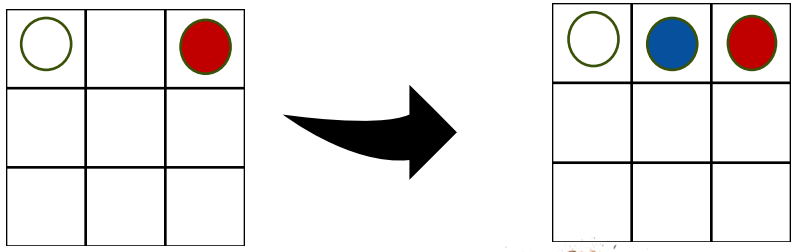




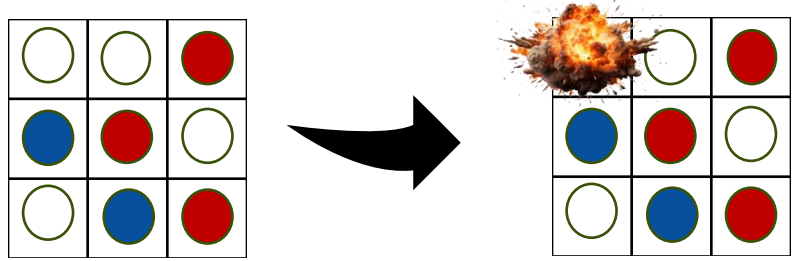
Idaho National Laboratory

Semantics are used to identify “bad” Message x State pairs.

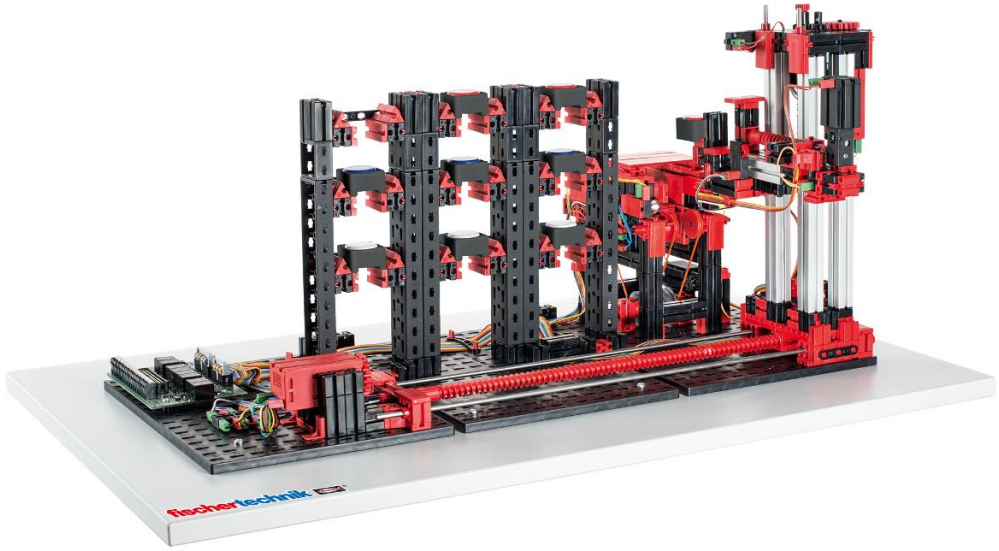
Store Blue +



Store Blue +

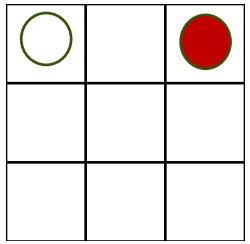


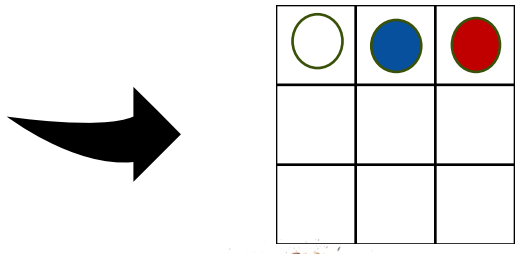
WRONG



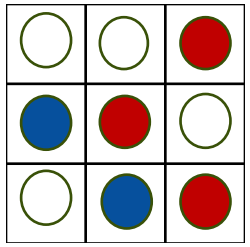
Semantics are used to identify “bad” Message x State pairs.

