Re-Configuration of IED for Decreasing Cyber Security Threat at SCADA based Substation

Zainal Arifin[1,2,3] and Wahyudi Setiawan*[2,4]
[1] PT PLN (Persero), JalanTrunojoyo, Blok M I/135, Jakarta, Indonesia
[2] Institut Teknologi PLN, Jl. Lingkar Luar Barat, Cengkareng, Jakarta, Indonesia
[3]zainal_pln@yahoo.com, [4]setiawan.wahyudi@yahoo.com

Abstract

SCADA systems have proven well to increase the efficiency and reliability of power grid system. However recent attack on SCADA system at some utility companies, put SCADA security to be a critical issue on power industry today. The use of TCP/IP as a carrier protocol and the trend to interconnect SCADA systems with enterprise networks, create serious security threats. This paper proposes re-configuration of IED (Intelligent Electronic Device) or microprocessor-based controllers of power system equipment, such as circuit breakers and transformers, at SCADA system to decrease cyber security threat at Substation level. The re-configuration is conducted by three methods; by not connecting the communication lines to the protection relays, change the bay control unit function to the bay monitor unit, and then optimizes the mimic bay control. It will limit the accessibility of Substation from the local HMI system, LAN remote station network, communication network between Master Station and Remote Station, communication network inside Master Station and office, and backdoor network to the vendors. Indeed this re-configuration still support the SCADA main functions to monitor all main parameters of power grid system, only disable the automatic mode of PMT operation at Substation. Using a risk matrix this study found that the reconfiguration can reduce significantly the cyber attack risk value. The change of standard of operation is proposed to ensure that reconfiguration will be worked well.

***Keywords**: SCADA, Cyber Security, Intelligent Electronic Device, Substation, Risk Analysis*

1. Introduction

The first high-power long distance three-phase transmission line was displayed at the International Electro-Technical Exhibition in Frankfurt in 1891. Along with the development of power generation, transmission, and distribution technologies, automation including remote monitoring and control of the electrical system has become an inseparable part [1]. During the early stage of electromechanical systems, a surveillance system has been developed to use solid-state components, electronic sensors, and analog-to-digital converters. In the 1980s process control companies began applying their technology and technical approaches to the SCADA (Supervisory Control and Data Acquisition) electric utility market. As a result, RTU (Remote Terminal Unit) uses microprocessor-based logic to perform extended functions. The adoption of microprocessors increases the flexibility of the surveillance system and creates new possibilities in operation [1]. SCADA technology experienced very rapid development in the 1970s, where software improvements resulted in a better human-machine interface [2]. As with many industrial technologies, the development of minicomputer and the development of data telecommunications have a profound effect on the SCADA development.

By adopting information technology, the SCADA operating system has interactions with physical equipment will certainly affect the physical processes that are taking place because the system integrates computing resources, communication capabilities, sensing and actuation in an effort to monitor and control physical processes. Then identifying information technology factors in security and reliability is the most important issue because SCADA integration into critical infrastructure systems can cause situations that adversely affect widespread public safety [3]. The more communication channels available, the higher risk of security threat because intruders from outside can break into the SCADA network system without warning. Vulnerabilities in this IT system can be exploited by irresponsible parties causing loss of SCADA assets as well as losses of electricity distribution operations. The extent of risk must be immediately mapped and given adequate security [4]. Many of the cyber intrusion incidents have added new terms or new uses for old terms. For example, old terms such as botnets (short for robotic networks, also balled bots, zombies, botnet fleets, and many others), indicate groups of computers that have been compromised with malware such as Trojan horses, worms, backdoors, remote control software, and virus, has taken a new connotation with respect to cyber security issues [5]. Additionally cyber security is affected by the structure of power systems, as well as by communication protocols and standards [6]-[8].

2. Cyber Security on SCADA

The Ukraine power grid cyber-attack on 23 December 2015 and is considered to be the first known successful cyber-attack on a power system. Hackers were able to successfully compromise information systems of three energy distribution companies in Ukraine and temporarily disrupt electricity supply to the end consumers [9]. An attacker who wants to take control of the SCADA system is faced with three challenges: get access to the control system LAN, through discovery and understanding the process, and get control of the process [10]. Unfortunately there are many methods that intruders can use to get this information. More and more these systems are well documented on the web and easily accessible. Understanding these weaknesses in the control system (SCADA) is the key to protecting the system itself. The British Columbia Institute of Technology (BCIT) study provides a report on 34 incidents that show operating violations on SCADA components including their origin [10].

