Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/IJCIP

A contribution of axiomatic design principles to the analysis and impact of attacks on critical infrastructures

Venkata Reddy Palleti[a,*], *Jude Victor Joseph*[b], *Arlindo Silva*[c]

[a] *iTrust Center for Research in Cyber Security, Singapore University of Technology and Design, Singapore*
[b] *Department of Mechanical Engineering, Universiti Tenaga Nasional, Malaysia*
[c] *SUTD-MIT International Design Center, Engineering Product Development Pillar, Singapore University of Technology and Design, Singapore*

ARTICLE INFO

Article history:
Received 23 April 2018
Accepted 3 August 2018
Available online 27 August 2018

Keywords:
Modeling
Critical infrastructures
Axiomatic design theory principles
Attacks
Security of critical infrastructures

ABSTRACT

Critical infrastructures (CIs) such as water, power, and transportation etc. are pivotal as they play a significant role in a nation's economic prosperity and governance. These critical infrastructures are complex in nature and therefore they may be vulnerable to attacks. In order to have effective critical infrastructure protection, it is necessary to develop models for CIs. Further, one can use these models for system security analysis and assess the impact on CIs when they are under attacks. In this work, axiomatic design theory principles from systems design are used to model CIs. This modeling provides an abstract representation of critical infrastructures to understand their behavior under potential attacks. Through a case study, we will show how one can assess the detection of attacks and vulnerabilities using axiomatic design principles. A realistic water distribution testbed is used for the purpose of studying the impact of attacks using axiomatic design principles.

1. Introduction

A critical infrastructure consists of systems, assets and networks, whether physical or virtual and it plays an important role in any nation's economy. Any disruption in critical infrastructures affects nations economy, public health, safety or any combination thereof. The Department of Homeland Security (DHS) identifies 16 major critical infrastructures which have a significant contribution to US economy [27]. Among those 16 CIs, water, energy and transportation systems are extremely important as they make human life better and easier. The modern CIs such as energy generation systems, electrical distribution, transportation systems, water treatment plant and water distribution networks are monitored and controlled by cyber components which include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCSs) and communication. Hence, one can treat these types of critical infrastructures as cyber-physical systems (CPSs). In these systems cyber components and physical components such as sensors and actuators tightly interact with each other. Moreover, these systems are vulnerable to attacks and are potential targets for attackers. The attackers can target cyber components which may disrupt the physical process and vice-versa.

The impact of terrorist attacks on September 11, 2001 dramatically underscored the fragility of the critical infrastructure and its importance to modern society [25]. In August 2003,

[*] Corresponding author.
E-mail address: venkata_palleti@sutd.edu.sg (V.R. Palleti).

https://doi.org/10.1016/j.ijcip.2018.08.007
1874-5482/© 2018 Elsevier B.V. All rights reserved.

more than 50 million people in eight states of the US and one Canadian province were left without power due to a large scale failure of power lines [26]. Several attacks on water distribution systems have been reported in recent years. The modern water distribution networks in particular are more vulnerable to a variety of natural and human-caused threats. These networks are vulnerable to a variety of attacks which include physical disruption, contamination, and cyber attack. Kemuri Water Company(KWC)[1], reported in mid-2016, was in the news for many days. In this attack hackers changed the chemicals used to treat tap water. Hackers entered exploiting unpatched web services. The same hack also resulted in the exposure of personal information of the utility's 2.5 million customers. Therefore, it is very important to protect these infrastructures from such kind of attacks. Further, it is also necessary to develop methodologies and models for CIs which can analyze the dependencies within and interdependencies across CIs.

In this paper, we model a critical infrastructure which can be used to analyze the dependencies within the system. Further, these models can be used to verify at an early stage of design, how the system will perform, without the full model of the system. This simplified dependency model based on axiomatic design principles, allows the designer to almost immediately find system vulnerabilities without complicated mathematical manipulations. This, coupled with an overall view of the system, makes this method particularly easy and powerful at an early stage of design, where changes to the system architecture (for security risk mitigation) can still be done at no, or limited extra cost.

2. Related work

The study of interdependency within and among CIs is an emerging research field. The attempts to model and simulate CIs can be divided into six major groups [29], they are: empirical approaches, agent based approaches, system dynamics based approaches, economic theory based approaches and network based approaches. The empirical approaches analyze historical accidental data or disaster data in order to identify the interdependencies in CIs. [8] and [26] developed a systematic database to understand the societal impacts of infrastructure failure interdependencies (IFIs) which are characterized by an impact index (as the product of the failure duration and severity weights) and an extent index (as the product of the failure spatial extent and number of people affected). These database systems were applied on the 2003 blackout (affecting the northeastern U.S. and eastern Canada), the 1998 Quebec ice storm, and three 2004 Florida hurricanes. In addition to these, [11,12] developed risk analysis models, and [16] used statistical methods to directly draw conclusions from large data sets and provide important support for risk management both immediately before extreme events and over the longer term.

Mathematical methods such as agent based modeling, input-output model, network or graph based models are used to analyze and simulate infrastructure interdependencies. CIs are usually considered complex adaptive systems (CASs) due to their intrinsic complex nature and decision-making process [3]. One of the effective ways to analyze CAS is through agent based approaches, which adopt a bottom-up method. Most CIs can be viewed as agents. Components in a CI (such as reservoirs or tanks in water distribution networks) are represented by individual agents, and a set of rules is defined to frame the interactions between agents. These agent based models can be used to model and simulate various infrastructures and social systems. Sandia National Laboratories developed the first agent-based model [5] to simulate the behavior of economic decision makers individually. Later, Barton et al. [4] modified these models to simulate the interdependent effects of power outages on other critical infrastructures. Further, CIs such as telecommunication, banking and finance are considered by Barton et al. [4] to study the interdependencies within and across CIs. Further, Kelic et al. [20] were proposed various methods to investigate the cyber and physical interdependencies.

Inoperability input–output models analyze how attacks on one critical infrastructure propagate to critical infrastructures through the exchange of input–output products that link them. Wassily Leontief proposed the input-output economic model [23] represented in Eq. (1).

$$x = Ax + c \iff x_i = \sum_j a_{ij} + c_i \forall i, \tag{1}$$

The term x_i refers to the total production output from the industry i, the Leontief technical coefficient a_{ij} is the ratio of inputs of industry i to industry j in terms of the total production requirements of the industry j, the notation c_i represents the industry i's total output for final consumption by end-users. This equation on critical infrastructures can be interpreted as the risk of inoperability which is defined as the inability of a CI to perform intended functions. The first interpreted model on CIs based on Eq. (1) was used by Haimes and Jiang [19]. In this model, x_i is the overall risk of inoperability of the ith infrastructure that can be triggered by malicious attacks or accidental disturbances, a_{ij} is the probability of inoperability that the jth infrastructure contributed to the ith infrastructure due to their interconnectedness. c_i is the additional risk of inoperability that is inherent in the complexity of the ith infrastructure. Therefore, for a given attack on one infrastructure, this model can estimate the propagation of these attacks on other critical infrastructures. Later, Refs. [18,32] extended these models to assess infrastructure interdependencies.

