Proceedings Paper:
Prabhu, V., Oyekan, J., Eng, S. et al. (2018) Towards data-driven cyber attack damage and vulnerability estimation for manufacturing enterprises. In: Auer, M.E. and Langmann, R., (eds.) Smart Industry & Smart Education : Proceedings of the 15th International Conference on Remote Engineering and Virtual Instrumentation. 15th International Conference on Remote Engineering and Virtual Instrumentation, 21-23 Mar 2018, Duesseldorf, Germany. Springer International Publishing, pp. 333-343. ISBN: 9783319956770. ISSN: 2367-3370. EISSN: 2367-3389.

https://doi.org/10.1007/978-3-319-95678-7_38

REV International Conference on Remote Engineering and Virtual Instrumentation

Towards Data-Driven Cyber Attack Damage and Vulnerability Estimation for Manufacturing Enterprises

Abstract

Defending networks against cyber attacks is often reactive rather than proactive. Attacks against enterprises are often monetary driven and are targeted to compromise Confidentiality, Integrity and Availability (CIA) of data. While the best practices in enterprise-level cyber security of IT infrastructures are well established, the same cannot be said for critical infrastructures that exist in the manufacturing industry. Often guided by these best practices, manufacturing enterprises apply blanket cyber security in order to protect their networks, resulting in either under or over protection. In addition, these networks comprise heterogeneous entities such as machinery, control systems, digital twins and interfaces to the external supply chain making them susceptible to cyber attacks. A breach in any of the entities could invariably serve as an entry point to the entire network and subsequently cripple the manufacturing enterprise. Therefore, it is necessary to analyse, comprehend and quantify the essential metrics of providing targeted and optimised cyber security for manufacturing enterprises. Currently, this is done using empirical and subjective means. This paper presents a novel data-driven approach to conceptualise and develop the essential metrics, namely, Damage Index (DI) and Vulnerability Index (VI) that quantify the extent of damage a manufacturing enterprise could suffer due to a cyber attack and the vulnerabilities of the heterogeneous entities within the enterprise respectively. A use case of computing the metrics for an academic lab that undertakes commercial manufacturing projects in Singapore is demonstrated. This work builds a strong foundation for development of an adaptive cyber security architecture with optimal use of IT resources for manufacturing enterprises.

Keywords: Data Driven, Cyber Security, Manufacturing Enterprises. Cyber Attack Damage, Cyber Attack Vulnerability, Metrics.

1. Introduction

Manufacturing has been immensely important to the prosperity of nations, with over 70% of income variations of 128 nations explained by differences in manufactured product export data alone. It is also a vital industry sector for the stability and growth of the global economy. It has 70% share in global trade and 16% share in global GDP, amounting to $12 Trillion [1] [2].

As a result, cyber attacks on the manufacturing industry could be crippling to the global economy. Nevertheless, the threat is real and its full damage potential may not have been fully comprehended yet. A recent Symantec report revealed that 20% of all cyber attacks on industry in 2014 were directed at the manufacturing sector [3]. McAfee identified that industrial networks were the most vulnerable to cyber security issues [4], a fact corroborated by the Dragonfly Espionage Malware Program incident in 2014 that affected 1000 industrial control systems [5]. In 2013, 91% of all cyber attacks took a matter of hours out of which 60% were left undetected for weeks and 53% took months to contain by which time the damage had been done [5]. As identified in a recent review paper [6], the purposes for such attacks were to alter critical data as in the Shamon attack on Aramco, impair or deny process control as in the Stuxnet attack on Iran's nuclear facility, and/or steal data as the "Shadow Network" espionage operation.

Another type of cyber attack aims to steal intellectual property of industries via Manufacturing data. Manufacturing data' takes the form of product data (e.g. CAD models), manufacturing process data (e.g. machine parameters) and critical infrastructure data (e.g. automation controls). The loss or damage of manufacturing data can cripple not only that enterprise but also the supply chain to which it is connected. This calls for security mechanisms to ensure the privacy of the enterprise. In a manufacturing system, different entities (such as machines, workstations, etc.) have different data access and transfer protocols, operating systems and data storage systems, all with varying levels of data security. This complex heterogeneity presents a strong case for the investigation of data-driven cyber security mechanisms to ensure the trust between entities as well as confidentiality, integrity and availability of manufacturing data.

