2017 IEEE 18th International Symposium on High Assurance Systems Engineering

Integrating Six-Step Model with Information Flow Diagrams for Comprehensive Analysis of Cyber-Physical System Safety and Security

Giedre Sabaliauskaite
iTrust Center for Research in Cyber Security
Singapore University of Technology and Design
487372 Singapore
giedre@sutd.edu.sg

Sridhar Adepu
iTrust Center for Research in Cyber Security
Singapore University of Technology and Design
487372 Singapore
adepu_sridhar@mymail.sutd.edu.sg

***Abstract*—An approach for integrating Six-Step Model (SSM) with Information Flow Diagrams (IFDs) is proposed. SSM is a model for Cyber-Physical System (CPS) safety and security analysis, which incorporates six hierarchies of CPS, namely, functions, structure, failures, safety countermeasures, cyber-attacks, and security countermeasures. Relationship matrices are used in SSM to identify inter-relationships between these hierarchies and determine the effect of failures and cyber-attacks on CPSs. Although SSM is a useful tool for CPS safety and security modeling, it lacks guidance for identifying failures and attacks, and selecting adequate set of safety and security countermeasures. To address this issue, an approach for integrating SSM with IFDs is proposed and explained using the water treatment system example.**

***Keywords*-cyber-physical system; safety; security; failures; cyber-attacks; ISA-99; GTST-MLD; 3-Step Model; Six-Step Model; Information Flow Diagram**

I. Introduction

Cyber Physical Systems (CPSs) are complex engineering systems that integrate embedded computing technology into the physical phenomena. Safety and security are two crucial inter-related properties of CPSs, which are focused at protecting them from accidental faults and failures, as well as from intentional attacks [1], [2].

In our previous work [3], we proposed a Six-Step Model (SSM) for modeling and analysis of CPS safety and security. SSM incorporates six dimensions (hierarchies) of a CPS, namely, functions, structure, failures, safety countermeasures, cyber-attacks, and security countermeasures. The inter-dependencies between these dimensions are defined using a set of relationship matrices. SSM enables in-depth analysis of CPS safety and security, as it uses system functions and structure as a knowledge-base for understanding what effect the failures, cyber-attacks, and selected safety and security countermeasures might have on the system [3]. However, it does not provide guidance for identifying failures and attacks.

To address this issue, we propose an approach for integrating SSM [3] with Information Flow Diagrams (IFDs) [4], [5] – behavior diagrams, which show information flow between system elements. SSM and IFDs integration provides valuable insight into communication channel vulnerabilities in CPSs, and helps in identifying failures and attacks, and selecting adequate safety and security countermeasures. The applicability of the proposed approach is demonstrated using a CPS testbed - Secure Water Treatment (SWaT) [6] system.

Organization: The remainder of this paper is structured as follows. Preliminaries and background are described in Section II. Section III explains the proposed approach. Section IV describes an application of proposed approach to SWaT system. Finally, Section V includes a summary and conclusions from this work.

II. Preliminaries and Background

A. CPS Safety and Security

Safety and security are two key properties of CPSs. They share similar goals, i.e., protecting systems failing [2], [7]. Safety is aimed at protecting the systems from accidental failures to avoid hazards, while security focuses on protecting systems from intentional attacks. Attacks on CPS include deception (attacker tampers with system components or data), man-in-the-middle (false messages are sent to operators), and denial-of-service (attacker block the traffic of CPS) among others [8].

The effects of cyber-attack in CPSs are the following: equipment damage (physical damage of equipment of infrastructure), production damage (product is spoiled, or production cost is increased), or compliance violation (safety requirements violation, environmental pollution, etc.) [9].

Safety and security are interdependent, often complementing or conflicting each other [2], [10], [11]. In [10], Kriaa et al. presented a survey of existing approaches for design and risk assessment that consider both safety and security for industrial control system. Several approaches have been proposed so far. They are either generic, which consider both safety and security at a very high level, or model-based, which rely on a formal or semi-formal representation of functional/non-functional aspects of system [10]. However, there is still a need of knowledge-based approaches that

1530-2059/17 $31.00 © 2017 IEEE
DOI 10.1109/HASE.2017.25

provide guidance to practitioners for selecting adequate safety and security countermeasures to protect CPSs.

B. The Six-Step Model

The SSM (see Fig. 1) has been proposed in [3]. It is based on two previously developed approaches: GTST-MLD [12] and the 3-Step Model [13]. GTST-MLD is a function-centered approach for complex physical system reliability and risk analysis. It comprises of Goal Tree-Success Tree (GTST) and Master Logic Diagram (MLD). GTST is a functional hierarchy of a system organized into different levels. The role of GT is to describe system functions starting with the goal (functional objective) and then defining functions and sub-functions, needed for achieving this goal. ST is aimed at describing the structure (configuration) of the system, used to achieve functions identified in GT. Finally, MLD is used to model the interrelationships between functions (GT) and structure (ST).