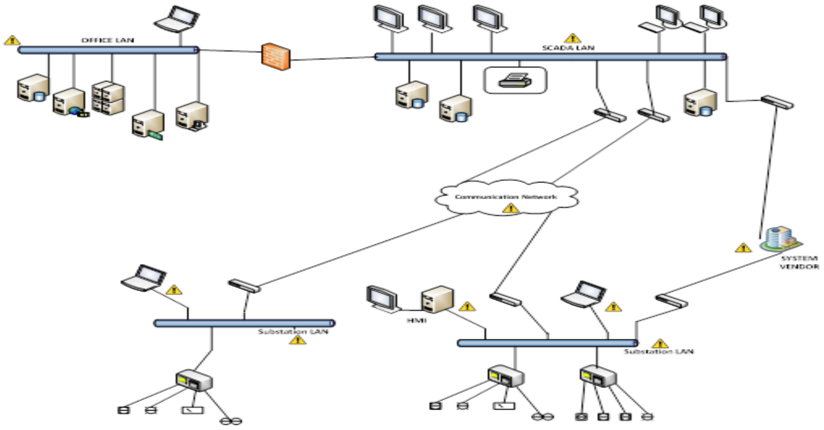

Fig. 1. Potential Cyber Security threats on SCADA [1]

Following fig 1, the potential for cyber attacks lies at the point related to the communication channels. These communication channel is an “entry gate” for the hackers to illegally access the SCADA even with the availability of a security system. Some those entery points including:

1. Business network connections (by utility company)
2. Back door coonection (by vendors)
3. Wireless computer connection (by engineers)
4. Insecure email and data flows (by empolyee)
5. Poor authentication in protocol elements and SCADA (by system)

Some research defined the source of cyber attck in SCADA from both basically internal and external. Reffering to Table 1, the largest potensial came from business network and remote internet [11]. The table also shows that threat of cyber attack is similar signifucat between internal and esternal sources.

Table1. Sources of Cyber Attack Threat

Cyber Attack Sources			
Internal		External	
Type	%	Type	%
Business network	43	Remote internet	36
HMI	29	VPN commerce	8
Laptop	7	Remote dial up modem	20
Other physical access	21	Remote wireless system	8
		Remote SCADA system	4
		TELCO network	8
		Trusted 3th party connection	4
		Unknown remote	12

Some incidents that can occur when the SCADA system has been hit by a cyber attack, such as:

1) Inaccurate information (false information) that appears on the HMI display so that the operator performs an inappropriate action, and has a negative effect on the system.
2) Unauthorized changes to instructions and thresholds that could endanger the system and the environment.
3) Changes in illegal control which can cut off high-voltage conductor lines so that the loss of electricity supply to the conductor.
4) Configuring IED settings or software infected with malware so that it has a dangerous impact.
5) Disruption of server systems that experience unnatural work processes so that the operation of SCADA becomes slow.

In a cyber attack scheme, hackers may carry out their actions on SCADA networks or other communication networks. In reality in the electric power industry, the operating targets aimed at are substations and distribution substations. Because the development of IEDs that are currently configured are monitors and controllers of high voltage equipment at the substation so that it becomes a potential for illegal cyber attacks. Therefore a security mechanism is needed that must be developed based on the principles of reliability, integrity and confidentiality at SCADA-based substations.

2. IED on SCADA

Gradually the use of tools with electromechanical systems in power system safety equipment is replaced with digitalization and computerized devices. As a result, the market for the production of these devices only provides new digital equipment, often called Intelligent Electronic Devices, IEDs. It is a microprocessor-based controller of power system equipment, such as circuit breakers, transformers, and capacitor banks. IEDs receive data from sensors and power equipment and can issue control commands, such as tripping circuit breakers if they sense voltage, current or frequency anomalies, or raise/lower voltage levels in order to maintain the desired level. Common types of IEDs include protective relaying devices, On Load Tap Changer controllers, circuit breaker controllers, capacitor bank switches, re-closer controllers, voltage regulators etc. This is generally controlled by a setting file. The testing of setting files is typically one of the most time-consuming roles of a protection tester. Digital protective relays are primarily IEDs, using a microprocessor to perform several protective, control and similar functions. A typical IED can contain around 5-12 protection functions, 5-8 control functions controlling separate devices, an auto-reclose function, self-monitoring function, communication functions etc.