2. Literature Review

Current research in implementing cyber secured systems for manufacturing has focused on high-level security issues, such as risk assessments and vulnerability analysis of manufacturing enterprises to cyber attacks [7]. In terms of cyber security solutions, the research focus has been on the development of detection and mitigation mechanisms for Supervisory Control and Data Acquisition (SCADA) networks [8]. In some cases, common security issues for critical infrastructures, such as industrial control systems, smart energy grids, water management and transportation systems, are investigated [9]. While manufacturing shares similarities with critical infrastructures, it has different requirements for guaranteeing cyber security,

because it comprises a complex mix of design, process and control entities within the product lifecycle. In the manufacturing domain, the focus has been on securing each manufacturing entity as a silo without considering entity-to-entity and entity-to-cloud connectivity and critical data flows which is the emphasis of this research [10]. Furthermore, as a result of recent edge-computing advances and computing power, there is scope for autonomous defence of IoT enabled manufacturing [11][12][13].

Towards autonomous defence of manufacturing enterprises, this paper focuses on developing a novel data-driven approach that can be used to understand how secured or vulnerable a manufacturing system is to cyber-attacks that target critical operations data. This will enable us to reveal and secure vital cyber-physical data flows within the system towards generating end-to-end protection and trust levels among entities within the manufacturing enterprise.

In order to address this, the paper proposes that the value of the data generated by each individual entity in a manufacturing system must be quantified. This is because, hackers are most likely to go after high value entities in a manufacturing system. Currently, the human perceived value of data at these nodes is often different from the actual value of the data. For example, a recent research [14] revealed that discarded process data logs produced by CNC machines during wing manufacturing could be fused with manufacturing instructions to produce a report that indicates how well the wing was manufactured resulting in an automated wing inspection process. As a result, the previously zero value "discarded" data is being currently used to inspect rivets for all produced A380 wings leading to a drastic reduction in production lead-time. In this case, the perceived value of the discarded data in the CNC was different from the actual value.

Consequently, deriving the actual value of data at an entity is important as it equips users with the knowledge of which node has a high value and hence more attractive or lucrative for cyber attacks. In quantifying the actual value of data, [15] suggested a financial model that takes into consideration the cost value of replacing lost data or generating data, the economic value of the data asset to the revenue of an organization (User 'likes' and profile data have a large economic value to Facebook for generating business revenue in the form of advertising), and the market value of data generated when sold, rented, or bartered in the market place. Other factors that contribute to determining the value of data in a system include its accuracy, its completeness towards an information goal, as well as its uniqueness in the information marketplace. In this paper, these factors will be utilized in quantifying manufacturing data value at individual entities in the network as well as how the value evolves with transfer between nodes. Through a visual graphical network map, users will be equipped with real-time knowledge of high value data flows in the enterprise as well as their levels of vulnerability. In order to ensure end-to-end data protection and defence, entity to entity vulnerability will be assessed using attack route-based vulnerability quantification [16] weighted according to the value of the data in entities. The output of the analysis could potentially reveal the trust vulnerability or secure index of entities in the system. During data transfers, the vulnerability or secure index of entities could be tagged onto data so that the receiving entity can determine its trust level in the data and can take the necessary actions. Actions could include those guided by the principles of IoT system security namely 1) the concealing of important information from untrusted parties and 2) the management of access rights (tokens) and security keys between two end points, namely, the data provider and the data consumer [17].

3. Method

Cyber security for the manufacturing industry is often being positioned at lowest priority to be taken care of. One of the reasons of low awareness on cyber security is due to the lack of quantitative tools for the industry to realise the extent of damage which the industry will suffer in terms of monetary loss upon cyber attack. Without the measurement tools for cyber attack vulnerability of the manufacturing system and the extent of damage caused, the cyber security protection architecture can only be deployed based on recommended best practices.

In the context of a manufacturing system, there are three major data types stored in the entities, namely, (i) product data, (ii) process data, and (iii) control data. In order to effectively utilise the cyber security protection resources, this research has developed a set of empirical metrics, namely Damage Index (DI) and Vulnerability Index (VI) to estimate the extent of damage and to estimate the cyber attack vulnerability of entities for each data type stored in the system respectively.

DI within a manufacturing enterprise is calculated based on the 'real value' of the manufacturing data that is stored within each of its entities. Meanwhile, VI is quantified based on the Common Vulnerability Scoring System (CVSS) which is applied on hardware and software within each entity, and the weighted score of each data types based on the Confidentiality, Integrity, and Availability (CIA) of data. By knowing the DI and VI of each entity within a manufacturing enterprise, a System Vulnerability Map (SVM) is produced as a graph that shows both high value data flows in relation to their vulnerabilities to cyber attacks.

3.1. Manufacturing Data Types

This research mainly focuses on stationary data that is stored in the system entities. In the context of a manufacturing system, data can be broadly categorised into product data, process data, and control data. With regards to these data types, the scope of each type may be slightly different for different manufacturing domains. Product data refers to the technical information or virtual models of products, components, or a system. Process data are those that govern the machine processes to produce the physical product. Control data refers to data that is used to operate a system such as programmable logic controller (PLC) data. In a machine, control data can be referred as the programming logic which translates the input process data to physical functions of the machine. Using a typical manufacturing shopfloor which comprises Computer Numerical Control (CNC) machines and CAD/CAM workstations, product data are computer-aided design (CAD) files, process data are computer aided manufacturing (CAM) programs, and control data are the ladder logic embedded in the PLC modules of each of CNC machine.