Brissaud et al. [13] extended GTST-MLD by integrating faults and failures into it. A new framework was named the 3-Step Model. It allowed modeling the relationships between faults and failures, and the system functions and structure. The analysis of these relationships could be used to assess the effect of any fault or failure on any material element and/or function of the system.

Although the GTST-MLD and the 3-Step Model are useful tools for physical system safety analysis, they are not sufficient for the vulnerability analysis of a CPSs that, in addition to faults and failures, are exposed to cyber-security vulnerabilities and related threats that may compromise system safety [10], [2]. Thus, in [3] we extend the 3-Step Model [13] and proposed the SSM for integrated CPS safety and security modeling and analysis.

The SSM (see Fig. 1) is constructed using the following six steps.

Step 1: The first step of SSM includes description of system functions by constructing a GT and identifying relationships between main and supporting functions. First, GT is formed starting with the goal function at the top that is decomposed into functions, sub-functions, and basic functions. The functions are grouped into main and supporting functions. Main functions are the functions directly derived from the goal function. Supporting functions contribute to fulfilling main functions. They may provide information, control, or appropriate environment. Second, a relationship matrix MF-SF (main functions : supporting functions) is constructed to show the relationships between the main and supporting functions by drawing dotted lines between them and identifying the degree of relationship: no circle at intersection of lines - no relationship; white circle - low relationship; gray circle - medium relationship; black circle - the elements are highly related (as shown in Fig. 1).

Step 2: In the second step, the structure of the system is defined by the use of the ST, and the relationships between system structure and functions are identified. At first, system is decomposed into sub-systems and units, which are grouped into main system and supporting systems. Then, relationship matrices S-S (structure : structure) and S-F (structure : functions) are constructed. S-S shows inter-relationships among system's units, while S-F identifies relationships between structure units and functions (see Fig. 1).

Step 3: In the third step, system failures are identified and added to the model. Furthermore, the relationships between failures and system structure and functions are established. The resulting SSM at the end of step 3 includes additional relationship matrices: B-B (failures : failures), B-S (failures : structure), and B-F (failures : functions).

Step 4: In this step, safety countermeasures are added to the model and the relationships between them and the failures, as well as system structure and functions, are defined. The following additional matrices are constructed: X-X (safety countermeasures : safety countermeasures), X-B (safety countermeasures : failures), X-S (safety countermeasures : structure), and X-F (safety countermeasures : functions). Matrix X-S shows how safety countermeasures affect system structure. If safety countermeasures require the use of additional equipment, e.g., duplicated PLCs or sensors, they are added to the system structure, initially defined in step 2 of the model. Then, their relationships to other elements of the model are established.

Step 5: In this step, attacks are added to the model, and their relationships with the remaining elements identified. Attacks can be either physical or cyber. Attack trees can be used in this step for defining possible attacks on the system. Several matrices are constructed in this step: A-A (attacks : attacks), A-X (attacks : safety countermeasures), A-B (attacks : failures), A-S (attacks : structure), and A-F (attacks : functions) (see Fig. 1). Safety countermeasures, defined in step 4, can be useful for protecting the system from failures and from some of the attacks. Thus, matrix A-X is used to define the coverage of attacks by safety countermeasures. Matrix A-B shows interrelated attacks and failures, while matrices A-S and A-F identify the parts of the system and the functions, which might be affected by each attack.

Step 6: In this last step of SSM, security countermeasures are added to the model, and the relationships between them and the other elements of the model are identified, as shown in Fig. 1. The following relationship matrices are constructed: Z-Z (security countermeasures : security countermeasures), Z-A (security countermeasures : attacks), Z-X (security countermeasures : safety countermeasures), Z-B (security countermeasures : failures), Z-S (security countermeasures : structure), and Z-F (security countermeasures : functions). Matrix Z-X is crucial in the analysis of system safety and security alignment and consistency. This matrix captures the inter-dependencies between safety and security countermeasures, such as reinforcement, antagonism, condi-

