The International Emergency Management Society
2015 Annual Conference, 30th September - 2nd October 2015, Rome, Italy

TOWARDS THREAT MODELING FOR CPS-BASED CRITICAL INFRASTRUCTURE PROTECTION

Jianguo Ding, Birgitta Lindström, Gunnar Mathiason, Sten F Andler

School of Informatics, University of Skövde, Sweden
Email: {jianguo.ding, birgitta.lindstrom, gunnar.mathiason, sten.f.andler}@his.se

ABSTRACT:
With the evolution of modern Critical Infrastructures (CI), more Cyber-Physical systems are integrated into the traditional CIs. This makes the CIs a multidimensional complex system, which is characterized by integrating cyber-physical systems into CI sectors (e.g., transportation, energy or food & agriculture). This integration creates complex interdependencies and dynamics among the system and its components. We suggest using a model with a multi-dimensional operational specification to allow detection of operational threats. Embedded (and distributed) information systems are critical parts of the CI where disruption can lead to serious consequences. Embedded information system protection is therefore crucial. As there are many different stakeholders of a CI, comprehensive protection must be viewed as a cross-sector activity to identify and monitor the critical elements, evaluate and determine the threat, and eliminate potential vulnerabilities in the CI. A systematic approach to threat modeling is necessary to support the CI threat and vulnerability assessment. We suggest a Threat Graph Model (TGM) to systematically model the complex CIs. Such modeling is expected to help the understanding of the nature of a threat and its impact on throughout the system. In order to handle threat cascading, the model must capture local vulnerabilities as well as how a threat might propagate to other components. The model can be used for improving the resilience of the CI by encouraging a design that enhances the system's ability to predict threats and mitigate their damages. This paper surveys and investigates the various threats and current approaches to threat modeling of CI. We suggest integrating both a vulnerability model and an attack model, and we incorporate the interdependencies within CI cross CI sectors. Finally, we present a multi-dimensional threat modeling approach for critical infrastructure protection.

KEYWORDS:
Critical infrastructure protection (CIP), threat modeling, threat cascading, threat mitigation

1. INTRODUCTION

Today's Critical Infrastructures (CI) are evolving by integrating embedded Cyber-Physical Systems (CPS) as well as other CIs. Such integration is typically based on the extension of functionality, and will introduce interdependencies where the operation of the CI may be jeopardized both by the CPS systems integrated and the emergent behavior. With this evolution, there is a need for multi-dimensional architecture modeling and analysis. CIs become interdependent with several other entities or sub-systems, with complex interdependencies. For example, food & agriculture is a CI that depends on, e.g., water and transportation. Hence, modeling a CI such as food & agriculture might also require modeling its dependencies to other CIs. Figure 1 shows an example of interdependencies between CIs.

1.1 CPS-based CIs

CPS are smart networked systems with embedded sensors, processors and actuators that are designed to sense and interact with the physical world (including the human users) in real-time, typically guaranteeing performance in safety-critical applications. CPS integrate computation, networking, and physical processes [Lee08]. In CPS, the "cyber", "physical", and "social" elements of the system are critical computing, control, sensing and networking elements, which can be deeply integrated into every component. These elements are important dimensions of a threat model and corresponding analysis. The actions of such system as well as its components must be safe and interoperable.

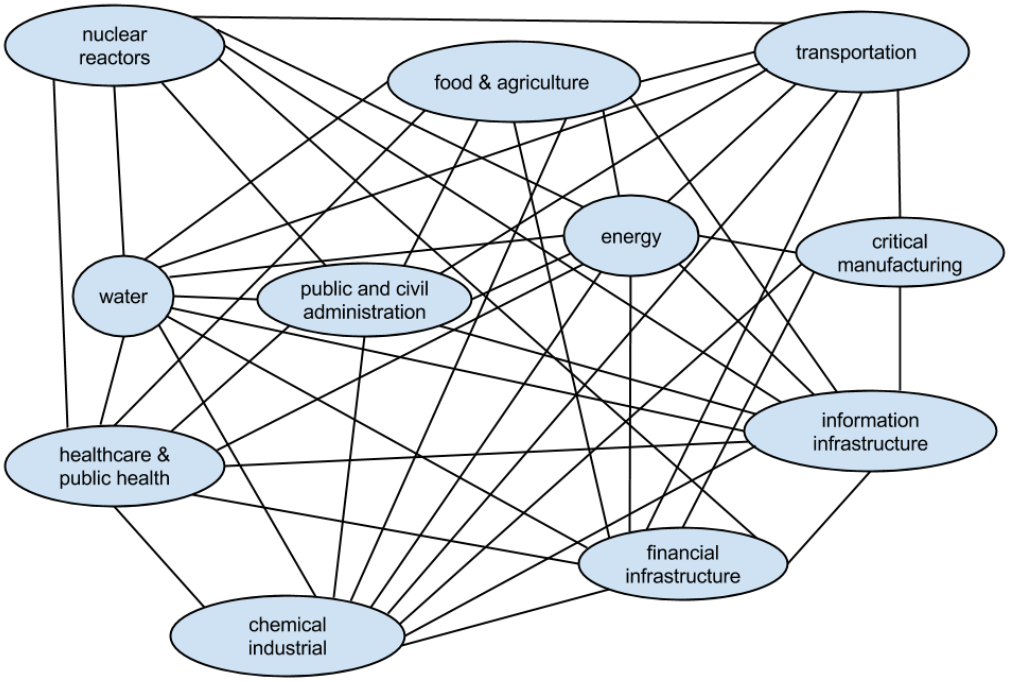


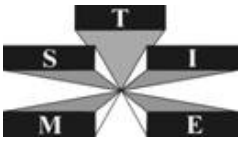
Figure 1 Example of the interdependencies between critical infrastructures

CPS has an intimate coupling between the cyber, physical, and social world manifests, from the nano-world to large-scale wide-area systems of systems (SoS), from the physical environment to social society. As the Internet transformed the way humans interact and access information, CPS have the potential to transform how humans interact with the physical, cyber, and social world around us [RLS+10].