3.2. Damage Index (DI)

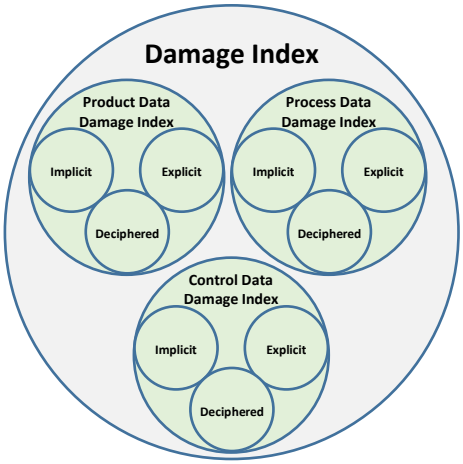

Figure 1: Overview of Damage Index composition

DI is to quantify the maximum extent of monetary damage which will be suffered by a manufacturing enterprise after a cyber attack. The calculation of DI is based on the 'real value' of stationary data which stored in each of the system entities. This research postulates that this 'real value' is made up of three components: (i) perceived or explicit component (ii) implicit component, and (iii) deciphered component (Figure 1).

Perceived/Explicit component is the price the enterprise has paid to obtain or create the data. Both data can be directly translated into monetary figure using the below formula where n is the number of datasets.

$$Perceived\ or\ Explicit\ Component = \sum_{i=1}^{n} (Price\ to\ Purchase\ Data)_n + (No.of\ hrs\ to\ create\ data_n \times Hourly\ Rate)$$

Implicit component refers to cost of non-availability of data. It can be the monetary loss by the manufacturing enterprise due to downtime, loss of reputation and reduced market share when the data is not available. This research suggests that both product data and process data share the same formula as below to compute the explicit component due to the fact that process data is able to be reverse engineered to obtain product data. Here n is the number of jobs.

Implicit component (for process and product data) =

$$\sum_{i=1}^{n}\Big[\underbrace{(Down\ Time_n \times Hourly\ Rate)}_{①} + \underbrace{\left(1+\frac{Job\ Revenue_n}{Yearly\ Revenue}\right)\times Job\ Price_n}_{②} + \underbrace{\left(1.2-\frac{Market\ Share\%}{100}\right)_n \times Job\ Price_n}_{③}\Big]$$

① in the equation quantifies the down time monetary loss when there is non-availability of product/process data. ② translates to the loss of reputation when data is non-available. The conversion involves the scaling up of the individual job price carried by the data based on the particular job revenue to the enterprise's yearly revenue ratio. ③ quantifies the

reduced market share in terms percentage converted to monetary loss by proportioning the individual job price carried by the data that is compromised.

The most significant damage suffered from a cyber attack to control data is the total downtime of the machine. The formula to quantify the implicit component carry by the control data can be simplified to solely consider the monetary loss due to downtime suffered by the machines only.

$$Implicit\ component\ (for\ control\ data) = \sum_{i=1}^{n}(Down\ Time_n \times Avg.\ Hourly\ Revenue)$$

Deciphered component involves cost of compromising confidentiality of data. It includes the monetary value of critical product or process information that can be obtained by mining the stolen data. The deciphered component only involves the product and process data due to the fact that control data does not carry any information related to the product or process by itself. The formula to quantify the deciphered component is as below where n is the number of jobs.

$$Deciphered\ Component = \sum_{i=1}^{n}\left(\frac{Complexity\ Index_n}{10} + \frac{Criticallity\ Index_n}{5}\right) \times Job\ Price_n$$

Complexity Index =Score A + Score B

Machine setup	Score A
Single setup	1
2 setup	2
3 setup	3
4 setup	4
5 setup and above	5

Critical Dimension	Score B
Zero	0
1 to 2	1
3 to 6	2
6 to 10	3
10 to 15	4
15 and above	5

Criticality Index

Description	Index
Non- critical part such as : Spacer block	1
Standard Component such as: pin, fastening components, connector, linkages, and gears.	2
General component such as : Housing or casing	3
Customised component (but not major component). E.g., non-major component with unique/special design.	4
Major component in an assembly such as: Mould insert, Impeller, parts with patented technology	5

This research proposes that to estimate the additional value of Intellectual Property (IP) which can be obtained by mining the product and process data, the calculation will need to take into account the complexity and criticality of the product itself. The suggested formula is by applying a multiplication factor (derived from complexity index and criticality index) to the job price carried by the product or process data. Using CNC machining as an example, complexity refers to the required machining setup to produce the product as well as the number of critical dimensions of the product. The criticality index is a measure on the functional existence of the parts as a standalone component or as a sub-component of an assembly. Both complexity and criticality index reference table are to be tailored based on different type of manufacturing systems s consisting different types of data.

