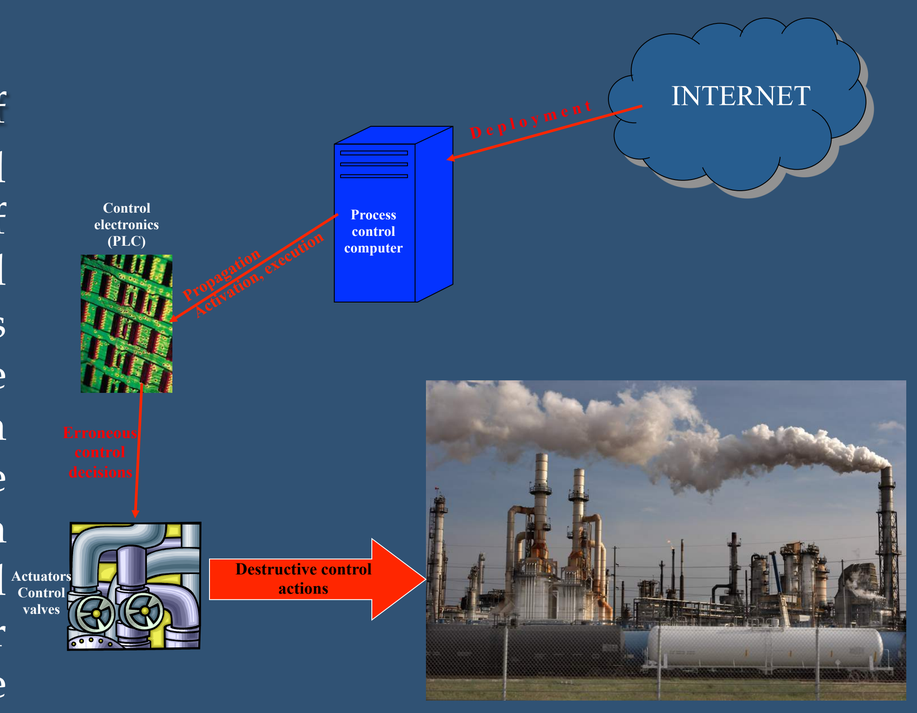
SCAN : A Framework for Security Management in Cyber Physical Systems (CPS) -- *Arash Nourian*

Securing a critical infrastructure is of paramount importance with the rapid growth of using commercial-of-the-shelf (COTS) products in industrial control **systems.** These changes have made CPSs more available target for attackers. The critical nature CPSs also makes them intriguing targets. For the first time in the history of the Internet, cyber attacks can have physical manifestations in the real world, providing easy access target for those who desire to either cause disruption to physical services or cause a national disaster.

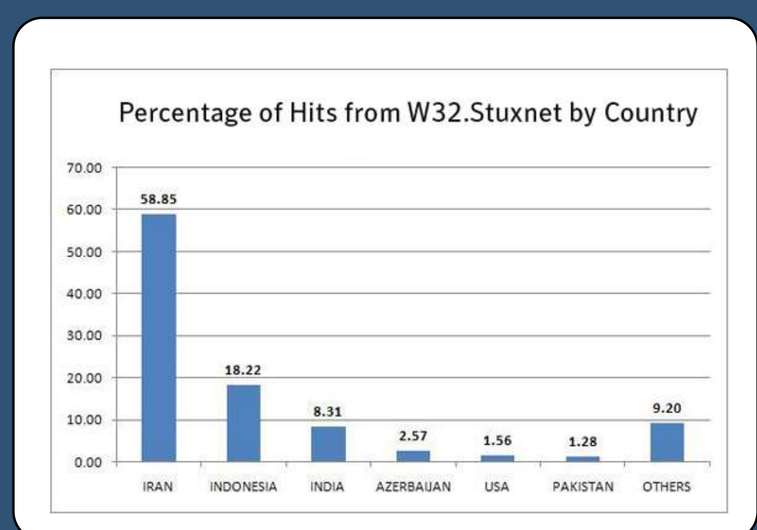


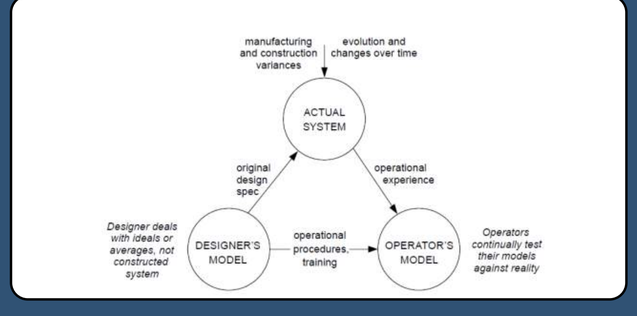
What is SCAN?