A failing CPS can potentially cause severe damage to humans, assets or CIs. The level of reliability, safety, security, dependability and usability must therefore be high. Moreover, the CPS must be resilient to potential attacks. From the perspective of a defender, increasing complexity of systems requires dramatically more effort to analyze and defend, because of the state–space explosion, caused by the combinations of events [MKB+11].

Extending CIs with CPS also extended the scale of CI architecture and the applications. One example of this is the airports, which have employed large numbers of CCTV (Closed-circuit television) cameras and security personnel for perimeter surveillance. The flat, open nature of airports allows radar-based sensor for primary detection of breaches of the airport perimeter, which has greatly improved the security protection of airports. V2X (vehicle to everything) networks are other CPS-based CI examples in modern transportation infrastructure. V2X includes both short-range wireless-based V2V (vehicle to vehicle) and V2I (vehicle to infrastructure) systems. The primary objective behind V2V and V2I is to prevent accidents and save lives. Transponders on the vehicle and around the highway can give warning of unseen congestion or danger ahead, provide braking assistance and give other warnings. The integration of the V2X into the traditional transportation networks as well as into modern information network systems makes the transportation infrastructure a multi-dimensional complex system. Other CPS applications are found in modern online financial system, power grid operation, body networks for healthcare, on-site monitoring of chemical systems, quality monitoring and control of the water system.

A CPS could be a monitoring/protection systems of a CI, but may also suffer from security attacks. This can be seen as a cybersecurity problem only, but this integration also somehow changes the operational model of the CI, which directly affects CI management. Regardless of whether the CPS is part of a CI or part of the perimeter protection of the CI, emerging threats to CPS-based CIs need to be examined and mitigated for proper CI operation. As there are many different stakeholders of a CI, comprehensive protection must be viewed as a cross-sector activity to identify and monitor critical elements, identify and evaluate threats, and eliminate potential vulnerabilities in the CI. Threat modeling looks at the system from an adversary's perspective to help designers anticipate attack goals and determine what the system is designed to protect, and from whom [MLY05].



A systematic approach to threat modeling is necessary to support assessment of threats and vulnerabilities of the CI. It helps understanding the nature of threats and their impact on the global system. Further, to handle threat cascading, the model must capture local vulnerabilities as well as how threats propagate to other components. Such model improves the resilience of the CI by encouraging a design that enhances the system's ability to predict threats and to delimit potential damage. This paper surveys the various threats and current threat modeling approaches to CI. We integrate the threat, vulnerability, and attack models, and also incorporate the interdependencies within CI and across CI sectors. Finally, we suggest a novel multi-dimensional approach for threat modeling.

1.2. Related Work on Threat Modeling

There are several approaches in literature on how to model threats and attacks.

Attack trees [Sch99] [TLG07] are conceptual multi-leveled diagrams showing how an asset, or target, might be attacked. Attack trees are very useful for determining threats and how to deal with them. Attack tree model works well as a non-quantitative model for attacks. But in CIs, a quantitative model is necessary to model the threats.

Defense trees [BDP06] extend attack trees. A defense tree is a qualitative instrument used for modeling attack scenarios, with countermeasures and economic quantitative indexes. The model can support to evaluate effectiveness and profitability of countermeasures as well as their deterrent effect on attackers. But it is not clear how to compute the value of the risk mitigated attribute in the model.

Fault tree [Sin90] is a top down, deductive failure analysis in which an undesired state of a system is analyzed using Boolean logic to combine a series of lower-level events. In safety engineering, it is used to reduce risk or to determine (or get a feeling for) event rates of a safety accident or a particular system level (functional) failure. But in realistic systems, the system/event state might not always be Boolean.

Attack graph [AWK02] is a handy tool which helps mapping isolated intrusion alerts to known multistage attack paths and thereby enabling prediction of future attack strategies of the attacker. An attack graph can be used to identify the attack chains and rank them. The quantitative expression in the model is limited.

DAD (defender-attacker-defender) model [ABC+11] is a three-stage, sequential game-based paradigm for planning budget-limited defenses and/or new construction that will maximize the resilience of a critical infrastructure system subject to attack by an intelligent adversary. The model is difficult to use for threat modeling in heterogeneous integrated CIs, since the investment and cost for attack and defense in different systems cannot be measured in the same magnitude. The system evolution brings challenges for the investment/cost measurement.

Although lots of works have been done on threat modeling, there is a lack of an integrated, systematic approach towards threat modeling for complex critical infrastructure [BM11]. Moreover, the consequence of an attack to a CI might be critical so this should be examined carefully and therefore, included in potential threat modeling. Based on the emerging CIP (critical infrastructure protection) requirements in CPS-based CIs, this paper proposes a threat modeling approach to systematically model the multi-dimensional threats to global CI systems. The model can support further analysis of attacks, threat cascading, threat mitigation and threat prediction analysis on CIs.

2 SECURITY CHALLENGES TO CPS-BASED CRITICAL INFRASTRUCTURES

CPS-based CIs have a high level of complexity, emerging system properties and also several new challenges in system security and protection. This section surveys the area with respect to complexity and the challenges.