After consolidating the explicit, implicit, and deciphered component into 'real value', the figure is then normalised to a product or process Damage Index (DI) based on the average single job value. The normalised DI provides a practical gauge of the magnitude of monetary loss with respect to the business scale of the enterprise if there is a cyber attack to the system entity. The formula for consolidated DI is:

Product Data DI and Process Data DI=

$$\frac{Explicit\ Component + Implicit\ Component + Deciphered\ Component}{Avrg\ Single\ Job\ Price}$$

As for control data DI, since there is no deciphered component, the formula will be the sum of explicit component and implicit component, normalised to yearly depreciation cost of that entity.

Control Data DI =

$$\frac{Explicit\ Component + Implicit\ Component}{Yearly\ Depreciation\ Cost}$$

3.3. Vulnerability Index (VI)

The vulnerability of a manufacturing enterprise to cyber attacks can be quantified based on the correlation between data types and cyber security principles as well as Common Vulnerability Score (CVS) of the hardware or software in each of the entities. Depending on the specificity and accuracy of each correlation, a deterministic mathematical model is derived to compute VI.

Each data type is assigned a weighted score based on the cyber security principle. The cyber security principle focusses on three aspects: (i) confidentiality, which relates to assurance that data is known only accessible authenticated and authorised entities, (ii) integrity, refers to data not altered, modified or corrupted, and (iii) availability, which relates to accessibility of data for use whenever needed. The weighted score based on these principles is assigned to each data type and consolidated into a Vulnerability Quantification Table (VQT). VQT is data type driven for each different manufacturing system. The VQT should be re-accessed and adjusted accordingly to improve the accuracy of the computation. A sample VQT for machining manufacturing system is shown in Table 1 below:

Table 1: Vulnerability Quantification Table (VQT)

	Confidentiality	Integrity	Availability	
Product Data	0.5	0.2	0.3	→ Sum = 1
Process Data	0.4	0.4	0.2	→ Sum = 1
Control Data	0.2	0.6	0.2	→ Sum = 1

Common Vulnerability Score System (CVSS) is a free and open industry standard for accessing the severity of computer system security vulnerabilities [18]. CVSS assesses entities in three areas: (i) base metrics, quantify qualities intrinsic to vulnerability, (ii) temporal metrics, taking care of characteristics that evolve over the lifetime of vulnerability (iii) environmental metrics, for vulnerabilities that depend on a particular implementation or environment. For this research, the proposed VI calculation will only involve the 'Impact Matrix' which is a subset assessment from environmental metrics. Impact Matrix rates the impact on the confidentiality, integrity, and availability (CIA) of data processed by the system (hardware/software) upon cyber attack. The impact is rated as either none, low or high (based on CVSS version 3).

After developing the VQT, within the system network, each systems entities is evaluated to obtain CVS. VI can be computed based on the deterministic mathematical model below:

$$V = \begin{bmatrix} V_{VI\ for\ Product\ Data} \\ V_{VI\ for\ Process\ Data} \\ V_{VI\ for\ Control\ Data} \end{bmatrix} = Q \times C$$

Where V, Q and C all are matrices

V → Vulnerability Index Matrix *Q → Vulnerability Quantification Matrix* *C → CVSS Weighted Score Matrix*

Vulnerability Quantification Matrix, Q is a matrix which directly results from the VQT, which is shown below:

Product Data	0.5 → $Q_{1,1}$	0.2 → $Q_{1,2}$	0.3 → $Q_{1,3}$
Process Data	0.4 → $Q_{2,1}$	0.4 → $Q_{2,2}$	0.2 → $Q_{2,3}$
Control Data	0.2 → $Q_{3,1}$	0.6 → $Q_{3,2}$	0.2 → $Q_{3,3}$
	Confidentiality	Integrity	Availability

$$Q = \begin{bmatrix} Q_{1,1} & Q_{1,2} & Q_{1,3} \\ Q_{2,1} & Q_{2,2} & Q_{2,3} \\ Q_{3,1} & Q_{3,2} & Q_{3,3} \end{bmatrix}$$

CVSS weighted score matrix, C, is required to evaluate each of the hardware and software within each system entity. The description of matrix C is shown below:

$$C = \begin{bmatrix} C_1 \\ C_2 \\ C_3 \end{bmatrix}$$

C_1 = (Count of high score for Confidentiality x 1) + (Count of low score for
C_2 = (Count of high score for Integrity x 1) + (Count of low score for Integrity x 0.5)
C_3 = (Count of high score for Availability x 1) + (Count of low score for Availability