The utilization of IEDs in the power distribution system has improved and concise function of the previous safety relays. With their advantages, the IED has proven as a reliable tool in the operation of the electric power system including SCADA. In the SCADA system itself, the IED is considered a converter that connects the parameters contained in the high voltage equipment on the downstream side with the communication component on the SCADA on the upstream side (see figure 2). The growth of communication infrastructure, protocol standardization, and interoperability were the main factors causing the explosion of IEDs. IEDs are now the eyes, ears, and hands of the system automation in an electric utility. Some recent IEDs are designed to support the IEC61850 standard for substation automation, which provides interoperability and advanced communications capabilities.

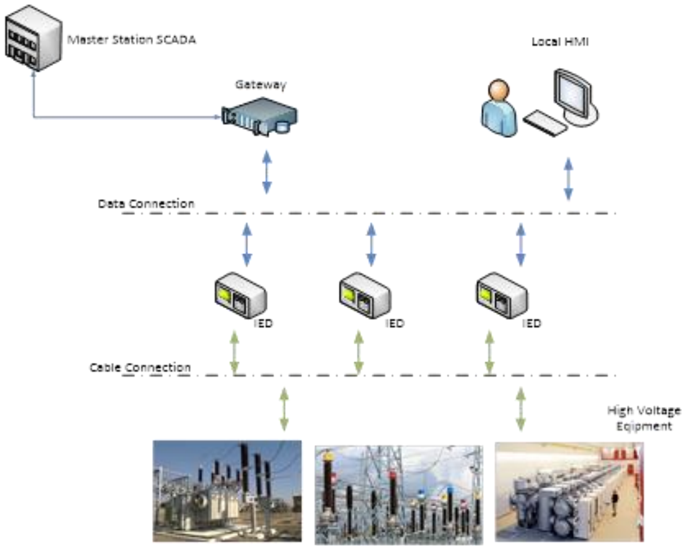

Fig. 2. IED data network on SCADA based Sybstation [11]

IED is packed with full control and monitoring capabilities and with analysis of error report data can manage substations without human intervention [1]. With the use of IEDs then a network topology is applied in the data transport process. This data communication network is designed in such a way that each IED can still be communicated with the local server for local, Gateway or RTU operations for communication with the main station. The data communication path from the substation to the master station can be in the form of a special line or from a third party provider. This line width is adjusted according to the needs of the data traffic transmitted during SCADA operations.

2.1. IED configuration in the substation

IED's communication capabilities include several selectable protocols, multi-drop facilities with multiple ports, and fast response to real-time data. It also has exceptional data processing capabilities for various functions, for various applications such as protection and measurement [1]. Typical IED functions can be classified into five main areas; protection, control, monitoring, measurement and communication (see Fig. 3).

Some IEDs may be more advanced than others, and some may emphasize certain functional aspects than others, but these main functions must be put to all degrees [5].

2.1.1. Input output

Input component output at IED is a piece of hardware that functions to connect all parameters of high voltage electrical equipment. The established connection system is a connection between the terminal contact on the IED and the cabling of each parameter as needed. The connected parameters are functions of:

1. Binary input: receiver information from parameters in high voltage electrical equipment such as the status of equipment, alarms, trip status and counters.
2. Analog input: is a receiver of information from the parameters of the high voltage equipment that is used as a measurement parameter such as the amount of Current and Voltage.
3. Binary output: is a contact command from IED to high voltage equipment such as PMT open and close orders.
4. Analog output: is a command contact from the IED to the component of the process equipment with the amount of current or voltage as the control parameter, generally at the Analog output substation this function is not enabled.

This wire connection has its own working voltage with their respective functions according to the needs and configuration of the substation.