In this project, we are planning to design a framework for CPSs to improve the security of them based on control check point analysis. SCAN can be used in CPS attack modeling and threat assessment as well as diagnosis methods for stealthy attacks against a CPS.

Example Attack: Stuxnet

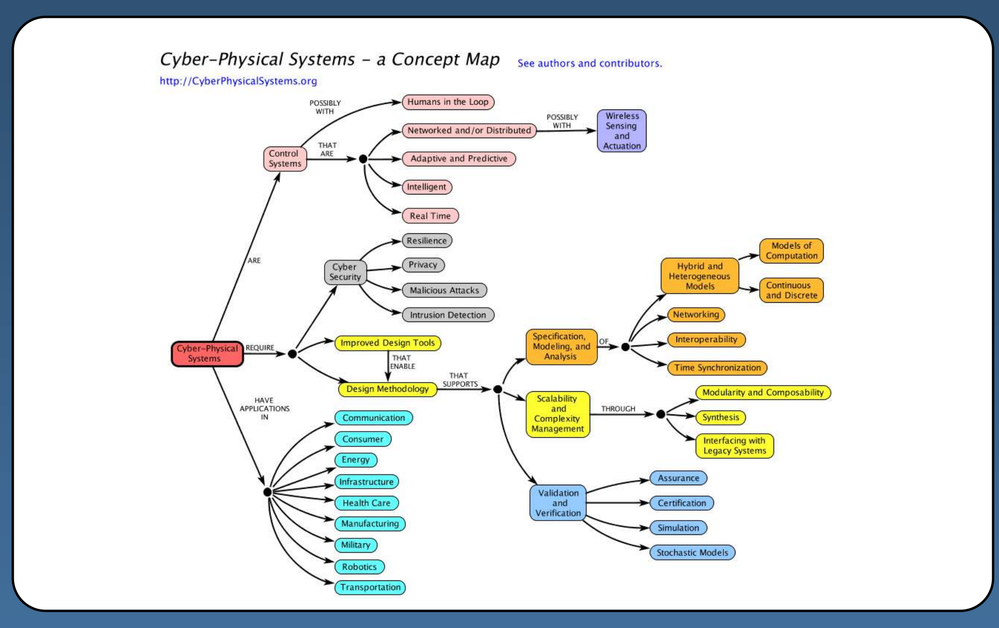
In June 2010 a sophisticated computer worm targeting Siemens WinCC industrial control system software infected Iranian nuclear power plant ICSs. It destroyed many centrifuges causing major disruptions in the Iranian nuclear program.

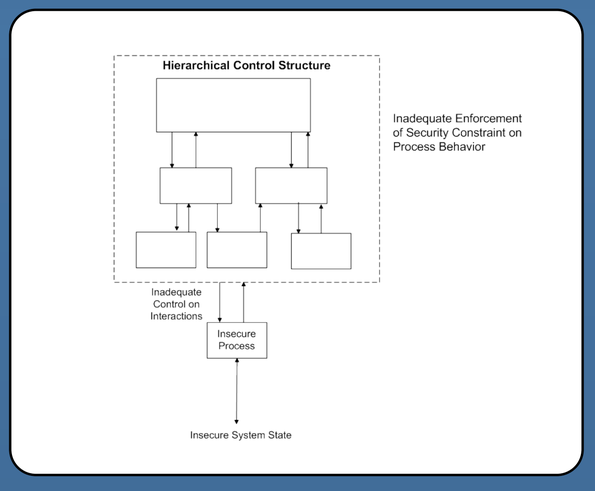




How SCAN works?