3.4. System Vulnerability Map (SVM)

The SVM provides a visual landscape of the cyber security needs of manufacturing enterprises by identifying high value data flows through manufacturing entities and the vulnerabilities of those entities. The SVM is represented as a graph comprising nodes (circles) and edges (lines). The nodes represent manufacturing entities, such as machining centres, CMMs, MES workstation, CAD/CAM/CAE workstations, DNC workstation, work computers, PLM servers, etc. These entities make up the manufacturing system and handle manufacturing data. The edges represent data flow channels between nodes. For example, an edge between a DNC workstation and a machining centre will represent the flow of post-processed CNC programme code from the workstation to the machine controller.

In the SVM, the DI and VI are graphically illustrated for each node (entity). The higher the DI of an entity, bigger is the node diameter. Each node is further circum-banded by sectors, denoting the proportion of product, process and control data that is stored inside the entity. The bands are colour coded to indicate the composite VI of the entity ranging from green (low vulnerability) to red (high vulnerability) and all the colours in between. Figure 2 illustrates a sample SVM that represents a manufacturing system comprising three entities. In this SVM, entity 2 has the highest DI whereas entities 1 and 3 have control data with the highest vulnerabilities to cyber attack.

When the SVM is developed for a large manufacturing enterprise with hundreds of entities, the SVM is a practical tool for a quick and inambiguous identification of entities along high value data flows that need priority protection from cyber attacks thereby enabling targeted cyber security. By knowing the vulnerabilities of prioritised entities, the type and extent of security can be identified and deployed thereby optimising IT resources and preventing under and over protection.

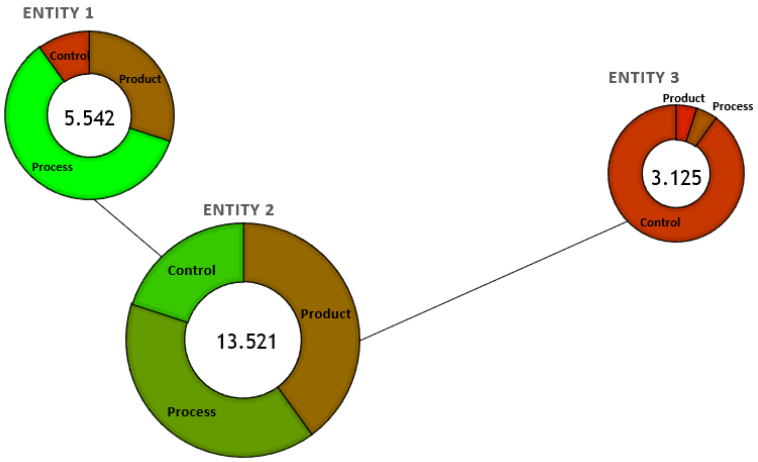

Figure 2: Sample SVM

4. Results and Discussion

The metrics, DI, VI and the resulting SVM that are defined and developed in this paper are computed for a manufacturing cell located within an academic laboratory of the Centre for Digital and Precision Engineering at Nanyang Polytechnic, Singapore and the SVM for the cell is illustrated.

The cell comprises a CAD/CAM workstation that is used to generate CAD models and CAM programs, a DNC workstation that is used to post-process CAM programs into NC codes that are fed to the MES server for execution, a Manufacturing Execution System (MES) server that is used to create, execute, control and monitor the sequence of manufacturing operations within the cell, an Electro-Discharge-Machining (EDM) machine and a 5-axis CNC milling machine. The cell is served by a robot that handles the workpieces, tools and electrodes associated with the manufacturing cell and is controlled by the MES server. The robot is excluded from this work as this stage and will be included in future. The 4-step process involved in generating the SVM for the cell is as follows:

Step 1:

Each of the above entities is studied for the amount of product, process and control data it holds and the resultant nodes for the SVM are shown in Figure 3.

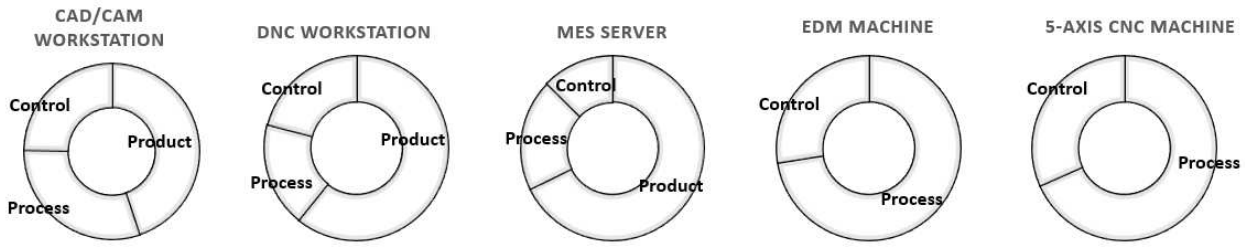

Figure 3: Nodes of the cell with the proportion of product, process and control data circum-banded