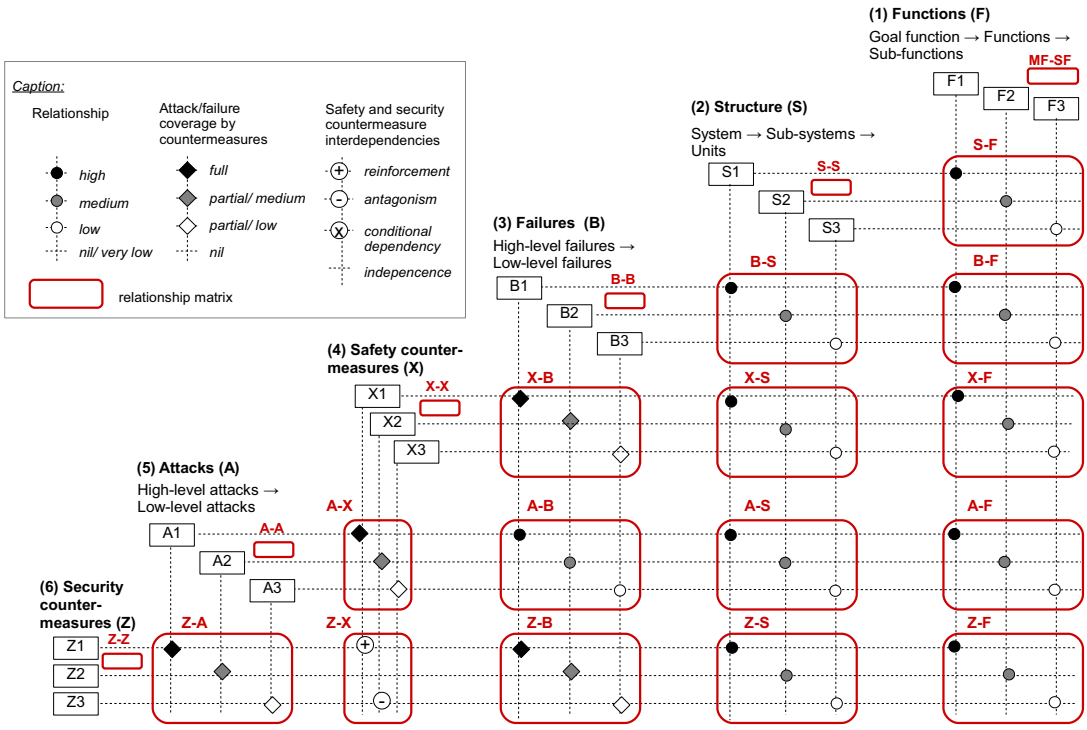

Figure 1. The Six-Step Model.

tional dependency, and independence, as defined in [14].

After completion of steps 5 and 6, it is necessary to return to steps 3 and 4 to verify if there are no changes in failures and safety countermeasures due to attacks and security countermeasures identified in these steps.

C. Information Flows in CPSs and Information Flow Diagrams

There are two types of flows in CPSs: cyber information flows (data exchange between cyber components to compute actions or responses), and physical commodity flows (physical resource flows between interconnected physical components, e.g. water, electricity or gas flows) [4]. In this paper, we focus on cyber information flows.

Communication channels are used to implement information flows. They can be either direct physical connections between system elements, or communication links through networks. Communication channels could be grouped into logical groups, called conduits, to help assess common threats, vulnerabilities, and the countermeasures needed to attain the level of security, as defined by the industrial automation and control system security standard ISA-99 [15].

IFD is a behavior diagram used for information flow modeling since as early as 1960s [5], [16]. Application of IFD for CPS analysis is described in [17], [4]. In [17], IFDs were applied for complex CPS safety analysis, specifically, for Conflict Detection and Resolution (CD&R) for airport surface traffic. IFDs of several alternative (CD&R) architectures were constructed and evaluated in order to choose the one which resolves all fault conditions. In [4], IFDs were used for CPS confidentiality analysis, where authors proposed a formal method that expressed the information flow security semantics in CPSs.

We propose to extend IFDs to enable comprehensive CPS safety and security analysis (see Section III-B).

D. The SWaT System

The Secure Water Treatment (SWaT) testbed [6] is used in this paper to demonstrate the applicability of the proposed approach. SWaT is an operational scaled down water treatment plant. In a small footprint producing 5-gallons/minute

of doubly filtered water, this testbed mimics large modern plants for water treatment such as those found in cities. It consists of the following six main sub-processes, labeled P1 through P6.

P1 (supply and storage) supplies water to the water treatment system. In P2 (pre-treatment), the water from tank in P1 is pumped via a chemical dosing station to the ultra-filtration feed tank in process P3. P3 (Ultra Filtration (UF)), is used to remove water solids by using fine filtration membranes. P4 is the de-chlorination process, where any free chlorine in water is converted to harmless chlorides through the ultraviolet chlorine destruction unit and by dosing a solution of sodium bisulphite. P5 (Reverse Osmosis (RO) process is designed to reduce inorganic impurities by pumping the water with high pressure through semipermeable membranes. Finally, P6 is the process of RO permeate transfer, backwash and cleaning. The filtered water from the RO process is stored in raw permeate tank and then transferred to the raw water tank in process P1 for reuse. Sub-process P6 controls the cleaning of membranes in the UF unit in P3 by turning on or off the UF backwash pump.