In network based approaches, CIs can be represented as a graph $G = (V, E)$ in which nodes Vare used to represent components of CIs and edges (E) represent connectivity between these nodes. Further, these network models are classified as topology-based methods and flow-based methods. Topology-based methods model CIs only on their topology by considering two discrete states (failed or normal) for each node or link. The failure of the nodes can be modeled directly from the attacks, disconnections between the nodes or failure

[1] http://www.securityweek.com/attackers-alter-water-treatment-systems-utility-hack-report.

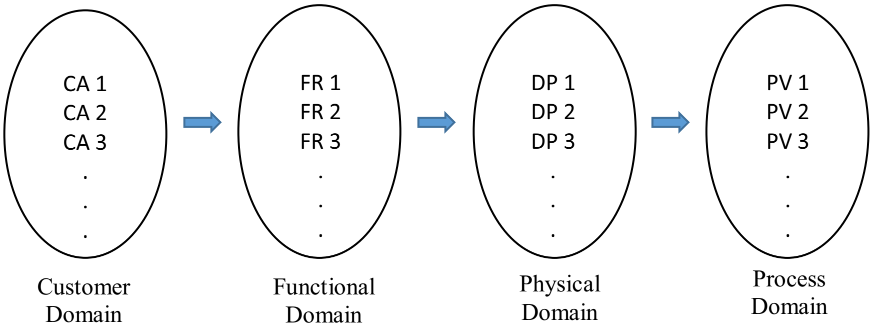

Fig. 1 – Overview of the domains in axiomatic design.

of the nodes. Topology-based methods are assessed by analytical methods [6,7,30] or simulation methods [1,10] to study the interdependent CIs. In contrast to the topology-based methods, the flow-based methods take account of the service or commodity made and delivered by the CIs. [22] represented CIs and their dependencies and interdependencies as network flow mathematical models. In their model, the movement of commodities correspond to flows, and the services correspond to a particular level of service. Further, Refs. [36–38] modeled CI components using a set of response functions which can incorporate the productions and consumptions in some CIs. [33] presented an efficient risk mitigation strategy by exploring the relation between dependency risk paths and graph centrality characteristics. Recent studies include: use of interdependent matrices to mitigate attacks on critical infrastructures [31], design of resilient infrastructures [14] and a methodology for modeling and measuring interdependencies within public administration and eGovernment services [28].

Apart from these approaches, there exist other approaches to model and analyze the CIs. These include, Petri-net (PN) based methods [21,24,35] dynamic control theory [13,15], Bayesian network based methods [17] etc. The approach proposed in this paper departs from those described above in that it does not require a detailed mathematical description of the system. In this paper, we use axiomatic design theory principles to model a critical infrastructure. Axiomatic design principles have been used in many situations, but the approach followed in the current paper appears to be novel. It starts with functional requirements and defines the design parameters that meet those functional requirements. The design parameters represent the cyber-physical system components, and the process of defining these parameters automatically sets their inter-relations. Design principles, used in this way, can help streamline the detection of potential attacks and analyze the impact of real attacks in a cyber- physical system.

The remainder of the paper is organized as follows. Section 3 explains the axiomatic design principles; Section 4 discusses the architecture and operation of a Water Distribution (WADI) System; Section 5 presents the modeling of the second stage of the WADI system using axiomatic design principles. Sections 5.1 and 5.2 discuss the derivation and use of a security check table for single and double attack points. Finally, conclusions and future research directions are discussed in Section 6.

3. Axiomatic design principles

Axiomatic design is a systems design methodology developed by Nam Pyo Suh at the Mechanical Engineering Department at MIT (Chapter 1 of [34]). It was first published in 1978 and derives its name from the use of design axioms-laws for which there is no proof, but also no counter-proof - governing the analysis and decision-making process in the design of high quality products or systems.

The objective of using axiomatic design for a system design is to create a scientific base for the design and to enhance design activities by providing an understanding of solid foundation based theories from logical and rational thinking process and tools. The system design is based on four domains that consist of, in the design world: the customer domain, the functional domain, the physical domain and the process domain (see Fig. 1). The customer domain is classified as the needs of the customer for the system. In the functional domain, the customer needs are then specified in terms of Functional Requirements (FRs) and Constraints (Cs). The physical domain is where Design Parameters (DPs) are devised to suit the specified FRs. Finally, the process domain represents the process development of the system based on the DPs formed in the physical domain. Fig. 1 shows the schematic representation of the four domains.

The functional requirements (FRs) refer to what the customers want to achieve with the system or what is the main goal of the design. The design parameters (DPs) describe how to fulfill the functional requirements. The relationships across adjacent domains are established with equations relating their components, which lend themselves to a matrix-like representation. The second fundamental concept of axiomatic design is the two axioms for which this method is named. They are formally defined as follows:

- Independence axiom
- Information axiom

The independence axiom states that the independence of the functional requirements should be preserved. When

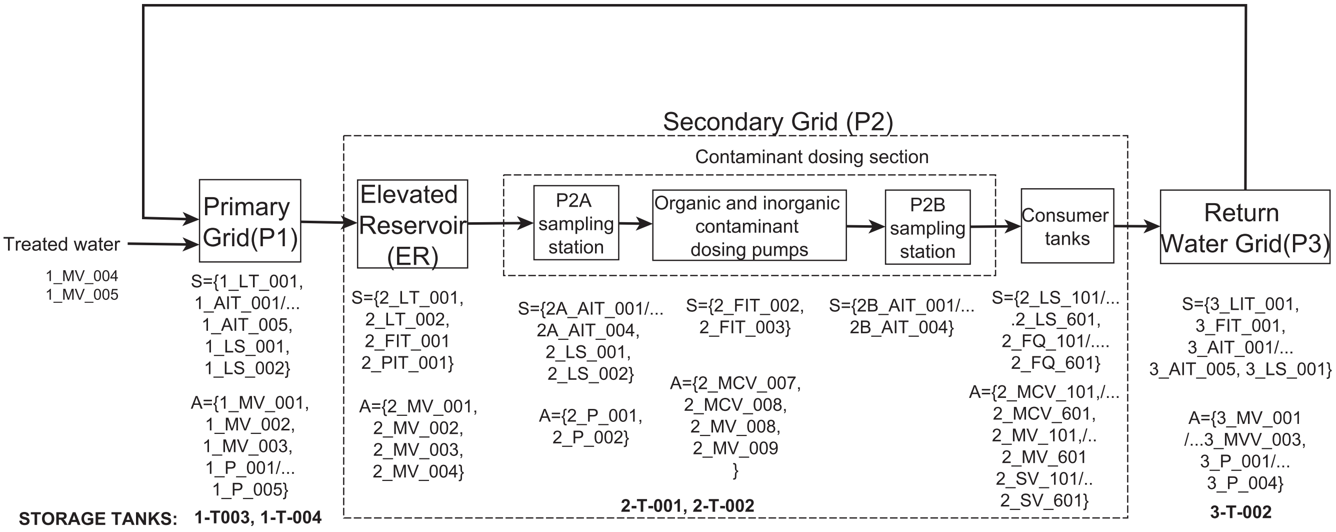
Secondary Grid (P2)
Contaminant dosing section
Treated water
1_MV_004
1_MV_005
Primary Grid(P1)
Elevated Reservoir (ER)
P2A sampling station
Organic and inorganic contaminant dosing pumps
P2B sampling station
Consumer tanks
Return Water Grid(P3)
S={1_LT_001, 1_AIT_001/... 1_AIT_005, 1_LS_001, 1_LS_002}
A={1_MV_001, 1_MV_002, 1_MV_003, 1_P_001/... 1_P_005}
S={2_LT_001, 2_LT_002, 2_FIT_001 2_PIT_001}
A={2_MV_001, 2_MV_002, 2_MV_003, 2_MV_004}
S={2A_AIT_001/... 2A_AIT_004, 2_LS_001, 2_LS_002}
A={2_P_001, 2_P_002}
S={2_FIT_002, 2_FIT_003}
A={2_MCV_007, 2_MCV_008, 2_MV_008, 2_MV_009 }
S={2B_AIT_001/... 2B_AIT_004}
S={2_LS_101/... .2_LS_601, 2_FQ_101/.... 2_FQ_601}
A={2_MCV_101,/... 2_MCV_601, 2_MV_101,/.. 2_MV_601 2_SV_101/.. 2_SV_601}
S={3_LIT_001, 3_FIT_001, 3_AIT_001/... 3_AIT_005, 3_LS_001}
A={3_MV_001 /...3_MVV_003, 3_P_001/... 3_P_004}
STORAGE TANKS: 1-T003, 1-T-004
2-T-001, 2-T-002
3-T-002

