Towards a Security Reference Architecture for Cyber- Physical Systems

Virginia M. Romero, PhD (C), Eduardo B. Fernandez, PhD
Florida Atlantic University, USA. vromero@fau.edu
Florida Atlantic University, USA. fernande@fau.edu

Abstract–Cyber Physical Systems (CPS) are physical entities whose operations are monitored, coordinated, controlled and integrated by a computing and communication core. Security for these systems requires solutions that are robust to threats, especially when securing critical infrastructures. Secure systems need to be built in a systematic way, where security and safety are not just add-ons or built in a piece-meal fashion but are able to handle their complexity in a safe and secure holistic way. All lifecycle stages and all architecture levels need to be considered. The only way to provide this unification in the presence of a myriad of implementation details of the component units, is to use abstraction. In particular, we can apply abstraction through the use of patterns and Reference Architectures (RA). The use of Reference Architectures and patterns is a powerful way to organize and describe security and other non-functional aspects and they have the potential to unify the design of the computational, communication, and control aspects of CPSs. In this paper we provide a survey of the current CPS Reference Architectures that will be used as a preamble to define a threat model and a Security Reference Architecture (SRA) to build safe and secure CPS systems.

Keywords—CPS, Reference Architectures, Security Reference Architectures, Survey.

Digital Object Identifier (DOI):
http://dx.doi.org/10.18687/LACCEI2017.1.1.435
ISBN: 978-0-9993443-0-9
ISSN: 2414-6390

Towards a Security Reference Architecture for Cyber- Physical Systems

Virginia M. Romero, PhD (C), Eduardo B. Fernandez, PhD
Florida Atlantic University, USA. vromero@fau.edu
Florida Atlantic University, USA. fernande@fau.edu

Abstract–Cyber Physical Systems (CPS) are physical entities whose operations are monitored, coordinated, controlled and integrated by a computing and communication core. Security for these systems requires solutions that are robust to threats, especially when securing critical infrastructures. Secure systems need to be built in a systematic way, where security and safety are not just add-ons or built in a piece-meal fashion but are able to handle their complexity in a safe and secure holistic way. All lifecycle stages and all architecture levels need to be considered. The only way to provide this unification in the presence of a myriad of implementation details of the component units, is to use abstraction. In particular, we can apply abstraction through the use of patterns and Reference Architectures (RA). The use of Reference Architectures and patterns is a powerful way to organize and describe security and other non-functional aspects and they have the potential to unify the design of the computational, communication, and control aspects of CPSs. In this paper we provide a survey of the current CPS Reference Architectures that will be used as a preamble to define a threat model and a Security Reference Architecture (SRA) to build safe and secure CPS systems.

Keywords—CPS, Reference Architectures, Security Reference Architectures, Survey.

I. Introduction

Cyber Physical Systems (CPS) are systems that integrate physical processes, computational resources, and communication capabilities with the monitoring and/or control of entities in the physical world. The components of a CPS can be centralized or distributed and usually include embedded devices, sensors, and wireless links. Many system components are remotely deployed, have unique constraints and may be physically inaccessible for maintenance but not for attacks. Examples include transportation systems, smart power grids, patient monitoring, smart buildings, flexible manufacturing systems, and many others. Often, CPSs are safety-critical because their failure could endanger lives or cause large economic losses. They exhibit at least two clear architectural levels: a hybrid control loop (lower level) and an information loop. CPSs require a high level of adaptability because of continuously-changing conditions and need situation awareness and modifiability [1]. They may include legacy systems and they increasingly include humans in the loop. Typically, they use combinations of Commercial Of The Shelf (COTS) components and real-time operating systems, as well as products from different vendors using different protocols. Many CPS also need to follow government or state regulations. The design of CPS systems needs to consider several disciplines such as embedded systems, computers and communications and others and the software is embedded in devices whose principal mission is not only computation.

For economic and productivity reasons, open networks are an attractive communication medium for CPSs, but doing this increases their vulnerability to intentional attacks. The objectives of attacks may vary, from terrorist objectives to economic objectives such as collecting private information. The complexity of modern CPSs makes their secure design and maintenance very difficult, and CPS attacks are increasing; for example, cyber-manipulation of container logistics in a port has become a realistic attack [2], Stuxnet demonstrated the feasibility of attacking physical systems using worms [3, 4, 5], and similar attacks are possible and expected [6]. Security attacks in CPSs where humans are present can affect the privacy and safety of those systems and may have catastrophic consequences [7, 8, 9, 10, 11, 12, 13].

Vulnerabilities in CPS come from their sheer complexity and their heterogeneity. Critical certified components often coexist with auxiliary systems built with lower standards [13]. CPSs and their components usually have strong dependencies on each other and attacks can easily propagate [14]. Another important reason is that security is built as an add-on, in a piecemeal fashion, parts of the system are secured using specific mechanisms but there is rarely a global security analysis of the complete system. If done, different models may be used in different parts, e.g., one for the databases and another for wireless devices. However, security requires a comprehensive approach to block all possible ways of attack or at least control their effects [15, 16]. Further, methodologies for building secure systems focus only on new systems, but the majority of the CPSs in practice are legacy systems, in constant maintenance. Even systems built carefully suffer from architecture erosion, where changes made after deployment can invalidate or weaken security defence. To address this problem, software legacy systems would need to be reengineered by tracing back code changes so that their impact on security mechanisms can be detected and corrected.

Digital Object Identifier (DOI): http://dx.doi.org/10.18687/LACCEI2017.1.1.435
ISBN: 978-0-9993443-0-9
ISSN: 2414-6390

To design a secure system, we need to understand the possible threats to the system. We need to understand how the specific components of the architecture are compromised and used by an attacker in order to fulfil his objectives. It is not enough to apply the same security measures used in Information Technology (IT) systems to CPSs. While superficially there are many commonalities, delving deeper one finds many differences when dealing with embedded and critical components. The main threat to information systems is illegal reading of information, a *confidentiality* attack; the attacker wants to collect information that he can sell or use directly. The main threats for CPSs are *integrity* attacks, illegal modifications or destructions of information, which may result in deception attacks. In this case the attacker wants to disrupt the operations of the physical system or to enable the introduction of physical threats.

Another difference is that IT attacks typically target any system and the attacker wants to collect as much information as possible, while CPS attacks target specific types of systems. These differences imply the need for a specialized analysis of threats as well as a corresponding use of security mechanisms and development methodologies. We surveyed existing secure system development methodologies in [17] but all of them are for IT systems. Attacks in IT systems can take only a few forms while attacks in CPSs have a much larger variety of ways to compromise a system [18, 19]. We know of no comprehensive secure development methodology specifically oriented to CPSs. There are also several studies of threats for IT systems but it is not clear if they apply to CPSs where only a few studies of threats have appeared.