2.1. Complexity of CPS-Based CIs [Lee08] [SGL+09].

Complexity has an important relationship to system resilience and robustness. Resilience mechanisms such as self-organization and autonomic behavior increase complexity, which may result in network vulnerability [Str01]. The complexity of modern CIs links to complex structure, running environments, network evolution, dynamic

behavior, large-scale usage, unbalance properties, probabilistic, entangled interdependencies, real-time performance, federated operation, management and control and the high requirement of security protection.

(1) *Heterogeneous integration.* One source to the complexity of CPS-based CIs is the heterogeneous integration. This integration concerns different levels and multi-dimensions. Integration of complex, heterogeneous large-scale systems creates universal definitions for representing ultra-large heterogeneous systems, builds an inter-connected and interoperable shared development infrastructure and develops abstraction infrastructure to bridge digital and physical system components. There is a macro integration of the social-cyber-physical worlds, which extends to informatization of physical world, network scale and network applications, and a micro integration of heterogeneous networked system, platform, protocol, interaction of devices, etc. Finally, the interaction between human, physical systems and cyber systems enables natural, more seamless human-CPS interactions. The computational and physical processes in such systems are tightly interconnected and coordinated to work together effectively, often with humans in the loop. The heterogeneous network integration demonstrates the integration of different structures, different functions, distinct performance, and even different network protocols. Integrated networks are not only the accumulation of networks, but also updated properties and emerging functions with the evolution.

(2) *Multi-dimensional dependencies*. A CPS-based CI is multi-layered. It is networked at multiple layers and at an extreme scale. The CPS is built with a layered stack structure, such as layered protocols and finally, the application models are layered. Moreover, there are complex multi-dependencies between components and elements in CIs such as: (i) cyber, physical and social dependencies, (ii) interdependencies between functional components within CI, and (iii) interdependencies between CIs.

(3) *Dynamics*. A CPS-based CI is dynamic in several aspects:

- Physical system in question has inherent mobility, particularly in the edge physical system of CPS.
- Changes to individual CPS components (hardware, software, protocol, etc.) and the applications/services.
- System degradation.
- Change of CPS users/operators and their behavior.
- Mobile and wireless communications are involved (unpredictable bandwidth and connectivity).
- Changes on social/system environment.
- Local and global changes are interdependent. That means any local changes may result in the variation of global network performance, any global modification can result in the changes in local network performance.
- Theoretically, the network function and structure have strong interdependence [New03]. The evolving structure of networks will bring the changes in network function. It's possible that network function modification can result in the redesign/reconfiguration on network structure.

(4) *Evolution*. Evolution is a time-related process. Evolving CIs can be considered as temporal systems, which can be modeled to elucidate the relation to the behaviors of dynamic systems. The fundamental properties in temporal networks could be quite different from those for static networks.

(5) *Probabilistic*. There are uncertainty (probabilistic) properties of the system, which adds to the complexity. In an evolving network, the system dynamics and the intrinsic complexity gives the network probabilistic properties. The incomplete and uncertain information need to be integrated into the research models, so that the system models can be more reasonable and realistic [Din08].

(6) *Emerging computing models*. As CPS become more dependent on computational processes, it becomes increasingly important to adapt and embrace the new computing models in a unified way: nomadic computing, autonomic computing, pervasive computing, cognitive computing, opportunistic computing, scalable computing, physical computing, situation computing, cloud computing and fog (edge) computing.

2.2. Security Requirements for CPS-based CIP

The many emerging security challenges lead to a number of requirements for CPS-based CIP. We discuss these CIP requirements in detail below based on [Din15] [Sin12] [Ven09].

CPS security needs to be integrated with CIP to guarantee resilience of the SoS. Dependence on widespread computing and networking naturally increases security concerns, as the availability, integrity and privacy of the data carried may be compromised. The presence of the physical system widens the range of possible attacks and constrains the set of feasible countermeasures. The interaction between the cyber and the physical dimensions offers many opportunities for detection and response when the physical system is equipped with computational and communications capabilities. Each function of CPS (sensing, communication, storage, actuation etc.) has its own set of security requirements, which are function dependent. The CPS have to deal with cross-organizational security information sharing, which is necessary but hard to manage in current scenarios. As federated systems, CPS security needs to be considered architecturally, not as a separated security architecture, but as a secure architecture for the deployment of such applications. The structure of data placement, system control, and monitoring of the system as a whole must consider the security implications.

The combination of cyber and physical vulnerabilities may lead to attack models that are fundamentally new, hard to analyze, and carry a substantial risk, difficult to maintain physical integrity of critical systems. The deep interaction with a distributed physical environment increases the risks (e.g., the potential physical damage due to a security breach) and offers new opportunities (e.g., the use of physical data to authenticate nodes or detect intruders). New threats, particularly on the main components of CPS and the interfaces between CPS and other systems are serious. The Stuxnet attack is a typical example attack on SCADA (supervisory control and data acquisition) systems [Kar11]. Attacks on networked, cyber-physical systems and critical infrastructure such as the Smart Grid, biomedical systems, and transportation networks will have grave consequences for our safety and wellbeing in addition a threat to our economy. It is critical that CPS systems are resilient to cyber attacks.

The environment, structure, sensing process, data analysis, function modification, real-time feedback control and the varying security requirements put CPS into a dynamically evolving situation. The evolution parallels with networked and integrated cyber-physical systems, particularly as systems become interconnected with legacy systems and across industry boundaries. Any change within the CPS, whatever the physical changes or system behavior changes, can result in unpredictable vulnerabilities. The static and fixed protection strategies mostly are not valid. Moreover, the running dynamic data flow, information flow and control flow should be under protection. Thus the security task includes the need to dynamically reassign monitoring, correlation, and intrusion detection management responsibilities to nodes as the topology evolves; to maintain availability and provide continuous coverage; and to address various risks that compromised nodes.