Fig. 2 – Three stages in WADI are shown. Solid arrows indicate flow of water and sequence of processes. S and A represent, respectively, sets of sensors and actuators. Sensors: LT-Level Transmitter, AIT-Analyzer Indication Transmitter, FIT-Flow Indication Transmitter, PIT-Pressure Indication Transmitter, LS-Level Switch. Actuators: P-Pump, MV-Motorized valve, MCV-Modulating Control Valve, SV-Solenoid Valve. Tag name of the instrument is indicated as XXX_YYY_ZZZ, where XXX, YYY and YYY represent stage number, instrument type and instrument index, respectively. For example, 1_LT_001 can be read as stage-P1, level transmitter and the index of level transmitter.

multiple FRs exist, the solution of the design should to be in a way where each FR is satisfied without affecting the other FRs. When this statement is achieved, an uncoupled design matrix is formed (see Eq. (2)). This matrix is diagonal which shows that each FR only corresponds to one DP.

$$\begin{pmatrix} FR1 \\ FR2 \end{pmatrix} = \begin{pmatrix} X & 0 \\ 0 & X \end{pmatrix} \begin{pmatrix} DP1 \\ DP2 \end{pmatrix} \tag{2}$$

In the above matrix, X indicates that there exists some relation between FRs and corresponding DPs and 0 indicates no relation between them. If this independence cannot be achieved, two possibilities arise. The first possibility is a decoupled design matrix. This will give a partially filled matrix where there are non-zero off-axis terms, as in Eq. (3).

$$\begin{pmatrix} FR1 \\ FR2 \end{pmatrix} = \begin{pmatrix} X & 0 \\ X & X \end{pmatrix} \begin{pmatrix} DP1 \\ DP2 \end{pmatrix} or \begin{pmatrix} FR1 \\ FR2 \end{pmatrix} = \begin{pmatrix} X & X \\ 0 & X \end{pmatrix} \begin{pmatrix} DP1 \\ DP2 \end{pmatrix} \tag{3}$$

$$\begin{pmatrix} FR1 \\ FR2 \end{pmatrix} = \begin{pmatrix} X & X \\ X & X \end{pmatrix} \begin{pmatrix} DP1 \\ DP2 \end{pmatrix} \tag{4}$$

The second possibility is a coupled design matrix, as in Eq. (4). In a design like this, all (or some) FRs are coupled and cannot be treated separately without affecting others.

The information axiom states that one should minimize or reduce the information content of the design. In this paper, we make use of axiomatic design principles to understand the interdependencies on the real operational testbed, a Water Distribution System (named WADI in short). We will use explicitly the first axiom only in our derivation, and we are specifically interested in the relations between the functional and physical domains.

4. Architecture of WADI

In this section, the design process and communication architecture of the WADI is described. WADI is an operational testbed [2] for a water distribution network, supplying 10 US gallons/min of filtered water. WADI represents a scaled-down version of a large water distribution network of any city. It is designed and built for research and training for the design of safe and secure large scale cyber-physical systems. WADI is designed to account for the likelihood of low (or no) demand occurring during weekends and allow user to input various flow rates (subjected to maximum of 10 US gallons/min) to simulate water consumption in accordance with time varying demand patterns. As shown in Fig. 2, the water distribution process in WADI is segmented into the following subprocesses: P1: Primary grid, P2: Secondary grid, P3: Return water grid.

The primary grid (P1) consists of two raw water (RW) tanks of 2500 liters each. These tanks are fed by three incoming sources: (1) from rooftop water tank which is controlled by valve 1_MV_001, (2) from a water treatment plant controlled by valves 1_MV_004 and 1_MV_005, and (3) from return water grid (i.e P3 stage) which has a direct connection to RW tanks. A level sensor (1_LT_001) is installed in the primary grid to monitor the levels in the RW tanks. Water quality analyzers are installed to measure pH, turbidity, conductivity and residual chlorine. Two chemical dosing pumping stations namely, $NaOCl$ and NH_4Cl are installed to maintain standard levels of water conductivity and residual chlorine respectively. The secondary grid consists of two Elevated Reservoir (ER) tanks (named as ER1 and ER2 tanks in rest of the paper), consumer tanks, and contamination sampling stations. RW tanks supply

