DATA-CENTRIC CYBER THREAT IMPACT ANALYSER FOR IOT AND MANUFACTURING

HITB GSEC Singapore
CommSec Track

31 August 2018

Presenter :

Lim Eng Woei

Simon Eng

NANYANG
THE INNOVATIVE POLYTECHNIC

Agenda

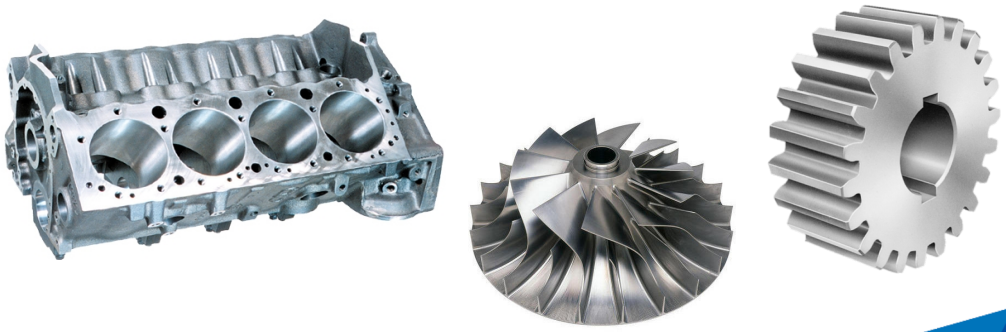
- Introduction to manufacturing
- Types of data in manufacturing shopfloor
- Current Situation and Limitation
- Damage Index
- Vulnerability Index
- Conclusion

Research Background

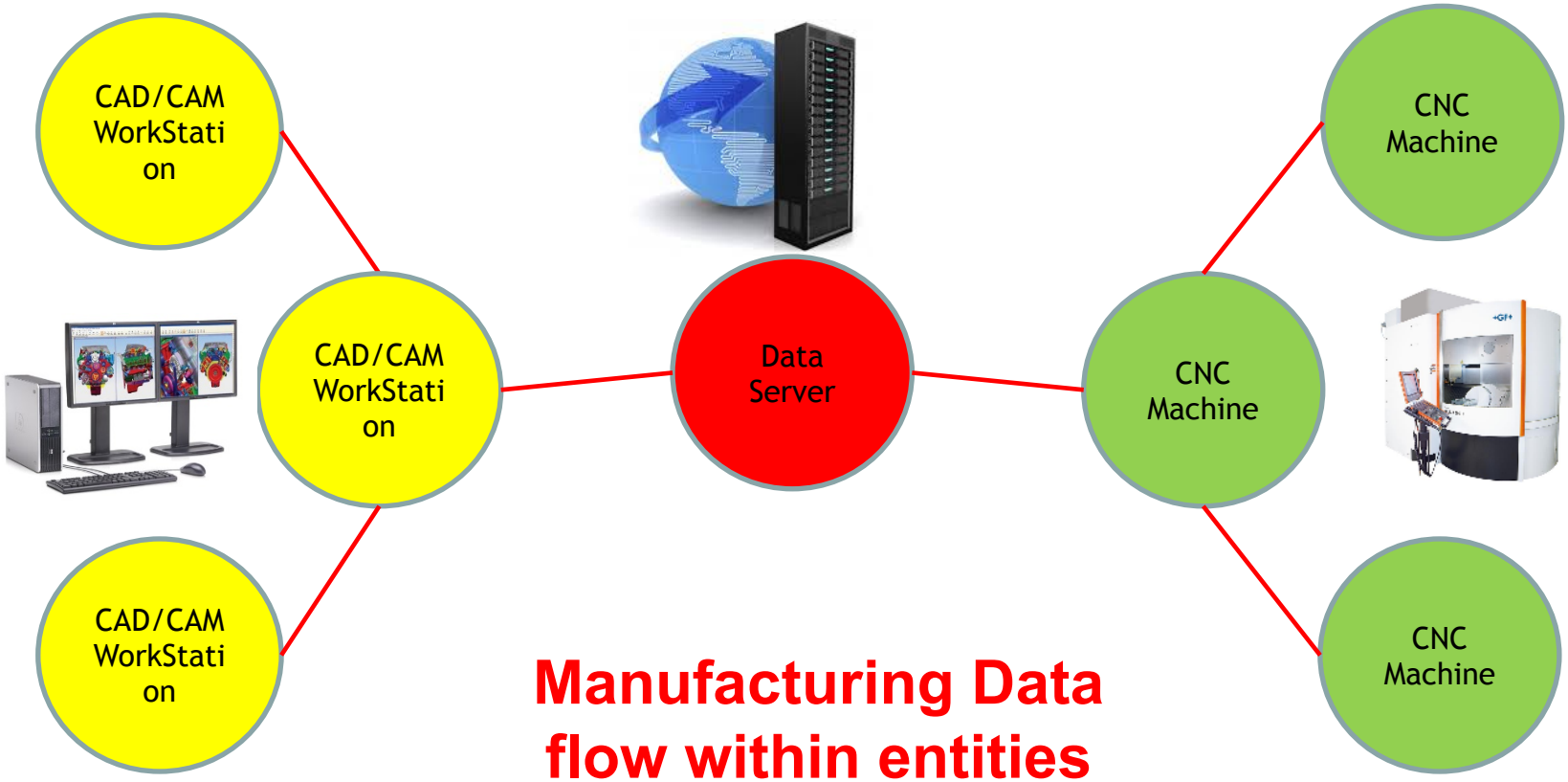
- Manufacturing is third among top 5 industries at greater risk of cyber attack (IBM, Jul 2017).

