The Resilience Model Supporting IIoT System Trustworthiness

Authors:

Semen Kort
Senior System Analyst
Kaspersky Lab
Semen.Kort@kaspersky.com

Ekaterina Rudina
Senior System Analyst
Kaspersky Lab
Ekaterina.Rudina@kaspersky.com

INTRODUCTION

Shifting the focus from security to trustworthiness, survivability, dependability and similar concepts characterizing IIoT system behavior is one of the current trends. These concepts determine the varying sets of basic characteristics and requirements for the IIoT system such as security, safety, reliability and others. The complicated concepts must also address the dependencies and inconsistencies of the separate aspects of IIoT system behavior. [1, 2, 3]

The main objective of this research is to understand and clearly describe the place and role of cyber resilience in support of the mentioned concepts. The approach to the research is the initial analysis of definitions and further investigation of their connections using the semiformal model of the IIoT system behavior.

Differences between the typical IT system and IIoT system require a particular attention during modeling system behavior. The National Institute of Standards and Technology (NIST) Guide to Industrial Control Systems Security [4] gives a good explanation of typical differences between an IT system and an industrial control system, which is a kind of IIoT system. These differences eventually result in varying implementation approaches to the resilience aspects. Moreover, different IIoT systems make their own interpretation of resilience by requiring enforcement of specific physical or cyber constraints.

According to the definition given in the Draft NIST Special Publication on Systems Security Engineering Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems,[5] "cyber resiliency is the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources regardless of the source."

According to the Industrial Internet Consortium (IIC) Industrial Internet Security

[1] F. Schneider, ed. Trust in Cyberspace. Nat'l Academy Press, 1999

[2] A. Avizienis, Jean-Claude Laprie, B. Randell, and C. Landwehr. Basic Concepts and Taxonomy of Dependable and Secure Computing. IEEE Transactions on dependable and secure computing, Vol. 1, № 1, January-March 2004

[3] Q. Zhang, A. King, F. Hirsch, S. Kort. Key Safety Challenges for the IIoT. An Industrial Internet Consortium Technical White Paper, 2018. https://www.iiconsortium.org/pdf/Key_Safety_Challenges_for_the_IIoT.pdf

[4] Keith Stouffer, Suzanne Lightman, Victoria Pillitteri, Marshall Abrams, and Adam Hahn. NIST Special Publication 800-82 Rev.2. Guide to Industrial Control Systems (ICS) Security. National Institute of Standards and Technology, U.S. Department of Commerce, 2015. https://doi.org/10.6028/NIST.SP.800-82r2

[5] R. Ross, R. Graubart, D. Bodeau, and R. Mcquaid. Draft NIST Special Publication 800-160 VOLUME 2. Systems Security Engineering Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems. National Institute of Standards and Technology, U.S. Department of Commerce, 2018. https://csrc.nist.gov/CSRC/media/Publications/sp/800-160/vol-2/draft/documents/sp800-160-vol2-draft.pdf

Framework,[6] resilience is one of the key system characteristics which make the system trustworthy. Trustworthiness is defined as "a degree of confidence one has that the system performs as expected with characteristics including safety, security, privacy, reliability and resilience in the face of environmental disruptions, human errors, system faults and attacks".

Related Work

The most pertinent document considering cyber resilience is the already mentioned Volume 2 of the NIST Special Publication 800-160 which is in a draft state at the moment of writing this paper. It defines the goals and objectives for resilience property, techniques and approaches for its implementation, and their relations.[7]