Once we determine the threats to a system we can use security patterns as a guideline to incorporate mechanisms to stop or mitigate them. A *security pattern* is a solution to a security problem in a given context and provides a way for guiding system designers who are not experts on security [113]. A R*eference Architecture* (RA) aggregates several patterns related to a given domain of knowledge. Data analysis has become very important for detecting security threats [21]; however, without an RA we only get a set of disjoint attacks, where we do not have a clear guidance on how to improve our architecture to stop them in the future.

Threats can be described as threat patterns and mapped to their corresponding defenses [22, 23]. A *misuse pattern* describes how an attack is performed using the architectural units of the system, indicating its use of these units along time.

We survey here what has been done about RAs and Security Reference Architectures (SRAs) for CPSs; we also consider work on cloud RAs because of the increasing use of clouds in CPSs. While our emphasis is on security, three other related aspects should also be considered because they affect or are affected by security: compliance, reliability, and safety. Ours is not a systematic survey, we do not claim completeness, we only focus on what we consider interesting or significant approaches and we get from them ideas for our own future work in producing a SRA for CPSs.

We start from the observation that the architecture of CPSs is a fundamental element in their susceptibility to attacks and it is also the source of strengthening to prevent these attacks. It is analog to a building, where its structural design and integrity is the most important aspect in the face of earthquakes. While it is possible that an earthquake damages part of the building the building as whole never collapses.

This paper is organized as follows: Section II outlines the general security limitations, challenges and implementation trade-offs of CPS systems. Section III reviews the existing literature on security solutions and security mechanisms for CPSs. Section IV presents an approach to building safe and secure systems by introducing threat enumeration as the base for defining policies that can stop or mitigate these threats and then realized with patterns. Section V presents our conclusions.

II. CPS Security challenges

We first survey challenges in CPSs to see later how RAs can help.

A. Limitations and Challenges of CPS

All CPS must be dependable, secure, safe and efficient and able to operate in real-time. They must also be scalable, cost-effective and adaptive. Interconnected networks of embedded (and possibly mobile) devices and sensors in a CPS present the following fundamental limitations and challenges:

Networking Challenges: Present architectures are defined to optimize point-to-point communication and reliable point to point connection. The current Internet architecture is not designed to support countless amount of physical data sources, sensors, actuators or any distributed amount of computing elements. CPS systems may require the integration of the data from an increasing number of embedded devices such as sensors into a unified view of this data (data fusion). Therefore, network architecture needs to be redefined to optimize distributed information synthesis and retrieval as opposed to point-to-point communication.

Computing Challenges: Past distributed computing templates abstract distributed communication, providing support for location transparency and hiding communication details. Future cyber-physical computing approaches will need to support a massively concurrent interaction with the physical world, and represent the external environment conveniently for the software developer. This type of computing is called, environmentally immersive computing.

Programming Language Design Challenges: Cyber-physical applications approach will be increasingly geared towards data fusion. A representative object in an object-oriented language can either exist or not. In CPS, an object that represents an external entity (e.g. a door in a smart

building) will have to be associated with a confidence level that describes how likely it is that this object truly exists in the external world. Abstractions should revolve directly around environmental elements such as data sources, objects and activities such as open door. A sense of timing needs be introduced.

Software Engineering Challenges: Currently software engineering practices are mostly concerned with system robustness in centralized or clustered systems. In CPS, an increase of functional and timing errors is introduced due to the integration of larger numbers of components into complex information processing networks. The fundamental concern of cyber-physical computing is to provide the same timeliness and robustness in the presence of complex timing interactions, complex software integration and programming errors.

Data Management Challenges: Data mining and machine learning techniques will play an increasingly important role in CPS systems due to their autonomy. Most of these systems do not require human assistance. In such systems the identification of data patterns, context learning and detection of complex events of interest will have an important role in the design of network protocols and programming abstractions [24]. In the next section we consider security implementation trade-offs.

B. CPS Security Implementation Trade-Offs

There are considerable implementation challenges, mainly because the physical components of a CPS system introduce safety and reliability requirements qualitatively different from those in general purpose computing. Furthermore, entities in the physical world are not entirely predictable. These systems will not be operating in a controlled environment and they need to be robust enough to operate even under subsystem failures and unexpected conditions. Furthermore, these systems need to consider the following implementation trade-offs:

Security vs. Efficiency: CPS sensors may be small, lightweight and run using small batteries (e.g. wireless body area network WBAN). Sensors may be resource constrained and must comply with real time requirements. This implies that communication protocols should be fast, consume less processing power, small memory and less communication overhead. This means that we need to use cryptographic techniques which are computationally light and possess smaller memory footprint while still being efficient, in order to prevent the drain of power and storage space of the nodes. Another consideration is that authentication protocols need to be fast enough in order to prevent downgrading the performance of the entire system [25].

Security vs. Safety: Implementing higher levels of security could affect safety requirements. A very strict and rigid data access control may prevent timely access of personnel in case of an emergency such as law enforcement. On the other hand, a much lenient access control allows attacks by the adversaries. So, trade-offs between security and safety aspects must be considered as they affect each other.

Security vs. Usability: Because some CPS systems have a good amount of human intervention in their operations, devices should be designed to be foolproof and in some instances easy to use even by naïve users. In other cases a good design should involve intuitive and little to no human interaction when setting up the data security mechanisms.

Security vs. Interoperability: Some security mechanisms should be transparent to users, for example, different sensor nodes can use different key distribution methods and/or cryptographic algorithms to implement security. This makes it difficult to have interoperability between wide ranges of devices.

Security vs. Quality of service: Applications like health-care require high quality of service (QoS) and CPSs should comply with these strict latency requirements. QoS for an application refers to providing assurance in terms of measurable service attributes like delay, jitter, available bandwidth and packet loss. It is required that the WBAN setup and the cryptographic algorithms used are fast enough to guarantee the assured QoS for the application.

Security vs. Flexibility: The administrator should have the flexibility to choose or change the access control mechanism. He should be able to change or revoke the privileges at will in case of a breach.

Security vs. Scalability: Security in a CPS system should be scalable to handle applications with large amount of user groups. Even in the large user group scenario, computational and storage overhead involved for security and access control should be kept low.

Algorithmic and architectural aspects of security. As shown below, most work on CPS security has focused on the effect of intentional disturbances on the system. The effect of the architecture has been neglected and it is our emphasis in this work.