Step 2:

In this step, the DI is computed for each of the above entities. In order to be as close as possible to the real manufacturing use case, the data from the commercial projects that the centre has completed for precision engineering companies in Singapore in the financial year 2016/17 has been used. Due to the confidential nature of the data, such as pricing, revenue generated, value of IP, machining hours per part, etc, only the final DI components, each constituting explicit, implicit and deciphered components, are tabulated in Table 2 below:

Table 2: Product, process, control data DIs and overall DI of the entities

Entity	DI (Product Data)	DI (Process Data)	DI (Control Data)	Overall DI
CAD/CAM workstation	3.949	2.672	2.175	8.796
DNC workstation	8.119	2.444	2.800	13.363
MES server	11.688	3.392	2.175	17.255
EDM machine	0	10.104	3.840	13.944
5-Axis CNC machine	0	8.277	3.840	12.117

Based on the above overall DIs, the nodes are redrawn with differing diameters to illustrate the proportionality to the DI (Figure 4).

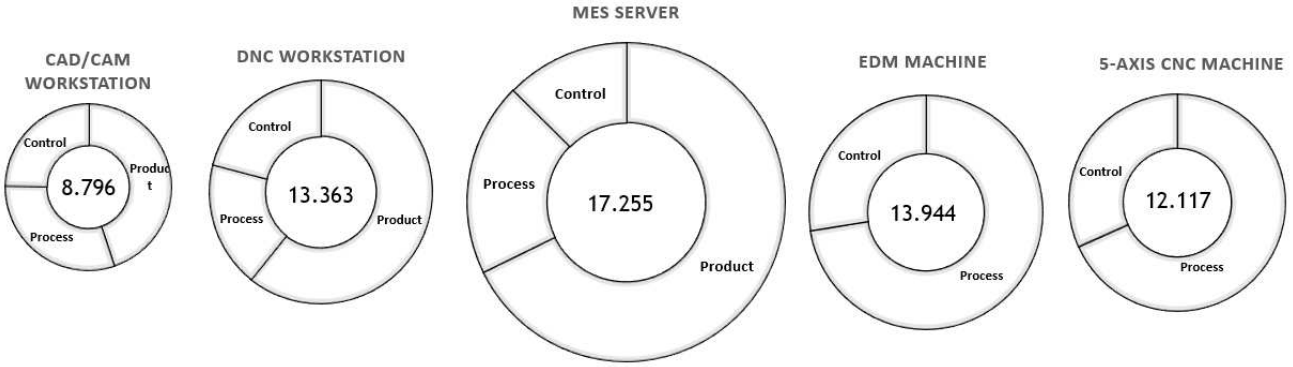

Figure 4: Nodes resized to denote their overall DIs

Step 3:

In this step, the VI is computed for each of the data type bands per node. Due to space constraints of the paper, the constituents of the VI for the 5-axis CNC milling machine only is shown in Table 3 below. A similar table is generated for the other four entities also.

Table 3: Constituents of the VI and overall VIs for the 5-axis CNC milling machine

Entity		Major Components	CVSS Reference	CVSS Confidentiality	CVSS Integrity	CVSS Availability
5-axis CNC Milling Machine	Hardware	Simplified PC (with Ethernet Card)	http://www.cvedetails.com/cve/CVE-2004-2048	High	High	High
Model: Mikron 500U		Siemens PLC	https://www.cvedetails.com/cve/CVE-2016-2201	None	Low	None
Make: Agie Charmilles	Software	Windows XP	http://www.cvedetails.com/cve/CVE-2017-0176	High	High	High
			No. of "Complete"/High (Score=1)	2	2	2
			No. of "Partial"/Low (Score =0.5)	0	1	0
			No. of "None"/Zero (Score=0)	1	0	1
				Total CVSS Confidentiality	**Total CVSS Integrity**	**Total CVSS Availability**
			Total CVSS Score	2	2.5	2
			VI for Product Data	**2.1**		
			VI for Process Data	**2.2**		
			VI for Control Data	**2.3**		

The nodes are redrawn in Figure 5 to denote the VIs of product, process and control data of the entities as a range of colours from Green (low vulnerability) to Red (high vulnerability). In this work, smart charting function of MS PowerPoint is used to automatically assign the colours to the data type bands.