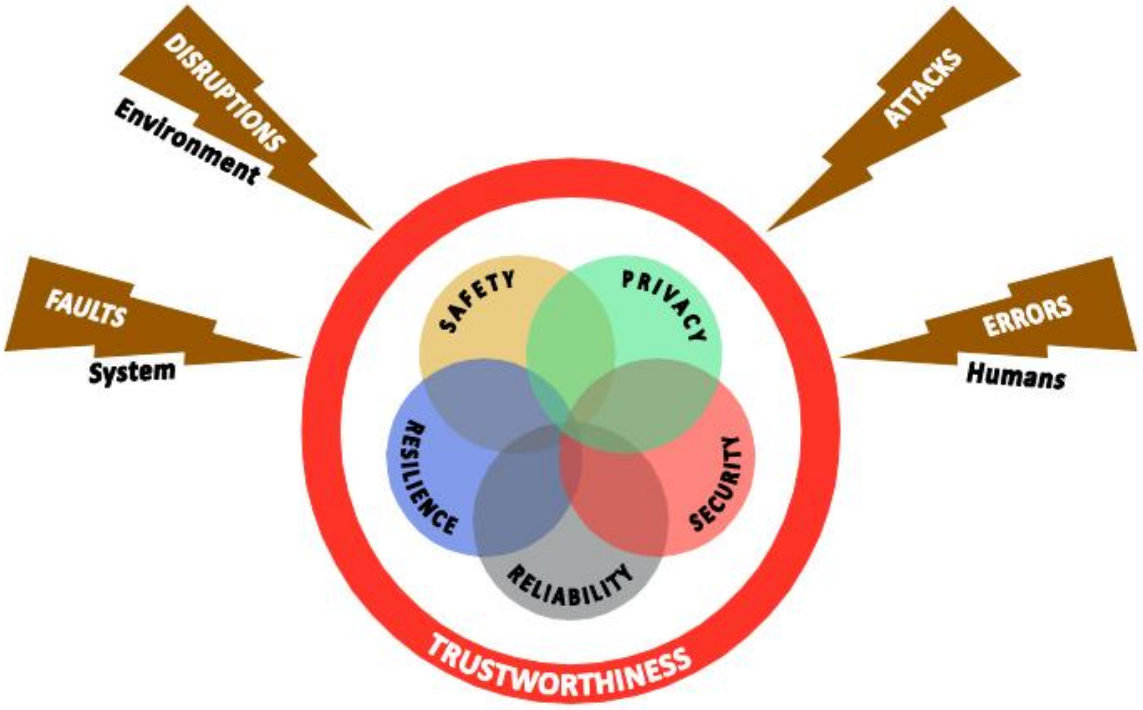

Figure 1: Trustworthiness of an IIoT System

The appropriate relationship is shown in Figure 1.

The mentioned NIST Special Publication on Cyber Resiliency Considerations defines the resilience goals as follows:

[6] Industrial Internet of Things. Volume G4: Security Framework. Industrial Internet Consortium, 2016. http://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf

[7] While the referred document is currently a draft, we believe that its key provisions will not change significantly in its stable version.

- Anticipate: maintain a state of informed preparedness for adversity
- Withstand: continue essential mission or business functions despite adversity
- Recover: restore mission or business functions during and after adversity, and
- Adapt: modify mission or business functions and/or supporting capabilities to predicted changes in the technical, operational or threat environments.

Resilience objectives are defined as follows:

- Understand
- Prepare
- Prevent
- Transform
- Re-Architect
- Continue
- Constrain
- Reconstitute
- Restore

Volume 2 of the NIST Special Publication 800-160 also considers the resilience approaches and techniques.

The Industrial Internet Security Framework defines resilience through the Quality of Service (QoS).[8] Desirable QoS determines the normal operating conditions for the system, while minimum QoS defines the lowest levels of service necessary to ensure a successful, although possibly degraded, service execution. A system whose performance is degrading will operate at progressively lower levels of QoS until it crosses its minimum QoS requirements, at which point it may still be operational, but it has failed to maintain service continuity. Possible responses of a system to an impulse at time A are depicted in Figure 2.

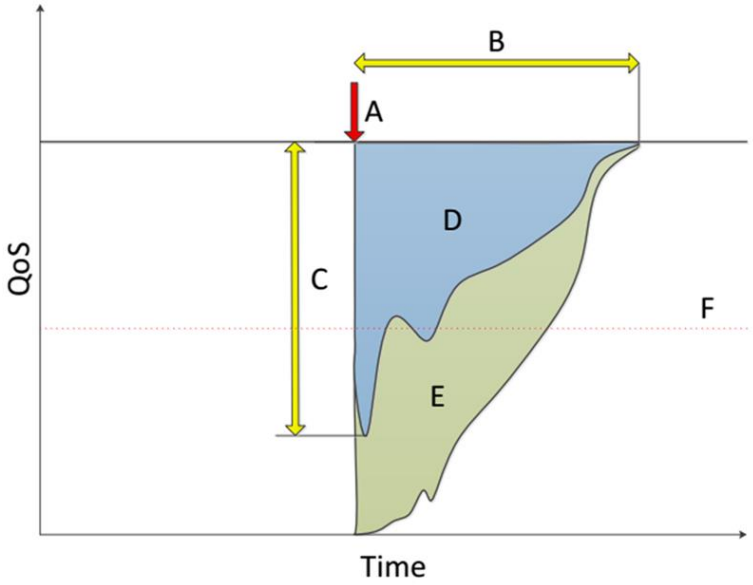

Figure 2: Possible responses of a system to an impulse at time A

The paper name "Resilience is More than Availability" of M. Bishop et al is based on the example shown in Figure 2.[9] In this figure, B represents the time taken for the system to return to its equilibrium QoS. C represents the maximum disturbance for system D. Another possible response is