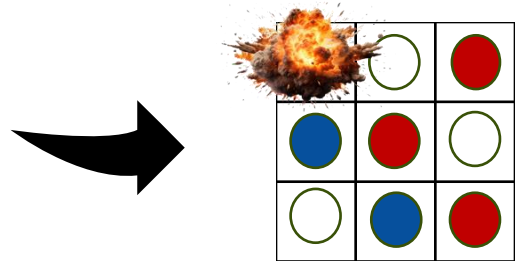
Store Blue +





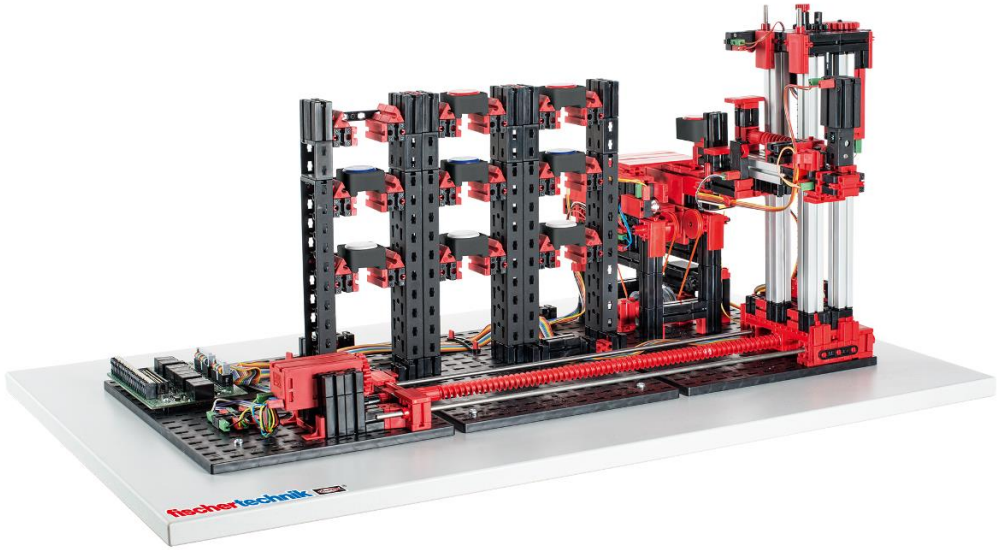
Store Blue +



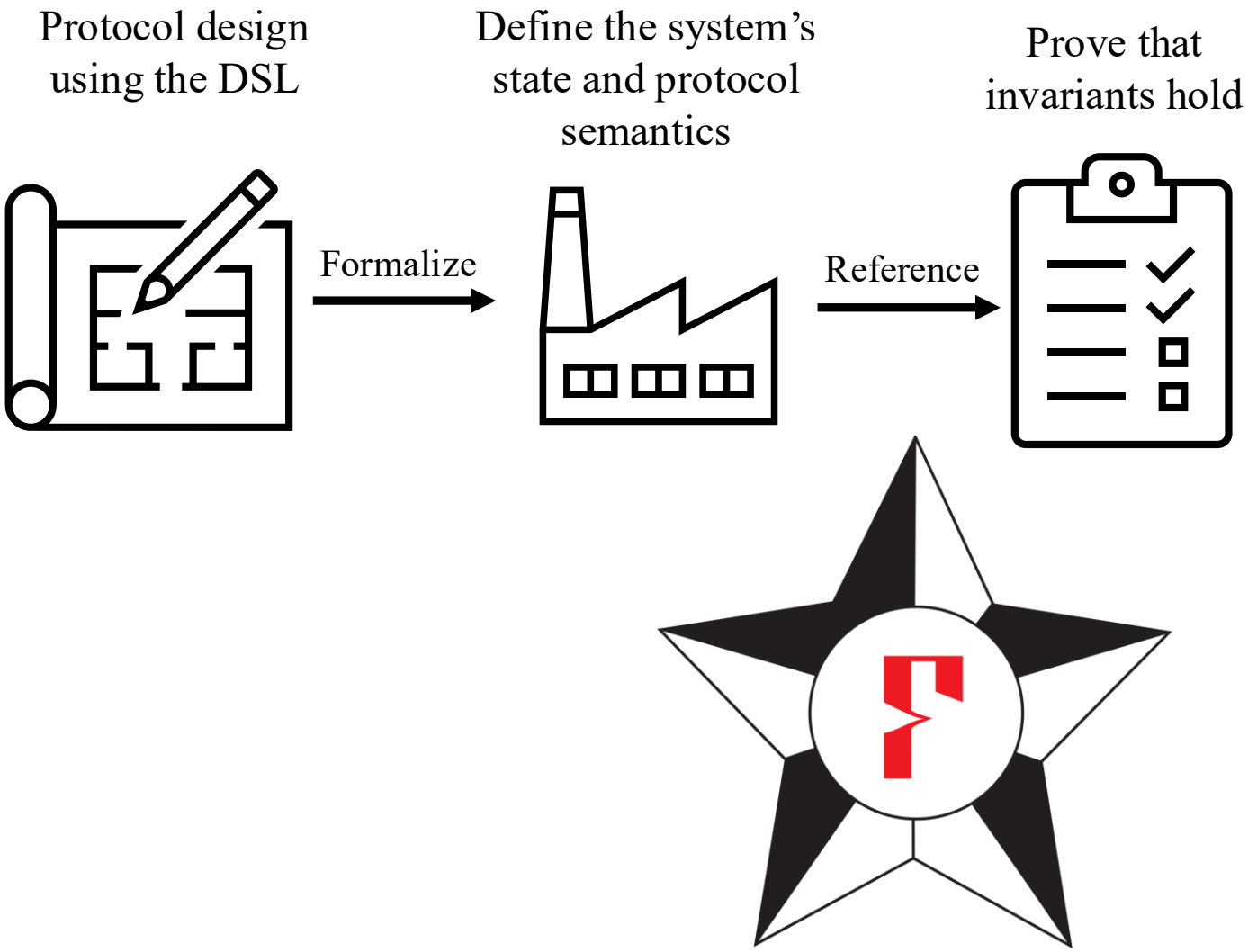


WRONG