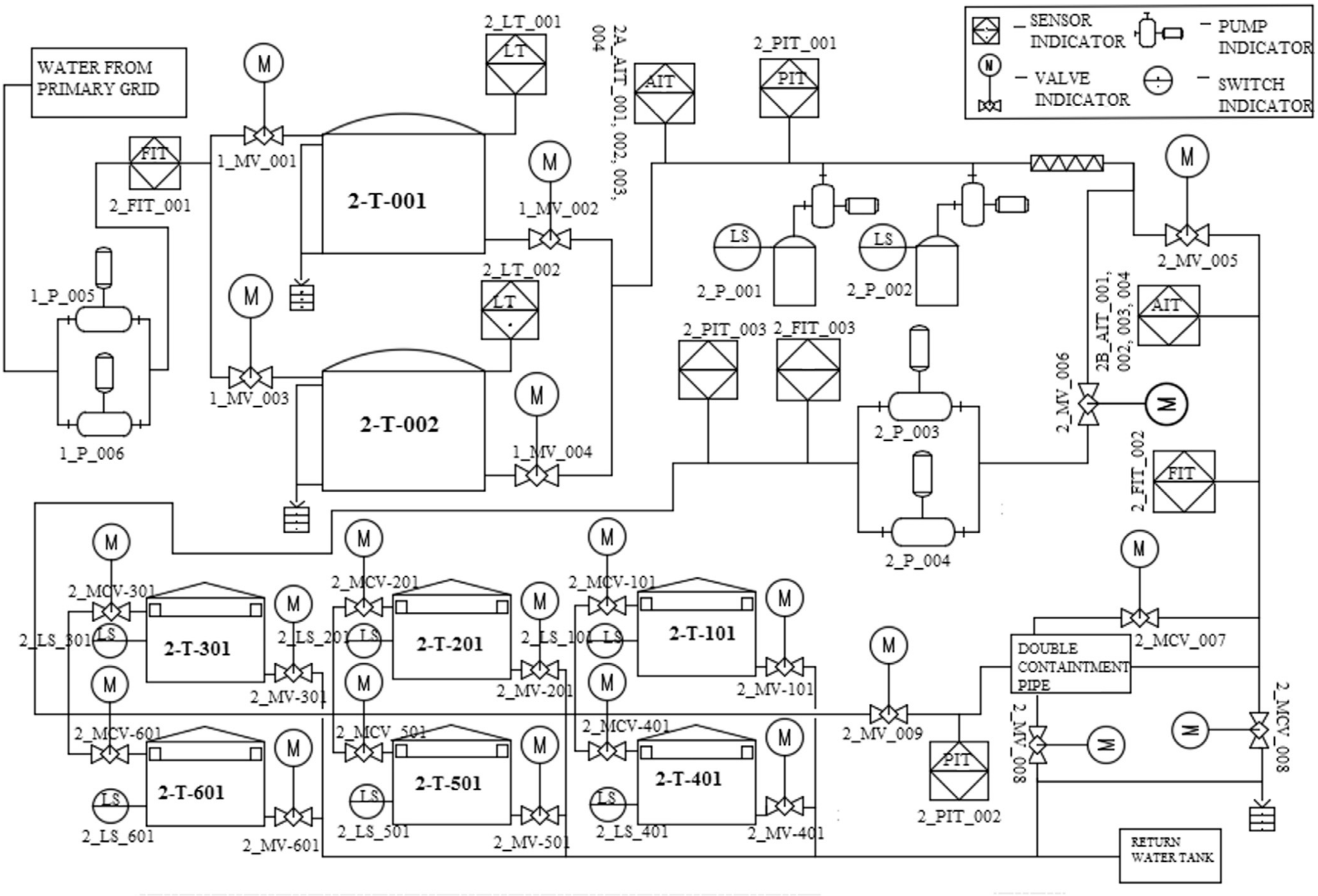

Fig. 3 – P&ID of P2 stage. 2-T-001 and 2-T-002 represent Elevated reservoir tanks, and labels 2-T-101, 201, 301, 401, 501, and 601 represent six consumer tanks.

water to the ER tanks using a raw water pump (1_P_003) which is installed in the primary grid. Two level sensors, 2_LT_001 and 2_LT_002 are installed in ER tanks to measure water levels. Further, water from ER tanks flows into the consumer tanks based on the preset demand pattern.

Two water quality monitoring stations are installed in the second stage of the testbed. One station is at the immediate downstream of the ER tanks and another is before the consumer tanks (P2A and P2B stations in Fig. 2). These stations ensure water quality before it is sent to the consumer tanks. Once a consumer tank is filled, a level switch installed in the consumer tanks raises an alarm and water from the tank drains into the return water grid. To recycle water, the return water grid pumps water back to the primary grid. Water quality analyzers are installed in return water grid to check water quality before pumping it into the primary grid. Three Programmable Logic Controllers (PLCs) are installed to control each stage of WADI. These PLCs use National Instruments CompactRIO as RIO (Remote Input Output) devices. In addition to the PLC in the secondary grid, two Schneider Electric Remote Terminal Units (RTUs), which use SCADAPack, are installed to measure the water quality. WADI consists of 103 sensors and actuators operating to measure water levels, water quality, flow rates, pressure, and status of motorized valves and pumps.

5. Modeling of WADI using axiomatic design principles

In this section, we use axiomatic design principles for critical infrastructure modeling. We consider a case study, WADI which is described in Section 4. Further, we consider the second stage, P2 of the testbed for the purpose of modeling. Fig. 3 shows the complete representation of the second stage. This stage is supplied with water from raw water tanks as shown in this figure. Based on the demand pattern of consumer tanks, the inlet valves (labeled as 2_MCV_101, 201, etc. in Fig. 3) control the flow of water from the ER tanks (2-T-001 and 002). Once the consumer tanks are filled, the outlet valves (2_MV_101, 102,.etc) open and drain water to the return water tank.

One can represent any critical infrastructure in terms of axiomatic design theory domains such as Functional Requirements (FRs) and Design parameters (DPs). The purpose in constructing an axiomatic design matrix for P2 is because we want to understand the system behavior when the system is under attack. We start by listing out the functional requirements (FR) with respect to the required design parameters (DP) of the system. Table 1 shows the list of FRs and DPs for the system. Table 1 shows the higher level decomposition of the

Table 1 – Set of FRs and DPs for characterization of the second stage of WADI testbed.

Functional Requirements (FRs)	Design Parameters (DPs)
FR1: Supply water to the elevated tanks	DP1: Pumps
FR2: Monitor water level of elevated tanks	DP2: Level sensors
FR3: Monitor water flow rate	DP3: Flow sensors
FR4: Monitor the water quality	DP4: Water quality sensors
FR5: Monitor the dosing agent	DP5: Dosing pumps
FR6: Supply water to the consumer tanks	DP6: Methods of distribution
FR7: Measure and monitor the pressure of water	DP7: Pressure meters
FR8: Control the direction flow of water	DP8: Control valves

second stage which consists of 8 FRs and 8 DPs. The mapping between the functional and physical domains in the first level decomposition in the form of a matrix is shown in Eq. (5).

$$\begin{pmatrix} FR1\\ FR2\\ FR3\\ FR4\\ FR5\\ FR6\\ FR7\\ FR8 \end{pmatrix} = \begin{pmatrix} X&0&0&0&0&0&0&0\\ 0&X&0&0&0&0&0&0\\ 0&0&X&0&0&0&0&0\\ 0&0&0&X&0&0&0&0\\ 0&0&0&0&X&0&0&0\\ 0&0&0&0&0&X&0&0\\ 0&0&0&0&0&0&X&0\\ 0&0&0&0&0&0&0&X \end{pmatrix} \begin{pmatrix} DP1\\ DP2\\ DP3\\ DP4\\ DP5\\ DP6\\ DP7\\ DP8 \end{pmatrix} \qquad (5)$$

At this point one can see that the design matrix in Eq. (5) pertains to an uncoupled design. Some coupling elements will now be introduced in this equation. These elements represent information coupling, and not physical coupling in the sense of traditional axiomatic design. In this context, these new elements tell us that the state of each DP actually hints at which state the other DP's should be in. These new elements are shown in Eq. (6) as $\otimes$, and they are present in the matrix in a symmetric way. The reason for this straight forward: for example, if DP2 is coupled with FR1, then FR2 will in the same way be coupled to DP1.

$$\begin{pmatrix} FR1\\ FR2\\ FR3\\ FR4\\ FR5\\ FR6\\ FR7\\ FR8 \end{pmatrix} = \begin{pmatrix} X&\otimes&0&0&0&0&0&\otimes\\ \otimes&X&0&0&0&0&0&0\\ 0&0&X&0&0&0&0&0\\ 0&0&0&X&0&0&0&\otimes\\ 0&0&0&0&X&0&0&0\\ 0&0&0&0&0&X&\otimes&\otimes\\ 0&0&0&0&0&\otimes&X&0\\ \otimes&0&0&\otimes&0&\otimes&0&X \end{pmatrix} \begin{pmatrix} DP1\\ DP2\\ DP3\\ DP4\\ DP5\\ DP6\\ DP7\\ DP8 \end{pmatrix} \qquad (6)$$

With this matrix one can determine how each design parameter is related directly or indirectly to their corresponding FR or other FRs. The marked box with the letter X or the symbol $\otimes$ means there is a relation or dependency on one another and 0 means there is no relation or dependency on one another. Lets take DP2 for example, it has a relation with FR1 and FR2. This means that if a level sensor is installed onto the elevated tank, we will be able to know the height of the water in the tank and if there is an increase in the water level, we will

Table 2 – Second level decomposition of FRs and DPs.