Currently, the network architecture of SWaT is organized into two layers labeled L0 and L1. Each of the six processes P1-P6 contains sensors and actuators, and is controlled by a Programmable Logic Controller (PLC). The physical process is manipulated by distributed actuators and measured by sensors. Remote Input/Output (RIO) units associated with each PLC convert the analog signals from sensors into digital form that are sent to PLCs via the L0 network. PLCs communicate with each other, and with centralized Supervisory Control and Data Acquisition (SCADA) system and Human-Machine Interface (HMI), through the L1 network.

III. Integration of Six-Step Model with Information-Flow Diagrams

A. Potential Benefits of SSM and IFD Integration

CPS cyber components exchange information, as described in Section II-C. This information exchange is depicted in the SSM by the use of relationships and degree of relationships, as described in Section II-B.

Although SSM shows information flows, it does not provide any additional details of the flows, and does not help to answer the the following questions:

- What information is being exchanged (*contents*)?
- Which unit is sending, and which one is receiving the information (*direction*)?
- How often is the information sent/received (*frequency*)?

This information is crucial for performing a comprehensive safety and security analysis. For example, to analyze vulnerabilities of CPSs to false or missing data, it is important to know flow contents and direction; for analyzing the effect of stale data - frequency [18].

This information could be captured in extended IFDs, as described in Section III-B. Furthermore, the integration of extended IFDs with the SSM could provide valuable insight into communication channel vulnerabilities and help in selecting safety and security countermeasures.

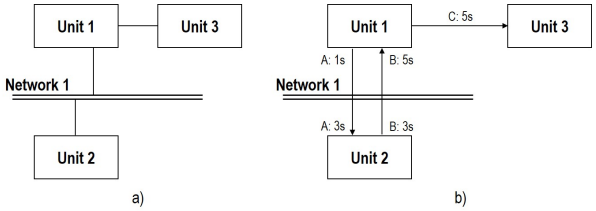

Figure 2. Information flow diagram (IFD): a) IFD framework generated from the SSM; b) refined IFD.

Information flow frequency data can be also used to improve the system design. For instance, if two units exchange information through the network, and the receiving unit is reading information from the network more frequently than the information is being sent to the network, it is overworking. IFDs will help to identify such inconsistencies and optimize system design.

The following sub-section describe the extended IFDs (Section III-B) and and approach for integrating SSM and IFDs (Section III-C).

B. Extended IFDs

Typically, IFD include two types of elements: units and information flows between them [5] (see Fig. 2.a)). To enable integration of SSM and IFD, we extend IFD by adding CPS-relevant elements and attributes. The following three types of elements are used in extended IFD (see Fig. 2.b)):

- Unit (denoted by a rectangle) - system unit, which sends or receives information to/from another unit;
- Network (denoted by double line) - network, used for communication between units;
- Information flow (denoted by an arrow) - information flow between units, which has two attributes: contents (information transmitted) and transmission frequency. If two units communicate through a network, two information flow frequencies are identified, as they might differ: the frequency of sending information by source unit, and the frequency of receiving information by destination unit.

IFD example, shown in Fig. 2.b), includes three units, three information flows, and one network. Units 1 and 3 are connected through information flow C, which is sent from unit 1 to unit 3 every 5 seconds. Units 1 and 2 exchange information through network 1: information A is sent from unit 1 to unit 2 every second, and received by unit 2 every 3 seconds; information B is sent by unit 2 every 3 seconds, and received by unit 1 every 5 seconds.

IFD construction consists of the following two phases:

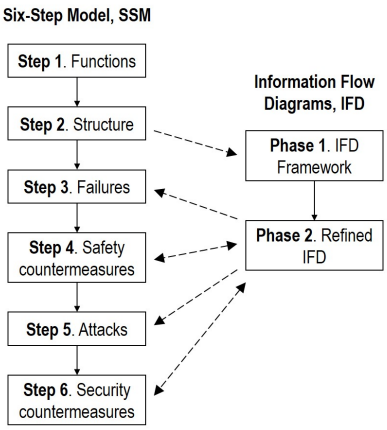

Figure 3. Integration of SSM steps with IFD phases.

Phase 1: construction of IFD framework. In this phase, IFD framework is constructed, which includes system units and their connections, as shown in Fig. 2.a). Framework is constructed using the knowledge of system's structure and interconnections between its units. In our approach, IFD framework is extracted from SSM, as described in Section III-C.

Phase 2: IFD refinement. In this phase, IFD framework is refined and an extended IFD is constructed by converting connections into information flows, and adding flow direction, contents, and transmission frequency, as shown in Fig. 2.b).

C. The SSM and IFD Integration Approach

The six steps of SSM development process and two phases of IFD construction process can be integrated in the following way, as shown in Fig. 3.