Identify MESSAGE x STATE pairs that derive WRONG

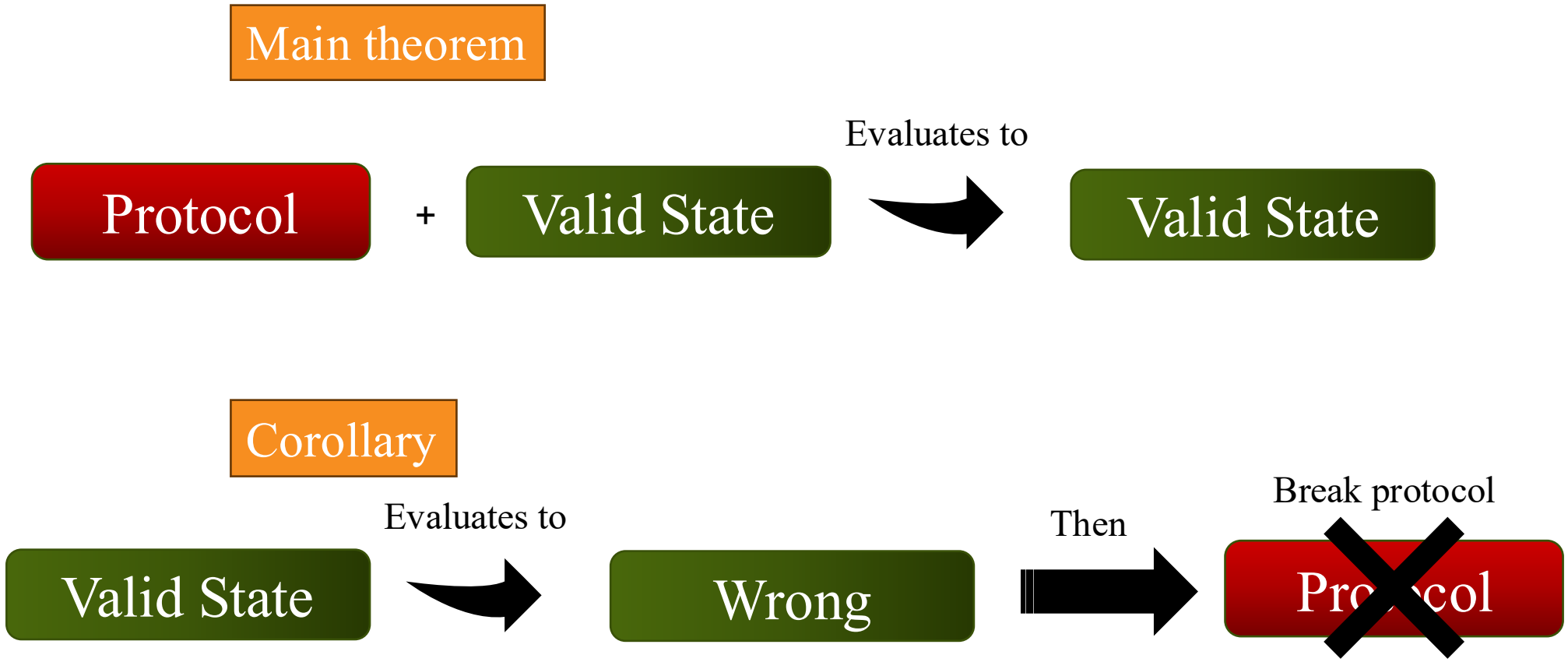


Inside the F* interactive theorem prover, we can prove that the protocol preserves invariants.