CPS security solutions depend upon the physical environment to enable security. Attacks on the physical environment can potentially be used to prevent the security solutions from functioning correctly. Attackers can artificially change the environment around the cyber elements of a CPS, causing unexpected results with security threats, including denial of service. Physical environment can be tampered with in CPS such as power grids and UAV (Unmanned Aerial Vehicles). Attackers can potentially control the sensors in a data center to cause overload of the air conditioner. Security for sensors and actuators in the field needs to be considered as well. Technique for detecting tampering, and validating the inputs provided by these sensors is important to prevent these control inputs to the CPS from being recruited by adversaries (e.g. botnets).

Many tiny smart devices have limited computing capability and limited resources. If such devices are deployed unprotected in a physical environment, they are very vulnerable for technical attacks, and may even suffer physical damage. Therefore, the physical environment itself should be safe and secured, some protection strategies and mechanism for authenticating the sensed value are required [BVM+12].
It is difficult to use software patching and frequent updates for adaptively and dynamically improve security for control systems. For example, upgrading a system may require months of advance in planning of how to take the system offline. It is, therefore, economically difficult to justify suspending the operation of an industrial computer on a regular basis to install new security patches. Some security patches may even violate the certification of control systems [CAS+09].

Control systems in CPS have real-time requirements. Control systems are autonomous decision making agents who need to take decisions in real time. Real-time availability provides a stricter operational environment than most traditional IT systems. CPS with large industrial control systems can consist of a large share of legacy systems or software. Most of the efforts done for legacy systems should be considered as short-term solutions. For properly securing critical control systems, the underlying technology must satisfy some minimum performance requirements to allow the implementation of well tested security mechanisms and standards.

The deployment of CPS is not limited to specialized systems managed by tech-savvy people. Many of the applications of CPS are systems of every-day use operated by non-technical people, e.g., medical monitoring, smart infrastructures etc. Therefore, security solutions for CPS should have a high degree of usability (e.g., plug-n-play nature and security transparency) a characteristic that today's cyber-only security solutions do not consider [BVM+12] .

Resilience is defined as the ability to prepare for and adapt to changing conditions, and withstand and recover rapidly from disruptions, including deliberate attacks, accidents, or naturally-occurring threats or incidents. The terms security and resilience are often used together. Both share common roots and requirements: the need to assess threats and vulnerabilities; the need to develop plans and procedures; and the need to have access to accurate and timely information. As an example, energy systems are often safety-critical, for instance a stopped industry operation may destroy expensive equipment. Even lives may depend on continued service. Hence, resilience becomes a key property; the system needs to continue operating under attacks, perhaps at a reduced performance, while still guaranteeing the basic safety properties through graceful degradation. Physical and analytical redundancies should be combined with security principles (e.g., diversity of and separation of duty) to adapt or reschedule its operation during attacks [CAS+09].

3. THREATS TO CPS-BASED CIP

Protecting and ensuring the continuity of the critical infrastructure and its key resources (CIKR) is essential to CIP and national security, public health and safety, economic vitality, and way of life. CIKR includes CI systems and assets (physical or virtual). An attack incapacitating or destroying such system or assets would have a debilitating impact on CIs. Security protection is a critical aspect of CPS-based CIs on many levels, including protection of national infrastructure, privacy of individuals, system integrity, and intellectual property. Attacks on CPS are becoming increasingly sophisticated, targeted and coordinated. CPS systems extend the attack surface of CIs. Figure 2 shows that the threats on a CI are directed, not only to the critical infrastructure itself but also to its physical and social environments. An ideal CI security protection should therefore cover these.

An attack on a CI system targets people, property assets or information. Targeted people may include employees and customers along with other invited persons such as contractors or guests. Property assets consist of both tangible and intangible items that can be assigned a value. Intangible assets include reputation and proprietary information. Information may include databases, software code, critical company records, and many other intangible items.

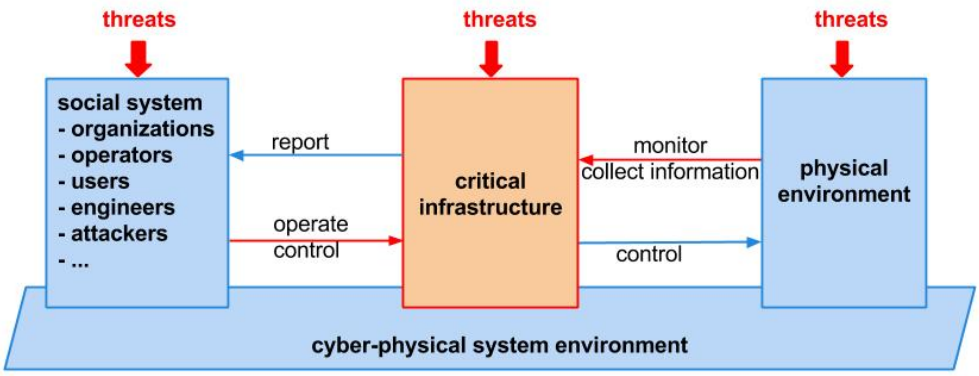


Figure 2 Extension of threats on CPS based CIs

Attacks on the CI environment can be divided into cyber, physical and social attacks (see Figure 2). Examples of cyber attacks are protocol attack, routing attack, intrusion attack, malware, DDoS (Distributed Denial of Service) attack. A physical attack means physical damage or stolen items. A social attack can be an insider attack, a social engineering attack or an operation and management attack.