[8] Industrial Internet of Things. Volume G4: Security Framework. Industrial Internet Consortium, 2016. http://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf

[9] M. Bishop, M. Carvalho, R. Ford, and L.M. Mayron. Resilience is More than Availability. In NSPW '11 Proceedings of the 2011 New Security Paradigms Workshop, Marin County, California, USA, 2011. http://nob.cs.ucdavis.edu/bishop/papers/2011-nspw/resilience.ps

shown for the system E. Finally, line F represents a QoS below which the system's mission is compromised. The research also pays attention to the difference between survivability, robustness and resilience aspects.

Some papers considering various types of resilience seek to define the appropriate metrics. In the paper of K. Tierney and M. Bruneau, the Resilience is evaluated using 4 separate metrics comprising the so-called R4 framework: Robustness, Redundancy, Resourcefulness, Rapidity.[10] The paper of C. Folke defines and measures using the ecological approach to the Resilience and Resistance properties.[11] According to the last paper, Resilience is the time it takes the system to return to its equilibrium state after a perturbation and Resistance of the system is the magnitude of change to a particular stimulus.

PROPOSED MODEL

In this research, we define the model for IIoT system Resilience contributing to the Trustworthiness of this system. The model of

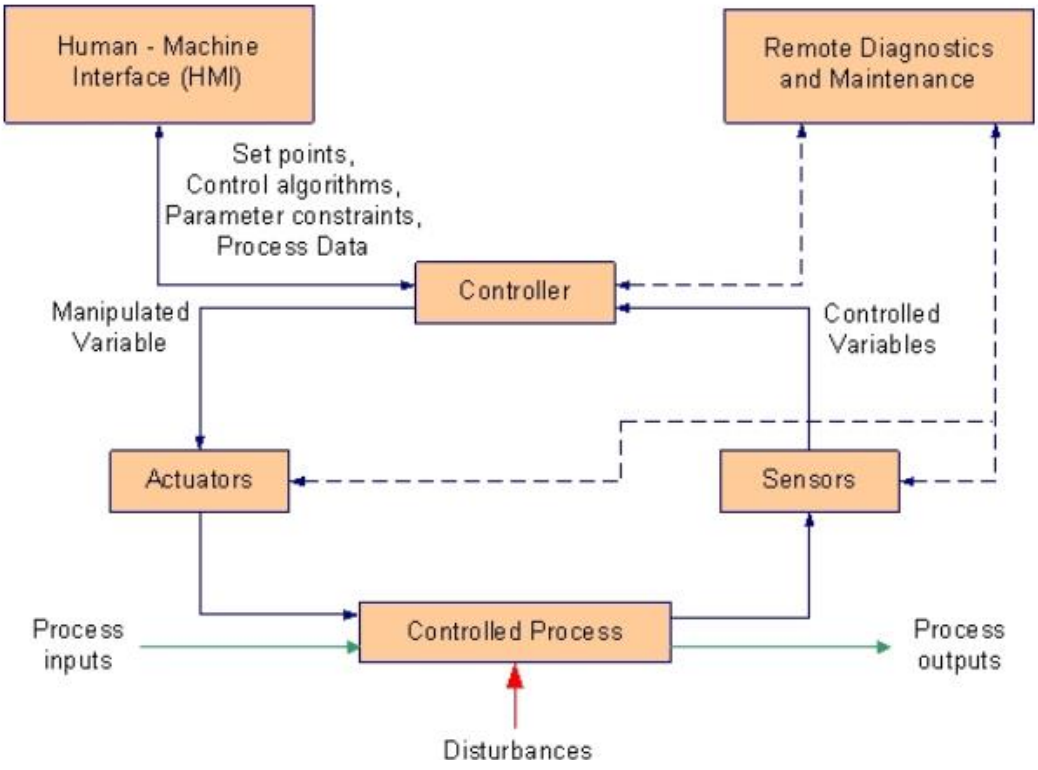

Figure 3: ICS Operation

[10] K. Tierney and M. Bruneau. Conceptualizing and measuring resilience - a key to disaster loss reduction. TR News, 250:14-17, 2007.