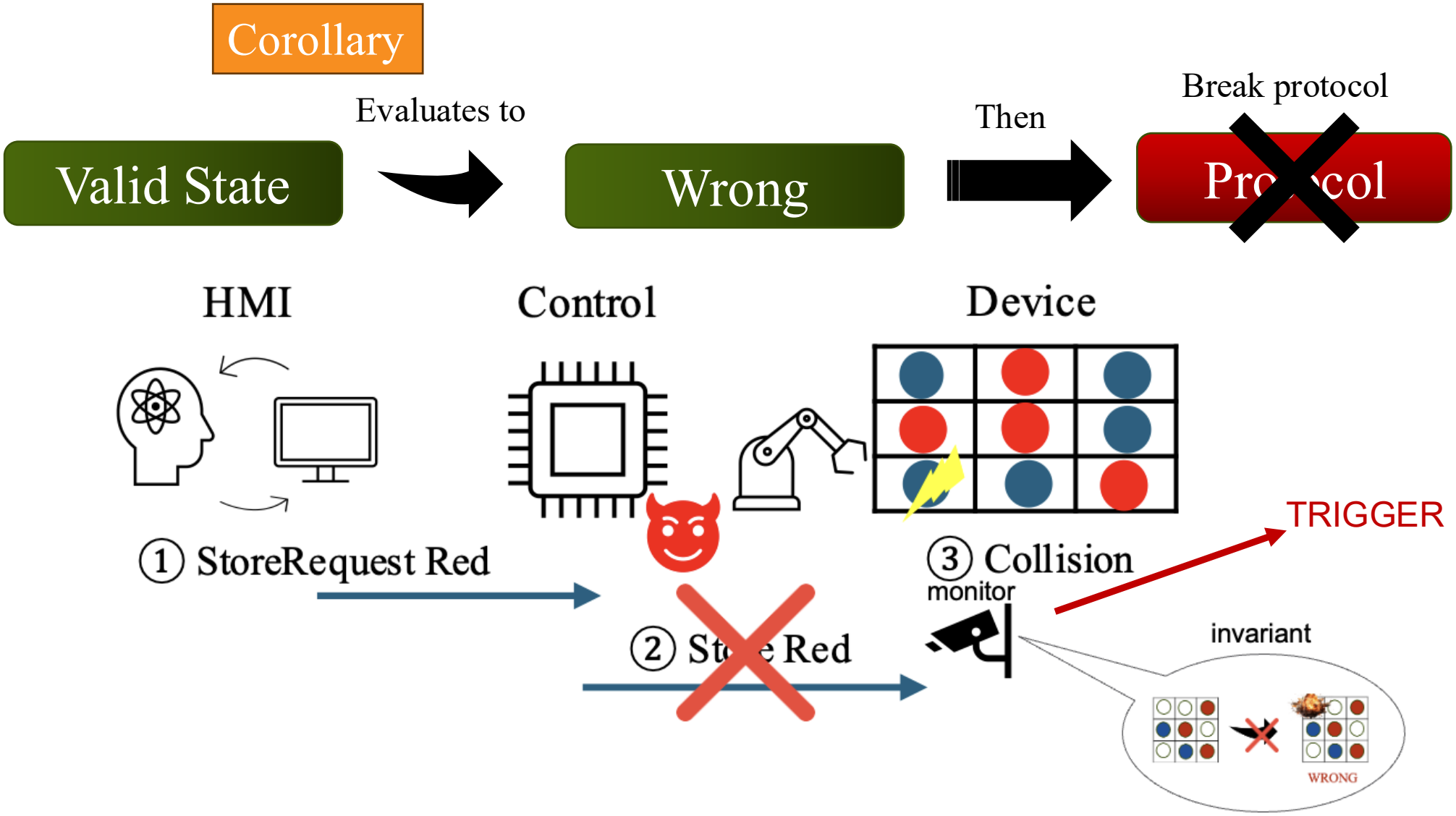


Given a valid state and and a message that satisfies our protocol, the system cannot enter a Wrong state.