Functional Requirements (FRs)	Design Parameters (DPs)
FR1.1: Pump1: Water to elevated tanks	DP1.1: 1_P_005
FR1.2: Pump2: Water to elevated tanks	DP1.2: 1_P_006
FR2.1: Measure the level of elevated tank	DP2.1: 2_LT_001 and 2_LT_002
FR2.2: Measure the level of consumer tank	DP2.2: 2_LS_101, 201, 301, 401, 501, 601
FR3.1: Measure the water flow into elevated tank	DP3.1: 2_FIT_001
FR3.2: Measure the gravity meter water flow	DP3.2: 2_FIT_002
FR3.3: Measure the booster pump water flow	DP3.3: 2_FIT_003
FR4.1: Measure p^H of water	DP4.1: 2A_AIT_003, 2B_AIT_003
FR4.2: Measure Oxidation Reduction Potential (ORP)	DP4.2: 2A_AIT_004, 2B_AIT_004
FR4.3: Measure the conductivity of water	DP4.3: 2A_AIT_001, 2B_AIT_001
FR4.4: Measure the turbidity of water	DP4.4: 2A_AIT_002, 2B_AIT_002
FR5.1: Monitor inorganic dosing pump	DP5.1: 2_P_001
FR5.2: Monitor organic dosing pump	DP5.2: 2_P_002
FR6.1: Total consumption flow rate met by the gravity feed	DP6.1: Gravity meter
FR6.2: Total consumption flow rate not met by the gravity feed	DP6.2: Turn on booster pump (2_P_003 or 2_P_004)
FR7.1: Reservoir outlet pressure	DP7.1: 2_PIT_001
FR7.2: Gravity feed pressure	DP7.2: 2_PIT_002
FR7.3: Booster pump outlet pressure	DP7.3: 2_PIT_003
FR8.1: Elevated tanks inlet	DP8.1: 2_MV_001 and 2_MV_003
FR8.2: Elevated tanks outlet	DP8.2: 2_MV_002 and 2_MV_004
FR8.3: Gravity grid inlet flow	DP8.3: 2_MV_005 and 2_MV_009
FR8.4: Booster grid inlet flow	DP8.4: 2_MV_006
FR8.5: Consumer tanks inlet	DP8.5: 2_MCV_101, 201, 301, 401, 501, 601
FR8.6: Consumer tanks outlet	DP8.6: 2_MV_101, 201, 301,401, 501, 601
FR8.7: Water leak simulation valves	DP8.7: 2_MCV_007, 2_MV_008

know that there is a supply of water into the elevated tank i.e, there is an information coupling. Eq. (6) shows that the first level mapping resulted in a information-coupled design. At this level, the designer develops the design concept based on the available knowledge; the designer develops the design intent. Therefore, to complete the detailed design, this high level decomposition of FRs and DPs can be further detailed into other levels, until there is a one-to-one relation between requirements and design parameters at that level. Consider FR2 which is monitoring water levels, there exist multiple locations to measure the water levels in the system. Therefore we further decompose FR2 into lower levels.

The decomposition of 8 FRs resulted in a total of 25 FRs for the second level. It is to be noted that FRs and DPs are decomposed in such a way that the design intent expressed by the higher level design matrices into realizable detailed designs is maintained by the lower level design matrices. Table 2 lists the corresponding FRs and DPs. Eq. (7) shows the design matrix as a sequence of the mapping made in Table 2. In general, FRs and DPs which are decomposed into lower levels are represented as follows: FRx.y can be read as functional requirement labeled x is further decomposed into index y. For example, in Table 2, FR1.1 and FR1.2 indicate decomposition of FR1 (supply water to elevated tanks) into lower level FRs which further represent pump1 (FR1.1) and pump2 (FR1.2) respectively. For example, consider FR1.2 which has the functional requirement of pumping water to elevated tanks, the dependency between FR1.2 and DP1.2, DP2.1 is identified and is shown in Eq. (7). It means that functional requirement FR1.2 is satisfied by DP1.2 which is pump 1_P_006. Furthermore, the level of the tank increases when the pump 1_P_006 is in operation, hence FR1.2 has dependency on 2_LT_001 and 2_LT_002.

With this matrix one can determine how each design parameter is related to their corresponding FR or other FRs. The decomposition continues until all sensors and actuators in the system have been fully captured. For this case, we need to go into three levels of decomposition. Table 3 shows the third level decomposition of FRs and DPs. It is observed from this table that each FR is controlled by only one DP at this level. Therefore, further decomposition is not necessary and the decomposition process is complete.

5.1. *A design structure matrix proxy for security purposes*

In the previous section, we built design matrices which show the relationship between FRs and DPs. From a security and safety stand point, we are interested in understanding the relationships across DPs. Dong [9] proposed a three steps transformation method between Design Matrix (DM) and Design Structure Matrix (DSM). However, given the fact that our DM is already symmetric, the resulting DSM will result identical. This is also known as an adjacency matrix, which shows the interdependency across system components. Therefore, we will use the DM directly for detection purposes. We make use of this matrix for detection of single and double attack points. Initially, we will show how we use this security matrix table for single attack point and later we extend it to double attack points.

5.2. *Detecting potential attacks with the security matrix*

Under the assumption of single point attack, the security matrix for the level one decomposition is shown in Table 4. This table shows the relationship between one DP and other DPs

$$\begin{pmatrix} FR1.1\\ FR1.2\\ FR2.1\\ FR2.2\\ FR3.1\\ FR3.2\\ FR3.3\\ FR4.1\\ FR4.2\\ FR4.3\\ FR4.4\\ FR5.1\\ FR5.2\\ FR6.1\\ FR6.2\\ FR7.1\\ FR7.2\\ FR7.3\\ FR8.1\\ FR8.2\\ FR8.3\\ FR8.4\\ FR8.5\\ FR8.6\\ FR8.7 \end{pmatrix} = \begin{pmatrix}
X&0&X&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&X&0&0&0&0&0&0\\
0&X&X&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&X&0&0&0&0&0&0\\
X&X&X&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&X&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&X&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&X&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&X&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&X&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&X\\
0&0&0&0&0&0&0&0&X&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&X\\
0&0&0&0&0&0&0&0&0&X&0&0&0&0&0&0&0&0&0&0&0&0&0&0&X\\
0&0&0&0&0&0&0&0&0&0&X&0&0&0&0&0&0&0&0&0&0&0&0&0&X\\
0&0&0&0&0&0&0&0&0&0&0&X&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&X&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&X&0&0&X&0&0&0&X&0&X&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&X&0&0&X&0&0&0&X&X&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&X&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&X&0&0&X&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&X&0&0&X&0&0&0&0&0&0&0\\
X&X&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&X&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&X&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&X&0&0&0&0&0&0&X&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&X&0&0&0&0&0&0&X&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&X&X&0&0&0&0&0&0&0&X&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&X&0\\
0&0&0&0&0&0&0&X&X&X&X&0&0&0&0&0&0&0&0&0&0&0&0&0&X
\end{pmatrix} \begin{pmatrix} DP1.1\\ DP1.2\\ DP2.1\\ DP2.2\\ DP3.1\\ DP3.2\\ DP3.3\\ DP4.1\\ DP4.2\\ DP4.3\\ DP4.4\\ DP5.1\\ DP5.2\\ DP6.1\\ DP6.2\\ DP7.1\\ DP7.2\\ DP7.3\\ DP8.1\\ DP8.2\\ DP8.3\\ DP8.4\\ DP8.5\\ DP8.6\\ DP8.7 \end{pmatrix} \tag{7}$$

Table 3 – Third level decomposition.