[11] C. Folke. Resilience: The emergence of a perspective for social-ecological systems analyses. Global Environmental Change 16, 2006.

the IIoT system behavior is based on the scheme of typical ICS operation shown in Figure 3[12]. The IIoT system exists in two contexts, Operational Technology (OT) and Information Technology (IT). The control process exists in the OT context while the informational flows controlling how this process goes come from the IT context. Sensors and actuators tie these contexts together.

Let's define the formal model for the IIoT system behavior by the subsequent definition of its following components:

- input data, output data and environment,
- process definition, and
- requirements to the IIoT system behavior.

Input data, output data and environment

The set of input variables $X = \{x_1, \dots x_N\}$ characterizes the input data for the control process (OT), or *Process Input*.

The set of output variables $Y = \{y_1, \dots y_M\}$ characterizes the output data for the control process (OT), or *Process Output*.

The set of variables S_{IOT} describes the system environment. These variables include the values describing the parameters of both the IT and OT context.

$S_{IoT} = \{s_i | i \in 1 \dots l\}$ – environment variables set

$$\forall s_i \; type\;(s_i) = \begin{cases} S_{OT} \\ S_{IT} \end{cases}, S_{IoT} = S_{OT} + S_{IT}$$

The set of variables $Ad = \{ad_i | i \in 1 \dots k\}$ represents the adversary. We consider only the adverse conditions that arise in the IT environment, $At \subseteq S_{IT}$.

Process definition

As cyber resilience requires some actions on "adverse conditions, stresses, attacks or compromises on systems that use or are enabled by cyber resources," there should be a possibility to recognize these conditions, stresses, attacks or compromises. In other words, we assume they are accountable. As they are accountable, the appropriate data describing them may be generated during the process. The data describing security and safety events are usually produced by sensors, for example, on the basis of a watchdog mechanism, detection of attack signatures or passive recognition of the new devices in a network.

Let's define *D* as a set of sensors and actuators data. These data are obtained by applying the functions transforming the OT data to their IT representation:

$$\delta_X : X \to D_x, \delta_Y : Y \to D_y, \delta_{IoT} : S_{IoT} \to D_{S_{IoT}}, D = D_x \cup D_y \cup D_{S_{IoT}}$$

The control system makes a decision based on data D. In our representation, the sensors and actuators that are the part of the system

[12] Source: Keith Stouffer, Suzanne Lightman, Victoria Pillitteri, Marshall Abrams, and Adam Hahn. NIST Special Publication 800-82 Rev.2. Guide to Industrial Control Systems (ICS) Security. National Institute of Standards and Technology, U.S. Department of Commerce, 2015. https://doi.org/10.6028/NIST.SP.800-82r2

transform these data according to the processing algorithm.

If the data obtained from sensors are inappropriate or sensors are incapable of providing the valuable indicators of adverse conditions, system resilience may be compromised because the decision of the monitoring mechanism is irrelevant with regard to the real system state. The example is the event in Maroochy, Australia, in 2000. [13] The event was an intentional, targeted attack by a knowledgeable person on an industrial control system. To conduct this attack and make the consequences of the failure more serious, the attacker suppressed and tampered with the data from the sensors, thus not revealing the attack.

The following formal assumption supports the resilience aspect from the perspective of accountability and monitoring:

Assumption. The basic condition for providing IIoT System Resilience. For any system state and any adverse condition, stress, attack or compromise, the functions transforming Process Input, Process Output and Environmental data to their IT representation remain unchanged.

This assumption must be valid if resilience is provided on the basis of monitoring. At the same time, it can be generally described only using the higher-order predicates. This makes the appropriate evaluation problem unsolvable in a formal way. The relevance of the control data in the IT context to the real physical values is usually supported by the technical engineering and design approach.

Let's describe formally the control process from the perspective of interaction of OT and IT. The generalized function *U* represents the appropriate generalized control function ***F*** represented in the IT context.

Control function

$$\boldsymbol{F}: (ST, C, R, D_x, D_{S_{IoT}}) \rightarrow D_y \quad (1)$$

Depends, except the data, on the following arguments:

ST – algorithmic structure of the functions; the set of algorithms determining how the process works (control algorithms, request handling, etc.)

C – the set of parameters for the algorithms (trigger values, default mode, etc.)

R – system resources used to perform the operations.