Threats can be classified into internal threats, external threats and failure propagation. An internal threat comes from a vulnerability of the CI, the internal factors of the CI itself, which origins from the incomplete design, lack of local resources, or lack of well-disciplined OMC (operation, management, control). An external threat is an attack that can be deliberate or undeliberate. Deliberate attacks are human-caused, e.g., by terrorism, cyber attacks, criminal activity, industrial espionage, insider attack, information warfare, cyber war etc. while undeliberate attacks can be human-caused (e.g., blunders, errors and omissions), accidental or technical (e.g., failure of CI, hazardous material accidents) or natural threats such as natural hazards and disasters. Failure propagation is caused by neighboring components.

With the evolution of CIs, there are a number of requirements that CIP has to fulfill [May13]: (i) business continuity plans should be developed and implemented, (ii) an all-hazards approach to protection-related activities should be promoted, (iii) dependencies and interdependencies that create cascading impacts throughout infrastructure assets, sectors and systems should be identified and analyzed, (iv) engagement in protection activities by diverse stakeholders (various levels and sectors of government, private sector and private citizens) should be expanded by defining roles and responsibilities as well as unique contributions, (v) information sharing should be enhanced across the diverse stakeholder communities, and (vi) cyber analysis capabilities and integrating cyber and physical infrastructure protection capabilities should be increased.

Effective threat modeling requires security expertise as well as intimate knowledge of the application and implementation.

4. PROPOSED MODELING APPROACH

Based on our survey and identified needs, we propose to combine modeling vulnerabilities and attacks in threat models. The models are multi-dimensional, integrating the CPS to its cyber, physical and social environments. Figure 3 gives an example of this from the railway domain. Figure 3 shows a component (control system) in a CPS and its dependencies to the cyber, physical and social environment. The environment is composed by a set of qualifying conditions that must be satisfied to guarantee the component's functional operation.

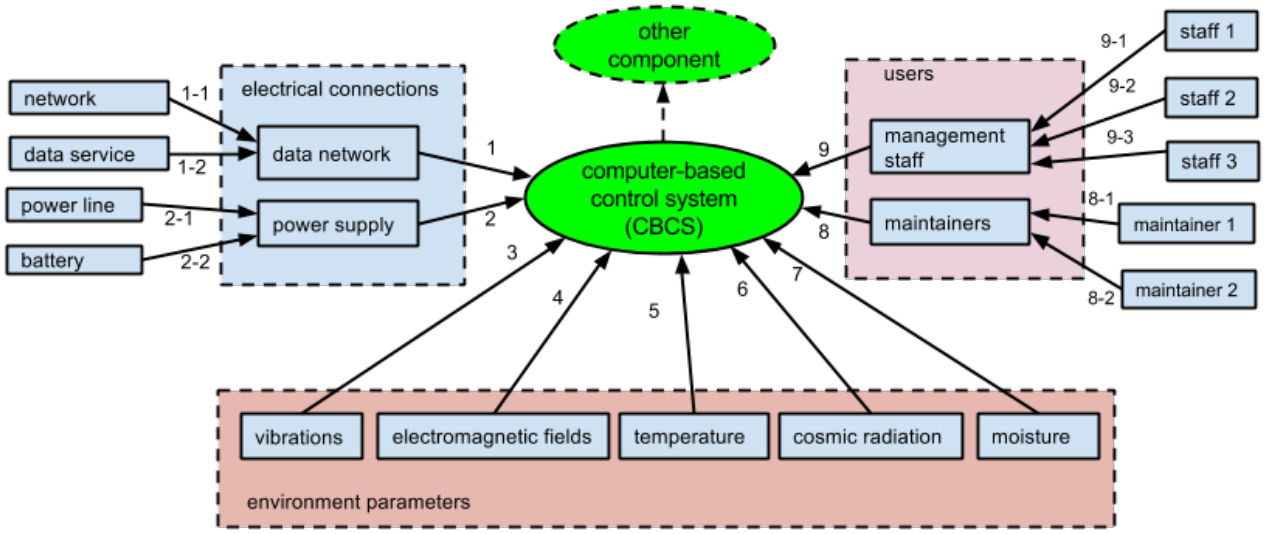


Figure 3 example of computer-based control system in railway infrastructure

We consider a CI functional component such as the CBCS in Figure 3 as a both a target (depending on condition/input) and a source (to output) serving its parent functional component. This model approach can easily explain the complex structure and the interdependencies in CIs in a semantic and quantitative way.

We design a **Threat Graph Model** (TGM) to conduct the threat modeling for CIs. For now, we consider one-directional dependencies. The TGM is a DAG (directed acyclic graph). We define *TM(t) = (V(t), L(t), Q(t))* as a time-related function. Here *V* is a set of variables (nodes of the DAG), *L* is the set of dependency links among the variables (input and output of the node), *Q* denotes the service quality of the component for both input and output. We define $Q(t)=P(v^{\pi}, t) / P(v^{\lambda}, t)$, $v \in V$, $v^{\pi} \in L$, v^{π} is the parent nodes (output) of v, $v^{\lambda} \in L$, v^{λ} is the children nodes (input) of v . $P(v^{\pi}, t)$ means the ratio of qualified output of v, $P(v^{\lambda}, t)$ *means to* ratio of qualified input of v. A TGM can model the structure of the CIs by the dependencies (links), key factors of the CI (nodes), directed link (directed stream: information stream/control stream), the functional component which takes use of an input with the qualified OMC to produce an output to another component. The threats are modeled indirectly by their effect on the system performance. Figure 4 shows the TGM for the example used in Figure 3. A single arc between two edges represents an AND relation and a double arc represents an OR relation.