Given a valid state and and a message that satisfies our protocol, the system cannot enter a Wrong state.

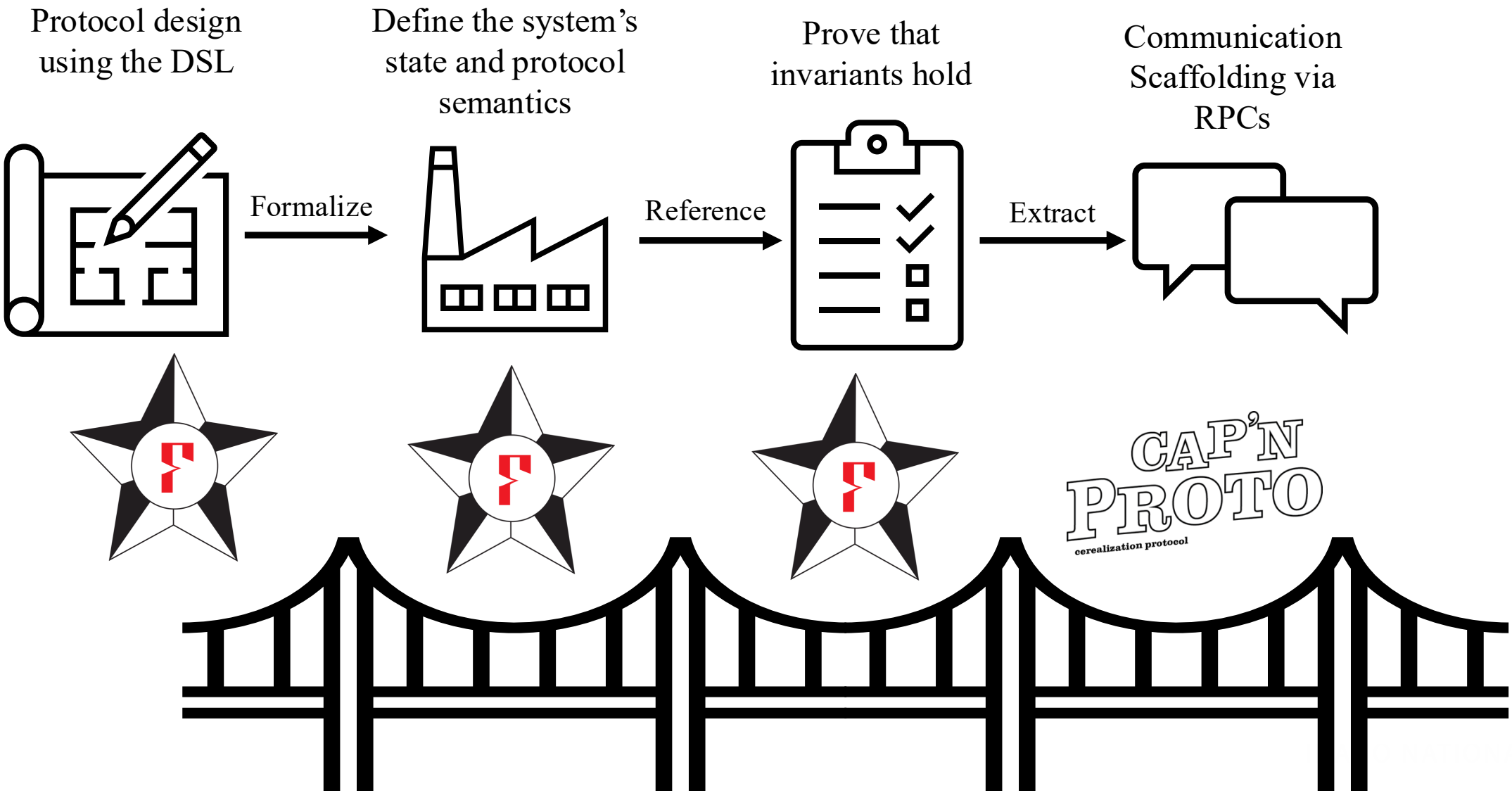


An attacker MUST break protocol to take the system from a valid state to a WRONG state.

