An Indicators-of-Risk Library for Industrial Network Security

Carolina Adaros-Boye
carolina.adarosboye@mail.bcu.ac.uk
Birmingham City University
Birmingham, UK

Paul Kearney
paul.kearney@.bcu.ac.uk
Birmingham City University
Birmingham, UK

Mark Josephs
mark.josephs@.bcu.ac.uk
Birmingham City University
Birmingham, UK

Hans Ulmer
hans.ulmer@de.bosch.com
Bosch
Stuttgart, Germany

ABSTRACT

This paper introduces an “Indicator of Risk (IoR) Library" that leverages the MITRE ATT&CK for Industrial Control Systems (ICS) knowledge base to support continuous risk monitoring. This allows also making use of variables that are already being monitored to analyse risks in a continuous basis. IoRs broaden the concept of Indicators of Compromise by combining detection strategies with probabilistic inference as a tool for quantifying cyber-security risks. The latest version of the Library has 95 IoRs and has been reviewed by professionals from three major companies and cross-referenced against detection use-cases implemented by other researchers to validate its potential to identify variables for monitoring cyber-risks in ICS.

CCS CONCEPTS

• cyber-security, risk monitoring, IoR, IIoT, ICS

KEYWORDS

datasets, neural networks, gaze detection, text tagging

1 INTRODUCTION

The convergence of Operational Technology and Information Technology has introduced new opportunities for cyber-attacks with potential to disrupt time-critical and hazardous industrial processes. In industrial networks security risks can have serious impacts that affect critical infrastructure, cause physical damage or incur high

costs. However, some security controls can have technical constraints [10] (e.g. interrupting 24x7 operations to install patches might not be an option) for which residual risks are accepted. Inthese cases, continuous risk monitoring aims to recognise conditions or events that could increase the likelihood of an incident, and even detect attack attempts at an early stage which can act as a compensating control.

To address this challenge, in [2] and [3] we proposed a methodology for continuous risk management in Industrial Control Systems (ICS) and the Industrial Internet of Things (IIoT) in which risk assessment is treated as a continuous data-driven process performed every time that a new security-relevant event occurs, rather than on a scheduled basis. In this context, we defined “Indicator of Risk” (IoR) as an observation that can modify probability estimations allowing the assessment of cyber-risks to be updated. IoRs go beyond security events detection by allowing monitoring also the risk exposure of the system.

In this paper we aim to answer two research questions: “What information is needed in order to monitor security risks in ICS/ IIoT?” and “How can that information be derived from variables that are measurable?” As is well known, the characterisation or quantification of risks is mainly based on two components: the probability and the impact [6][15][25]. As impacts are asset dependent and are not likely to change frequently, continuous risk monitoring is based on awareness of factors that could influence the probability of a cyber-security related event. To help identifying these factors, we developed an artefact called the “IoR Library", in which IoRs are mapped to adversary techniques from the ICS MITRE ATT&CK [21].

In contrast to enterprise IT, industrial control and automation systems are diverse and each particular environment is fairly unique. This means that the specifics of an IoR can vary from system to system. Hence, our work consists of a catalogue with a high-level overview of IoRs that can be specialised to a specific system. For

each IoR, the library provides guidance on its interpretation, how it relates to various techniques and how it may be implemented in particular contexts.

The purpose of the IoR Library is to help identifying variables that can be used to monitor cyber-risks in ICS based on observation of events and conditions at all levels of the system. IoRs are then based on observations made on different assets such as hosts, endpoints, work-stations, Human-Machine Interfases (HMI), IT and OT networks,

and field devices. The main contribution of this work is to provide a model with a common language for defining and sharing risk information. This can serve as a basis to enable real-time risk monitoring using suitable tooling at the same time of advocating for the integration between the risk management and the security operations. This forms part of a bigger picture which relates to the idea of continuous risk management in ICS.

Despite that, at this stage, the work on IoRs could be considered as rather conceptual, the IoR Library can be a useful resource to share knowledge among the ICS security community. One of the motivations of sharing this work is to gather inputs from the end users community to enhance the descriptions and use case examples for each existing IoRs and to add new IoRs to the library. The relevance and novelty of IoRs is that they allow using information from operations security for assessing risks dynamically. This could enable the development of future approaches for continuous risk monitoring, such as the ones proposed in [2] and [3]. The rest of this paper is organised as follows. Section 2 describes the MITRE ATT&CK framework and its use in our work, followed by an explanation of the IoR concept in Section 3 and a summary of related work in Section 4. Section 5 describes the IoR Library and Section 6 a method for applying it to continuous risk monitoring. Section 7 provides an evaluation of the IoR Library, and Section 8 mentions future work and challenges followed by the conclusions in Section 9.

2 USE OF THE MITRE ATT&CK FRAMEWORK

The ATT&CK (Adversarial Tactics, Techniques & Common Knowledge) framework [21] developed by the MITRE Corporation of adversary Tactics, Techniques, and Procedures (TTPs). It is based on real-world observations, such as reported attack cases or malware detected in the wild, and presented as a set of matrices relevant to different contexts, which currently are of three types: Enterprise (including Windows, MacOS, Linux, and cloud and network platforms), Mobile (including Android and iOS platforms), and ICS, which is the one referred to in this paper. ATT&CK is used as a foundation for threat models in the private and government sectors. Several well-known security tools and SIEM (Security Information and Event Management) platforms are aligned with ATT&CK [27][12] including tools specific to OT [13]. Thanks to the collaboration of the security community, ATT&CK is a rich source of information about adversary TTPs and has the potential to form the basis of a common framework for security professionals, enabling interoperability of tools and platforms.