Use Case Environment @

Manufacturing Shopfloor



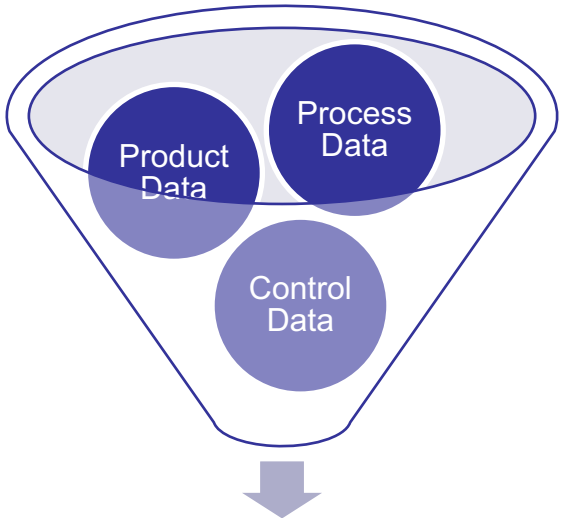
System Data Network (SDN)



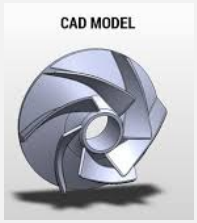
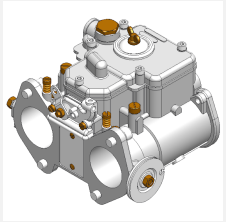
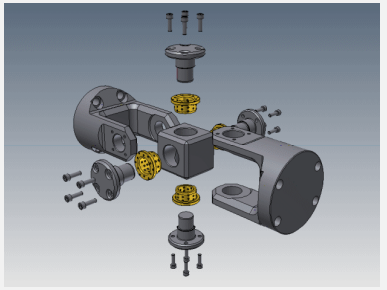
Manufacturing Data flow within entities

Data Types

- **Product Data:** Technical information or virtual models of products, component or a system.
- **Process Data:** Data which govern the machine processes to produce physical product.
- **Control Data:** Data that is used to operate a system.



Examples of Data

	Precision Manufacturing Shopfloor
Product Data	Computer-aided design (CAD) files    

Existing Situation and Limitations

- Current cyber security approach, based on best practices:
  - IT asset centric
  - Require prioritisation of high value assets