First, SSM development steps 1 and 2 are performed and system functions and structure are defined. At the end of SSM step 2, SSM includes all CPS functions, units, and their relationship.

Next, IFD development phase 1 is performed, during which IFD framework is constructed by extracting units and their connection from the SSM in the following way: interrelated network and control sub-system units from SSM become units in IFD framework, while their relationships from S-S matrix in SSM are transformed into connections in IFD framework (see Fig. 2.a)).

Then, IFD development phase 2 is performed, during which IFD framework is refined and transformed into extended IFD, as shown in Fig. 2.b).

Finally, SSM development steps 3 - 6 are performed, where IFDs are used to help in identifying possible information flow failures and cyber-attacks, and selecting adequate safety and security countermeasures in the following way:

- CPS failures are identified in SSM step 3. Information flow failures may affect exchange of data in CPS, as the missing or incorrect data may lead to incorrect actions and responses. IFDs could be used to identify these failures, which should be then added to SSM, and their relationships with system structure and functions should be analyzed.
- In SSM step 4, IFDs could be used for designing safety countermeasures. By knowing what information should be sent/received and how frequently to enable safe CPS operation (from IFDs), safety analysts will be able to select adequate safety countermeasures to withstand information flow failures, and add them to SSM. If safety countermeasures require additional information flows, these flows should be added to IFDs to analyze their relation to other information flows in the system.
- Attacks are identified in SSM step 5. Cyber-attacks on information flows could affect information contents (false information is received) as well as frequency (it is received too late, or not received at all). IFDs can be used to identify possible attacks on individual information flows as well as their groups (e.g. all information flow that use the same network for communication). These attacks should be added to SSM and their relationships with other elements of the model should be analyzed. As mentioned in Section II-C, ISA-99 standard recommends grouping communication channels to help assess common vulnerabilities. Extended IFDs could help to implement this standard.
- IFDs could be used for designing security countermeasures to achieve required level of security. Security countermeasures, identified in SSM step 6, often require to use additional information flows. These flows should be added to IFDs to investigate their consistency with existing information flows in CPS.

For more details, see SWaT system example in Section IV.

IV. SWaT System Example

A. SWaT System SSM Steps 1 and 2

SWaT system consists of six main sub-systems that correspond to processes P1-P6, as described in Section II-D. There are three supporting sub-systems in SWaT: control, power supply, and network (see Fig. 4). Control sub-system can be further decomposed into supervisory and process control sub-systems. Supervisor control comprises of SCADA and HMI. Processes P1-P6 have their control sub-systems, which include PLCs, RIOs, sensors, and actuators. Power supply sub-system consists of three phase power supply to distribution board from outside plant, from which power is supplied to each PLC panel, and from there it is supplied to all the devices, sensors and communication switches. Finally, network sub-system comprises L0-L1 network sub-systems and their components.

Due to space limitations, we chose one SWaT process, P1, to illustrate the proposed approach. P1 is the first process of SWaT, which supplies system with the raw water.