An ATT&CK Matrix is essentially a hierarchically structured tactical library for understanding the behaviour of threat agents. A Tactic is a high-level part of a threat agent's repertoire. Each Tactic is associated with a number of Techniques, which are alternative ways of carrying out the Tactic. A concrete way to execute a technique is known as Procedure. An adversary's general strategy will include Tactics as the major steps in the plan and one or more techniques for each tactic. The Technique is the central concept in the ATT&CK framework. Tactics are means of grouping Techniques used at a similar stage in an attack. Procedures are too numerous, varied and technology-specific to be catalogued exhaustively, and appear primarily as illustrative examples. Each entry in a Matrix gives account of the technique in question, and has a number of sub-sections, such as: Description, Procedure Examples, Mitigations (controls that can reduce susceptibility to the Technique), and Detection (means by which use of the Technique may be recognised). The Technique entries in the ICS Matrix do not have Detection sections, but often do list examples of Data Sources and Assets that are useful for this purpose. ATT&CK for ICS was released in January 2020, and has its focus on adversary TTPs whose primary goal is to disrupt an industrial control process. This can cause physical damage, harm to the environment, injury and even death. As ICS are also integrated with or connected to enterprise IT systems, ATT&CK for Enterprise serves as a complement to ATT&CK for ICS. However, since enterprise cyber-security is a more developed area for which several playbooks and detection use cases are already known, the IoR Library is focused on the ICS matrix.

Previously to writing this paper and developing the IoR Library, we presented the idea of using IoRs for ICS continuous cyber-risk monitoring at a European MITRE ATT&CK workshop, in May 2020. This idea, not yet mature at the time, was conceived from the need to find a systematic way to identify IoRs regarding which the recent release of the ICS matrix of ATT&CK came as an opportunity to relate our work on continuous risk management to a well-known and widely used framework. As a follow-up of this presentation this idea was discussed in more depth with members of the security community who showed interest in the IoR concept. Following this, a more elaborated presentation was done in the European MITRE ATT&CK workshop, in June 2021. By the time of writing the present paper, we have transformed this idea in a concrete product, which consists on a knowledge base [1] that extends ATT&CK for ICS and provides examples of means that can allow inferring the risk of various adversary Techniques to be used against a system. We term these mechanisms Indicators of Risk (IoR). Their concept and value is explained in more detail in the following section.We envisage relevant IoRs being referenced from the Detection section of Technique entries. The same approach could in future also be applied to the other Matrices.

3 WHAT IS AN INDICATOR OF RISK (IOR)

The conception of IoR developed in our research is based on integrating cyber-security monitoring with continuous risk monitoring. While the first allows investigation and identification of possible events related to adversarial actions and blocking these actions, the second analyses events to provide an overview of the risk exposure. Threat detection strategies can be based on discovering changes in the system's environment or on discovering signs of adversaries' activities [19]. IoRs, as defined in our research, can be either environment or threat based, as well as based on conditions that make a system more vulnerable to attacks.

Overall, IoRs can refer to any detectable condition, the observation of which alters the estimated probability of one or more possible threat events. When IoRs are observed, the risk of an attack attempt being performed in the present or immediate future increases. This differs from IoCs whose purpose is detecting an attack with the highest degree of certainty as possible. In the case of IoRs the purpose is to support the reduction of uncertainty, which is the main goal of risk management. Hence, data already obtained through security monitoring but which is not efficient for detection, for example, due to a high rate of false positives, can still provide valuable information about risk exposure.

Our idea of IoR comes from a merger of the concepts of “Key Risk Indicator”, commonly used in risk management, and Indicator of Compromise (IoC). An IoC can be defined as “one or more artefacts that relate to a particular security incident or attack” [4] or “artefacts observed on a network or in an operating system that indicate a computer intrusion with a high degree of confidence” [12]. IoCs with a lower degree of confidence are not taken into account because they can generate a high number of false alerts, which can overwhelm security operators. However, this information can still be of value for risk analysis. An IoR will not necessarily trigger a

security alert but will raise awareness of an increased level of risk. This can be useful for an organisation to continuously assess their security posture and act proactively to counter-act cyber-security threats. Figure 1 represents a conceptual relationship between IoRs, IoCs, and security alerts, as conceived in our continuous risk management approach [3].We consider that IoRs cover and extend IoCs. Whereas IoCs can give a more deterministic indication of a threat for which they can be used for threat detection in security operations, IoRs refer to risk exposure, for which they can be also related to system vulnerabilities and misconfigurations. It must be noted that some definitions of IoC restrict them to specific characteristics of an attack procedure, such as IP addresses, hashes, signatures, URLs, domain names, or attack tools [19] [17]. However, wider definitions of IoC [14] consider as such any event that meets requisites to be considered as such, regardless of the detection mechanisms used. According to this last definition, our IoR concept shares with an IoC the property of being an observation of any condition which can provide evidence of a security event. However, the IoRs have the purpose of providing indication of the likelihood of an event, not necessarily alerting about a threat. For example, the observation of a set of IoRs can allow inferring that the current probability of a Denial of Service attack, which was initially estimated as negligible had raised to 5%. This would mean that previous risk evaluations about this threat and the corresponding security controls might need to be revised. IoRs, differently to IoCs, also cover vulnerable conditions and observations that can be related to threats and that can be valuable from the risk analysis perspective but could be ignored or dismissed by a SOC.