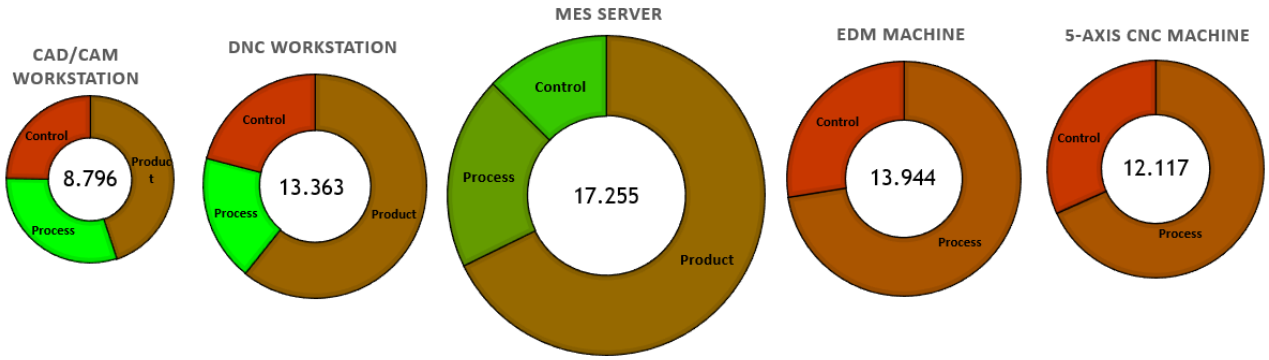

Figure 5: Nodes redrawn to denote VIs of the data type bands using colour code

Step 4:

In this step, the nodes are connected by edges to denote the presence of data flow between them. The complete graph, which is now the final SVM is shown in Figure 6 below. The CAM programs generated at the CAD/CAM workstation is transferred to the DNC workstation as well as the MES server for association with manufacturing jobs. The DNC workstation post processes the CAM programs received from the CAD/CAM workstation and sends it to the MES server for execution in the cell. The MES server also sends machining status information to the DNC server. Finally, the MES server communicates with the two machines, sending programs and controls as well as receiving status and log data from the machines.

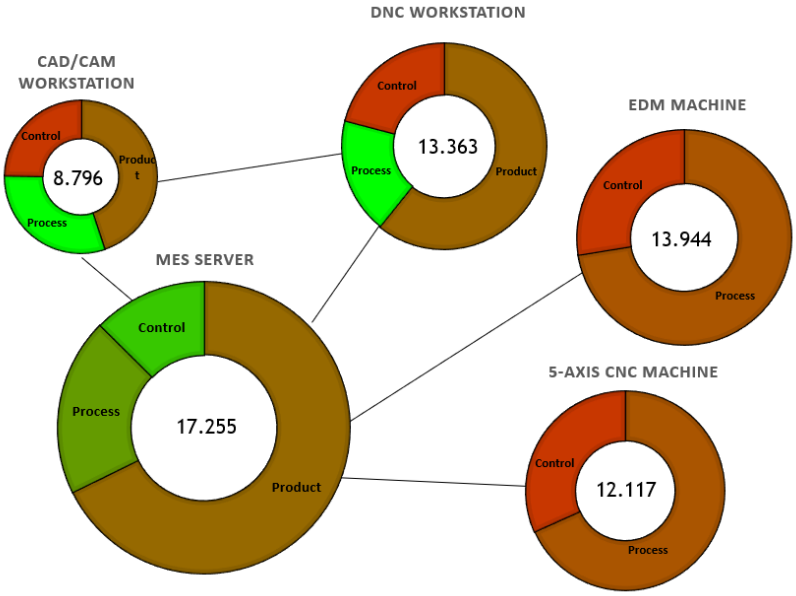

Figure 6: Final SVM of the manufacturing cell

From the above SVM, it is clear that while MES server contains the highest value of data, it is also the least vulnerable to cyber attacks due to the enterprise cyber security solutions in place. In this case, since the MES server is a high end computer, the enterprise cyber security solutions are applied thereby providing adequate protection against cyber attacks. The SVM also reveals that the control data residing in the other four entities is highly vulnerable to cyber attacks and therefore need the highest extent of protection. Further analysis would be required by the IT administrators to select the type of cyber solution that can be deployed to reduce the vulnerabilities of these entities. Therefore, using a simple graphical format, the SVN enables targeted and customised cyber security to protect the manufacturing cell from cyber attacks.

5. Conclusion

Standard enterprise cyber security solutions, such as firewalls, are not adequate for manufacturing enterprises due to the heterogeneity of entities and the myriad of interfaces between the entities both internally and externally to the enterprises. Furthermore, there are no standard metrics available for manufacturing enterprises to gauge their vulnerabilities to cyber attacks and to deploy targeted and customised cyber security for optimum protection.