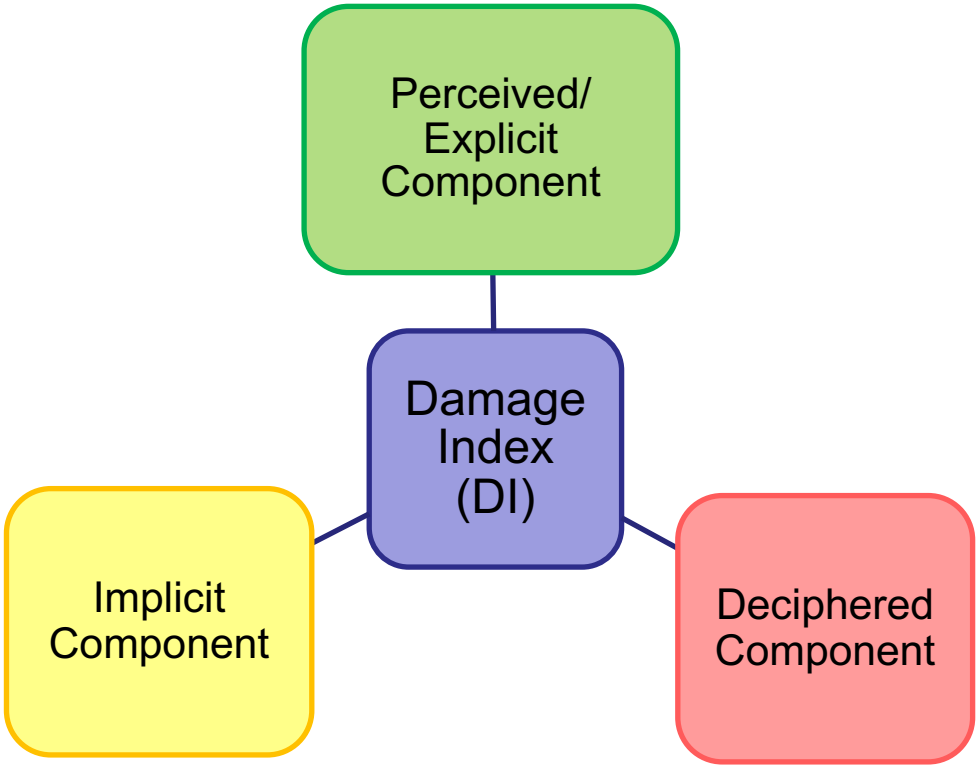
- The above approach does not work for *manufacturing systems*
  - Cyber attacks target critical manufacturing data BUT not IT assets
  - Difficult to determine "real" value of assets

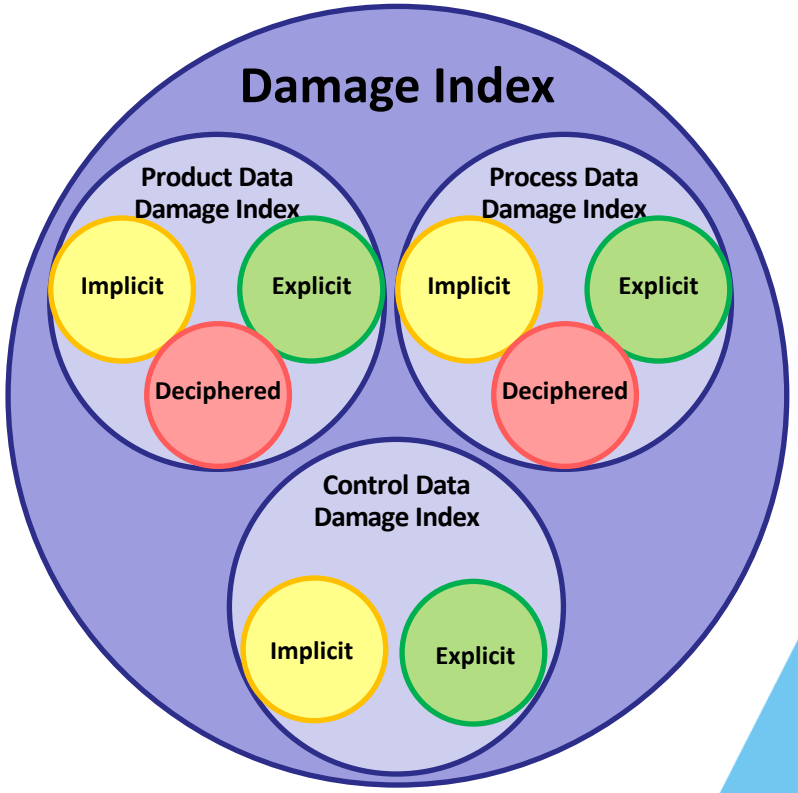
Manufacturing needs a *data driven and data-differentiated* cyber security approach.