Figure 1: Indicators of Risk uncertainty levels

For an IoR to be successfully implemented it is important to have the appropriate tools to capture and process the data that exposes the conditions that the IoR is meant to observe. These observations can include also configuration analysis and behavioural analysis for detection of oddities or anomalies in the system and its processes that can be related with cyber-security risks. This also follows recommended practices for ICS security monitoring [19] [20].

In “A Survey of Security Tools for the Industrial Control System Environment” [17] different attributes are defined to characterise currently available security tools for ICS. These attributes include the ICS level in which they work, their purpose or functions, and their transport means or interfaces. The availability of tools will ultimately define the types of IoRs that can be feasible to detect from all the possible conceivable ones. Examples of functions defined in [17] are IoC detection, network traffic anomaly detection, outlier analysis, and log review. Organisations that have already implemented ICS security monitoring tools can benefit from the inputs that they provide to generate IoRs. The goal of monitoring IoRs is to provide valuable information about the state of cyber-risks, and even support cyber-security operations by improving detection capabilities. In our work, IoRs are defined from a high-level perspective and should be defined in more detail for a specific implementation. For example, the IoR “VPN suspicious Access log” can be decomposed into a higher number of lower level detection use cases such as “remote access from foreign country”, “login successful after scan attempt”, “possible shared accounts”, and “VPN sneak attack” [24]. These use cases shall be defined by rules at a tool level, for example, to define what is a foreign country it is necessary to whitelist IP addressed from the local country and/or blacklisting the ones from foreign countries.

4 RELATEDWORK

Continuous risk monitoring can allow making use of additional data gathered during operation to improve the risk estimates, as well as to track changing risk values. One of the first academic works proposing a real-time cyber security risk assessment based on network sensors and IDS was done by Årnes and Haslum in 2005 [6] [16]. They propose a multi-agent architecture in which each assessed element has a security state vector “S". States are probabilistic and have three qualitative values: Good, Attacked, or Compromised. In most recent years, other theoretical approaches have been built based on their work in which the probability of a state is based on observations [7][31]. Other pioneering work proposing a method to provide a dynamic cyber-risk picture was published by Refsdal and Stølen in 2009 [25].

Among the main techniques and methods reviewed that were found to be potentially useful for dynamic risk calculations are Bayesian Networks [29] [30], Hidden Markov Models [31], and fuzzy logic [18]. Another important reference of continuous or real-time cyber-security risk assessment is the Wide-Impact Cyber Security Risk Framework (Wiser) which was a project developed under the Horizon 2020 European Initiative [33]. There are also several examples of methods developed specifically for industrial networks and ICS, which gather real-time data for industrial operations [11][32][15][8]. Other publications such as [28] [26] and [20] provide useful insight on security detection tools and techniques for ICS, which constitute a useful reference for the present work. However, as far as our knowledge not work has been previously published that is focused on providing a structured knowledge base for identifying cyber-risk indicators for ICS.

5 BUILDING THE IOR LIBRARY BASED ON ICS ATT&CK

The IoR Library is a knowledge base aligned with MITRE ATT&CK for ICS, to be used to identify IoRs that can be related to different adversary Techniques. Its main purpose is to facilitate the implementation of continuous risk assessment in a variety of contexts and industrial environments. The complete overview of the IoR Library can be found in a publicly accessible repository, specified in [1].

IoRs shall be selected according to the risks that have been already identified and analysed and to implementation feasibility. Thus, each continuous risk monitoring implementation will be different and unique, depending on the ICS environment, business objectives, security posture, and detection and monitoring capabilities. It is not possible to define the use of IoRs in a prescriptive way, hence, we provide a structured high-level guidance to identify and select the IoRs that are more appropriate. This has the advantage of not excluding the use of well-known standards for security information sharing such as STIX and TAXII [5].

The latest version of the IoR library has 95 IoRs and covers 50 techniques from ICS ATT&CK. The ID naming scheme, shown in Table 1 groups IoRs according to the level of the ICS to which they apply, based on the Purdue model [22] (see Figure 2). IDs have “IoR" as a prefix followed by three digits, the first one represents the group to which the indicators belong and the others are an incremental counter. The third and fourth columns of Table 1 describe the levels in which each IoR group can be originated and observed, respectively. For example, the data from a sensor is originated in Level 0 (physical process) but can be observed also through a control and monitoring application. We also include IoRs from perimeter security and safety systems to acknowledge that they can provide useful data for an holistic risk monitoring, but the main focus of our work is centred on groups IoR0XX to IoR5XX.