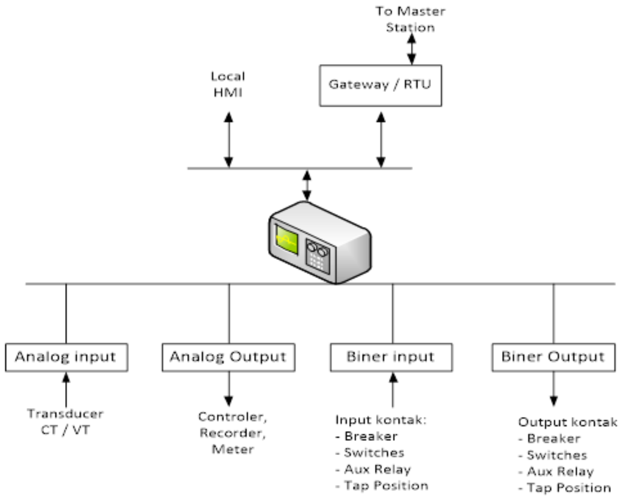

Fig. 3. Equipment that is integrated with the Substation LAN

2.1.2. Data Process

The whole process at IED works at a level that involves programming, algorithms and calculations in software. In the data process produces the following functions:

1. Protection: is the main function of the high voltage equipment, is the result of a computerized process of parameters that receive symptoms of interference in the power supply system. So that the security functions against disturbance symptoms can secure high voltage equipment from damage.
2. Metering: is the calculation result of reading the analog input parameters.
3. Event record: is a record of every event or status change that is monitored by an IED,
4. Fault recording: is a recording of every disturbance and anomaly that is detected on an IED.
5. Application logic: an internal process in an IED to determine the value or step of an IED work order.

2.1.3. Communication / protocol

Communication on the IED is the entrance and exit of any information for other functions. Development of serial-based communication, TCP / IP allows freedom of access to IEDs that are in vital facilities including high voltage distribution systems. As previously elaborated, the presence of data communication itself has presented vulnerability to the risk of illegal access. Breakthrough breakdown in the SCADA operating network, the next anticipated step is to use the IEC 61850 protocol, because this protocol has been embedded in many IED or electric safety equipment. The IEC 61850 protocol itself can be considered a self-taught protocol that can be studied with each IED application. Addressing IEC61850 using Logical Node (LN) can be understood because the naming factor has been standardized so that it will present a vulnerability of its own.

It can be explained when the hacker has gained access to the SCADA communication network, then the operation of the HMI system or direct access to the target IED uses the protocol that is known and the target address of the equipment (PMT) has known the Logical Node. Then an illegal command change can be executed, and the data process accepts the illegal command and continues on the output contact that activates driving at the open command (Voltage Disconnect, PMT).

3. Methodology

This study was conducted qualitatively with the following stages.

The first is to identify potential sources of cyber attacks on SCADA-based substations based on literature studies or interviews with relevant experts.

After that, a study of system configuration in the substation is carried out, particularly the relation between the communication device and the hardware that controls the operation of equipment in the substation, especially the breaker or re-closer, switches and so on. At this stage also studied the characteristics and role of IEDs in the operation of the substation based on SCADA.

Therefore reconfigure the IED connection in the system is proposed with a number of relevant scenarios based on expert input and previous case studies.

The further stage is calculating the value of risk using a risk matrix based on the level of probabilities and the impact of cyber attack on the substation. Using the risk calculation value before and after the reconfiguration, the benefit will be defined as the results of this study.

Then the SOP improvement is recommended as a result of the IED reconfiguration above providing the technical recommendations needed to keep the SCDA system still function normally.

4. Re-Configuration of IED

4.1. The existing data network configuration

Referring to the design or general configuration at the substation, all equipment in the form of Main Protection Relay (MPU), Backup Protection Relay (BPU) and Bay Control Unit (BCU) are integrated with the Local Area Network (LAN) providing access and remote function of the substation. For communication channel, the devices are interconnected with optical fiber media or LAN cables. However the connection of this device provides a loophole in illegal access that could have happened without prior notice. This configuration allows access to high voltage equipment maneuvers in the substation through IEDS-based equipment via LAN networks or wireless communication lines (Fig 4). The cyber attacks that penetrates into the system mostly through the SCADA equipment loopholes includes server, local HMI, BCU/RTU, protection relay and database hardware. Through those loopholes the hacker can control the operation of the substation remotely.

4.2. Re-configuration of the data network

Considering all the risks of cyber attacks through interconnected equipment and data communication at the substation, it is necessary to reconfigure the existing SCADA system. The strategic step needed to be taken is to reduce the risk of cyber attacks by minimizing data communication access at the substation. Hierarchically, the main aim of reconfiguration of data network is to eliminate the IED connection that functions as a Protection Relay with all forms of data communication which potentially generate cyber threats for outsiders.