Damage Index (DI)

- Quantify maximum extent of monetary damage
- Calculation of DI based on the 'real value' of stationary data which store in each system entities ("data at rest").
- 'Real Value' made of:
  - Explicit/Perceived Component:
  - Implicit Component:
  - Deciphered Component
- Individual Damage Index (DI) for each data type (process vs product vs control data) will be calculated and sum up as each entity's DI

Damage Index (DI)





DI – Explicit/Perceived Component

- Composed of :
  1. Price to purchase data
  2. Price to create data

- Formula:

  Explicit Component=

$$\sum_{i=1}^{n} (Price\ to\ Purchase\ Data)_n + (No.hr\ to\ create\ data_n \times Hourly\ Rate)$$

n is number of datasets

- ***Same formula will be applied for all 3 data types (process vs product vs control data)***

DI – Implicit Component

- Refer to cost of non-availability of data
- Composed of :
  1. Monetary loss during down time
  2. Loss of reputation
  3. Reduced market share
- Formula:

For Product/Process data	For Control Data
$Implicit\ component =$ $\sum_{i=1}^{n} (Down\ Time_n \times Hourly\ Rate) + \left(1 + \frac{Job\ Revenue_n}{Yearly\ Revenue}\right) \times Job\ Price_n + \left(1.2 - \frac{Market\ Share\%}{100}\right)_n \times Job\ Price_n$	$Implicit\ component =$ $\sum_{i=1}^{n} (Down\ Time_n \times Avg.\ Hourly\ Revenue)$

n is number of datasets

DI – Deciphered Component

- Involves cost of compromising confidentiality of data.
- Estimate the monetary value of mining the stolen data.
- Composed of :
    1. Value of IP which can be obtained by mining the stolen data
- Formula:

Deciphered Component=

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

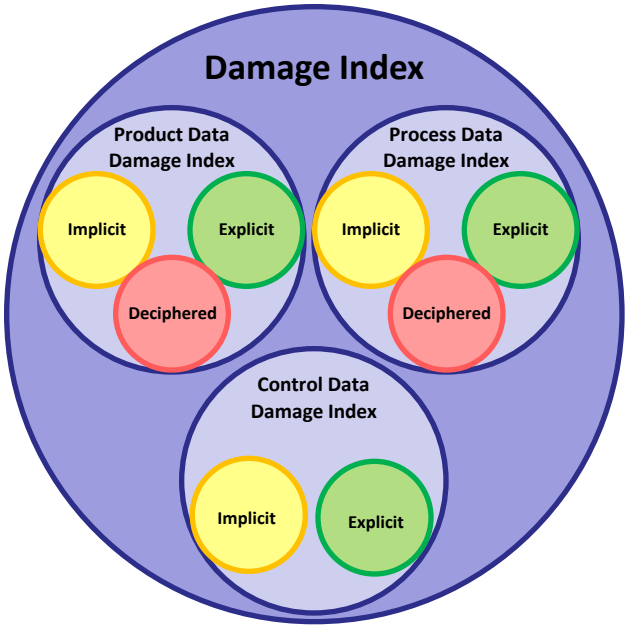
n is number of datasets

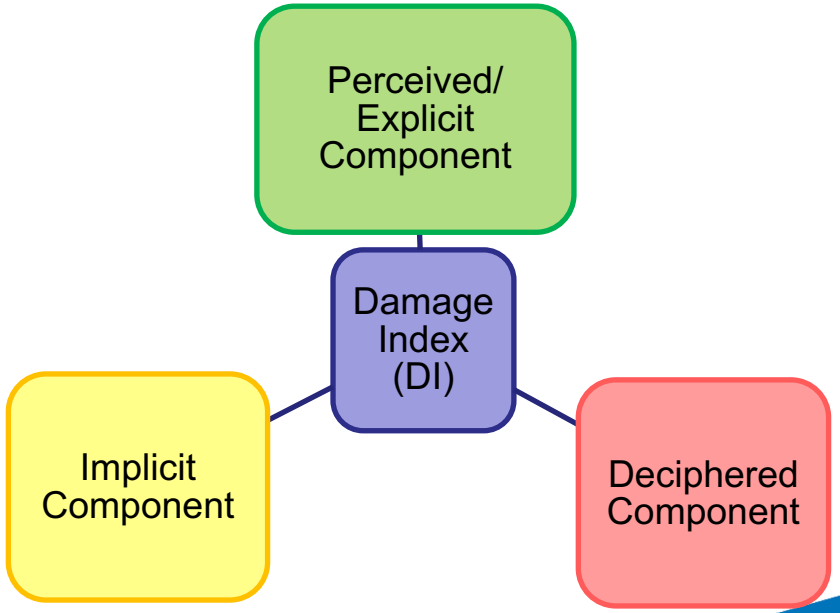
- Deciphered component only involve product and process data <u>but not for control data.</u>

Damage Index (DI)

Damage Index=

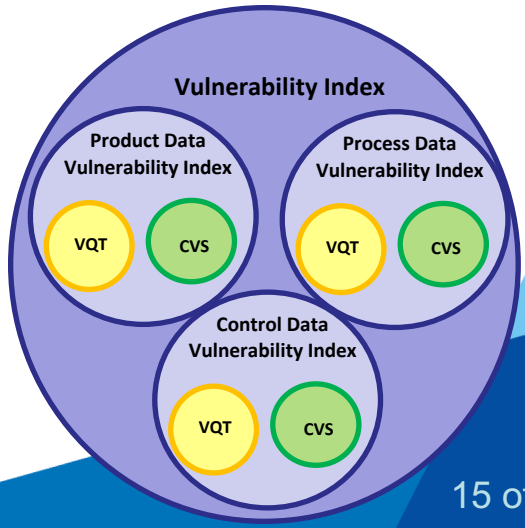
$$\frac{Explicit\ Component + Implicit\ Component + Deciphered\ Component}{Avg.Single\ Job\ Price}$$





Vulnerability Index (VI)

- Serve as reference to implement adaptive cyber security to each manufacturing system entity.
- VI formula is derived from :
  1. Data type to cyber security principles correlation. The correlation is tabulated into Vulnerability Quantification Table (VQT).
  2. Common Vulnerability Score (CVS) of hardware and software within each system entities.



Data Type to Cyber Security Principles Correlation

Data Type:

- Product data
- Process data
- Control data

Cyber Security Principles: (CIA)

- Confidentiality: Assurance of data access by authorize entities only.
- Integrity: Refers to data not altered, modified or corrupted.
- Availability: Relates to accessibility of data when needed

➢ The correlation is tabulated in a Vulnerability Quantification Table (VQT).

Product Data	0.5	0.2	0.3	→ Sum=1.0
Process Data	0.4	0.4	0.2	→ Sum=1.0
Control Data	0.2	0.6	0.2	→ Sum=1.0
	Confidentiality	Integrity	Availability	

❖ VQT is to be tailored for different manufacturing system

Common Vulnerability Score System (CVSS)

- Common Vulnerability Score System (CVSS) is a free and open industry standard for accessing the severity of computer system security vulnerabilities.
- For Vulnerability Index (VI) calculation, only the “Impact Matrix” from CVSS
- Impact Matrix- rate the impact on the Confidentiality, Integrity, and Availability (CIA) of data processed by the system upon attack.
- CVS of each system entities need to be computed and put in matrix form.

Vulnerability Index (VI)

- Formula:

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

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

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

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

C_1 = (Count of high score for Confidentiality x 1) + (Count of low score for Confidentiality x 0.5)

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 x 0.5)

Example - Vulnerability Index (VI)

Entities	Hardware	Software	Total No. of CVSS Confidentiality	Total No. of CVSS Integrity	Total No. of CVSS Availability
5-axis CNC Micron Machine 1	• Simplified PC (with Ethernet Card) • Siemens PLC	• Windows XP	• High = 2 • Low = 0 • None = 1	• High = 2 • Low = 1 • None = 0	• High = 2 • Low = 0 • None = 1
Total CVSS Score (per category) # High =1;LOW=0.5; None =0			(2*1) + (0*0.5) +(1*0) =2	(2*1) + (1*0.5) + (0*0) =2.5	(2*1) + (0*0.5) + (1*0) =2