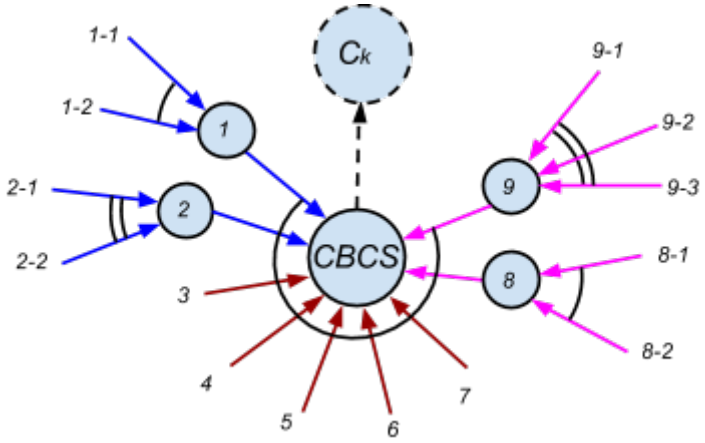


Figure 4 Threat Model for the computer-based control system in Figure 3

4.1 Modeling key factors (parameters) and the interdependencies

Generally, in the graph model, one node has several input (from children nodes), and several output (to parent nodes).

- *node C*: components (could be physical components, functional components, logical components) of CI, including local resource, OMC (operation, management, control).
  - A component is dependent on the condition of different resources to execute its function. The correct intervals or thresholds for the conditions define the operational envelope.
    - Available resources and the qualified OMC can keep the component function in a correct state. Or else the function of the component will be degraded or absent.
    - The dysfunctional situation on a component is defined as a consequence of certain threats.
  - All the modeled conditions could be measured quantitatively or qualitatively. For example the required power supply can be denoted as *20*kw. The management staff can be denoted as qualified staff. The measurement can be set as a benchmark for further application.
- *link L*: **direction** of the link indicates the dependency between component, **weight** of the link indicates the quantitative condition (both class and the quantity). The input source node could be (1) a physical resource, such as power, water etc. (2) a service resource, such as the human staff, management police, etc, (3) an environment condition, such as temperature, moisture, etc. (4) other logic resource, which is necessary for a CI component to finished the transaction.
- *time t*: related to *context/situation.*
- *probabilistic factor:*
  - *P*: extent of dependencies (quality of input/output transferring among the nodes)
  - *Q*: health status of component, can be expressed from the quality of OMC (operation, management, control) in the questioned components. This parameter can indicate the extent of the internal vulnerability of the component.

4.2 Modeling the threats

Threat shows the comprehensive risks of a system.

(1) *Threat from inputs.* A threat may come from a child node with an abnormal status. Suppose a normal transaction in a component *C* needs *m* AND resources, *n* OR resources. Each resource in *C* should have the input benchmark (minimization) $\underline{R_i}$, $i \in k$, *k* is the total number of inputs (required resources).

- For all AND inputs,
  - if $\forall i$, *input* $i \geq \underline{R_i}$ $(i \in m)$, the component runs in normal status.
  - if $\exists i$, *input* $i < \underline{R_i}$ $(i \in m)$, the component runs in an abnormal status. This means some input condition for the component's correct function is not fulfilled, for example a resource that is reduced or unavailable. This implies a dysfunctional from its children.
- For all OR inputs,
  - if $\exists j$, *input* $j \geq \underline{R_j}$ $(j \in n)$, the component runs in normal status.
  - if $\forall j$, *input* $j < \underline{R_j}$ $(j \in n)$, the component runs in an abnormal status. This means all input condition for the component's correct function is not fulfilled. This implies a dysfunctional from its children.

(2) *Threat from internal vulnerabilities*. Vulnerability refers to the inability to withstand the effects of a hostile environment. Vulnerability demonstrates the internal health of a system, mostly from design and operation. If the set of inputs satisfy the requirement of the component, but the output is below the threshold for its parent. This means the component is suffering a threat from internal vulnerability, such as lack of local resources or lack of qualified OMC for the component. Such vulnerability can be indicated in the model by the service quality (health status) *Q* of the component. *Q* = (the ratio of qualified output)/(the ratio of qualified input).

(3) *Threat from external attacks*. If part or all inputs to a component *i* is below R_i, this implies that the component suffers a serious external threat (from a deliberate or indeliberate attack), which damages the dependencies between the questioned component and its children nodes. If an external attack succeeds, the targeted component is considered to be isolated from the system.

All threats, independent on what caused them, might propagate along the dependency links to other components. If the propagation covers large part of the system or results in serious linkage failures, the phenomenon is called cascading. Cascading might result in serious damage to CIs. Analysis of cascading end its effects in order to avoid and mitigate them is highly required for modern CIs. Our proposed model will support such analysis.

4.3 Pruning operation

In TGM, two pruning operations are possible, input based pruning and output based pruning. Input based pruning is a descendant traversal for the considered component. The statistic of the input shows the possibility of the system suffering external threats. Output based pruning is an ancestor traversal for the considered component. The statistic of the output shows the extent of the effects under an attack.