Table 1: IoR naming scheme

IoR ID	IoR group	Data origin	Data observation
IoR0XX	Vulnerabilities	All levels	All levels
IoR1XX	IT threat (servers, workstations)	Level 2	Level 2
IoR2XX	IT network threat (ICT protocols)	Levels 1 and 2	Levels 1 and 2
IoR3XX	Field devices threats (controllers)	Level 1	Levels 1 and 2
IoR4XX	OT Network (Industrial protocols)	Levels 0 to 2	Levels 0 to 2
IoR5XX	I/O data threat (sensors, actuators)	Level 0	Levels 0 to 2
IoR6XX	Physical security threat	Building Mgmnt	Independent system
IoR7XX	Safety threat	Safety zone	Independent system

This scheme was developed under the assumption that an ICS will have a general network architecture similar to the one on the SANS version of the Purdue model [22]. However, it is expected for the system to present variations on its architecture and have their own naming for levels or zones. Hence, it can be chosen to modify the IDs accordingly. In our model communication between Level 3 and the Cell/Area zone is done via a standard IT network. In this case, only Level 2 is capable of processing both OT and standard IT protocols. Figure 2 also includes a variant in which the Manufacturing zone (Level 3) could be added to the scope, as a possible extension, which could incorporate other IoRs based on the techniques of the ATT&CK Enterprise matrices.

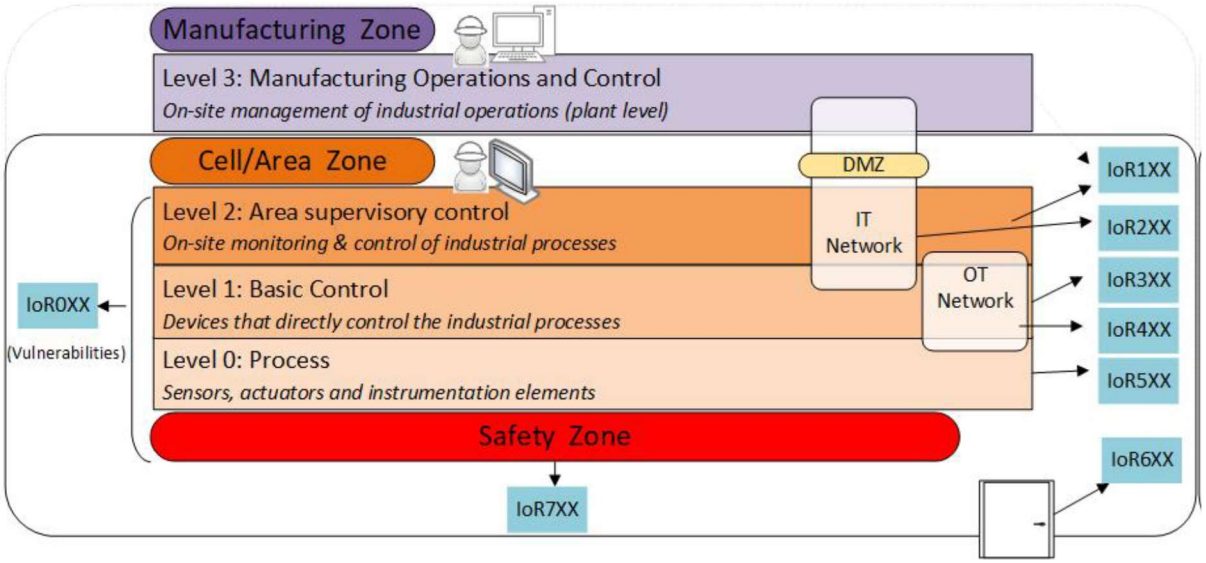

Figure 2: IoRs scheme related to Purdue model

The IoR library provides a list of IoRs cross-referenced with adversary techniques. Each IoR has its unique ID and name, and its entry in the library provides a rationale, examples of possible observations, examples, and a list of Techniques it is applicable to. The rationale explains the IoR and why it can be related to cyber-security risks, observations outline means of measurement or detection, and the examples provide use cases or illustrations of malicious actions that can be related to the IoR. The relationship IoR-Technique matrix and described further for each Technique in a separate Technique page. We propose a table to be added to ATT&CK Technique entries that lists the applicable IoRs, explaining how each one of them is linked to the Technique.

Figure 3 gives an example of four entries from different IoR types with their corresponding description fields. The first example correspond to having an outdated Operating System, which is a common situation on ICS servers and workstations. This gives an indication of a higher risk exposure since it can allow adversaries to take advantage of known vulnerabilities. A concrete implementation of this can be to make use of an asset inventory management system which can indicate how many devices are running outdated OS versions. The second example refers to the OPC protocol, which is widely used for servers and computers to communicate with industrial systems. Through this protocol, it is possible to send malicious commands, which can modify control rules. The OPC Unified Architecture supports Audit logging by providing traceability of activities through the log entries of multiple clients and servers [23]. This logs could be checked against a white-list of messages to identify unusual or forbidden messages or can be contrasted with a baseline of normal activities for recognition of unusual communication patterns. The in the third example, which refers to changes in a controller's program, the IoR can be implemented by monitoring change logs. For the fourth example, it is possible to implement rules in a SIEM tool to check the integrity of sensor's data by comparing different inputs.

Each IoR-Technique pair can be assigned an indication of the evidential strength of the IoR for this Technique named as "degree of influence". This can ultimately be translated into conditional probabilities. The degree of influence is an integer from 1 to 5 that suggests how much influence an IoR can have on estimating the risk of a technique. It can also be used to represent the influence that a technique or tactic has on the likelihood of another technique being performed. Each integer in the scale represents a 20% range of conditional probabilities. The default value is 1 (0 to 20%), used when there is not enough evidence for a higher probability. To estimate risk probabilities, we suggest using Bayesian Networks, which allow to calculate the conditional probabilities of different TTPs and events given the observation of IoRs. However, this is out of the scope of this paper.