CVSS Weighted Score Matrix

$$C = \begin{bmatrix} C_1 \\ C_2 \\ C_3 \end{bmatrix} = \begin{bmatrix} 2 \\ 2.5 \\ 2 \end{bmatrix}$$

Vulnerability Quantification Table (VQT)

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

Vulnerability Quantification Matrix

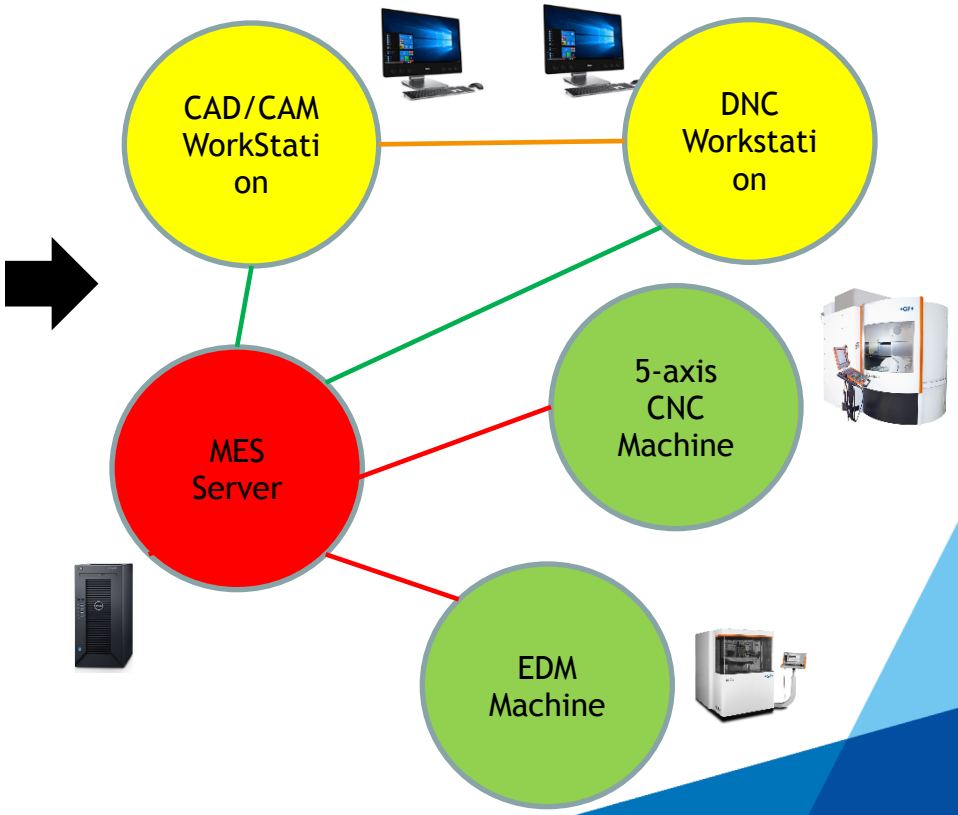
$$Q = \begin{bmatrix} Q_{1,1} & Q_{1,2} & Q_{1,3} \\ Q_{2,1} & Q_{2,2} & Q_{2,3} \\ Q_{3,1} & Q_{3,2} & Q_{3,3} \end{bmatrix}$$

$$V = \begin{bmatrix} V_{VI\ for\ Product\ Data} \\ V_{VI\ for\ Process\ Data} \\ V_{VI\ for\ Control\ Data} \end{bmatrix} = Q \times C = \begin{bmatrix} 0.5 & 0.2 & 0.3 \\ 0.4 & 0.4 & 0.2 \\ 0.2 & 0.6 & 0.2 \end{bmatrix} \times \begin{bmatrix} 2 \\ 2.5 \\ 2 \end{bmatrix} = \begin{bmatrix} \mathbf{2.1} \\ \mathbf{2.2} \\ \mathbf{2.3} \end{bmatrix}$$