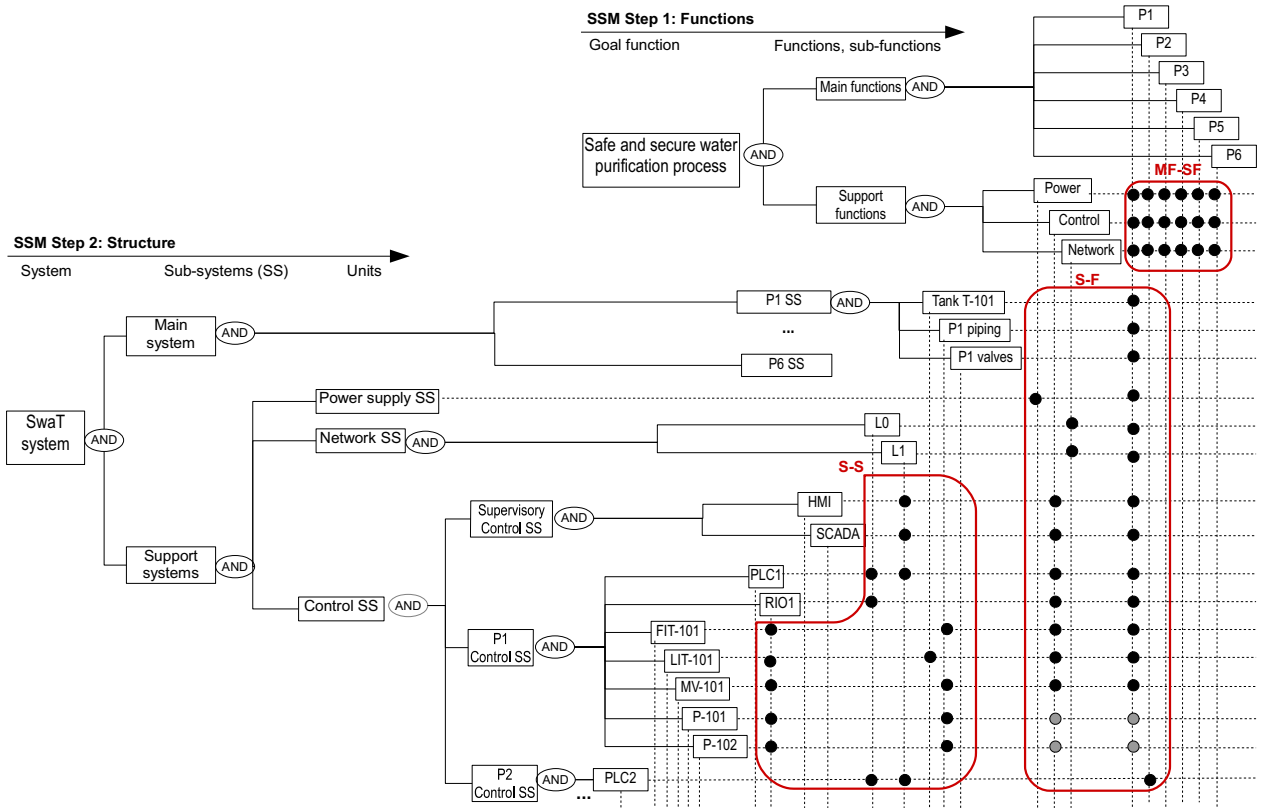

Figure 4. An extract from the Six-Step Model of SWaT system.

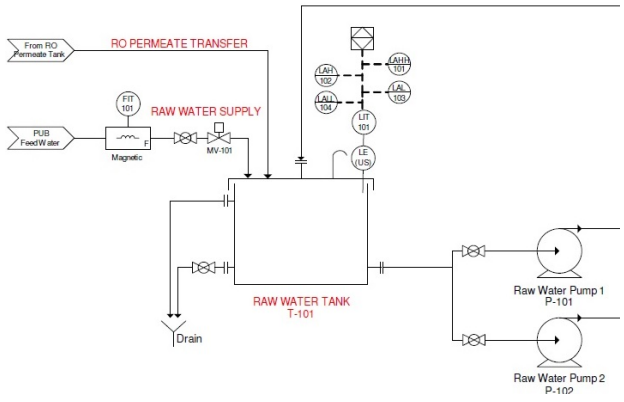

Figure 5. Process P1 piping and instrumentation diagram [6].

The piping and instrumentation diagram of process P1 is shown in Fig. 5. As we can see from Fig. 5, raw water tank (T-101) is the main element of P1 along with pipes and several manual valves. In addition, there are several sensors and actuators. Sensor FIT-101 is used to measure water flow (m3/hour), while LIT-101 - to measure water level in tank T-101 (mm). MV-101 is an actuator - a motorized valve to control water flow into the tank (can be either open or closed). Furthermore, two pumps, P-101 and P-102, are used to control water flow out of the tank (can be either on or off). Pumps are duplicated (one is on duty and one standby) for safety reasons: if the first pump fails or water flow is insufficient, the second one is activated.

Sensors and actuators are connected to RIO1, which provides interface between them and PLC, as described in Section II-D. Process P1 is controlled by PLC1, which sends control inputs to RIO through network L0. Furthermore, PLC1 exchanges information with supervisory control elements HMI and SCADA, and controllers of other processes (e.g. P2) through network L1.

An extract from SWaT system's SSM, which includes functions, structure, and corresponding relationship matrices of process P1 is shown in Fig. 4. As we can see from Fig. 4, SWaT goal function ("safe and secure water purification

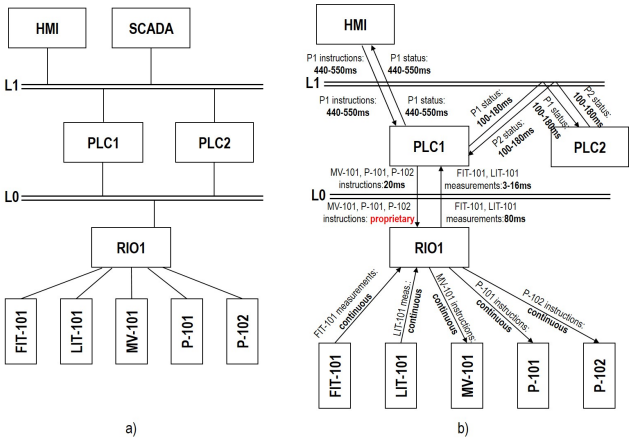

Figure 6. SWaT process P1 information flow diagram: a) IFD framework; b) refined IFD.

process") is decomposed into main and support functions, and relationships between these functions are identified in matrix MF-SF. Furthermore, SWaT system is decomposed into main and support sub-systems and units, and relationships between different units are identified in matrix S-S, while the relationships between units and functions – in matrix S-F.