6 USING THE IOR LIBRARY FOR CONTINUOUS RISK MONITORING

As explained earlier, the IoR Library describes observables, termed IoRs, which can be correlated with factors that enable, enhance the likelihood of, or are consequences of, the execution of adversarial Techniques listed in the ICS ATT&CK matrix. This includes systems configuration settings, alerts, logs, and measures of deviation from normal behaviour. We propose the following method to identify and select IoRs:

IoR	Rationale *Why this is consider an IoR?*	Observations *Examples of how this IoR can be observed*	Examples *Scenarios where the IoR might be observed*	Related Techniques
IoR008-Outdated OS	Outdate OS can be missing security patches against known vulnerabilities. Also an OS that has passed the EOL will have no support and no further security updates.	Not having the latest version of the OS.	Adversaries might use known means of exploit of OS vulnerabilities, which can allow actions such as arbitrary code execution or a DoS attack.	T0810, T0818, T0866
IoR117-Suspicious OPC commands	OPC is a vendor-agnostic protocol used for IT systems to communicate with ICS and access data. For this IoR it is necessary to define a baseline of normally used commands in order to identify suspicious behaviour.	Use of OPC commands blacklisted or not whitelisted. Use of certain OPC commands with an unusually high frequency or under unexpected conditions.	An adversary uses an OPC command to reset all active alarms. An adversary uses OPC commands to make queries about the state of the system.	T0801, T0802, T0808, T0825, T0868, T0870, T0877
IoR302-Controller program change logs	A controller's program should be only changed during scheduled maintenance periods or under other pre-defined conditions, for which any changes under other circumstances can have risks.	Logs indicate a change in a controller's program outside the maintenance period.	An adversary changes a controller's program to change operational rules and disrupt industrial operations. For example, changing the doses of a component on a chemical process.	T0831
IoR511-Inconsistency between different sources of data	If I/O data is inconsistent between different sources or between redundant measurements, or at different levels of the system it can mean that I/O data have been tampered with.	The I/O value given by a redundant sensor differs significantly from the main sensor. I/O value displayed in an HMI to the one displayed in SCADA application in the engineering workstation.	An adversary spoofs the I/O image in the SCADA application running in the workstation.	T0832, T0835, T0878

Figure 3: Extract of IoR Library

- **Step 1: Identify the Techniques within scope.**

The techniques from the ATT&CK framework are considered in the light of the identified risks and threats and those most relevant to the system of interest are selected for continuous risk monitoring.

- **Step 2: Look up the IoRs that are applicable to** those techniques.

The IoR Library contains a Technique-IoR Matrix overview mapping IoRs to Techniques and also a page for each individual Technique with an explanation of the rationale for the specific IoR-Technique pair. A general description of each IoR can be also found in the "Definitions" view including rationale, observations, and examples. If any IoRs not mentioned in the IoR library are identified, they can be added and considered in the following steps.

- **Step 3: Translate the generic IoRs in more detailed use cases applicable to the specific ICS context.**

To aid the re-expression of the abstract information in a more concrete form, the "Definitions" view provides a rationale, observations, and examples of each IoR. Based on this, and their knowledge of the system, the user has to define use cases for each IoR. For example, "IoR502- Misbehaviour in sensor data", which refers in general terms to an input of the ICS that exhibits a behaviour that is unusual. Even if it might present trends, oscillations, or changes that are not commonly observed. In order to implement this IoR, it is necessary to define the specific sensors that would be monitored (such as temperature, pressure, humidity, presence), and a profile of normal behaviour, deviation from which constitutes "misbehaviour". Key questions for this step are "Can this IoR be decomposed in a set or more specific indicators?" and "How different sub-sets of this IoR type apply to different techniques?"

- **Step 4: Define which IoRs are feasible to be monitored and how**

Once the IoRs are identified and defined at a concrete level, feasibility of continuous monitoring should be checked. Depending on the type of IoR it might be possible to derive it from data already being collected in a SIEM tool. First, it should be identified which IoRs are based on observations that are been already been monitored in the system based on the current use cases monitored by a SIEM. Next, it can be checked which IoRs are based on observations that can be obtained from the security sensors and monitoring tools that are already implemented. At last, it should be analysed the feasibility to increase the monitoring capabilities in order to generate the remaining IoRs. The feasibility of implementing an IoR could also be constrained by the limitations of legacy systems. For example, if they do not have the necessary ports to communicate with the network monitoring tools. The output of

this step should be a final list of low-level IoRs to be monitored. Key questions for this step are “Can this IoR be monitored and how?” and “For which systems, devices or communication protocols, and in what parts of the network can this IoR be used?”

- **Step 5: Adjust the degree of influence for each IoR-Technique pair**

The degree of influence indicates at what extent an IoR can increase an estimated risk likelihood. Users should check and adjust the degree of influence suggested in the IoR Library and assign conditional probabilities accordingly.