5 ANALYSIS AND DISCUSSION

5.1 Modeling Analysis

CPS components are on the edge of CIs. The main function of the components is to act on input and environmental conditions given by its cyber, physical or social environment. The input to this component is often inconcise, imprecise and disturbed by noise. To improve the system's robustness and resilience, the CPS component should be designed with more OR nodes to mitigate the unhealthy environment. Comparing with CI internal components, the CPS components have more dynamic properties. CPS components focus more on edge computing (dynamic and uncertainty), while the CI backbone components are more on stable computing.

CPS-based CIs have components with diverse and multi-dimensional dependencies (input), which come from the component's social-cyber-physical environment and children components. The diverse inputs imply the structure complexity and the resource diversity. The inputs demonstrate two kinds of interdependencies (links): (i) CI

internal based (within CIs) where component threats come from both CI internal components and CPS components, and (ii) CI external based (CPS related) where component threats come from the external CPS environment.

In CPS, control stream (downstream from parents to children) and information stream (upstream from children to parents) can be modeled in the same way, except the directions are opposite. Thanks to the functional dependencies, the multi-dimensional inputs and the heterogeneous structures could be integrated into one global modeling system. The performance of the CI is expressed by the accumulation of all included components. For individual component, vulnerability (health status) is the direct factor for its performance. This is measured by the quality of outputs for the component.

In CPS based CIs, there are several factors that contribute to the dynamics.

- The structure dynamics by the change of interdependencies
- Individual changes on specific resource that is the input/output change
- Performance change with system vulnerability (health status)
- Context/situation based change on functions and performance
- System evolution and degradation

Time is one important parameter to bind the dynamics. Evolution procedure could be described as serial changes over the time. Prediction of a potential tampering with the system is very important for proactive CIP.

5.2 Functional Analysis

In TMG, in-degree (inputs) and out-degree (outputs) are important structure properties. The in-degree of the component shows the extent of the possibility of suffering potential attacks. While the out-degree of the component shows the consequence to the system (to other component) of an attack. Research showed the network structure has strong relationship with system security (robustness and vulnerability). Scale-free networks (a network whose degree distribution follows a power law) are more robust against random attacks (i.e. removal of randomly chosen nodes) than against targeted attacks [AJB00].

The TGM enables the rank of the descendant in-degree and ancestor out-degree of the considered components. This can help (1) to evaluate the external threats to the CIs and (2) to evaluate the extent of the consequence to an attack on the component.

Based on the in-degree and out-degree analysis, centralized systems are more vulnerable than distributed systems under target attacks. Thus in the CI system design, we need to improve the robust and resilience and mitigate the effects of deliberate attacks, by minimizing the centralized structure.

Security can be seen as a chain that is only as secure as the weakest link in it. Security is a process, not a product [Sch00]. Accordingly, CI security is not depended on the strongest (or main) part on the system, but on the weakest part. In TGM, the weakest input, weakest output and weakest component are important in evaluate the system security and robustness. The importance of the input/output is not measured by the quantity, but is measured by the impact extent to the component functions. Thus weakest input/output can be defined as the easiest tampered input/output. The weakest component is determined by the most vulnerable locale resource, or weakest OMC.

In modern CIs, with (1) the large scale resource sharing, (2) wide ICT application in CIs, CIs shows complex and strong interdependencies between function components. The failure or accident on one component could be propagated to another and maybe further to all ancestor components. In TGM, the cascading behavior is easy to be identified by the dependency traversal. One major task for cascading mitigation is to quickly block the propagation of the failure by cutting down the dependencies to its parent component (the outputs). Another optional solution is to switch the children components to alternative (backup) component in time.

In TGM, to identify the cascading at an earlier stage, we can monitor the abnormal resource transferring (inputs and outputs) of each component. Once the abnormal is detected, a local structure adjusting might be conducted: (1) priories the dependencies for input/output and react from the priority resource, (2) cut down the failure

propagation to parent component, (3) switch the input /output to a backup candidate, if the system has a redundant design. OR input is a promising solution to support the redundant design.

Resilience is defined as the ability to resist, absorb, recover from, or successfully adapt to adversity or a change in conditions [NIPP09]. Resilience of CI requires the system to be adaptive and resilient to threats. Thus the CIP needs to be *context-awareness* or *situation awareness*. That means the threat modeling could have one parameter to denote the context/situation of the system. The context could be *time*, *space* or *specific application environment*. In TGM, we can import one extra condition parameter *S* to specify the situation of an application. *S* is a function of some *monitored parameters* and/or *time*. For example, in railway infrastructure, we can set two situations (summer situation and winter situation) for train running environment. When the environment parameter indicates winter (e.g., a temperature below -5°C), then the system should switch to the winter model and implement necessary adjustments on the resource dispatch and operation. For a dynamically evolving system, context-awareness and dynamic adaption are good properties in CIP to improve the resilience. For the system resilient design, there are several approaches to obtaining the goal: (1) adaptable structure of the system, (2) adaptable inputs, (3) adaptive protection network by pooling of shared resources.

As a fact to CIs, we can never prevent all attacks. Sufficiently skilled, motivated, and funded attackers will always be able to get in. We have to improve the system resilience design, identify the potential threats, avoid the cascading situations and mitigate the damage of attacks. Efficient tool and approaches are always necessary to CIP.

6 CONCLUSIONS

This paper investigates current approaches for modeling threats for critical infrastructures that are interacting with the environment (Cyber-Physical Systems). We elaborate the need of a multi-dimensional modeling approach, due to the complexity of threats and for threat evaluation of such systems. We also suggest a multi-dimensional modeling approach to capture complexity and dependencies, and that scales to model large emergent critical infrastructures. Such integrated modeling approach allows for analysis for threat ranking, threat propagation, cascading analysis, cascading mitigation, threat prediction and for resilience improvements.