B. Construction of IFD of SWaT System

To construct IFD framework, we extract control and network sub-system units from the SSM, and their interconnections from the SSM relationship matrix S-S (see Fig. 4). The resulting framework is shown in Fig. 6.a), which includes sensors, actuators, RIO, PLCs, HMI, SCADA, networks L0 and L1, and their inter-connections.

The IFD framework of process P1 is then refined with the help of system designers. First, the connections between units are analyzed, and information flows and their directions are established. E.g. RIO1, PLC1 and PLC2 are connected to network L0, as shown in Fig. 6.a). However, it is not clear if there are information flows between all units. Further analysis reveals that there are two information flows between RIO1 and PLC1, however there are no flows between RIO1 and PLC2, and PLC1 and SCADA (see Fig. 6.b)).

Then, information flow contents and frequencies are added to IFD. As we can see from Fig. 6.b), information flow frequencies between units are different, e.g. flow between sensors, actuators, and RIO1 is continuous, while between PLCs – every 100-180ms, and between PLC1 and HMI – every 450-550ms. Flow frequencies between PLC1 and RIO1 vary: RIO1 send information to L0 every 80ms, while PLC1 reads it every execution cycle, i.e. every 3-16ms; PLC1 sends instructions to L0 every 20ms (see Fig. 6.b)). The frequency of the flow between L0 and RIO1 is unknown, as it is proprietary information not provided by RIO supplier.

As we can see from Fig. 6.b), PLC1 reads information from network L0 more frequently (every 3-16ms) than RIO1 sends it to the network (every 80ms). System designers could consider reducing the PLC1 reading frequency to match sending frequency to optimize system design.

C. SWaT System SSM Steps 3 – 6

1) IFDs in SSM step 3 (failures): SWaT failures include main system element failures, such as pipe, tank, or filter failures, and the supporting component failures, such as of PLC, sensor, actuator failures. These failures can be derived from system structure, defined in step 2 of SSM. However, SSM is not sufficient for deriving all communication channel failures, as the model lacks details of information flows. Extended IFDs can be used for this purpose. For example, if PLC1 fails to read information from network L0, IFD (see Fig. 6.b)) will help in identifying the exact information that is be lost, and identifying related failures and consequences.

2) IFDs in SSM step 4 (safety countermeasures): IFDs could aid in selecting a sufficient set safety countermeasures to achieve required level of safety in SWaT. These countermeasures include precautions for for fire, flooding, water leakage, electrical shock, injury and chemical exposure. There are hardware (PLC duplication, IP cameras to monitor the plant; overflow pipe associated with each tank; etc.) and software related countermeasures (encoded in the PLC logic to provide safety to specific components). If safety countermeasures require the use of additional information flows, these flows should be added to IFDs.

3) IFDs in SSM step 5 (attacks): There could be numerous cyber-attacks on the SWaT system, such as attacks on the communication channels between sensors to PLC, PLC to PLC, PLC to actuators, and PLC to HMI; firmware attacks such as attacks on PLC or sensor firmware. Cyber-attacks could tamper with information contents and/or flow frequency. Extended IFDs can be used for analyzing vulnerabilities of SWaT to different types of attacks, and particularly identifying attacks, that could effect system safety. These should be added to SSM, and their relationships with other elements of the model should be identified.

4) IFDs in SSM step 6 (security countermeasures): Various security countermeasures can be implemented in SWaT, such as access control mechanism to protect from unauthorized intrusion, and different intrusion detection and response to attacks mechanisms (such as e.g. [19]). For example, if the information flow between RIO1 and PLC1 (see Fig. 6.b)) is attacked and sensor readings are corrupted, they could be replaced by estimated values computed using historical data, or additional sensors could be used to collect measurements. Additional information flows, used by security countermeasures, should be added to IFDs to analyze their relationships to other information flows in SWaT.

V. Summary and Conclusions

In this paper, Extended IFDs and an approach for integrating SSM with IFDs to enable comprehensive CPS safety and security analysis are proposed.

Extended IFDs are particularly useful for analyzing CPS communication channel vulnerabilities, as they provide valuable insight on information flow contents, direction and frequency.

The integration of extended IFDs with the SSM provides guidance for identifying possible failures and cyber-attacks, and selecting safety and security countermeasures. Furthermore, it could be used for implementing ISA-99 standard.

Moreover, extended IFDs could be used for analyzing information flow inconsistencies and improving system design.

The applicability of the proposed approach is explained using the SWaT system example.

Future work will include refinement of the proposed approach and its application to different types of CPSs. Furthermore, we will investigate the possibility to integrate physical resource flow models with SSM and IFDs.