The above method assumes that a risk management process is in place, as part of which, the risks and threats to be monitored were already identified. The following is an example of using these steps to implement continuous risk monitoring based on IoRs, which is independent of how the IoRs are processed:

- **Step 1:** The Techniques within scope are T0803 Block Command Message, T0808 Control Device Identification, and T0813 Denial of Control.
- **Step 2:** 20 IoRs were identified in the IoR Library for these Techniques, 8 of which are shown in Table 2, as an example.
-

Table 2: Example of results of Step 2

IoR	T0803	T0808	T0813
IoR002-Unnecesary open ports	1	1	
IoR117-Suspicious OPC commands	1	1	
IoR206-Unusual or unexpected commands in network packets	1	1	
IoR305-Controller in stop mode			2
IoR403-Commands and responses do not match	1		2
IoR404-Unresponded connection requests (port probes)		1	
IoR405-Unresponded commands	1		2
IoR406-Unexpected command sequence over network	1	1	

- **Step 3:** IoRs should be reviewed to identify observations for each technique. For example, in the case of IoR002-Unnecessary open ports, ports can be opened to prevent other processes accessing them, which is related to technique T0803. A procedure example of this is Industroyer [9]. A related observation for this IoR is that logs indicating that a typically unused port has been enabled and not subsequently disabled.
- **Step 4:** it should be checked if the appropriate tools and methods for gathering and processing these observations are already in place or are feasible to be implemented. The output of this step is the final list of IoRs to be monitored and the monitoring means.
- **Step 5:** The degree of influence for each Technique-IoR pair to be monitored is adjusted and translated into conditional probabilities for each technique to be performed when one or more IoRs are observed. For example, IoR403 is consider to be more strongly related to T0813 than to T0803.

It must be noted that IoRs are relatively abstract, and must be given a concrete interpretation that is meaningful in the given technical context and also can be implemented differently for different techniques. For example, in “IoR113-Malware detected” different malware executes procedures related to different Techniques, examples of which can be also found in ICS ATT&CK. Another example is “unusually high levels of traffic in the OT network”, which has to be defined with respect to typical range of traffic in a given network to establish a fixed threshold, if possible. In other cases there might be processes that increase the volume of network traffic under specific conditions making it necessary to have profiles of normal traffic for different states of the system. The same applies to modelling other communication patterns such as frequency with which two devices communicate or use of certain commands on an OT network protocol.

- 7 VALIDATION OF THE IOR LIBRARY

Up to the current stage of this research, the validation of the IoR Library has been done by two independent methods. The first validation was focused on utility and quality of descriptions and consisted on a peer review to collect feedback and ideas for improvement from potential users. The second validation was focused on the feasibility to implement the IoRs and consisted on cross-referencing IoRs with the implementation of detection use cases done by other researchers using different tools.

For the first validation, an earlier version of the IoR Library was presented to security professionals who were invited to conduct a peer review. This review was undertaken by five from three major German companies who checked the indicators and provided feedback and suggestions, as well as ideas for future work. These suggestions were incorporated in the latest version, which now openly available for the security community through a publicly accessible link [1].

For the second validation IoRs were cross-checked against experimental ICS security detection use cases from three sources: The NIST IR8219 [20] identifies a total of 53 ICS behavioural anomaly detection use cases using four different tools; [28] lists 15 example events corresponding to violation of security policies in ICS; and the third is a report on a PoC performed in a manufacturing company in 2019. Table 3 lists the IoRs that match the observable events from these sources, indicating the tools used and the number of detection use cases or anomaly event types reviewed. It should be noted that the relationship between the use cases and the IoRs is not one to one since sometimes one use case was described by more than one IoR and other times an IoR covered more than one use case.

Table 3: Results of Validation against OT detection PoCs

Ref.	Tool	Use Cases	Related IoRs
[20]	SilentDefense	15	IoR004, IoR015, IoR102, IoR202, IoR203, IoR205, IoR302, IoR304, IoR308, IoR413, IoR414
[20]	SNOK	15	IoR004, IoR017, IoR018, IoR107, IoR113, IoR202, IoR203, IoR205, IoR207, IoR302, IoR304, IoR308, IoR408
[20]	CyberX	15	IoR004, IoR015, IoR102, IoR113, IoR202, IoR203, IoR205, IoR207, IoR302, IoR308, IoR401, IoR402, IoR405, IoR413
[20]	OSIsoft	8	IoR305, IoR309, IoR310, IoR311, IoR501
[28]	Industrial IPS	15	IoR002, IoR011, IoR012, IoR102, IoR113, IoR120, IoR123, IoR302, IoR304, IoR401, IoR408, IoR410
Industry PoC	SilentDefense + Splunk	10	IoR101, IoR102, IoR114, IoR117, IoR205, IoR402, IoR406, IoR408, IoR411, IoR412

The cross-reference results described in Table 3 cover 39% of the IoRs currently in the library, which were matched to at least one of the use cases reviewed. For the rest of the IoRs feasibility was inferred based on vendor and third party information about different detection tool's capabilities, as well as SIEM capabilities. It must be noted that an important proportion of the IoRs from the first five IoR groups are based on inputs that are commonly used in security monitoring. Hence, organisations can make use of metrics that they already have and use information that otherwise would be dismissed by the security operators as false positive for the use of the risk analysts.