Functional Requirements (FRs)	Design Parameters (DPs)
FR2.1.1: Measure water level of ER 1	DP2.2.1: 2_LT_001
FR2.1.2: Measure water level of ER 2	DP2.2.2: 2_LT_002
FR2.2.1: Measure water level of consumer tank1	DP2.3.1: 2_LS_101
FR2.2.2: Measure water level of consumer tank2	DP2.3.2: 2_LS_201
FR2.2.3: Measure water level of consumer tank3	DP2.3.3: 2_LS_301
FR2.2.4: Measure water level of consumer tank4	DP2.3.4: 2_LS_401
FR2.2.5: Measure water level of consumer tank5	DP2.3.5: 2_LS_501
FR2.2.6: Measure water level of consumer tank5	DP2.3.6: 2_LS_601
FR4.1.1: Measure p^H at the outlet of ER	DP4.1.1: 2A_AIT_003
FR4.1.2: Measure p^H at the inlet of consumer tank	DP4.1.2: 2B_AIT_003
FR4.2.1: Measure ORP at the outlet of ER	DP4.2.1: 2A_AIT_004
FR4.2.2: Measure ORP at the inlet of consumer tank	DP4.2.2: 2B_AIT_004
FR4.3.1: Measure conductivity at the outlet of ER	DP4.3.1: 2A_AIT_001
FR4.3.2: Measure conductivity at the inlet of consumer tank	DP4.3.1: 2B_AIT_001
FR4.4.1: Measure turbidity at the outlet of ER	DP4.4.1: 2A_AIT_002
FR4.4.2: Measure turbidity at the inlet of consumer tank	DP4.4.2: 2B_AIT_002
FR6.2.1: Turn on booster pump1	DP6.2.1: 2_P_003
FR6.2.2: Turn on booster pump2	DP6.2.2: 2_P_004
FR8.1.1: ER1 inlet	DP8.1.1: 2_MV_001
FR8.1.2: ER2 inlet	DP8.1.2: 2_MV_003
FR8.2.1: ER1 outlet	DP8.2.1: 2_MV_002
FR8.2.2: ER2 outlet	DP8.2.2: 2_MV_004
FR8.3.1: Gravity inlet 1	DP8.3.1: 2_MV_005
FR8.3.2: Gravity inlet 2	DP8.3.2: 2_MV_009
FR8.5.1: Consumer tank 1 inlet	DP8.5.1: 2_MCV_101
FR8.5.2: Consumer tank 2 inlet	DP8.5.2: 2_MCV_201
FR8.5.3: Consumer tank 3 inlet	DP8.5.3: 2_MCV_301
FR8.5.4: Consumer tank 4 inlet	DP8.5.4: 2_MCV_401
FR8.5.5: Consumer tank 5 inlet	DP8.5.5: 2_MCV_501
FR8.5.6: Consumer tank 6 inlet	DP8.5.6: 2_MCV_601
FR8.6.1: Consumer tank 1 outlet	DP8.6.1: 2_MV_101
FR8.6.2: Consumer tank 2 outlet	DP8.6.2: 2-MV-201
FR8.6.3: Consumer tank 3 outlet	DP8.6.3: 2-MV-301
FR8.6.4: Consumer tank 4 outlet	DP8.6.4: 2-MV-401
FR8.6.5: Consumer tank 5 outlet	DP8.6.5: 2-MV-501
FR8.6.6: Consumer tank 6 outlet	DP8.6.6: 2-MV-601
FR8.7.1: Leakage inlet valve	DP8.7.1: 2-MCV-007
FR8.7.2: Leakage drain valve	DP8.7.2: 2-MV-008

Table 4 – Security check table under first level decomposition.

Design parameter	DP1	DP2	DP3	DP4	DP5	DP6	DP7	DP8
DP1	X	X	0	0	0	0	0	X
DP2	X	X	0	0	0	0	0	0
DP3	0	0	X	0	0	0	0	0
DP4	0	0	0	X	0	0	0	X
DP5	0	0	0	0	X	0	0	0
DP6	0	0	0	0	0	X	X	X
DP7	0	0	0	0	0	X	X	0
DP8	X	0	0	X	0	X	0	X

and is identical to the design matrix shown in Eq. (6). For example, consider DP1 is a pump which supplies water from the primary grid to the ER tanks. In Table 4, DP1 shows the dependency on DP2 and DP8 which are a level sensor and control valves, respectively. Dependencies between all DPs are shown in this table. These dependencies are useful to detect attacks on a particular DP. For example, let us consider the system under normal operation: Assume that DP1 (pump) is in operation and supplying water to the ER tank, then one can expect a rise in the tank level (level sensor DP2 shows the reading). It is to be observed that when DP1 is in operation then the corresponding control valves (DP8) should be opened. Now, consider a scenario where an attacker has a set of intentions (such as damage system components and cut off water supply to consumers etc.) and tries to trick the system into believing that the pump and valves are off. In this situation, a quick check of the level sensors will show a rise in water levels. Clearly, the dependency between DP1, DP2 and DP8 is not satisfied and hence one can conclude that there is something wrong in the system. Therefore, the security table is useful in checking whether the system is under normal operation and if there exist any attack in the system, it can be detected. We also define a vulnerable component if there is no other check point to detect an attack. For example, one can observe from Table 4 that DP3 and DP5 are considered as vulnerable components as there are no other DPs to detect whether they are under attack. It is also possible to derive the security-check table for second level decomposition and this is shown in Table 5. A

Table 5 – Security check table under second level decomposition of P2 stage.

