SYSTEM & SOFTWARE SAFETY

COMP8180

TAKE HOME EXAMINATION (THE)

2014

Name: Sai Ma

Student ID: u5224340

Question 1

i) Use the hazard checklist provided in the file named “Q1-Hazard-Checklist-2014.pdf” to identify potential hazards from the Home-Spa steam shower system.

Solution: In order to solve this question, there are several characters which relative to risk rank should be analysis firstly. In the analysis process, the hazard severity and probability category would be describe, and form the hazard risk classification to rank hazard risk. The following table 1, table 2 and table 3 represent the process to form risk classification.

- **Hazard Severity Category**

Table 1: Hazard Severity Category

Category Name	Description
Catastrophic	Injures or major damage to the multiple people
Critical	Injure or major damage to users inside of enclosure, lead to loss of the major system
Marginal	Minor injury and significant threat to the service, lead to server system damage
Insignificant	Possible minor injury or effect on service, lead to minor system damage

- **Hazard Probability Category**

Table 2: Hazard Probability Category

Category Name	Description
Frequent	Likely to occur frequently, the hazard will be continually experienced
Probable	Will occur several times, the hazard can be expected to occur often
Occasional	Likely to occur several times. The hazard can be expected to occur several times
Remote	Likely to occur sometime in the system lifecycle. The hazard can reasonably be expected to occur
Improbable	Unlikely to occur, but possible. It can be assumed that the hazard will exceptionally occur
Incredible	Extremely unlikely to occur. It can be assumed that the hazard may not occur

- **Hazard Risk Classifications**

Table 3: Hazard Risk Classifications

Frequence of occurrence of a hazardous event	Risk Levels			
Frequent	Undesirable	Intolerable	Intolerable	Intolerable
Probable	Tolerable	Undesirable	Intolerable	Intolerable
Occasional	Broadly Acceptable	Undesirable	Undesirable	Intolerable
Remote	Broadly Acceptable	Tolerable	Undesirable	Undesirable
Improbable	Broadly Acceptable	Broadly Acceptable	Tolerable	Tolerable
Incredible	Broadly Acceptable	Broadly Acceptable	Broadly Acceptable	Broadly Acceptable
	Catastrophic	Critical	Marginal	Insignificant

As the result, the hazard risk classification could be divided into 4 levels, there are: A – **Intolerable,** B - **Undesirable**, and tolerable only where the costs of reduction are grossly disproportionate to the improvement gained, C - **Tolerable** if the cost of Reduction would exceed the improvement gained and D - **Broadly Acceptable.**

The following table 4 shows the potential hazards identified by *Hazard-Checklist-2014*.

Table 4: Identified Potential Hazard by Hazard Checklist

No	Hazard Source Type	Possible Causes	Possible Effects	Risk Rating	Potential Hazard in Case
H001	Toxic Materials	**Gas which can be inhaled** : 1) Outgassing of gasses in confined spaces	1) Respiratory Stem Blood System, 2) Body Organs, 3) irritation of eyes, nose 4) Nervous System	D	Fragrance system could only control by users without senor to detect the density of fragrance in enclosure or runtime. The long running time of this function could hurt user's health.
H002	Toxic Materials	**Inadequate oxygen for respiration due to**: 1) Insufficient ventilation if occupied, enclosed space	1) Blood System, 2) Body Organs, 3) Asphyxiation, 4) Reduction in personnel efficiency or capabilities	B	The shower enclosure is a single-piece moulding in acrylic sheeting, which could from a enclosed environment. Then, it could effect on human health.
H003	Toxic Materials	Use of food, cosmetic, or drug that is a carcinogen: 1) Bacteria and viruses	1) Irritation of eyes, nose, throat, or respiratory passages	A	The water softener have the hazard in long time usage, which could breed Bacteria or viruses in this device, and dispense into enclosure with steam.
H004	Pressure	**Pressure relief failure**: 1) No pressure relief valve or vent 2) Incorrectly installed, incorrectly adjusted, not calibrated. **Low Pressure**: 3) Compressor or pump failure	1) Container explodes, or Leakage	B	The Fragrance pumped into steam inlet nozzle by a non-return valve, as the result, the Fragrance tank have no opportunity to modify its pressure. Once the non-return valve install in the wrong direction, the system would failure immediately.
H005	Pressure	**Pressure changes**: Changes of temperature	1) Container explodes, or Leakage	D	The improving temperature could arise the pressure in Fragrance tank increasing, and lead to leakage.