8 FUTUREWORK

Activities planned to develop the IoR Library further, include the following:

- **Library maintenance:** Review and improve the current IoR descriptions and examples, add further IoRs, and cover more adversary Techniques.
- **Develop structured guidelines:** Refine the process outlined in Section 6, including process for generation of appropriate IoRs for a particular context.
- **Exposure to a wider audience:** Get feedback and contributions.
- **Engaging with MITRE:** Propose discussion about possible adoption of the IoR Library as an extension to ATT&CK.
- **Case studies:** Develop use cases in particular contexts to test and drive development of the IoR Library and associated methods.
- **Propose a standard format for the exchange of IoRs:** using a clearly defined ontology for IoR sharing, as well as machine readable standards would facilitate dissemination, adoption as well as community contributions.
- **Design methods to asses efficacy of IoRs:** as IoRs are meant to be used to estimate probabilities there is no straight forward method to calculate their efficacy such as detection rate or false positive rate, which can be used for IoCs. Hence, for assessing their efficacy it would be required designing a method that could quantify how their use could improve the organisation's security posture and reduce risks.

One significant question to answer is whether low level IoR specifications can be elaborated in sufficient detail to be useful without making them highly technology and context specific. Another important challenge is the availability of appropriate monitoring and detection tools, in particular for legacy systems. In the absence of such tools, we recommend focusing on links in the kill chain, such as the Initial Access Tactic, that typically involve IT systems for which monitoring tools are available and in monitoring misbehaviour in sensor's data which can be

associated with techniques that belong to the Impair Process Control and Impact tactics. We are working in parallel on a Bayesian Network-based continuous cyber-risk assessment method that takes IoRs as input.

9 CONCLUSIONS

The IoR library systematizes observable conditions that are indicative of an elevated level of security risk and provides guidance on how to detect them. The IoR concept is in alignment with emerging industry best practices and recommendations which call for security detection based on behavioural models rather than only signature based IoCs. Basing the library on the MITRE ATT&CK for ICS matrix allows us to tap into and extend an existing semantic framework that is becoming widely adopted by practitioners and tool vendors.

Our main motivation in developing the IoR Library is to provide organisations that use ICS with continuously-updated situational awareness of their exposure to cyber-risks. In this context, the work presented in this paper can help to identify the type of information that needs to be monitored and processed to assess cyber risks in a continuous fashion. Uses and advantages of the library include:

- **Creation of templates and playbooks for security risk monitoring:** IoRs in combination with the ATT&CK matrices provide a common language for describing observable events and their implications that can be used in defining automated and manual SOC procedures.
- **Risk-based security monitoring:** Detecting IoRs rather than just IoCs enables threats to be anticipated, yielding a more proactive approach to defence.
- **Use in Forensics:** The IoR concept can assist in the analysis and documentation of successful attacks. Correlation of observable events (IoRs) with novel adversary techniques will allow anticipation and early detection of future similar occurrences.
- **Prioritisation of investments:** The most frequent IoRs observed and their associated Techniques can provide quantitative data of the attack vectors causing the highest risk exposures. Security controls with the highest cost-benefit ratios in terms of addressing these vectors can then be prioritised.

The IoR Library has been developed as an independent resource and is compatible with a variety of security and risk monitoring approaches. Overall, the IoR Library constitutes a valuable and logical extension of MITRE ATT&CK to encompass detection strategies.

REFERENCES

[1] Carolina Adaros-Boye. 2021. IoR Library 2021 V1.0. https://tinyurl.com/7hthzpc5.

[2] Carolina Adaros Boye, Paul Kearney, and Mark Josephs. 2018. Cyber-Risks in the Industrial Internet of Things (IIoT): Towards a Method for Continuous Assessment. In International Conference on Information Security. Springer, 502–519.

[3] Carolina Adaros-Boye, Paul Kearney, and Mark Josephs. 2019. Continuous Risk Management for Industrial IoT: a Methodological View. In 14th International Conference CRiSIS.

[4] Jason Andress. 2015. Working with indicators of compromise. ISSA Journal (2015), 14–20.

[5] Anomali. [n.d.]. What Are STIX/TAXII. https://www.anomali.com/resources/what-are-stix-taxii. Accessed: 2021-03-24.

[6] André Årnes, Karin Sallhammar, Kjetil Haslum, Tønnes Brekne, Marie Elisabeth Gaup Moe, and Svein Johan Knapskog. 2005. Real-time risk assessment with network sensors and intrusion detection systems. In International Conference on Computational and Information Science. Springer, 388–397.

[7] El Mostapha Chakir, Mohamed Moughit, and Youness Idrissi Khamlichi. 2017. A real-time risk assessment model for intrusion detection systems. In 2017 International Symposium on Networks, Computers and Communications (ISNCC). IEEE, 1–6.

[8] Long Chen, Yujian Chao, and Yuandong Ma. 2016. Risk Warning System Based on Big Data Applied in the Power Informatization of State Grid. In 2016 3rd International Conference on Information Science and Control Engineering (ICISCE). IEEE, 578–582.

[9] Anton Cherepanov. 2017. WIN32/INDUSTROYER A new threat for industrial control systems. https://www.welivesecurity.com/wpcontent/ uploads/2017/06/Win32_Industroyer.pdf. Accessed: 2020-12-27.

[10] Cyber-X Labs. 2019. 2020 Global ICS & IIoT Risk. A data-driven analysis of vulnerabilities in our industrial and critical infrastructure. Technical Report. Cyber-X Labs.