Future work will include: (1) extend the TGM with details, (2) dynamic evolving threat modeling for CIs, (3) apply the model to real infrastructure analysis.

ACKNOWLEDGEMENT

Thank Jonas Mellin for his constructive discussion at earlier stage.

REFERENCES

[ABC+11] Alderson D, Brown G, Carlyle W, Wood RK. Solving defender-attacker-defender models for infrastructure defense. Pp. 28–49 in Wood K, Dell R (eds). Operations Research, Computing and Homeland Defense. Hanover, MD: Institute for Operations Research and the Management Sciences, 2011.
[AJB00] Réka Albert, Hawoong Jeong & Albert-László Barabási. Error and attack tolerance of complex networks. Nature 406, 378–382, 2000.
[AWK02] Paul Ammann , Duminda Wijesekera , Saket Kaushik, Scalable, graph-based network vulnerability analysis, Proceedings of the 9th ACM conference on Computer and communications security, November 18-22, 2002
[BDP06] Stefano Bistarelli , Marco Dall'Aglio , Pamela Peretti, Strategic games on defense trees, Proceedings of the 4th international conference on Formal aspects in security and trust, p.1-15, August 26-27, 2006.
[BM11] Bau, J.; Mitchell, J.C., "Security Modeling and Analysis," Security & Privacy, IEEE , vol.9, no.3, pp.18,25, May-June 2011
[BVM+12] Banerjee, A., Venkatasubramanian, K. K., Mukherjee, T., and Gupta, S. K. S. Ensuring safety, security, and sustainability of mission-critical cyber–physical systems. Proceedings of the IEEE, vol. 100, no. 1, pp. 283–299, 2012.

[CAS+09] Cardenas, A., Amin, S., Sinopoli, B., Giani, A., Perrig, A., and Sastry, S. Challenges for securing cyber physical systems. In Workshop on Future Directions in Cyber-physical Systems Security, DHS, Newark, NJ, July 23, 2009.
[Din08] Jianguo Ding. Probabilistic Fault Management in Distributed Systems, ISSN: 0178-9627, ISBN: 978-3-18-379110-1, VDI Verlag, Germany, 2008
[Din15] Jianguo Ding. Intrusion Detection, Prevention and Response System (IDPRS) for Cyber Physical Systems (CPS). To appear in: Securing Cyber Physical Systems, Al-Sakib Khan Pathan (Editor), CRC press, ISBN-13: 978-1498700986, 2015.
[Kar11] Karnouskos, S., Stuxnet worm impact on industrial cyber-physical system security. In IECON 2011—37th Annual Conference on IEEE Industrial Electronics Society, pp. 4490–4494, November 7–10, 2011.
[Lee08] Lee, E.A., "Cyber Physical Systems: Design Challenges," Object Oriented Real-Time Distributed Computing (ISORC), 2008 11th IEEE International Symposium on , vol., no., pp.363,369, 5-7 May 2008.
[NIPP09] U.S. Department of Homeland Security (DHS). National Infrastructure Protection Plan (NIPP): Partnering to Enhance Protection and Resiliency, 2009, pp. 111. Available at http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.
[May13] Jonna Mayberry. The Evolution Of Critical Infrastructure Protection. http://www.continuityinsights.com/articles/2013/11/evolution-critical-infrastructure-protection, 2013.
[MKB+11] Yilin Mo; Kim, T.H.-H.; Brancik, K.; Dickinson, D.; Heejo Lee; Perrig, A.; Sinopoli, B., "Cyber–Physical Security of a Smart Grid Infrastructure," Proceedings of the IEEE , vol.100, no.1, pp.195,209, Jan. 2012
[MLY05] Suvda Myagmar, Adam J. Lee and William Yurcik, Threat Modeling as a Basis for Security Requirements, Proceeding of Symposium on Requirements Engineering for Information Security (SREIS), 2005.
[New03] M. E. J. Newman. The Structure and Function of Complex Networks, SIAM Rev. 45, pp. 167-256, 2003.
[RLS+10] Rajkumar, R., Lee, I., Sha, L., and Stankovic, J. Cyber-physical systems: The next computing revolution. In Proceedings of the 47th Design Automation Conference (DAC'10). ACM, New York, pp. 731– 736, 2010.
[Sch99] Schneier, Bruce (December 1999). "Attack Trees". Dr Dobb's Journal, v.24, n.12.
[Sch00] Schneier, B. (2000). The process of security. Information Security, 3(4), 32.
[Sin90] Singer, D. (1990). A fuzzy set approach to fault tree and reliability analysis. Fuzzy sets and systems, 34(2), 145-155.
[Sin12] Sinopoli, B. Cyber-physical security: A whole new ballgame. IEEE Smart Grid, November 2012.
[SGL+09] Sha, Lui, Sathish Gopalakrishnan, Xue Liu, and Qixin Wang. "Cyber-physical systems: A new frontier." In Machine Learning in Cyber Trust, pp. 3-13. Springer US, 2009.
[Str01] Strogatz SH. 2001. Exploring complex networks. Nature 410: 268–276.
[TLG07] Chee-Wooi Ten; Chen-Ching Liu; Govindarasu, M., "Vulnerability Assessment of Cybersecurity for SCADA Systems Using Attack Trees," Power Engineering Society General Meeting, 2007. IEEE , vol., no., pp.1,8, 24-28 June 2007.
[Ven09] Venkatasubramanian, K. Security solutions for cyber-physical systems. PhD Dissertation. Arizona State University, Tempe, AZ, 2009.