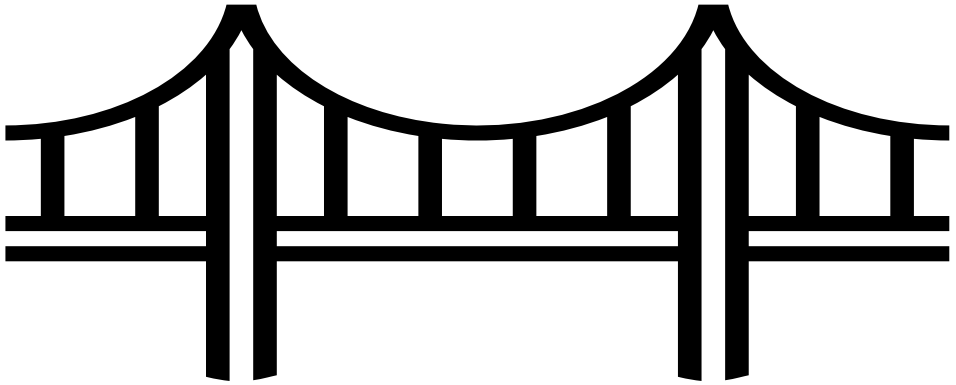


Idaho National Laboratory

Our methodology bridges the gap between formal, provably correct, protocol designs and low-level implementations.