The reconfiguration for this study can be conducted by some scenarios as follows:

1) By not connecting the communication lines to the protection relays,
2) Changing the Bay Control Unit (BCU) function to the Bay Monitor Unit (BMU),
3) Optimizing the Mimic Bay Control (MBC) as a main tools for controlling the high voltage equipments of the substation

Then IEDs' data network before and after the reconfiguration can be seen in Fig. 4 and 5. Indeed the reconfiguration less the SCADA role due to the decreasing in the level of automation at the substation. Consequently not all SCADA functions can be carried out on substations. Thus the substation cannot be controlled remotely by the dispatchers and still require local operators. At many cases, includes on Indonesia, this scenario is still most effective way to control substations. Some substations still need a direct visual supervision to ensure that the operation and maneuvering of high voltage equipment at the substation actually work well according to SCADA's instructions.

After reconfiguration, physical authority is back to the operators in each substation using controls on the mimic panel with supervision from the dispatcher through the SCADA wall display. For SCADA command or control, authorities can coordinate between dispatchers and substation operators via radio communication lines or internal telephone networks. By applying personal authentication and implementing work permit procedures, the control functions on SCADA will be more secure. The cyber security threat from the IED loopholes can be reduced significantly.

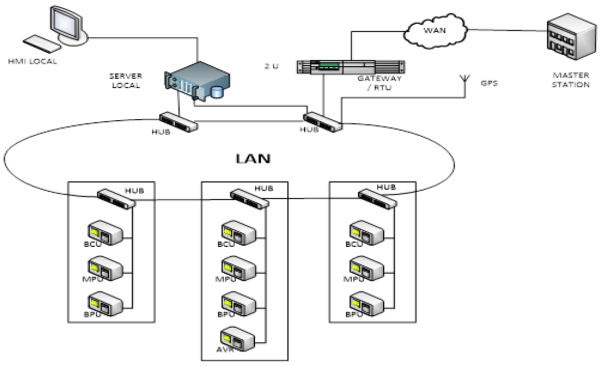

Figure 4. IED exiting configuration data network

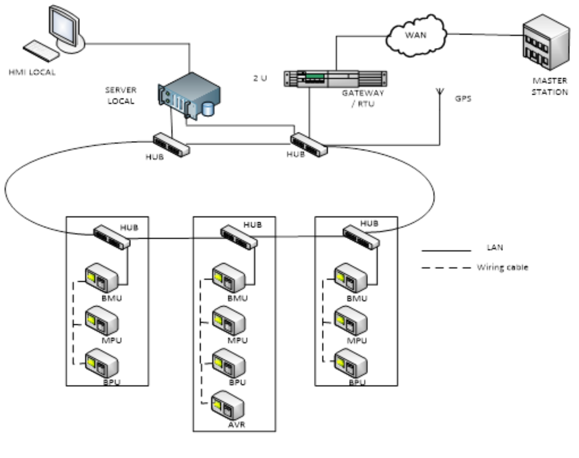

Fig 5. Reconfiguration of IED data network

ISSN: 2207-6360 IJSAT

4.3. Risk Analysis

Risk is the lack of certainty about the outcome of making a particular choice. Statistically, the level of downside risk can be calculated as the product of the probability that harm occurs (e.g., that an accident happens) multiplied by the severity of that harm (i.e., the average amount of harm or more conservatively the maximum credible amount of harm). In practice, the risk matrix is a useful approach where either the probability or the harm severity cannot be estimated with accuracy and precision. It is a matrix that is used during risk assessment to define the level of risk by considering the category of probability or likelihood against the category of consequence severity. This is a simple mechanism to increase visibility of risks and assist management decision making [12]. By such analysis, the risk matrix of cyber attack at the SCADA based substation can be defined as table 2. Based on the table, the risk value/score between before and after reconfiguration can be calculated. The table shows that the risk value after reconfiguration is significantly decreasing from 89 to 54. However as a result of the configuration changes, there are differences in the performance of the SCADA function before and after reconfiguration. Referring to table 3, the all SCADA function is still working well except for the feature of command and control by HMI remotely. Consequently this feature can be only executed by local operator of the substation.