Acknowledgment

This work was supported by research grant from the iTrust Centre for Research in Cyber Security at the Singapore University of Technology and Design.

References

[1] G. Sabaliauskaite and A. P. Mathur, "Aligning cyber-physical system safety and security," in *Proceedings of the 1st Asia-Pacific Conference on Complex Systems Design & Management (CSD&M Asia 2014)*, 2014, pp. 41–53.

[2] A. J. Kornecki, N. Subramanian, and J. Zalewski, "Studying interrelationships of safety and security for software assurance in cyber-physical systems: Approach based on bayesian belief networks," in *Computer Science and Information Systems (FedCSIS), 2013 Federated Conference on*. IEEE, 2013, pp. 1393–1399.

[3] G. Sabaliauskaite, S. Adepu, and A. Mathur, "A six-step model for safety and security analysis of cyber-physical systems," in *The 11th International Conference on Critical Information Infrastructures Security (in Press),*, October, 2016.

[4] R. Akella, H. Tang, and B. M. McMillin, "Analysis of information flow security in cyber-physical systems," *International Journal of Critical Infrastructure Protection*, vol. 3, no. 3-4, pp. 157 – 173, 2010.

[5] L. Moonen and A. R. Yazdanshenas, "Analyzing and visualizing information flow in heterogeneous component-based software systems," *Information and Software Technology*, vol. 77, pp. 34 – 55, 2016.

[6] "SWaT: Secure Water Treatment Testbed," 2015, http://itrust.sutd.edu.sg/research/testbeds/ .

[7] T. Novak and A. Treytl, "Functional safety and system security in automation systems-a life cycle model," in *Emerging Technologies and Factory Automation, 2008. ETFA 2008. IEEE International Conference on*. IEEE, 2008, pp. 311–318.

[8] T. Lu, J. Zhao, L. Zhao, Y. Li, and X. Zhang, "Towards a framework for assuring cyber physical system security," *International Journal of Security and Its Applications*, vol. 9, no. 3, pp. 25–40, 2015.

[9] D. Gollmann, P. Gurikov, A. Isakov, M. Krotofil, J. Larsen, and A. Winnicki, "Cyber-physical systems security: Experimental analysis of a vinyl acetate monomer plant," in *Proceedings of the 1st ACM Workshop on Cyber-Physical System Security*, ser. CPSS '15. New York, NY, USA: ACM, 2015, pp. 1–12.

[10] S. Kriaa, L. Pietre-Cambacedes, M. Bouissou, and Y. Halgand, "A survey of approaches combining safety and security for industrial control systems," *Reliability Engineering & System Safety*, vol. 139, pp. 156–178, 2015.

[11] L. Piètre-Cambacédès and M. Bouissou, "Cross-fertilization between safety and security engineering," *Reliability Engineering & System Safety*, vol. 110, pp. 110–126, 2013.

[12] M. Modarres and S. W. Cheon, "Function-centered modeling of engineering systems using the goal tree–success tree technique and functional primitives," *Reliability Engineering & System Safety*, vol. 64, no. 2, pp. 181–200, 1999.

[13] F. Brissaud, A. Barros, C. Bérenguer, and D. Charpentier, "Reliability study of an intelligent transmitter," in *15th ISSAT International Conference on Reliability and Quality in Design*. International Society of Science and Applied Technologies, 2009, pp. 224–233.

[14] L. Piètre-Cambacédès and M. Bouissou, "Modeling safety and security interdependencies with bdmp (boolean logic driven markov processes)," in *Systems Man and Cybernetics (SMC), 2010 IEEE International Conference on*. IEEE, 2010, pp. 2852–2861.

[15] "ANSI/ISA-99-00-01-2007. security for industrial automation and control systems. part 1: Terminology, concepts, and models."

[16] H. Marko, "Information theory and cybernetics," *IEEE Spectrum*, vol. 4, no. 11, pp. 75–83, Nov 1967.

[17] F. Saunders, J. Rife, S. Vaddi, and V. Cheng, "Information flow diagram analysis of a model cyber-physical system: Conflict detection and resolution for airport surface traffic," *IEEE Aerospace and Electronic Systems Magazine*, vol. 28, no. 12, pp. 26–35, Dec 2013.

[18] M. Krotofil, A. Cardenas, J. Larsen, and D. Gollmann, "Vulnerabilities of cyber-physical systems to stale data - determining the optimal time to launch attacks," *International Journal of Critical Infrastructure Protection*, vol. 7, no. 4, pp. 213 – 232, 2014.

[19] S. Adepu and A. Mathur, "Distributed detection of single-stage multipoint cyber attacks in a water treatment plant," in *the 11th ACM Asia Conference on Computer and Communications Security (in Press),*, May, 2016.