Design Parameter	DP1.1	DP1.2	DP2.1	DP2.2	DP3.1	DP3.2	DP3.3	DP4.1	DP4.2	DP4.3	DP4.4	DP5.1	DP5.2	DP6.1	DP6.2	DP7.1	DP7.2	DP7.3	DP8.1	DP8.2	DP8.3	DP8.4	DP8.5	DP8.6	DP8.7
DP1.1	X	0	X	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	X	0	0	0	0	0	0
DP1.2	0	X	X	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	X	0	0	0	0	0	0
DP2.1	X	X	X	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
DP2.2	0	0	0	X	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
DP3.1	0	0	0	0	X	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
DP3.2	0	0	0	0	0	X	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
DP3.3	0	0	0	0	0	0	X	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
DP4.1	0	0	0	0	0	0	0	X	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	X
DP4.2	0	0	0	0	0	0	0	0	X	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	X
DP4.3	0	0	0	0	0	0	0	0	0	X	0	0	0	0	0	0	0	0	0	0	0	0	0	0	X
DP4.4	0	0	0	0	0	0	0	0	0	0	X	0	0	0	0	0	0	0	0	0	0	0	0	0	X
DP5.1	0	0	0	0	0	0	0	0	0	0	0	X	0	0	0	0	0	0	0	0	0	0	0	0	0
DP5.2	0	0	0	0	0	0	0	0	0	0	0	0	X	0	0	0	0	0	0	0	0	0	0	0	0
DP6.1	0	0	0	0	0	0	0	0	0	0	0	0	0	X	0	0	X	0	0	0	X	0	X	0	0
DP6.2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	X	0	0	X	0	0	0	X	X	0	0
DP7.1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	X	0	0	0	0	0	0	0	0	0
DP7.2	0	0	0	0	0	0	0	0	0	0	0	0	0	X	0	0	X	0	0	0	0	0	0	0	0
DP7.3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	X	0	0	X	0	0	0	0	0	0	0
DP8.1	X	X	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	X	0	0	0	0	0	0
DP8.2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	X	0	0	0	0	0
DP8.3	0	0	0	0	0	0	0	0	0	0	0	0	0	X	0	0	0	0	0	0	X	0	0	0	0
DP8.4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	X	0	0	0	0	0	0	X	0	0	0
DP8.5	0	0	0	0	0	0	0	0	0	0	0	0	0	X	X	0	0	0	0	0	0	0	X	0	0
DP8.6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	X	0
DP8.7	0	0	0	0	0	0	0	X	X	X	X	0	0	0	0	0	0	0	0	0	0	0	0	0	X

Table 6 – Detection of double attack points under first level decomposition.

Attack pairs of DPs	High detectability	Low detectability
(DP1, DP2)	–	DP8
(DP1, DP3)	Vulnerable	
(DP1, DP4)	DP2, DP8	–
(DP1, DP5)	Vulnerable	
(DP1, DP6)	DP2, DP7, DP8	–
(DP1, DP7)	DP2, DP6, DP8	–
(DP1, DP8)	DP2, DP4, DP8	
(DP2, DP3)	Vulnerable	
(DP2, DP4)	DP1, DP8	–
(DP2, DP5)	Vulnerable	
(DP2, DP6)	DP1, DP7, DP8	–
(DP2, DP7)	DP1, DP6	–
(DP2, DP8)	DP1, DP4, DP6	–
(DP3, DP4)	Vulnerable	
(DP3, DP5)	Vulnerable	
(DP3, DP6)	Vulnerable	
(DP3, DP7)	Vulnerable	
(DP3, DP8)	Vulnerable	
(DP4, DP5)	Vulnerable	
(DP4, DP6)	DP7, DP8	–
(DP4, DP7)	DP6, DP8	–
(DP4, DP8)	DP1, DP6	–
(DP5, DP6)	Vulnerable	
(DP5, DP7)	Vulnerable	
(DP5, DP8)	Vulnerable	
(DP6, DP7)	–	DP8
(DP6, DP8)	DP1, DP4, DP7	–
(DP7, DP8)	DP1, DP4, DP6	

similar table for the third level decomposition is not shown in this paper, but can also be obtained following the same procedure.

For the sake of clarity and simplicity, we will demonstrate the situation of two-point attacks only for the first level decomposition. Here we will test whether any combination of attacks on two DPs can be detected using the security-check table shown in Table 4. The possible two attack points are $\binom{8}{2}$. The attack pairs and their corresponding detection design parameters are represented in Table 6. In this table, the high and low detectabilities are related to the level of detection redundancy that each potential attack has on each DP. A high detectability happens when there are two points presumably under attack and there are at least two other points (cross-check points, presumably not under attack) where you can find anomalies that enable you to check whether the two initial points might be under attack. A low detectability happens when there is only one cross-check point. As stated earlier, a vulnerability happens when there are no cross-check points available to detect potential attacks.

As an example, let us consider a potential two-point attack on DP1 and DP2 simultaneously (please refer to the first row below the header of Tables 4 and 6). Looking simultaneously at rows 1 and 2 of Table 4, we immediately see that, apart from DP1 and DP2, only DP8 shows up in these rows. This means that one can detect any anomalies or attacks by checking DP8 only; under our previous definition an attack on DP1 and DP2 has a low detectability. Another example could be to consider a potential two-point attack on DP2 and DP6. DP1 can help you to detect an attack on DP2, and DP7 and DP8 can help you detect an attack on DP6, but none can help you detect simultaneously both attacks. Nevertheless, according to our definition for a two point attack on DP2 and DP6 there is high detectability. Furthermore, please also note that any two point attacks involving DP3 or DP5 will reveal a system vulnerability, as none of these have check points of their own.

This mode of analyzing a CPS will shed light into which design parameters (system components) need more or less redundancy in the form of cross-check points, for as many presumable attack points as deemed necessary or economically viable. This analysis can be performed early on during the design of the CPS to understand where there might be vulnerabilities in the system, and cater for those vulnerabilities by building in more cross-checkpoints where needed.

6. Conclusion and future work

This paper presented an easy and user friendly way of detecting potential attacks on a cyber-physical system using axiomatic design principles. It takes advantage of the need to define functional requirements (FR) for the system and come up with design parameters (DP) that meet those system requirements at an early stage of the design of the system. Ultimately, these design parameters will be materialized in system components that either act on the system or sense the system variables, and the relations between DP and FR constitute an abstract model of the system. This early abstract model is enough to have a first assessment of potential vulnerabilities of the system, and change the system accordingly with limited or no cost involved. An example was presented based on the design of a water distribution system, for which a security-check table is built, based on those relations. Scenarios were derived for one-point and two-point attacks, for which high and low detectability were defined and exemplified. The method is revealed to be simple, fast and easy to use.

The current derivation of this method keeps the relations across DPs in an abstract form, i.e. there is no mathematical expression that can relate DPs with any physical meaning. Future developments will look into assigning meaning to these relations by deriving mathematical expressions to these relations. This will enable the design team to compare the ideal state of the system (the values of each design parameter at a given point in time as calculated by these mathematical expressions) with the real time state of the system (the real values measured in the system in real time). It is expected that logic expressions involving the state of each DP will help in assessing the vulnerability and the normal operation of CIs without the need for complicated mathematical manipulations.

ACKNOWLEDGMENT

This work was supported in part by the National Research Foundation (NRF), Prime Ministers Office, Singapore, under its National Cybersecurity R&D Programme (Award No.

NRF2015NCR-NCR003-001) and administered by the National Cybersecurity R&D Directorate.

REFERENCES

[1] T. Adachi, B. R. Ellingwood, Serviceability of earthquake-damaged water systems: Effects of electrical power availability and power backup systems on system vulnerability, Reliability Engineering & System Safety, vol. 93(1), pp. 78 – 88, 2008.

[2] C. M. Ahmed, V. R. Palleti, A. P. Mathur, Wadi: A water distribution testbed for research in the design of secure cyber physical systems, in: Proceedings of the 3rd International Workshop on Cyber-Physical Systems for Smart Water Networks, CySWATER '17, pp. 25–28, 2017.

[3] M. Amin, Toward secure and resilient interdependent infrastructures, Journal of Infrastructure Systems, vol. 8(3), pp. 67–75, 2002.

[4] D.C. Barton, E.D. Eidson, R.G.C. David A Schoenwald, R.K. Reinert, Simulating economic effects of disruptions in the telecommunications infrastructure, Sandia report. SAND 2004-0101, 2004.