Output of the control functions based on fixed algorithms, parameters and resources depends only on the sensors data and environment.

$$F = \boldsymbol{F} < ST, C, R >$$

From (1) we have the following parametrized function:

$$D_y = F\left(D_x, D_{S_{IoT}}\right) \quad (2)$$

Process Output depends on the Process Input and feedback from equipment (if the operation was performed successfully, etc.):

[13] Marshall Abrams and Joe Weiss. Malicious Control System Cyber Security Attack Case Study – Maroochy Water Services, Australia. August 2008. https://www.mitre.org/sites/default/files/pdf/08_1145.pdf

$$Y = U(D_y, X) \quad (3)$$

Thus by substitution of the (2) in (3) we gain:

$$Y = U(D_y, X) = U(F(D_x, D_{S_{IoT}}), X) \quad (4)$$

Requirements

Let's now define the requirements to the system behavior from the IT perspective that allow this behavior to remain resilient. That means keeping the Process Output relevant to its IT representation event under adverse conditions. That also means facilitating security and privacy and keeping the appropriate physical process safe and reliable even under the impact of the human factor.

We define the requirements $Z = \{z_i | i \in 1 \dots l\}$ as conditions set for the accountable data in one of the following forms: threshold, equality, optimization. The form of the system requirements is

$$\{\langle y_i \geq a_i \mid y_i = b_i \mid y_i \to min \rangle\}$$

Conditions that are more complex do not change the reasoning.

Among the system requirements, we highlight the essential requirements that comprise a subset of all requirements and generally determine the conditions that must be kept invariant in any system state.

$\exists r \leq l: Z^* = \{z_i\} | i \in 1 \dots r\}$ – essential output requirements;

To consider the system's dynamic behavior, we introduce the time *t* represented by one of the environment variables.

Definition 1. System requirements. The IIoT system meets the requirements for any system state and all conditions determining these requirements are satisfied. The appropriate predicate P depending on the system output is true if the system meets all requirements.

$$P(Y(t), Z) = TRUE \leftrightarrow \forall t \, \forall i \, (y_i, z_i) = TRUE \quad (5)$$

Let's define the Resilience aspect on the basis of the proposed model.

RESILIENCE DEFINITION IN TERMS OF THE PROPOSED MODEL

The Formal Definition of the Resilience Aspect

The basic idea behind the resilience aspect is that the system meets the established requirements in any state. In other words, we assume that the predicate P remains true even under adverse conditions.

Definition 2. Resilience. The system is considered resilient if in any system state the predicate P is true.

Let's make a substitution in (5) using (4) to elaborate on the connection of the Process Output and Process Input in the context of Resilience.

$$P(Y(t), Z) = P(U(F(D_x, D_{S_{IoT}}, t), X), Z)$$

$$P(Y(t), Z) = P(U(\boldsymbol{F} < ST, C, R > (D_x, D_{S_{IoT}})(t), X), Z) \quad (6)$$

Formal Consideration of Resilience Goals

Using this detailed expression, we now consider the Resilience goals defined in Draft NIST Special Publication 800-160 VOLUME 2: anticipate, withstand, recover and adapt.

Anticipate is to maintain a state of informed preparedness for adversity.

The need for preparedness for adverse conditions should be addressed by assurance on the proper choice of one or more parameters for the generic control function ***F***: control algorithms, parameters of control and the available resources. Assurance on control algorithms means the verification of their behavior against adversity. Assurance of parameters and resources means checking their adequacy and sufficiency for supporting that behavior.

Maintaining the state of informed preparedness requires the situational awareness based on the indicators of possible compromise. For this purpose validation of input data D_x and monitoring of environmental data D_S should be continuously performed.

Withstand is to continue the essential mission or business functions despite adversity.

The violation of requirements for continuous mission execution means that the predicate P is FALSE for some period of time.

$$\exists ad_i, \exists T_{ad}: P(Y(T_{ad}), Z) = FALSE$$

To support the required property we need to reduce the time period T_{ad}. Thus, supporting resilient execution turns to the optimization problem $T_{ad} \to min$. This approach to the system resilience by withstanding the adverse conditions is best illustrated by the interpretation referred to earlier of resilience through the quality of service.

Adapt is to modify the mission or business functions and/or supporting capabilities to predicted changes in the technical, operational or threat environments. Adaptation may be required when the attack is successful:

$$\exists ad_i, \exists T_{suc}: P(Y(T_{suc}), Z^*) = FALSE$$

T_{suc} is the time period to reduce $T_{suc} \to min$. during this period the current system behavior does not satisfy Z^*.

Adaptation helps to withstand the adverse conditions and recover in minimal time (for example, by changing the parameters of the generic control function ***F***) but it also leaves the system in a configuration better prepared for further adversity.