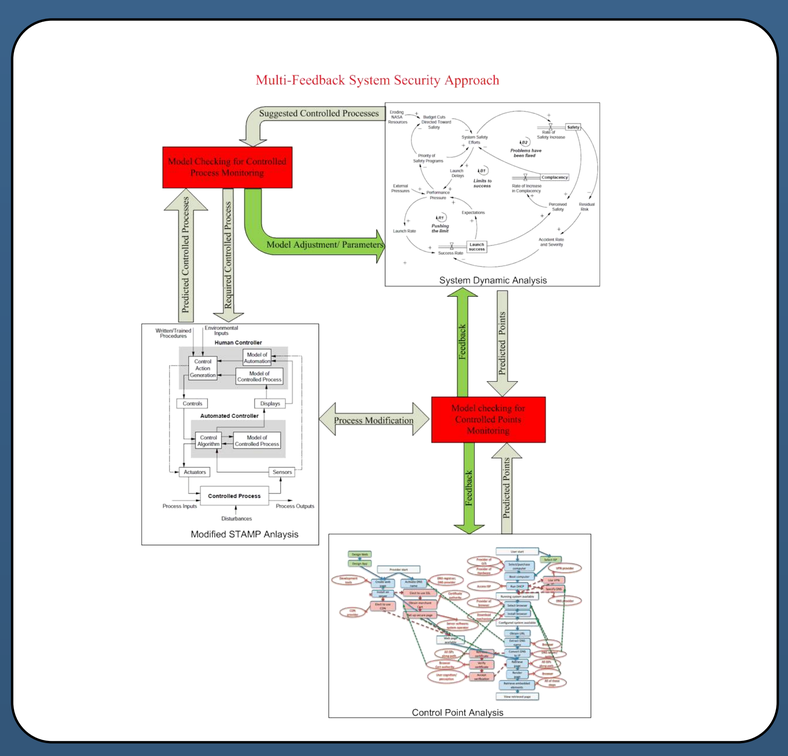
SCAN leverages the combination of functional decomposition of a CPS along with the control point analysis to identify the vulnerable points against cyber attacks. First, a CPS is decomposed to its subsystems and its component hierarchy is generated. Based on component level, two levels of security are provided. Level one is security at the component level and level two of security is done by looking at the system as one complex system by providing security measures to protect the subsystem interactions.





Benefits of SCAN

SCAN will help CPS designers to evaluate the security of their systems before construction and apply necessary changes to address the security concerns identified by SCAN analysis. It also helps operating CPSs to increase their security against cyber threats. SCAN also has a potential to benefit society by restricting cyber threats on critical infrastructures. Without such a framework in place and with the advent of cyber attacks against CPSs, society is at risk. In the near future many critical infrastructure providers need frameworks like SCAN to enhance the security and privacy of their systems.



The interaction among components is a critical factor that attackers try to exploit to gain information about the CPS. For each component, its interaction with other components is analyzed.

System Components

Component	Responsibilities
Physical end points	Receiving the system command values, performing the requested operations, and reporting the results as well as the status of the end points after completed operations
Operator	The main user of the system that issue command, create report, and react to the system output
SCADA	The intermediate component between operators and physical end points that translate the operators command for each physical component. It also receives the results back from physical end points and prepare it for the operator review.
Communication networks	Carrying information between different components within the network
Monitoring sensors	Monitoring the results of actions performed by each physical end points and report them back to the controller

After component analysis, the threats are identified. For each threat, the security constraint and security requirement are identified. The security requirements are used in ensuring the security at all levels.

System Threats

Threats(T)	Description
T1	The system reports fake/recorded operation results to the controllers
T2	The system asks for malicious operations by Stuxnet
T3	The system hide the malicious operations from operators by manipulating the process view of SCADA systems
T4	The system hide the actual results of Stuxnet operations from SCADA
T5	The system reports the required results to the controllers too late

Sample threat analysis for Stuxnet

Threat(T)	Security Constraint	Security Requirements
T1	Correct operational results need to be reported to the controllers	The system shall ensure correct result reporting based on existing standards for each physical end points
T2	The system must only perform operations requested by a legitimate operator	The system shall ensure that only legitimate operations are performed
T3	The system must recognize any tampering on critical core functions (CCF) such as process monitoring.	The system shall ensure that any CCF tampering is detected and reported to the operator
T4	They system must ensure a direct link without any intermediary between SCADA and physical end points	They shall ensure that all the communications between SCADA and physical end points are not modified by an eavesdropper
T5	The operational results must be received by SCADA in a required timeframe	The system shall have the specific turn-around time for each requested operations