Table2. Risk matrix of IED SCADA Configuration

No	**Cyber Security Threats**	**Before Reconfiguration**			**After Reconfiguration**		
		Probability	Impact	Score	Probability	Impact	Score
1	SCADA Server	4	5	20	2	5	10
2	Communication channel	5	5	25	2	5	10
3	Local HMI	4	5	20	2	5	10
4	BCU/RTU	2	5	10	2	5	10
5	Protection relay	2	5	10	2	5	10
6	SCADA database	1	4	4	1	4	4
				89			54

Table 3. Main SCADA before and after Reconfiguration

No	SCADA Function	Initial Condition	After Reconfiguration
1	High voltage equipment status	Monitored	Monitored
2	Metering (V, I, W, Var, F, PF)	Monitored	Monitored
3	Faults status (trip, alarm, fault, invalid)	Monitored	Monitored
4	Command and Control by remote HMI	In service	Disable

4. Conclusions

Along with automation and digitalization, all electricity power system devices can be controlled remotely through data network and communication. In power grid systems, this remote control function is performed by the SCADA system. By adopting information technology, the SCADA operating system has interactions with physical equipment will certainly affect the physical processes. The more communication channels available, the higher risk of security threat because intruders from outside can break into the SCADA network system remotely. With their advantages, the IED has proven as a reliable tool in the operation of the electric power system including SCADA. However the IEDs' data network on substation based on SCADA has some loopholes for cyber security attacks. Then a reconfiguration proposed on the study is needed to limit the access illegally to the high voltage equipment operation controlling. Using a risk matrix, this configuration can reduce the risk value of cyber security attack from 89 to 54. A simulation testing for this reconfiguration should be conducted to ensure that the threat reduction is really related. The limitation of some data channeling access by this configuration make the operation of substation cannot be fully operated by SCADA yet the security level of the system is higher than the existing configuration. The configuration make authority for operation and control the substation is depend on collaboration between local operator and dispatchers at control centre. This study emphasized that whole automation and digitalization of power system not only increase the efficiency and reliability of system but also the vulnerability for cyber security attack. Then a further research is recommended to study how digitalization will increase the reliability and effectiveness of power system operation without significantly increases the threat of cyber security attack.

References

[1] M. S. McDonald, “Power System SCADA and Smart Grid”, Boca Raton: CRC Press, 2015.

[2] G. C. a. D. Rynders, “Practical Modern SCADA Protocol DNP3, IEC 60870.5 and Related System”, Burlington: Elsevier, 2004.

[3] S. A. Boyer, “SCADA Supervisory Control and Data Actuation 3th Edition”, USA: ISA, 2004.

[4] E. J. Kott, “Cyber-security of SCADA and Other Industrial Control System, Switzerland”: Springer, 2016.

[5] R. R. Brodsky, “Handbook of SCADA/Control Systems Security”, Boca Raton: CRC Press, 2016.

[6] A. Dagoumas, "Assessing the Impact of Cybersecurity Attacks on Power Systems," *Energies* , vol. XII, no. 12, p. 725, 22 February 2019.

[7] S. Vaidyanathan, A. Sambas, M. Mamat and W. S. M. Sanjaya. “Analysis, synchronisation and circuit implementation of a novel jerk chaotic system and its application for voice encryption.” *International Journal of Modelling, Identification and Control*, vol. 28, no. 2, pp. 153-166, 2017.

[8] A. Sambas, W. S, M. Sanjaya and M. Mamat. Bidirectional Coupling Scheme of Chaotic Systems and its Application in Secure Communication System. *Journal of Engineering Science & Technology Review*, vol. 8, no. 2, pp. 89-95, 2015.

[9] K. Zette, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," Wired, new york, 2016.

[10] J. Wiles, “Techno Security's Guide to Securing SCADA. A Comprehensive Handbook On Protecting The Critical Infrastructure”, New York: Syngress, 2008.

[11] G. Björkman, "Smart Grids Security SICS Security," in *Seminar in Kista*, ABB Mannheim, 2014.

[12] J. Talbot, "What's right with risk matrices?," Julian Talbot Productions, 31 07 2018. [Online]. Available: https://www.juliantalbot.com/post/2018/07/31/whats-right-with-risk-matrices. [Accessed 31 07 2018].