A variety of adaptations may enhance resilience, including:

a) **Adaptation of requirements**
   $\forall t \forall s_i \; P(Y(t), Z^*) = TRUE;$
   The set of requirements may be reduced to the set of essential requirements, the minimal set for which system functioning remains satisfactory.

b) **Parametric adaptation**
   $\forall t \forall s_i \exists C^* \neq C: P(U(F < ST, C^*, R > (D_x, D_{S_{IoT}})(t), Z) = TRUE$
   The set of parameters determining how the system functions may be changed.

c) **Algorithmic adaptation**
   $\forall t \forall s_i \exists ST^* \neq ST: P(U(F < ST^*, C, R > (D_x, D_{S_{IoT}})(t), Z) = TRUE;$
   The algorithms of the process control may be changed.

d) **Resource adaptation**

$\forall t \forall s_i \exists R^* \neq R: P(U(F < ST, C, R^* > (D_x, D_{S_{IoT}})(t), Z) = TRUE$

An example of resource adaptation is increasing the resources to mitigate a DDoS attack.

e) Environment adaptation

$\forall t \forall s_i \exists (D_x, D_{S_{IoT}})^* \neq (D_x, D_{S_{IoT}}):$
$P(U(F < ST, C, \text{К} > (D_x, D_{S_{IoT}})^*(t), Z) = TRUE$

The system may be put into a restricted environment or an environment with different characteristics (such as a virtual machine), or the source of the disturbance may be removed from the environment.

Recover is to restore the mission or business functions during and after adversity.

In case the system, due to its exposure to adverse conditions, cannot restore its execution during some period of time, we consider its capability to recover after this period:

$$\forall t \forall s_i \exists T_{RES}: P(Y(t), Z^*) = TRUE, P(Y(t + T_{RES}), Z)$$

The recovery problem focuses on optimizing the restoration period $T_{RES} \rightarrow min$. It may be implemented by temporarily adjusting the parameters for the generic control function ***F***; changing control algorithms, parameters of control and employing extra resources until conditions normalize.

According to the considered interpretation of the resilience goals, the following high-level metrics for cyber resilience may be proposed in terms of the model:

- T_{ad}, the time period during which the system is capable of withstanding the adversity,
- T_{suc}, the time period during which the system does not satisfy the set of essential requirements because of adversity, and
- T_{RES}, the time period during which the system is capable of restoring its functioning during and/or after adversity.

Classification of Resilience Techniques and Approaches

The Draft NIST Special Publication 800-160 VOLUME 2 considers the resilience approaches: Adaptive Response (AR [14]), Analytic Monitoring (AM), Coordinated Defense (CD), Deception (De), Diversity (Di), Dynamic Positioning (DP), Dynamic Representation (DR), Non-Persistence (NP), Privilege Restriction (PR), Realignment (Ra), Redundancy (Re), Segmentation (Se), Substantiated Integrity (SI), Unpredictability (Up). Let's consider this list using the proposed model from the perspective of choosing the approaches and techniques according to existing constraints.

Applying a technique or approach from the list requires accountability of some characteristics and may entail a change in one or more parameters of the predicate P

[14] This and the following acronyms for the approaches are not defined in the Draft NIST Special Publication 800-160 VOLUME 2. We introduce them here to use further in the table.

(6). This makes the value of P true. This is how these techniques and approaches help to achieve the resilience goals considered earlier in this article.

The approaches listed in Table E-1 of the Draft NIST Special Publication 800-160 VOLUME 2 may be implemented either at design phase or at runtime.

Approaches implemented at design phase provide the foundation for building resilience capacity. These approaches and techniques are mostly passive. They set up the types and appropriate ranges for the factors of the generalized predicate P in (6).

Approaches used at runtime help in dynamic realignment of algorithms, resources and data according to dynamically changing environment and constraints. These approaches and techniques are considered active because they influence the factors determining resilience according to (6).

Not all approaches can be implemented for every given system. Depending on the initial state and functional constraints the stakeholders may consider the options of how to increase system resilience. The classification shown in the Table 1 helps to clarify these options.