III. CPS Security Survey and Discussion

There are several methodologies for producing secure systems [26, 23], but none of them is specifically intended for CPSs. A systematic approach to safety-critical systems was proposed in [27]. However, they did not consider data aspects, but worked mostly with dynamic aspects described by statecharts and do not consider security. Later, they proposed a systems approach to security and safety [28, 29], but it has not been fully developed.

D. Garlan and his group have written several papers on the architecture of CPSs. However, their emphasis is on modeling the physical functions of these systems, not on building secure architectures. Although they show some architectural examples of their methodology they did not try to build specific architectures and never considered security. They use graphic symbols to identify their views but we think that UML stereotypes are more general. There is a need to abstract security concerns from all the other aspects and try to define a secure view that is not mingled with these other views.

M. Tichy studied pattern-based synthesis of fault-tolerant embedded systems [30]. His objective was to automate the application of fault tolerance into embedded systems. For this purpose, he developed a formal model based on Petri nets. In order to define the points where to apply fault tolerance mechanisms, he considered the possible faults of the system.

L. Grunske focused on validation of safety properties: If a software architecture does not satisfy its requirements, it is modified by adding patterns that improve its safety properties [31]. His approach is based on transformational patterns that effectively perform model refactoring [32]. Y. Choi [33] converted use cases scenarios into activity diagrams, which in turn become Finite State Machines modeled using RSML^{-e}, a formal language that has a model checker where hazard conditions can be identified. None of these works considers security, they discuss only safety; however, some of these ideas can be used for security as well.

There are several discussions of general issues and challenges in CPSs but they barely mention security [34, 35]. Some papers analyze the security of specific CPSs; [36] discusses the need for security in railway systems but considers only communication aspects, [8] discusses cryptography for railway systems, [37] discusses general aspects of railway security. Refs. [38] and [39] consider car security. Refs. [40, 41, 42, 43] discuss aviation security. Ref. [44] discusses threats in electric power grids but he considers only ad hoc solutions. Ref. [45] studied how to reduce vulnerabilities in CPSs. All these studies consider very specific aspects and make no attempt for a unified and systematic approach to security.

Campbell and his group have done extensive work on these and related topics. Refs. [46, 43] studied security policies for CPSs, in particular buildings and airports. Their emphasis was to classify the necessary policies and create an architecture to enforce these policies. They defined a framework for acquiring information about infrastructure state and for checking if the current situation would violate any of the policies. They did not try to identify specific threats and did not indicate how the policies would be generated. Their approach is mostly formal using 1st-order predicate calculus assertions.

Much security work on CPS centers on attack detection. An approach to detect attacks monitors inputs based on a model of the system and tries to find anomalies [47, 48]. Ref. [49] discusses deception attacks in water SCADA systems. Later, they proposed the analysis of different types of data and historical data for access control [50]. These papers and others [51] apply system modeling to detect attacks by detecting behaviour anomalies. The authors of those papers recognize that they have no general defense methods, they estimate correct state values to replace suspicious sensor values. Their approach requires models for each type of system. Ref. [52] shows that a CPS can have a multiplicity of inputs where an attacker can produce disruption using false data injection. We are not attempting to model systems but we want to define a framework where the way to conduct specific attacks can be described with relation to the system architecture. Our approach is simpler in that we consider only structural properties of the system, and we use its architecture to stop the attack.

Ref. [53] mentions the possibility of using domain models but no details are given. Refs. [47, 54, 55, 53] all give basic block diagram architectures with short description of the units. A more detailed architecture is given in [56]. Ref. [57] uses a SOA approach to design CPSs, including patterns but their approach is oriented to dynamic composition of services, not security. Microsoft defined an RA for smart grids [58], and [59] described a secure architecture for smart grids. These descriptions are not detailed or formal enough to analyse threats.

Some papers, e.g., [55], propose implementation-oriented architectures, [55] is based on wireless networks. Ref. [60] describes a pattern language for safe adaptive control. The language includes a type of patterns about cases, where safety is proven by argument. Ref. [61] also used safety case patterns, where each pattern presents a safety argument that can be reused to assert safety in different situations. Ref. [62] describes a case study combining security and safety restrictions and also using arguments. Arguments have the problem that they do not have a clear reference to system units as patterns do; but they could make useful complements to patterns, especially for safety [115].

None of the surveys on CPSs [15, 63, 35, 53] or about CPS/SCADA security [49, 64, 65, 66, 39], mentions the possibility of using patterns for describing threats or their countermeasures. Ref. [67] uses patterns to build a collection of building modules with formal properties but his patterns are not of the standard type and do not consider security or safety. Ref. [68] uses SysML to describe software-hardware interfaces of safety-critical systems, but they do not use patterns. Other related work includes [69, 70]. Few safety patterns exist [71, 72]. There is also some work on security of embedded systems [73, 74]. There is some use of UML to find security requirements of cars [75], as well as for traceability [76]. Some work focuses on general middleware aspects for CPSs [77]. Ref. [78] considers compliance aspects. Ref. [79] has proposed a new format for CPS patterns.

Threat analysis and enumeration in different types of CPSs can be found in [80, 81, 82, 83, 52, 84]. These enumerations are helpful for finding analogies between threats and to understand the possibilities of attackers.

As discussed in [85], general attack taxonomies can be extended to CPSs. He describes the possible use of a multidimensional attack taxonomy. Since we represent threats

using patterns we can use our multidimensional patterns taxonomy [86]. There has been a large amount of work on threat modeling for IT systems, including attack trees, attack graphs, misuse cases, misuse patterns, Data Flow Diagrams, and other artifacts. A common approach is the misuse case [87], which are malicious use cases initiated by attackers. This approach does not show how to associate the misuse cases to legitimate behavior and concrete assets; therefore, it is not clear what misuse case should be considered, nor in what context. Ref. [88] considers attack surfaces, modeling attacks using SysML. GSN (Goal Structured Notation) uses arguments about the security of a system, and appears useful to evaluate the security level of a system but it is not clear if it can be used to study threats.

Refs. [89, 90, 91, 92, 93, 94, 95, 96] describe threats in different types of CPSs but without attempting generic modeling or systematic enumeration. Loukas [97] describes a variety of CPS attacks without attempting rigorous modeling or systematic enumeration. Zalewski et al. [98], analyze the effects of attacks with Markov models. Ref. [99] models threats using data flow graphs related to hardware units, while we use patterns and relate threats to architectural units, which we believe are more precise. In [100] they introduce a language (using UML and BNF) to describe CPS attacks. The model emphasizes the mechanics of the attacks and does not consider the attacker goals. There is no relative timing representation for the attack either. Ref. [101] uses a reference architecture to trace propagation of attacks. Another interesting approach to threat modelling uses aspects [102]. Aspects model cross-cutting functionality and improve reusability; we think that patterns are more powerful to describe attacks than these models. Stuxnet has been modeled using Boolean logic Driven Markov Processes (BDMP), a combination of attack trees and Markov processes.