Research Demonstrator

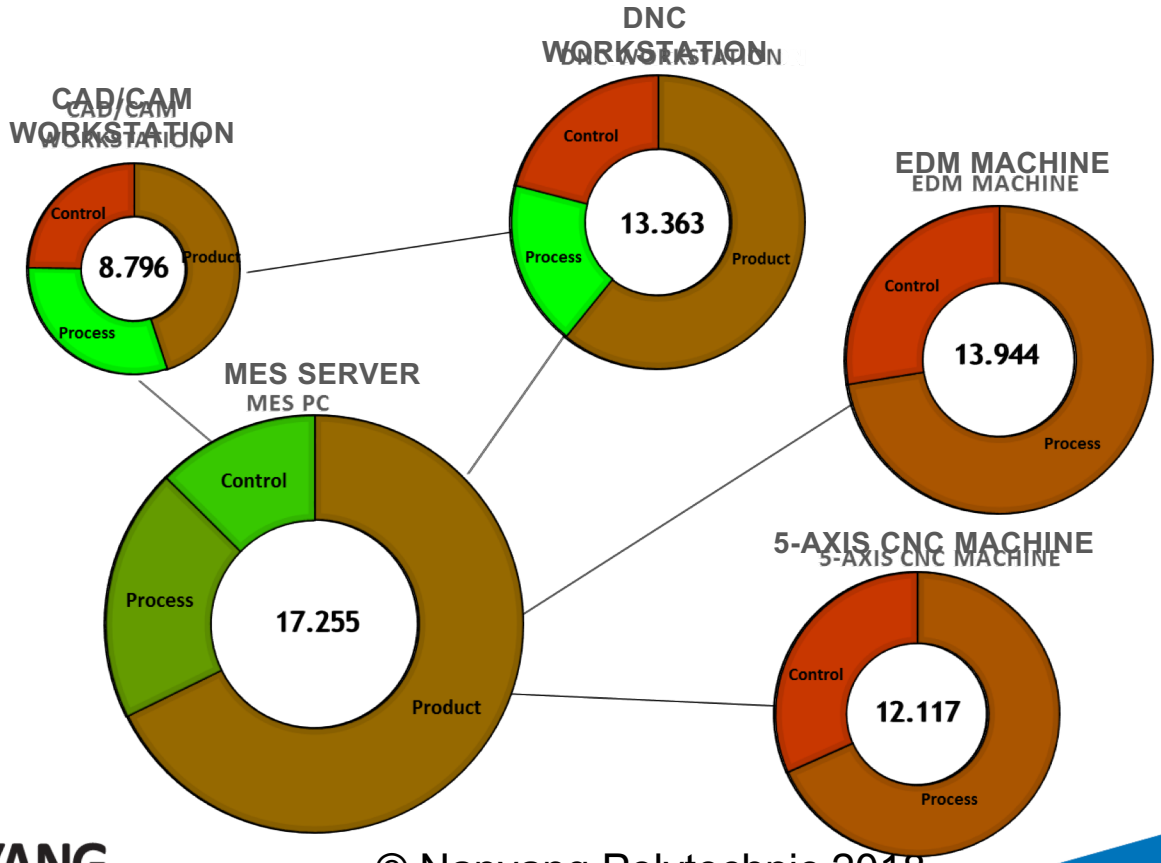
Nanyang Polytechnic Singapore
Digital Manufacturing Lab

System Data Network (SDN)



System Vulnerability Map (SVM)

- Serves as cyber security landscape visualisation tool for enterprises.
- Represented by nodes and lines.
- Node size represents DI, colour of node represents VI.



Conclusions

- Data-Driven and Data-Differentiated approach is needed to handle the heterogeneity of manufacturing system.
- Damage Index (DI) and Vulnerability Index (VI) serve as good indicators to determine highest value entities to be protected and level of protection to be implement.
- SVM provides graphical visualisation for manufacturing owners to prioritize and optimize resources for the enterprise.

Future Work

- Expand the matrix to cover, 1) data in-use/work-in-progress, 2) data on move.
- Develop a machine learning technique to stochastically determine the DI and VI mathematical metrics.
- Expend and test bedding the DI and VI model on different industry such as chemical plant system, oil and gas industry and etc.

Thank You

NANYANG
THE INNOVATIVE POLYTECHNIC