[5] N. Basu, R. Pryor, T. Quint, Aspen: A microsimulation model of the economy, Computational Economics, vol. 12(3), pp. 223–241, 1998.

[6] S.V. Buldyrev, R. Parshani, G. Paul, S. Stanley, H. Eugene andHavlin, Catastrophic cascade of failures in interdependent networks, Nature, vol. 464, pp. 1025–1028, 2010.

[7] S.V. Buldyrev, N.W. Shere, G.A. Cwilich, Interdependent networks with identical degrees of mutually dependent nodes, Phys. Rev. E, vol. 83, paper no. 016112, 2011.

[8] S.E. Chang, T.L. McDaniels, C. Beaubien, Societal impacts of infrastructure failure interdependencies: Building an empirical knowledge base, Proc. of 2009 Technical Council on Lifeline Earthquake Engineering (TCLEE) Conference, Oakland, CA, pp. 693–702, 2009.

[9] Q. Dong, Predicting and managing system interactions at early phase of the product development process, PhD Dissertation, Massachusetts Institute of Technology, 2002.

[10] L. DueØas-Osorio, J.I. Craig, B.J. Goodno, A. Bostrom, Interdependent response of networked systems, Journal of Infrastructure Systems, vol. 13(3), pp. 185–194, 2007.

[11] B.C. Ezell, J.V. Farr, I. Wiese, Infrastructure risk analysis model, Journal of Infrastructure Systems, 6(3), pp. 114–117, 2000.

[12] B.C. Ezell, J.V. Farr, I. Wiese, Infrastructure risk analysis of municipal water distribution system, Journal of Infrastructure Systems, vol. 6(3), pp. 118–122, 2000.

[13] V. Fioriti, G. D'Agostino, S. Bologna, On modeling and measuring inter-dependencies among critical infrastructures, in: 2010 Complexity in Engineering, pp. 85–87, 2010.

[14] B. Genge, P. Haller, I. Kiss, A framework for designing resilient distributed intrusion detection systems for critical infrastructures, International Journal of Critical Infrastructure Protection, vol. 15, pp. 3–11, 2016.

[15] B. Genge, I. Kiss, P. Haller, A system dynamics approach for assessing the impact of cyber attacks on critical infrastructures, International Journal of Critical Infrastructure Protection, vol. 10, pp. 3–17, 2015.

[16] S.D. Guikema, Natural disaster risk analysis for critical infrastructure systems: An approach based on statistical learning theory, Reliability Engineering & System Safety, vol. 94(4), pp. 855–860, 2009.

[17] N. HadjSaid, C. Tranchita, B. Rozel, M. Viziteu, R. Caire, Modeling cyber and physical interdependencies - application in ict and power grids, in: 2009 IEEE/PES Power Systems Conference and Exposition, pp. 1–6, 2009.

[18] Y.Y. Haimes, B.M. Horowitz, J.H. Lambert, J.R. Santos, C. Lian, K.G. Crowther, Inoperability input-output model for interdependent infrastructure sectors. i: Theory and methodology, Journal of Infrastructure Systems, vol. 11(2), pp. 67–79, 2005.

[19] Y.Y. Haimes, P. Jiang, Leontief-based model of risk in complex interconnected infrastructures, Journal of Infrastructure Systems, vol. 7(1), pp. 1–12, 2001.

[20] A. Kelic, D.E. Warren, L.R. Phillips, Cyber and physical infrastructure interdependencies, Snadia report, SAND 2008-6192, 2008.

[21] J.-C. Laprie, K. Kanoun, M. Kaâniche, Modelling interdependencies between the electricity and information infrastructures, in: F. Saglietti, N. Oster (Eds.), Computer Safety, Reliability, and Security, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 54–67, 2007.

[22] E. Lee, J.E. Mitchell, W.A. Wallace, Restoration of services in interdependent infrastructure systems: A network flows approach, IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), vol. 37(6), pp. 1303–1317, 2007.

[23] W. Leontief, Input-output economics, Oxford University Press, 1986.

[24] X. Liu, J. Zhang, P. Zhu, Modeling cyber-physical attacks based on probabilistic colored petri nets and mixed-strategy game theory, International Journal of Critical Infrastructure Protection, vol. 16, pp. 13–25, 2017.

[25] S. Marrone, R. Nardone, A. Tedesco, P. D'Amore, V. Vittorini, R. Setola, F.D. Cillis, N. Mazzocca, Vulnerability modeling and analysis for critical infrastructure protection applications, International Journal of Critical Infrastructure Protection, vol. 6(3), pp. 217–227, 2013.

[26] T. McDaniels, S. Chang, K. Peterson, J. Mikawoz, D. Reed, Empirical framework for characterizing infrastructure failure interdependencies, Journal of Infrastructure Systems, vol. 13(3), pp. 175–184, 2007.

[27] J. Moteff, P. Parfomak, Critical infrastructure and key assets: Definition and identification, Congressional Research Service, The Library of Congress, Washington, DC, 2004.

[28] A.D. Nicola, M.L. Villani, M.C. Brugnoli, G. D'Agostino, A methodology for modeling and measuring interdependencies of information and communications systems used for public administration and egovernment services, International Journal of Critical Infrastructure Protection, vol. 14, pp. 18–27, 2016.

[29] M. Ouyang, Review on modeling and simulation of interdependent critical infrastructure systems, Reliability Engineering & System Safety, vol. 121, pp. 43–60, 2014.

[30] R. Parshani, S.V. Buldyrev, S. Havlin, Interdependent Networks: Reducing the Coupling Strength Leads to a Change from a First to Second Order Percolation Transition, Physical Review Letters, vol. 105(4), paper no. 048701, 2010.

[31] D.F. Rueda, E. Calle, Using interdependency matrices to mitigate targeted attacks on interdependent networks: A case study involving a power grid and backbone telecommunications networks, International Journal of Critical Infrastructure Protection, vol. 16, pp. 3–12, 2017.

[32] J.R. Santos, Y.Y. Haimes, Modeling the demand reduction input-output (i-o) inoperability due to terrorism of interconnected infrastructures*, Risk Analysis, vol. 24(6), pp. 1437–1451, 2004.

[33] G. Stergiopoulos, P. Kotzanikolaou, M. Theocharidou, D. Gritzalis, Risk mitigation strategies for critical infrastructures based on graph centrality analysis, International Journal of Critical Infrastructure Protection, vol. 10, pp. 34–44, 2015.

[34] N. Suh, Axiomatic Design: Advances and Applications, MIT-Pappalardo series in mechanical engineering, Oxford University Press, 2001.

[35] S. Sultana, Z. Chen, Modeling flood induced interdependencies among hydroelectricity generating infrastructures, Journal of Environmental Management, vol. 90(11), pp. 3272–3282, 2009.

[36] N. Svendsen, S. Wolthusen, Multigraph Dependency Models for Heterogeneous Infrastructures, Springer US, Boston, MA, pp. 337–350.

[37] N.K. Svendsen, S.D. Wolthusen, Connectivity models of interdependency in mixed-type critical infrastructure networks, Information Security Technical Report, vol. 12(1), pp. 44–55, 2007.

[38] N.K. Svendsen, S.D. Wolthusen, Graph Models of Critical Infrastructure Interdependencies, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 208–211.