Yampolski et al's work model threats using data flow graphs related to hardware units. They improved their model in [103]. Another interesting approach to threat modeling uses aspects [104]. Ref. [105] discusses general aspects of CPS security and emphasizes the need to be able to simulate CPS traffic to validate security mechanisms.

In our paper [116] we proposed:

- Define a new model to represent CPS threats using patterns that are related to architectural aspects of the system and consider cross domain (from cyber to physical) effects.
- Extend our threat enumeration system to identify threats in specific systems based on their use cases.
- Propose an idea to unify threats that behave in similar ways in different types of CPSs and that can be controlled in similar ways. We look for commonalities in their modus operandi to reduce them to specific types.

IV. Threat Enumeration

The need to control the access to restricted areas and protect assets in buildings such as government agencies, airports, naval ports or nuclear plants created a great business opportunity for the physical access control industry. In addition, the growing demands of the industry for increased connectivity between the physical entities and the corporate network or the internet resulted in increased security threats and vulnerabilities that are not limited to physical attacks [106, 107]. Prior to 2000, studies indicate that the majority of the attacks were perpetrated by disgruntled employees or people familiar with its operations. Since 2001, studies revealed that 70% of these attacks where originated by an outside source [117]. Researches have recognized that access control to information and access control to physical entities have many common aspects and that there is a clear need for a Safe and Secure Reference Architecture (SSRA) for these systems.

In the literature, much of the work has concentrated on designing a security architecture that focuses on the cyber system and the physical system individually and not on the interaction of both systems. They concentrate on the access control aspects on the one hand, and offer many solutions for the security requirements of CPS including authenticity, confidentiality, authentication and availability on the other. Other work focuses on the robustness and fault tolerant aspect of the CPS. Yet other studies focus on context-aware applications and their security policies in this information rich environment. Policies in this environment may need to restrict access to information or resources based on multiple factors including attributes pertaining to the subject, the resource or the environment. [109].

An effective approach for threat enumeration is presented in the literature [110, 111]. It starts with the activity diagram of each use case in a system. Each activity is analyzed to see how it could be used improperly to produce a misuse of information. This analysis results in a set of threats, and since they are derived from all the interactions of the system, this presents a list that can identify most threats. With this list in place, policies that can stop or mitigate these threats are defined and then realized with patterns. Furthermore, threats can be classified by their risk and likelihood. This process is performed during the requirements and the design stages of the software development cycle.

Another approach to enumerating threats can be seen in [106] where we look at possible attacks against each component of the system if its platform structure is predefined. A CPS system usually presents three different components: 1. Physical entities or field units, such as sensors or actuators in the case of a Wireless Body Area Network (WBAN), or, meters, generators, transformers and equipment that delivers electricity in a traditional power grid in the case of a SmartGrid. 2. A central controller unit that collects and stores information from the controlled process and/or sends

commands to the physical entities based on the information collected adjusting parameters based on these collected values and their set points. This central controller unit includes the human-machine interface (HMI) that may also display status and historical information. 3. The remote base stations that can provide diagnostic and maintenance functions used to identify and recover from failures or attacks. This component uses intelligent transmission and communication networks. An example of the approach presented in the literature is as follows: [106, 111]

We categorized threats based on these three components:

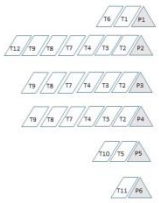
1. Attacks against/through the central controller include (i) physical attacks (T1), (ii) malicious settings of the field units (T2), (iii) wrong commands to the field units (T3), (iv) malicious alteration of the runtime parameters of the central controller (T4), and (v) denial of service attacks (T5).

2. Attacks against/through the field units include (i) physical attacks (T6), (ii) malicious alteration of the runtime parameters of the field units (T7), (iii) wrong commands to the field units (T8), (iv) malicious alarms to the central controller (T9), and (v) denial of service (T10).

3. Attacks against/through the communication networks include (i) sniffing (T11), (ii) spoofing (T12), and (iii) denial of service (T13).

Attacks against the central controller and the network are more harmful since they may disable the whole system, while attacks against field units only affect specific units. Attacks due to malware are not considered in this example. Figure 1 shows the identified threats and policies to handle them [112].

Threats	
T1	Attacker destroys hard drive from control unit
T2	Disgruntled employee changes settings of the field units in the controller
T3	Attacker sends destructive commands to field units
T4	Disgruntled employee alters runtime parameters of the central controller
T5	Attacker floods central controller with commands. (DoS)
T6	Attacker tampers with field unit.
T7	Disgruntled employee changes settings of the field units
T8	Attacker sends wrong commands to field units
T9	Malicious alarms to the central controller
T10	DoS to the field unit
T11	Sniffing
T12	Spoofing
T13	DoS



Policies	
P1	Physical Access Control, Role Based Access Control
P2	Mutual Authentication
P3	Logging
P4	Authorization
P5	Protection Against Denial of Service (Firewall and Intrusion Detection)
P6	Encryption, secure channel

Figure 1 Threat Enumeration and Policies

V. CONCLUSIONS

Although there are numerous works on the security of CPSs, only a few address general aspects of their threats. Most concentrate on architectures that model physical functions of a CPS system and not on building secure architectures. Authors use very specific aspects of a system to reduce vulnerabilities but make no attempt for a unified and systematic approach to security. Some analyze the security of specific CPSs, e.g. aviation, railway systems, automobiles, while others have studied security policies for CPSs, in particular buildings and airports. Their approach defines a framework to retrieve information about infrastructure state to then check if the current situation violates any of their policies. Other authors focus on attack detection, threat enumeration, attack surfaces in different types of CPSs but without attempting generic modeling or systematic threat enumeration. In the literature, much of the work has concentrated on designing a security architecture that focuses on the cyber system and the physical system individually and not on the interaction of both.

Our emphasis on Reference Architectures is on the structural aspects of CPSs, since these are shared by many systems and security strongly depends on structural properties. The notion is that once we refine the high level blocks, the structure of many systems will still be similar within a range defined by architectural patterns. We can then apply security patterns to these units and define SRAs for ranges of systems that describe related applications and have similar threats.

Future work will focus on finding use cases for specific CPS, e.g. cargo ports, and show that even though there is an enormous variety of threats specific to each type of system, many of them are similar in effect and can be prevented in similar ways. We intend to create a structured approach to CPS security by addressing the top threats that have the greatest potential impact, then by identifying objectives and vulnerabilities we can define countermeasures to prevent or mitigate their effects. Once our threat model is complete, we can identify patterns and create a Reference Architecture to guarantee CPS security.