This work makes an attempt to develop metrics such as 'Damage Index' (DI) and 'Vulnerability Index' (VI) to serve as tools for manufacturing enterprises to quantify the maximum damage caused by cyber attacks and their vulnerability to cyber attacks respectively. These metric inherently take the heterogeneity of the manufacturing entities as shown in the paper above. Graphically representing the DI and VI into a graphical System Vulnerability Map (SVM) allows IT administrators to easily and effectively prioritise resources to provide targeted and optimised cyber security for the enterprise. These tools also provide lifetime management of cyber security by regular monitoring of the manufacturing system to continually refine and validate its DIs and VIs, while the cyber attack landscape and the enterprise itself evolve over time.

The work presented in this paper is in no manner complete and requires deepening of the study to ensure that all parameters and factors are taken into account to compute the damage and vulnerabilities of manufacturing entities to cyber attacks. Also, while expanding the use case to include all the manufacturing entities in the Centre for Digital and Precision Engineering, a validation study that uses the manufacturing shopfloor of a commercial manufacturing enterprise is required to establish credibility of this work. This work suffers from the deficiency of requiring all the data to be deterministic in nature for computing DI and VI of the entities but in reality this may not be possible. A machine learning technique to stochastically determine these metrics when data is not fully available or is available as a range will be required to be developed. This work provides a solid foundation for all this future work to be carried out.

6. References

[1] McKinsey&Company. (2012). Manufacturing the Future: The Next Era of Global Growth and Innovation, McKinsey Global, USA.

[2] World Economic Forum (WEF). (2012). The Future of Manufacturing: Opportunities to Drive Economic Growth, WEF, Switzerland.

[3] Symantec. (2015). Internet Security Threat Report, vol. 20, Symantec Corporation, USA.

[4] McAfee Labs. (2011). 2012 Threat Predictions, McAfee, USA.

[5] Cisco. (2014). Cisco Connected Factory – Security, Infographic Report, Cisco, USA.

[6] Wangen, G. (2015). Role of malware in reported cyber espionage: A review of impact & mechanism, Information, vol. 6(2), 183-211.

[7] Wells, L.J., Camelio, J.A., Williams, C.B. and White J. (2014). Cyber-physical security challenges in manufacturing systems, Manufacturing Letters, vol. 2(2), 74-77.

[8] Yang, W. and Qianchuan Z. (2014). Cyber security issues of critical components for industrial control system, In: IEEE International Conference on Guidance, Navigation and Control (CGNCC), Yantai, China, 8–10 August.

[9] Dacer, M.C., Kargl, F., König, H. and Valdes, A. (2014). Network attack detection and defense: Securing industrial control systems for critical infrastructures, Dagstuhl Seminar 14292: Dagstuhl Reports, vol. 4(7), 62-79.

[10] Knowles, W., Prince, D., Hutchison, D., Disso, J.F.P. and Jones, K. (2015). A survey of cyber security management in industrial control systems, International Journal of Critical Infrastructure Protection, vol. 9, 52-80.

[11] He, H., Maple, C., Watson, T., Tiwari, A., Mehnen, J., Jin, Y. and Gabrys, B., 2016, July. The security challenges in the IoT enabled cyber-physical systems and opportunities for evolutionary computing & other computational intelligence. In Evolutionary Computation (CEC), 2016 IEEE Congress on (pp. 1015-1021). IEEE.

[12] Meshram, A. and Haas, C., 2017. Anomaly detection in industrial networks using machine learning: a roadmap. In Machine Learning for Cyber Physical Systems (pp. 65-72). Springer Berlin Heidelberg.

[13] Thames, L. and Schaefer, D., 2017. Cybersecurity for Industry 4.0 and Advanced Manufacturing Environments with Ensemble Intelligence. In Cybersecurity for Industry 4.0 (pp. 243-265). Springer International Publishing.

[14] Tiwari, A., Vergidis, K., Lloyd, R. and Cushen, J. (2008). Automated inspection using database technology within the aerospace industry. Proceedings of the Institution of Mechanical Engineers, Part B: Journal of Engineering Manufacture, vol. 222(2), 175-183.

[15] Ko, J., Lee, S., & Shon, T. (2015). Towards a novel quantification approach based on smart grid network vulnerability score. International Journal of Energy Research.

[16] Ko J, Lim H, Lee S, Shon T. (2014). AVQS: Attack route-based vulnerability quantification scheme for smart grid. The Scientific World Journal, 1–6.

[17] IERC - IoT Governance, Privacy and Security Issues - Cluster AC05. (2015). Internet of Things, IoT Governance, Privacy and Security Issues. IERC European Research Cluster On The Internet of Things, AC05, European Communities.

[18] Common Vulnerability Scoring System (CVSS). https://www.first.org/cvss/. Assessed on 1 Oct 2017