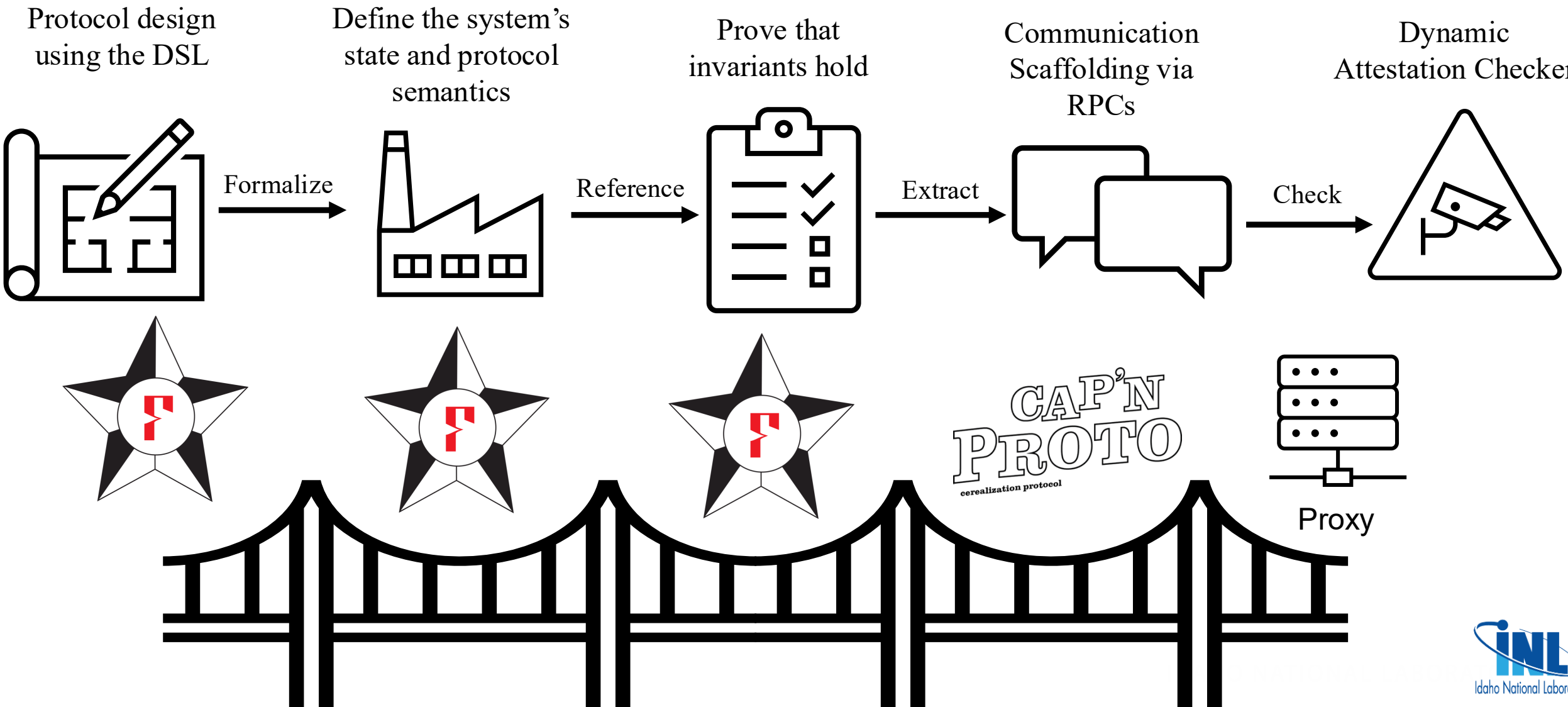


RPC frameworks provide the low-level communication scaffolding.

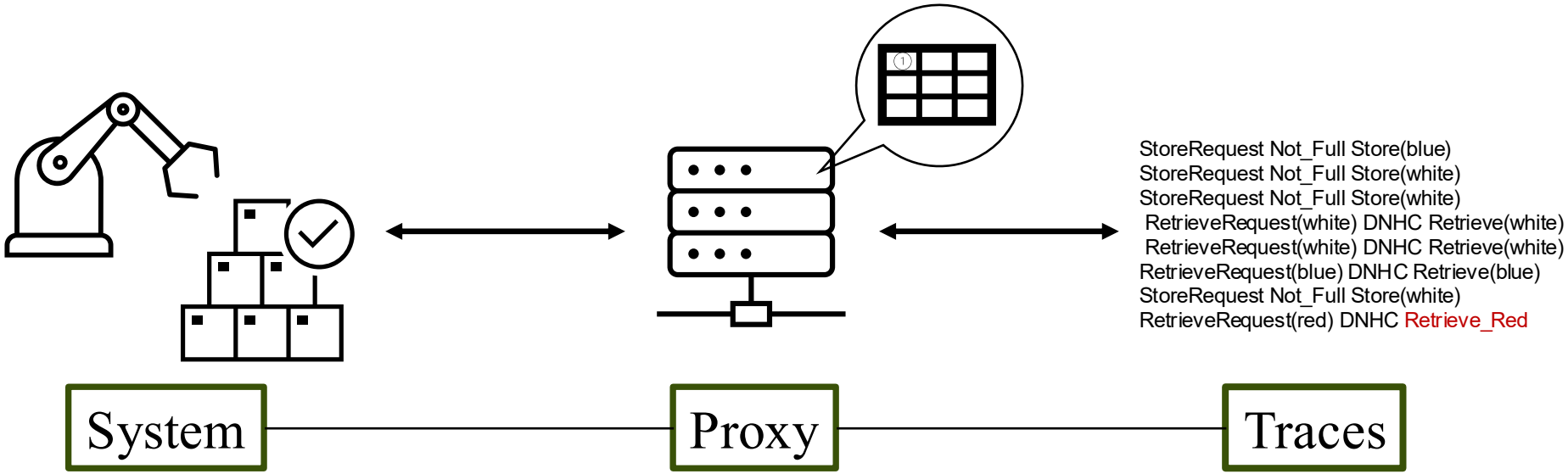


Framework	Overhead	C?	C++?	Rust?	Custom Networking?	Code Scanning	Fuzzing
Cap'n Proto	Low	No	Yes	Yes	No	No	Yes
COAP	High	Yes	Yes	Yes	No	No	No
eRPC	Low	Yes	No	No	Yes	No	No
gRPC	Medium	No	Yes	Yes	No	No	Yes

The dynamic attestation checker verifies that ICS communication traces follow the verified protocol.