Table 1 – Classification of resilience approaches and techniques according to the proposed model

Factors	**Active resilience techniques and approaches implemented at runtime**	**Passive resilience techniques and approaches implemented at design phase**
ST ***Algorithmic structure of the functions determining the control process behavior***	Non-Persistent Services / NP Non-Persistent Connectivity / NP Dynamic Segmentation and Isolation / Se Temporal Unpredictability / Up Contextual Unpredictability / Up	Consistency Analysis / CD Orchestration / CD Architectural Diversity / Di Design Diversity / Di Synthetic Diversity / Di Supply Chain Diversity / Di Distributed Functionality / DP Restriction / Ra Replacement / Ra Specialization / Ra Predefined Segmentation / Se

C ***The set of parameters for the algorithms***	Dynamic Reconfiguration / AR Attribute-Based Usage Restriction / PR Dynamic Privileges / PR	Path Diversity / Di Trust-Based Privilege Management / PR
R ***System resources used to perform the operations***	Dynamic Resource Allocation / AR	Asset Mobility / DP Purposing / Ra Offloading / Ra Protected Backup and Restore / Re Surplus Capacity / Re Replication / Re
D_X ***Input data in the IT context***	Obfuscation / De Functional Relocation of Cyber Resources / DP Non-Persistent Information / NP	Synthetic Diversity / Di Fragmentation / DP
D_{SIoT} ***Environment represented in the IT context***	Disinformation / De Misdirection / De Tainting / De Functional Relocation of Sensors / DP	Monitoring and Damage Assessment / AM Sensor Fusion and Analysis / AM Dynamic Mapping and Profiling / DR
Z ***System requirements***	Adaptive Management / AR Monitoring and Damage Assessment / AM Malware and Forensic Analysis / AM Integrity Checks / SI Provenance Tracking / SI Behavior Validation / SI	Calibrated Defense-in-Depth / CD Sensor Fusion and Analysis / AM Self-Challenge / CD Dynamic Threat Modeling / DR Mission Dependency and Status Visualization / DR

Now, to identify the appropriate technique and the approach to enhance the system resilience, the stakeholders must consider which of the IIoT system characteristics may be varied during the design phase. When the system is functioning, feasibility analysis is applied to consider the appropriate algorithms, technologies and implementation options.

The illustration for applying this method is provided in the following case studies:

> Case study 1. In the industrial network, increasing the resilience of the data historian to the external impact
>
> Case study 2. Increasing the resilience of an e-commerce website to DDoS attacks

While these case studies seem to be similar, the tactic for their protection against malicious impact varies.

This is primarily due to the nature of connected risks. The impact on the data historian is linked to either occasional events or to the attempts to compromise the control equipment. The data historian server is unlikely to provide an economically attractive goal for a targeted attack. At the same time, the data historian may be a goal for a rogue person trying to sabotage the control process. Thus, some efforts are required to provide the resilient execution of the functions implemented by the data historian.

Among the factors that influence the ways to enhance resilience for this case study, the following may change: algorithmic structure of the monitoring functions (ST), the set of parameters for the algorithms (C) and system resources used to perform the operations (R). Input data (monitoring data from the control equipment), environment and criteria for resilient execution cannot change.

The data historian server in the industrial network is usually placed in the demilitarized zone, a network segment behind the perimeter of subnetwork containing the control equipment. This zone is also separated from the corporate network connected to the Internet but can be reached from specific computers in this network. This best practice, being properly implemented, also facilitates the resilience of the data historian server but it still remains exposed to the attacks via these specific computers. Changing the algorithmic structure of the monitoring functions and parameters for these functions to implement self-monitoring may help to reveal the attacks. Installing the secondary data historian server and periodic backups are ways of enhancing the resilience of monitoring the control process by allocation extra resources (R).

This is the simple case but the second one is much more complicated. Most of the attacks have financial underpinnings so the e-commerce websites, such as payment system, are the likely target for many threats. Among these threats, we specifically consider DDoS attacks which may be implemented on different layers. The first level is L2, linked to the depletion of channel capacity (any flood attacks, implemented, for example, through amplification of ICMP, NTP, DNS or other requests). The second level is L3, attacks at this level influence the functioning of the network infrastructure.

These are the attacks that cause the problems of routing (such as BGP hijacking) and any general problems on transit network equipment. The third level is L4, at which attacks to exploit the weaknesses of the transport protocol. The most known example is the SYN flood attack. The fourth level, L7, is degrading the web application by various methods, from the simple GET/POST flood to the specifically formed search requests targeting the database, memory or disk space depletion on the server.[15] The most damaging DDoS attacks mix volumetric attacks with targeted, application-specific attacks.[16]

It is worth mentioning that these attack tactics against the data historian would be an overkill. For the financially relevant web service, their existence imposes the advanced strategy for supporting a resilient execution of the services. The separate measures employ the techniques and approaches linked to the factors as listed below.