.

REFERENCES

[1] G. Denker, N. Dutt, S. Mehrotra, M.-O. Stehr, C. Talcott, and N. Venkatasubramanian, "Resilient dependable cyber-physical systems: a middleware perspective", J. Internet Serv. Appl., vol. 3, 2012, 41-49.

[2] Tom Bateman, "Police warning after drug traffickers' cyber-attack", http://www.bbc.co.uk/news/world-europe-24539417, 16 October 2013.

[3] D. E. Denning, "Stuxnet: What has changed", Future Internet, vol. 4, 2012, 672-687. doi: 10.3390/fi4030672

[4] D. Kushner, "The real story of Stuxnet", IEEE Spectrum, Feb. 2013, http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

[5] Stuxnet, HYPERLINK "http://en.wikipedia.org/wiki/Stuxnet" http://en.wikipedia.org/wiki/Stuxnet

[6] M. Lee, "Hackers could control Brisbane traffic controls: Report I"http://www.zdnet.com/au/hackers-could-control-brisbane-traffic-controls-report-7000023405/

[7] United States Government Accountability Office, Statement before the Committee on Commerce, Science and Transportation, U.S. Senate, Wed. December 2, 2009 , DHS's Progress and Challenges in Key Areas of Maritime, Aviation, and Cybersecurity Statement for the Record http://www.gao.gov/new.items/d10106.pdf

[8] S. Katzenbeisser, "Can trains be hacked? Die Technik der Eisenbahnsicherungsanlagen.", presentation at 28th Chaos Computer Congress, 2011, http://www.youtube.com/watch?v=C3sGgRtsTbg (in German).

[9] J. Kramek, "The Critical Infrastructure Gap: U.S. Port Facilities and Cyber Vulnerabilities ", Brookings Inst., 2013, http://www.brookings.edu/~/media/research/files/papers/2013/07/02%20c

yber%20port%20security%20kramek/03%20cyber%20port%20security%20kramek.pdf
[10] Executive Office of the President, National Science and Technology Council, The networking and Information technology Research and development (NITRD) Program, 2012 Strategic Plan, July 2012.
[11] D. Pauli, "Hackers pop German steel mill, wreck furnace", The Register, UK http://www.theregister.co.uk/2014/12/22/hackers_pop_german_steel_mill_wreck_furnace/
[12] RadTown USA, Shipping port security, http://www.epa.gov/radtown/port-security.html
[13] Y. Laarouchi, Y. Deswarte, D. Powell, J. Arlat, and E. De Nadai, "Ensuring safety and security for avionics: A case study", Proc. Data Systs. and Aerospace Conf. (DASIA 2009), Istambul, May 2009.
[14] A. Lauge, J. Hernantes and J. M. Sarriegi, "Critical infrastructure dependencies: A holistic, dynamic and quantitative approach", International Journal of Critical Infrastructure Protection, Volume 8, January 2015, Pages 16–23
[15] D. Broman et al., "Viewpoints, formalisms, languages, and tools for cyber-physical systems", In Proceedings of the 6th International Workshop on Multi-Paradigm Modeling (MPM 2012), Innsbruck, Austria, ACM, 2012.
[16] E. B. Fernandez, Nobukazu Yoshioka, Hironori Washizaki, and Michael VanHilst, "An approach to model-based development of secure and reliable systems", Procs. Sixth International Conference on Availability, Reliability and Security (ARES 2011), August 22-26, Vienna, Austria.
[17] Anton V. Uzunov, E.B.Fernandez, and K. Falkner, "Engineering Security into Distributed Systems: A Survey of Methodologies", Journal of Universal Computer Science, Vol. 18, No. 20, 2013, pp. 2920-3006. http://www.jucs.org/jucs_18_20/engineering_security_into_distributed
[18] D. Dzung, M. Naedele, T. Von Hoff, and M. Crevatin, "Security for industrial communication systems", Procs. of the IEEE, vol. 93, No 6, June 2005, 1152-1177.
[19] M. Naedele, "Addressing IT security for critical control systems", Procs. 40th Hawaii Int. Conf. on Sys. Science (HICSS-40), January 2007.
[20] E.B.Fernandez, Security patterns in practice: Building secure architectures using software patterns, Wiley Series on Software Design Patterns, 2013.
[21] E. Bou-Harb, M. Debbabi, and C. Assi. "On fingerprinting probing activities". Computers & Security, 43, 2014, 35-48.
[22] E.B. Fernandez, J.C. Pelaez, and M.M. Larrondo-Petrie, "Attack patterns: A new forensic and design tool", Procs. of the Third Annual IFIP WG 11.9 Int. Conf. on Digital Forensics, Orlando, FL, Jan. 29-31, 2007. Chapter 24 in Advances in Digital Forensics III, P. Craiger and S. Shenoi (Eds.), Springer/IFIP, 2007, 345-357.
[23] A. Uzunov and E.B.Fernandez, "An Extensible Pattern-based Library and Taxonomy of Security Threats for Distributed Systems"- Special Issue on Security in Information Systems of the Journal of Computer Standards & Interfaces, 36(4), 734–747. 2013. http://dx.doi.org/10.1016/j.csi.2013.12.008
[24] Tarek Abdelzaher, Associate Professor, UIUC, "Towards an Architecture for Distributed Cyber-Physical Systems". http://www.cs.uiuc.edu/homes/zaher.
[25] M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks," Wireless Communications, IEEE , vol.17, no.1, pp.51-58, February 2010 http://ieeexplore.ieee.org.ezproxy.fau.edu/stamp/stamp.jsp?tp=&arnumber=5416350
[26] A. Uzunov, E.B.Fernandez, and K. Falkner, "Securing Distributed Systems using Patterns: A Survey", Computers & Security, 2012 http://dx.doi.org/10.1016/j.cose.2012.04.005
[27] N.G.Leveson, M.P.E.Heimdahl, H. Hildreth, and J.D.Reese, "Requirements specification for process-control systems", IEEE Trans. on Soft. Eng., vol 20, No 9, September 1994, 684-707.
[28] W. Young and N. G. Leveson, "Systems thinking for safety and security", Procs. of the 2013 Ann. Computer Sec. Apps. Conf., ACSAC2013, Dec. 2013
[29] W. Young and N.G. Leveson, "An integrated approach to safety and security based on systems theory", Comm. of the ACM, vol. 57, No 2, Feb. 2014, 31-35.
[30] M. Tichy, "Pattern-based synthesis of fault-tolerant embedded systems", Procs. of SIGSOFT'06/FSE-14, November 2006, Portland, OR.
[31] L. Grunske, "Transformational patterns for the improvement of safety properties in architectural specification", Procs. 2nd Nordic Conf. on Pattern Languages of Programs (VikingPLoP'03).
[32] M. Fowler, Refactoring: Improving the design of existing code, Addison-Wesley 1999.
[33] Yunja Choi: "Early Safety Analysis: from Use Cases to - Component-based Software Development", in Journal of Object Technology, vol. 6, no. 8, September - October 2007, 185-203 http://www.jot.fm/issues/issue_2007_09/article4.
[34] G. Karsai, D. Balasubramanian, A. Dubey, and W.R. Otte, "Distributed and managed: Research challenges and opportunities of the next generation cyber-physical systems', IEEE 17th Int. Symp. on Object/Component/Service-Oriented Real-Time Distributed Computing (ISORC), 2014
[35] Edward A. Lee, "Cyber Physical Systems: Design Challenges", Procs. of ISORC, Orlando, FL May, 2008
[36] J. Smith, S. Russell, and M. Looi , Security as a safety issue in rail communicationsProceeding SCS '03, the 8th Australian workshop on Safety critical systems and software - Volume 33 Australian Computer Society, Inc., Darlinghurst, Australia, Australia ©2003
[37] A. H. Carlson, D. Frincke, and M. J. Laude, " Railway Security Issues: A Survey of Developing Railway Technology", http://laude-web.net/documents/CCCT_03_T760GD.pdf
[38] S. Checkoway, D. McCoy, B. Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno, "Comprehensive Experimental Analyses of Automotive Attack Surfaces", http://www.autosec.org/pubs/cars-usenixsec2011.pdf
[39] I. Rouf, R. Miller, H. Mustafa, T. Taylor, S. Oh, W. Xu, M. Gruteser, W. Trappe, and I. Seskar , "Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study," in Proceedings of the 19th USENIX Security Symposium, Washington DC, August 11-13, 2010
[40] Air Traffic Organization Operations Planning Office of Aviation Research and Development. USA, Handbook for networked local area networks in aircraft http://www.tc.faa.gov/its/worldpac/techrpt/ar0835.pdf
[41] Air Traffic Organization Operations Planning Office of Aviation Research and Development Washington, DC 20591, Networked Local Area Networks in Aircraft: Safety, Security, and Certification Issues, and Initial Acceptance Criteria (Phases 1 and 2) http://www.tc.faa.gov/its/worldpac/techrpt/ar0831.pdf
[42] E. Fleischmann, R. Smith, and N. Multari, LANs in Aircraft, including Safety and Security Issues. FAA LAN study Phase 1 result summary. 29 Jun 2007. http://spiderman-2.laas.fr/IFIPWG/Workshops&Meetings/52/workshop/03%20Multari.pdf
[43] M. Montanari, R.H. Campbell, K. Sampigethaya, and M. Li, "A security policy framework for sEnabled fleets and airports", IEEE Aerospace Conf. 2011, 1-11.
[44] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system security for the electric power grid", Procs, of the IEEE, Vol. 100, No 1, Jan. 2012, 210-224.
[45] D.H.Ryu, H. Kim, and K. Um, "Reducing security vulnerabilities for critical infrastructure", J. of Loss Prevention in the Process Industries, vol. 22, 2009, 1020-1024, doi:10.1016/jlp.2009.07.015
[46] Montanari, Mirko, L. Mingyan, S. Krishna, and C. Roy H "A Formal Security Model for Networked Control Systems ", AIAA InfoTech@Aerospace American Institute of Aeronautics and Astronautics , Seattle, WA, USA 04/2009 http://srg.cs.illinois.edu/srg/node/518
[47] A.A. Cardenas, S. Amin, Z.-S. Lin, Y.-L.Huang, C.H.Huang, and S. Sastry, "Attacks against process control systems: Risk assessment, detection, and response", Procs. of ASSIACS'11, March 22-24, 2011, Hong Kong, China, 355-366.
[48] A. Hahn, R. K. Thomas, I. Lozano, and A. Cardenas, "A multi-layered and kill-chain based security analysis framework for cyber-physical systems", International Journal of Critical Infrastructure Protection, August 2015.
[49] S. Amin, X. Litrico, S.S.Sastry, and A.M.Bayen, "Stealthy deception attacks on water SCADA systems", Procs. HSCC'10, April 2010, Stockholm, Sweden, ACM, 161-170.
[50] R. Chow, E. Uzun, A. A. Cardenas, Z. Song, and S. Lee, "Enhancing Cyber-Physical Security through Data Patterns", Workshop on