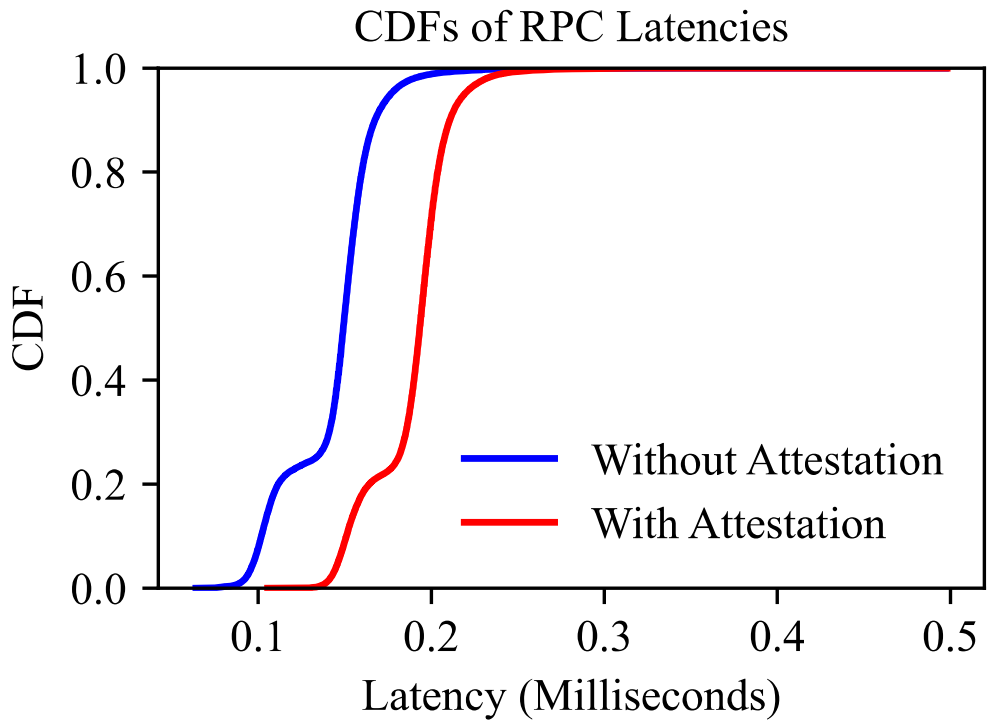
Dynamic protocol attestation ensures that the protocol specification is enforced at runtime.



We were able to thwart the effect of attackers with only a slight increase of latency.

Latency Analysis

Configuration	Avg. Latency(ms)	Messages	KB
Without Attestation	0.1452 ± 0.0007	191,250	3,060
With Attestation	0.1903 ± 0.0007	145,054	2,321



Idaho National Laboratory

For future work, we aim to embed a core language defining arbitrary protocols in F* and extend automation.

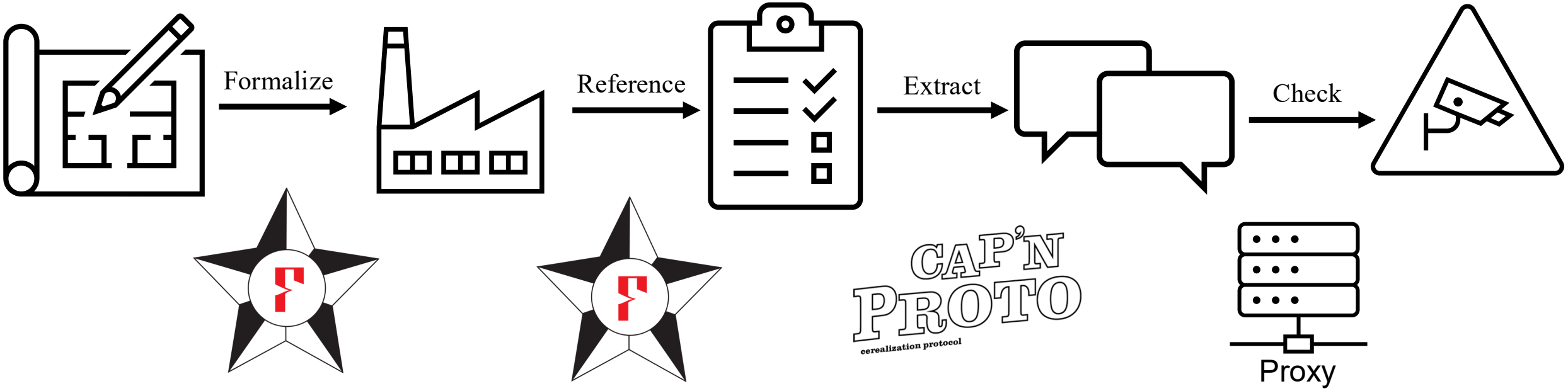
Protocol design using session types

Define the system's state and protocol semantics

Automate the main proof via metaprogramming

Communication Scaffolding via RPCs

Generate the dynamic attestation checker



Our methodology retrofits legacy ICS to mitigate real-world safety and security weaknesses with little overhead.

Arthur Amorim
Arthur.Amorim@ucf.edu

Dr. Max Taylor
maxhtaylor@proton.me
https://maxtaylor.dev