Algorithmic structure of the functions determining the control process behavior (*ST*): At the design phase, the architect performs consistency analysis to identify bottlenecks, minimize potential cascading failures and cover gaps. Orchestration helps to coordinate the mechanisms at different network layers. Proper privilege restrictions should help in containing attacks. As a supportive measure, diversity may foster the resilience to exploit the specific vulnerabilities by attackers. At runtime, non-persistent services and connectivity are usually used to minimize the downtime period (for example, through promptly changing the hosting provider). Dynamic segmentation and isolation serve similar purposes for the complex environment under attack.

The set of parameters for the algorithms (*C*): At the design phase, the architect can consider the trust-based privilege management where trust is determined through the set of attributes and current threat landscape. Dynamic reconfiguration of attributes values and attribute-based usage restriction at runtime will help to rule out the parasite traffic.

System resources used to perform the operations (*R*): Redundancy is the most known factor supporting continuous operation under challenging conditions. However, it is not only about the additional disk capacity. The website architecture supporting purposing, offloading and asset mobility is not only sustainable, it also facilitates dynamic resource reallocation and reasonable reservation scenarios. These scenarios may implement different strategies to cure a failure through infrastructural means. This may be automated, for example, through the use of high-availability clusters (also known as fail-over clusters) that are the groups of

[15] The level numbers correspond the OSI model level at which the attacks are implemented

[16] Stephen Gates. Understanding and Defending Against the Modern DDoS Threat. RSA Conference 2014: Asia Pacific and Japan. https://www.rsaconference.com/writable/presentations/file_upload/cle-t09-understanding-and-defending-against-the-modern-ddos-threat.pdf

computers supporting server applications reliably utilized with a minimum amount of downtime. They operate by using high availability software to harness redundant computers in groups or clusters that provide continued service when system components fail.

Input data in the IT context (D_X): This factor is the most difficult to influence because of the fact that the attack is concealed in requests that look ordinary, but taken together, may cause a failure. Filtering alone does not work for the volumetric attacks (L2) at all and is not useful for mitigating L3 and L4 attacks. It may be helpful to withstand some of L7 attacks and for the surgical strike at attack sources identified due to the environment monitoring.

Environment represented in the IT context (D_{SIoT}): This factor also plays a supportive role. At the design phase, the architect may incorporate the means for the monitoring and damage assessment, dynamic mapping and profiling which would help to detect the attack at the early stage.

System requirements (Z): Changing the system requirement to the resilience of the e-commerce website represents the next level of approaching the problem. During some periods, the uninterrupted execution may be more important than it usually is. For online stores, the simplest example is the time before some public holidays and periods of sale. For the payment system, this is the time period during which it expects significant transactions. Requirements may depend on the time of the day in different time zones, the season, political landscape and processes, and so on.

Thus, the listed measures must be constantly updated by the operations team to keep up to date with the latest threats. DDoS tactics change almost daily and the supporting personnel must be prepared to update services to the latest threats.

CONCLUSION

The resilience aspect is one of the most demanded IIoT system characteristics. Often resilience is achieved by designing the system so that failures are compartmentalized. If a single function fails it should not cause other functions to fail, and there should be alternate ways of performing the failed function in the design that can be invoked automatically, immediately and reliably. Resilience may also be achieved through the dynamic adaptation of the system characteristics to the changing adverse conditions and even through adaptation of requirements to the system behavior (for example, when one of the aspects comes to the forefront).

The proposed semiformal model of the IIoT system behavior approaches the problem with the clear understanding of which techniques facilitate the resilience of the IIoT system, and which are not useful. It may be further used as the basis for the method of identifying appropriate approaches for enhancing IIoT system resilience.

The key takeaways from the proposed model are:

1. The high-level resilience metrics for cyber resilience are the time periods: the period during which the system is capable of withstanding the

adversity; the period during which the system does not satisfy the set of essential requirements because of adversity, and the time period during which the system is capable of restoring its functioning during and/or after adversity. These metrics are formalized and can further be evaluated. This method of evaluation require additional research.

2. Resilience approaches and techniques which can be used to increase the system's resilience to attacks may be classified according to the factor which they consider and influence. This is quite helpful in identifying the applicable approaches for a particular case.
3. The risks connected to the use of the IT and IIoT services determine much of the strategies applied to increase the resilience of these services. The comparative examples demonstrate how the resilience strategies may vary significantly even for similar technologies. Currently, the process of identification is based on the expertise of the system architect. However, the method of semi-automated analysis may comprise a scope of further research.

➢ Return to IIC Journal of Innovation landing page for more articles and past editions.