Foundations of Dependable and Secure Cyber-Physical Systems. Associated with CPSWeek 2011. April 11, 2011.
[51] M. Caselli, E. Zambon, and F. Kargl. "Sequence-aware intrusion detection in industrial control systems". Proceedings of the 1st ACM Workshop on Cyber-Physical System Security, ACM 2015, 13-24.
[52] R. Tan, H.H. Nguyen, E.Y.S. Foo, X. Dong, D.K.Y. Yau, Z. Kalbarczyk, R.K. Iyer, and H.B. Gooi, "Optimal false data injection attack against automatic generation control in power grids", 2016 ACM/IEEE 7th International Conference on Cyber-Physical Systems (ICCPS), DOI: 10.1109/ICCPS.2016.7479109
[53] J. Shi, J. Wan, H. Yan, and H. Suo, "A survey of cyber-physical systems", Proc. Int. Conf. on Wireless Comm. and Signal Processing, Nanjing, China, Nov.9-11, 2011
[54] A. Miller, "Trends in process control systems security", IEEE Security and Privacy, Sept./October 2005, 57-60.
[55] H.A. Rahman and K. Beznosov, "SPAPI: A security and protection architecture for physical infrastructures and its deployment strategy using wireless sensor networks", Proceedings of 10th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA 2005), Catania, Italy, 2005, 885-892
[56] Y. Tan, S. Goddard, and L.C.Perez, "A prototype architecture for cyber-physical systems", ACM Sigbed Rev., Vol. 5, No1, 2008, 1-2
[57] H.J. La and S.D. Kim, "A service-based approach to designing cyber-physical systems", Procs. 9th IEEE/ACIS Int. Conf. on Computer and Information Sci., 2010, 895-900.
[58] Microsoft Power and Utilities, Smart Energy Reference Architecture, Oct. 2009, http://www.Microsoft.com/Utilities
[59] P. Verissimo, "CRUTIAL: Towards a reference critical information infrastructure architecture", European CIIP Newsletter, May/June 2007, vol. 3, No 2, 6-8
[60] A. A. Hauge, and K. Stølen. SACS - A pattern language for safe adaptive control software. Proc. 18th Conference on Pattern Languages of Programs (PLOP'11).
[61] A. Ayoub, B.G. Kim, I. Lee, and O. Sokolsky, "A safety case pattern for model-based development approach", LNCS Volume 7226, 2012, NASA Formal methods 2012, 141-146. http://shemesh.larc.nasa.gov/nfm2012/talks/NFM2012_141_146.pdf
[62] T.J. Cockram and S.R. Lautieri, "Combining security and safety principles in practice", Procs. 2nd IET Int. Conf. on Sys. Safety, 2007, 159-164.
[63] B.H. Krogh, "Cyber Physical Systems: The Need for New Models and Design Paradigms", Presentation, CMU
[64] A. Banerjee, K.K. Venkatasubramanian,T. Mukherjee, and S.K.S. Gupta, "Ensuring safety, security, and sustainability of mission-critical cyber-physical systems", Procs. of the IEEE, vol. 100, No 1, January 2012, 283-299.
[65] M. Cardei, E. B.Fernandez, A. Sahu, and I. Cardei, "A pattern for Wireless System Architectures", Procs. of Asian PLoP 2011.
[66] "Malware infections in the control environment", ICS-CERT Monitor, Oct., Nov., Dec. 2012 http://www.us-cert.gov/control_systems/pdf/ICS-CERT_Monthly_Monitor_Oct-Dec2012.pdf
[67] D. Cofer, "Complexity-reducing design patterns for cyber-physical systems", Rockwell Int. Rept., 2011
[68] M. Sabetzadeh, S. Nejati, L. Briand, and A.H. Evensen Mills. Using SysML for Modeling of Safety-Critical Software-Hardware Interfaces: Guidelines and Industry Experience, 13th IEEE International High Assurance Systems Engineering Symposium (HASE'11), 2011.
[69] R. Akella, H. Tang, and B. M.McMillin, "Analysis of information flow security in cyber-physical systems", Int. J. of Crit. Infrastructure Protection, vol. 3, 2010, 157-173, doi:10.1016/j.ijcip.2010.09.001
[70] M. Bourrier, "The contribution of organizational design to safety", European Mgmt. J., vol. 23, No 1, 2005, 98-104.
[71] R. Alexander, T. Kelly, Z. Kurd, and J. McDermid, Safety Cases for Advanced Control Software: Safety Case Patterns, Department of Computer Science, University of York, 15th October 2007 http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA491299
[72] C. Rehn, "Software architectural tactics and patterns for safety and security", http://www.christian-rehn.de/wp-content/uploads/downloads/2010/06/seminar_safe_sec.pdf
[73] D.D. Hwang, P. Schaumont, K. Tiri, and I. Verbauwhede, "Securing embedded systems", IEEE Security and Privacy, March/April 2006, 40-49.
[74] J.F. Ruiz, R. Harjani, and A. Maña, "A security-focused engineering process for systems of embedded components", Procs. of SD4RCES'11, Naples, Italy, 2011.
[75] W. Längst , K. Knorr , H.P. Schneider, J. Schirmer , D. Kraft , and U. Kiencke, "CARTRONIC-UML Models: Basis for Partially Automated Risk Analysis in Early Development Phases", http://www-jj.cs.tu-dortmund.de/jj/organization/csduml02/24.pdf
[76] M. Mirakhori and J. Cleland-Huang: Using tactic traceability information models to reduce the risk of architectural degradation during system maintenance. ICSM 2011, 123-132
[77] M. Little, S. Shrivastava, and S. Wheater, "Another look at the middleware for dependable distributed computing", J. Internet Serv. Appl., 2011, doi 10.1007/s13174-011-0055-6
[78] T.D.Breaux and A.I. Anton, "Analyzing regulatory rules for privacy and security requirements", IEEE Trans. on Soft. Eng., vol. 34, No 1, Jan./Feb. 2008, 5-20.
[79] A. Maña, E. Damiani, S. Guergens, and G. Spanoudakis, "Extensions to pattern formats for cyber physical systems", Procs. of PLoP 2014.
[80] C. Alcaraz, G. Fernandez, and F. Carvajal, "Security aspects of SCADA and DCS", in Critical Infrastructure Protection: Information Infrastructure Models, Analysis, and Defense, Advances in Critical Infrastructure Protection: Information Infrastructure Models, Analysis, and Defense, LNCS 7130, Springer-Verlag, 120-149, 2012.
[81] H.J. Kim, Security and Vulnerability of SCADA Systems over IP-Based Wireless Sensor Networks", International Journal of Distributed Sensor Networks, Vol. 2012 (2012), Article ID 268478, http://dx.doi.org/10.1155/2012/268478
[82] A. Nicholson, S. Webber, S. Dyer, T. Patel, and H. Janicke, "SCADA security in the light of cyber-warfare", Computers & Security, vol. 31, 2012, 418-436.
[83] A. Refsdal, B. Solhaug, and K. Stolen, "Security risk analysis of system changes exemplified within the oil and gas industry domain", Int. J. on Software Tools for Technology Transfer", October 2014, DOI 10.1007/s10009-014-0351-0
[84] A.S. Uluagac, V. Subramanian, and R. Beyah, "Sensory channel threats to cyber physical systems: A wake-up call", 2014 IEEE Conf. on Comm. and Network Security, 301-309.
[85] M. Yampolskiy, P. Horvath, X.D. Koutsoukos, Y. Xue, and J. Sztipanovits, "Taxonomy for description of cross-domain attacks in CPS", Procs. HiCoNS'13, Philadelphia, PA, USA, April 2013.135-142
[86] M. VanHilst, E.B.Fernandez, and F. Braz, "A multidimensional classification for users of security patterns", Journal of Research and Practice in Information Technology, vol. 41, No 2, May 2009, 87-97.
[87] G. Sindre and L. Opdahl, "Eliciting security requirements with misuse cases". Requir. Eng., 10(1):34–44, 2005.
[88] S. Ouchani and G. Lenzini, "Attack generation by detecting attack surfaces", 5th Int. Conf. on Ambient Systems, Networks and Technologies (ANT-2014), doi:10.1016/j.procs.2014.05.457
[89] C. Alcaraz, G. Fernandez, and F. Carvajal, "Security aspets of SCADA and DCS", in Critical Infrastructure Protection: Information Infrastructure Models, Analysis, and Defense, Advances in Critical Infrastructure Protection: Information Infrastructure Models, Analysis, and Defense, LNCS 7130, Springer-Verlag, 120-149, 2012.
[90] A. Nicholson, S. Webber, S. Dyer, T. Patel, and H. Janicke, "SCADA security in the light of cyber-warfare", Computers & Security, vol. 31, 2012, 418-436.
[91] National Institute of Standards and Technology , "Framework for Improving Critical Infrastructure Cybersecurity ", Version 1.0 , February 12, 2014
[92] A. Refsdal, B. Solhaug, and K. Stolen, "Security risk analysis of system changes exemplified within the oil and gas industry domain", Int. J. on Software Tools for Technology Transfer", October 2014, DOI 10.1007/s10009-014-0351-0
[93] J.F. Ruiz, R. Harjani, A. Maña, V. Desnitsky, I. Kotenko, and A. Chechulin, "A methodology for the analysis and modeling of security threats and attacks for systems of embedded components", Procs. 20th Euromicro Int. Conf. on Parallel, Distr., and Network-based Processing, 2012, 261-268.
[94] K. Sampigethaya and R. Poovendran, "Aviation cyber-physical systems: Foundations for future aircraft and air transport", Procs. of the IEEE, vol. 101, No 8, August 2013, 1834-1855.