[11] Xuejun Ding, Yong Tian, and Yan Yu. 2015. A real-time big data gathering algorithm based on indoor wireless sensor networks for risk analysis of industrial operations. IEEE transactions on industrial informatics 12, 3 (2015), 1232–1242.

[12] Exabeam. 2020. Using the MITRE ATT&CK knowledge base to improve Threat Hunting and Incident Response. https://www.exabeam.com/library/usingthe-

mitre-attck-knowledge-base-to-improve-threat-hunting-and-incidentresponse/. Accessed: 2020-12-27.

[13] Forescout. 2019. Cybersecurity in Building Automation Systems (BAS). https://icitech.org/wpcontent/ uploads/2019/04/ForescoutOT_WP_Cybersecurity-in-BAS.pdf. Accessed: 2020-12-27.

[14] Foulon, Hugues and Van Den Berghe, Michel. 2020. Security Navigator 2021. Research-driven insights to build a safer digital society.

https://orangecyberdefense.com/global/security-navigator/. Accessed: 2020-12-27.

[15] Gustavo Gonzalez-Granadillo, Samuel Dubus, Alexander Motzek, Joaquin Garcia-Alfaro, Ender Alvarez, Matteo Merialdo, Serge Papillon, and Hervé Debar. 2018. Dynamic risk management response system to handle cyber threats. Future Generation Computer Systems 83 (2018), 535–552.

[16] Kjetil Haslum and André Årnes. 2006. Multisensor real-time risk assessment using continuous-time hidden markov models. In International Conference on Computational and Information Science. Springer, 694–703.

[17] Carl M Hurd and Michael V McCarty. 2017. A survey of security tools for the industrial control system environment. Technical Report. Idaho National Lab.(INL), Idaho Falls, ID (United States).

[18] Igor Kotenko, Igor Saenko, and Sergey Ageev. 2015. Countermeasure security risks management in the internet of things based on fuzzy logic inference. In 2015 IEEE Trustcom/BigDataSE/ISPA, Vol. 1. IEEE, 654–659.

[19] Robert M Lee. 2018. ICS Active defense and Incident Response 515.2 – Asset Identification and Network Security Monitoring. In ICS Active defense and Incident Response. SANS Institute.

[20] James McCarthy, Michael Powell, Keith Stouffer, CheeYee Tang, Timothy Zimmerman, William Barker, Titilayo Ogunyale, DevinWynne, and Johnathan Wiltberger. 2018. Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection. Technical Report. National Institute of Standards and Technology.

[21] MITRE Institute. [n.d.]. MITRE ATT&CK. https://attack.mitre.org/. Accessed: 2020-12-27.

[22] Luciana Obregon. 2015. Secure architecture for industrial control systems. SANS Institute InfoSec Reading Room (2015).

[23] OPC Foundation. [n.d.]. OPC Unified Architecture. Part 2: Security Model. https://reference.opcfoundation.org/src/v104/Core/docs/Part2/readme.htm. Accessed: 2021-03-24.

[24] Paladion. 2020. SIEM Use Cases - 45 use cases for Security Monitoring. https://securereading.com/downloads/45-siem-use-cases-for-securitymonitoring- paladion/. Accessed: 2020-12-27.

[25] Atle Refsdal and Ketil Stølen. 2009. Employing key indicators to provide a dynamic risk picture with a notion of confidence. In IFIP International Conference on Trust Management. Springer, 215–233.

[26] Juan Enrique Rubio, Cristina Alcaraz, Rodrigo Roman, and Javier Lopez. 2017. Analysis of Intrusion Detection Systems in Industrial Ecosystems.. In SECRYPT. 116–128.

[27] Splunk. 2020. 10 Ways to Take the MITRE ATT&CK Framework From Plan to Action - A guide to creating a threat-informed defense for your organization. https://www.splunk.com/pdfs/ebooks/10-ways-to-take-the-mitre-att-andck- framework-from-plan-to-action.pdf.. Accessed: 2020-12-27.

[28] Cyntia Vargas Martínez and Birgit Vogel-Heuser. 2018. Towards Industrial Intrusion Prevention Systems: A Concept and Implementation for Reactive Protection. Applied Sciences 8, 12 (2018), 2460.

[29] Jiao Wang, Kefeng Fan, Wei Mo, and Dongyang Xu. 2016. A method for information security risk assessment based on the dynamic bayesian network. In 2016 International Conference on Networking and Network Applications (NaNA). IEEE, 279–283.

[30] JialiWang, Martin Neil, and Norman Fenton. 2020. A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model. Computers & Security 89 (2020), 101659.

[31] Ding Yu-Ting, Qu Hai-Peng, and Teng Xi-Long. 2014. Real-time risk assessment based on hidden Markov model and security configuration. In 2014 International Conference on Information Science, Electronics and Electrical Engineering, Vol. 3. IEEE, 1600–1603.

[32] Qi Zhang, Chunjie Zhou, Yu-Chu Tian, Naixue Xiong, Yuanqing Qin, and Bowen Hu. 2018. A fuzzy probability bayesian network approach for dynamic cybersecurity risk assessment in industrial control systems. IEEE Transactions on Industrial Informatics 14, 6 (2018), 2497–2506.

[33] Álvarez, Antonio. 2020. WISER. Wide – Impact cyber Security Risk framework. https://www.cyberwiser.eu/content/d52-wiser-real-time-assessmentinfrastructure. Accessed: 2020-12-27.