[95] S. Sridhar, A. Hahn, and M. Govindarasu, “Cyber-physical system security for the electric power grid”, Procs, of the IEEE, Vol. 100, No 1, Jan. 2012, 210-224.
[96] A.S. Uluagac, V. Subramanian, and R. Beyah, “Sensory channel threats to cyber physical systems: A wake-up call”, 2014 IEEE Conf. on Comm. And Network Security, 301-309.
[97] George Loukas, Cyber-physical attacks, Elsevier 2015.\
[98] J. Zalewski, S. Drager. and A.J.Komecki, “Threat modeling for security assessment in cyberphysical systems”, Procs. of CSIIRW, Oct. 30-Nov. 1, 2012, Oak Ridge, TN, USA, ACM 2012.
physical systems”, Int.J. of Critical Infrastructure Protection, August 2015.
[102] A. Wasicek, P. Derler, and E.A. Lee, “Aspect-oriented modeling of attacks in automotive cyber-physical systems”, Procs. of DAC’14, ACM, June 2014
[103] M. Yampolskiy, P. Horváth, X. D. Koutsoukos, Y. Xue, and J. Sztipanovits, “A language for describing attacks on cyber-physical systems”, International Journal of Critical Infrastructure Protection, Jan. 2015.
[104] A. Wasicek, P. Derler, and E.A. Lee, “Aspect-oriented modeling of attacks in automotive cyber-physical systems”, Procs. of DAC’14, ACM, June 2014.
[105] M. Krotofil, D. Gollmann, “Industrial control systems security: What is happening?” Procs. IEEE INDIN 2013, 664-669.
[106] E.B.Fernandez and M.M. Larrondo-Petrie, "Designing secure SCADA systems using security patterns", Procs. of the 43rd Hawaii Conf. on Systems Science, Honolulu, Jan.2010, 1-8. March http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5428672
[107] E.B.Fernandez, J. Ballesteros, A. C. Desouza-Doucet, and M.M. Larrondo-Petrie, “Security Patterns for Physical Access Control Systems”, in S. Barker and G.J. Ahn (Eds.), Data and Applications Security XXI, LNCS 4602, 259-274, Springer 2007. Procs. of the 21st Annual IFIP WG 11.3 Working Conference on Data and Applications Security, Redondo Beach, California, U.S.A, July 8-11, 2007
[108] N. Delessy, E.B.Fernandez, and M.M. Larrondo-Petrie, "A pattern language for identity management", Procs. of the 2nd IEEE Int. Multiconference on Computing in the Global Information Technology (ICCGI 2007), March 4- 9, Guadeloupe, French Caribbean.
[109] N. Delessy. E.B.Fernandez, M.M. Larrondo-Petrie, and J. Wu, "Patterns for access control in distributed systems", Procs. of the 14th Pattern Languages of Programs Conference (PLoP2007), Monticello, Illinois,
[99] M. Yampolskiy, P. Horvath, X.D. Koutsoukos, Y. Xue, J. Sztipanovits, “Systematic analysis of cyber-attacks on CPS-Evaluating applicability of DFD-based approach”, Procs. ISRCS 2012, IEEE, 55-62.
[100] M. Yampolskiy, P. Horváth, X. D. Koutsoukos, Y. Xue, J. Sztipanovits, “A language for describing attacks on cyber-physical systems”, International Journal of Critical Infrastructure Protection, Jan. 2015.
[101] Hahn, R. K. Thomas, I. Lozano, and A. Cardenas, “A multi-layered and kill-chain based security analysis framework for cyber-

USA, September 5-8, 2007,
http://hillside.net/plop/2007/index.php?nav=program
[110] F. Braz, E.B.Fernandez, and M. VanHilst, "Eliciting security requirements through misuse activities" Procs. of the 2nd Int. Workshop on Secure Systems Methodologies using Patterns (SPattern'08). In conjunction with the 4th International Conference onTrust, Privacy & Security in Digital Business (TrustBus'08), Turin, Italy, September 1-5, 2008. 328-333.
[111] E. B. Fernandez, M. VanHilst, M. M. Larrondo Petrie, S. Huang, "Defining Security Requirements through Misuse Actions", in Advanced Software Engineering: Expanding the Frontiers of Software Technology, S. F. Ochoa and G.-C. Roman (Eds.), International Federation for Information Processing, Springer, 2006, 123-137.
[112] E.B.Fernandez, G. Pernul, and M. M. Larrondo-Petrie, “Patterns and pattern diagrams for access control”, Procs. of the 5th Int. Conf. on Trust, Privacy, and Security in Digital Systems (Trustbus'08), Turin, Italy, Sept. 1-5, 2008. Springer LNCS 5185, 38-47
[113] E.B.Fernandez, “Security patterns in practice: Building secure architectures using software patterns”, Wiley Series on Software Design Patterns, 2013.
[114] E. B. Fernandez, M.M. Larrondo-Petrie, T. Sorgente, and M. VanHilst, "A methodology to develop secure systems using patterns", Chapter 5 in "*Integrating security and software engineering: Advances and future vision",* H. Mouratidis and P. Giorgini (Eds.), IDEA Press, 2006, 107-126.
[115] W. Wu, and T. Kelly, “Managing Architectural Design Decisions for Safety-Critical Software Ssytems, QoSA 2006: 59-77.
[116] E.B.Fernandez, “Threat modeling in cyber-physical systems”, *IEEE Dependable Autonomic and Secure Computing,* Aug. 8-12, 2016, Auckland, New Zealand
[117] E. Byres and J. Lowe. “The myths and facts behind cyber security risks for industrial control systems”. *Proc. of VDE Congress*, 2004.