No	Hazard Source Type	Possible Causes	Possible Effects	Risk Rating	Potential Hazard in Case
H006	Heat and Temperature	**High Temperature: Generation or absorption of heat from**: 1) Inadequate heat dissipation capacity or cooling system failure	1) Heat cramps, strokes, and exhaustion 2) Reduced personnel efficiency and errors 3)	D	The temperature sensor in the enclosure have hazard to fail to work, and cannot protect user from hurt from high temperature shower environment.
H007	Explosives and Explosions	**Inadvertent activation by electrical current…**of 1) Combustible gases in containers or confined spaces	1) Over-pressures, 2) Container rupture	B	When the Fragrance tank contains the material which is flammable, the tiny spark from control panel or lighting would cause explosion.
H008	Electrical and Electronic	**Short circuits caused by**: 1) Dirt, contamination, or moisture, 2) Corrosion **Accidental contact with live circuit through**: 1) Erroneous connection, 2) Lightning strike	1) Ignition of combustibles, 2) Surface damage to metals, 3) Interference with electrical equipment operation	B	The environment inside enclosure would moist and high- temperature sometimes, and effects on the performance in control device inside the enclosure. As the result, these devices have the hazard to raise failure because of their working environment.
H009	Vibration and Noise	**Fluid dynamics**: 1) High-velocity fluid hitting a surface or object that can vibrate	1) Metal fatigue and other changes in crystalline structure 2) Interference with communications	B	The water go through overhead jet and boy jets, could in a considerable velocity to raise noise and vibration in the closed environment in enclosure. This cause problem on structure of shower and effects on the communication with the people inside and outside.
H010	Mechanical Hazards	1) Impact by moving equipment or part 2) Toppling or overturning of unstable products	1) Part of body caught in pinch point	C	When moving the door of the enclosure, people would be extruded by the edge between door and sheeting.
H011	Mechanical Hazards	1) Fall from an elevated position	1) Bruises and crushed or broken bones 2) Strain	B	The moist environment inside enclosure improve the smooth of moulded seat and shower tray. As the result, there is hazard in people fall down inside the enclosure or fall onto seat.
H012	Mechanical Hazards	1) Falling objects, covers, or parts	1) Bruises and crushed or broken bones 2) Cuts, scratches, and puncture wounds	D	The overhead jet have the hazard to fall down from installation position, and cause damage.
H013	Mechanical Hazards	1) Fall from an elevated position	1) Bruises and crushed or broken bones 2) Cuts, scratches, and puncture wounds	B	The instalment seat would fall down when people sit on it, and this would raise damage.
H014	Chemical Reactions	1) Ground moisture 2) Condensation of atmospheric moisture	Material degradation	D	The moisture working environment of metal devices in enclosure could raise material detrition. Contains of fragrance would raise the chemical reactions because of its chemical contains.
H015	Human Factors	1) Unable to control panel immediately 2) Make mistake on other kinds of control operation	Error or delay in use of controls	D	The lighting function and steam, fragrance function install outside the enclosure, which make user cannot control these function when he inside of enclosure.

ii) Repeat your hazard identification, this time using Energy Trace and Barrier Analysis.

Solution: According to ETBA Procedure, define Home Spa steam shower system energy source is **AC electrical current flows**, at the same time, the **Pressure** from **Current Water** and **Fragrance** in shower system could also be one kind of energy in the system which could help system to provide service to users.

First of all, select **electrical flow** as the energy to analysis. The flow **enters** into system by mains power to **Steam Generator** [10], and it will work at **Steam Generator** [10], **Fragrance Pump** [15], **Control Unit** [20], **Control Panel** [17], **Temperature Sensor** [19] and **Lights** [18]. It will **exit** system at **Steam Generator** [10]. The following is the details on define planned barriers to control flows, barrier problems, consider energy converter problems, and effects on targets.

Moreover, select **current water** and **fragrance flow** as **Pressure** to analysis. The flow **enters** into system by Hot supply and Cold supply to **Water Softener** [12] and **Mixer / Selector Valve** [9]. It will work at **Water Softener** [12], **Steam Generator** [10], **Pressure Relief Valve** [13], **Steam Inlet Nozzle** [11], **Mixer / Selector Valve** [9], **Body Jets** [8] and **Overhead Jet** [7]. The flow into system by **Fragrance Tank** [14], it will work in **Fragrance Pump** [15], **Non-Return Valve** [16] and **Steam Inlet Nozzle** [11]. The following is the details on define planned barriers to control flows, barrier problems, consider energy converter problems, and effects on targets.

Furthermore, select gravity of **domed roof**, **moulded seat** and **overhead jet** as **Mass / Gravity / Height** to analysis. This energy enters the system at the component's working location. The following is the details on define planned barriers to control flows, barrier problems, consider energy converter problems, and effects on targets. The following table 5 is represent the hazard identified by ETBA.

Table 5: Identified Potential Hazard by ETBA

No	Pinpoint Energy Input	Planned Barriers	Hazard	Barrier Problems	Valued Target	Risk Rating	Recommended Barriers
H001	Steam Generator	None	electrical shock, power cut or long time running makes device broken	Barrier ineffective	Steam Generator	D	● install the electrical shock protection device. ● install Noise Sensor in System find broken.
H002	Control Unit	None	electrical shock, power cut or long time running makes device broken	Barrier ineffective / incorrectly designed	Control Unit	A	● install the electrical shock protected device or energy storage system to supply power.
H003	Fragrance Pump	None	electrical shock, power cut or long time running makes device broken	Barrier ineffective / incorrectly designed	Fragrance Pump	D	● install the electrical shock protection device or energy storage system to supply electrical power.

No	Pinpoint Energy Input	Planned Barriers	Hazard	Barrier Problems	Valued Target	Risk Rating	Recommended Barriers
H004	Control Panel	None	electrical shock, power cut or long time running makes device broken	Barrier ineffective / incorrectly designed	Control Panel	B	● install the electrical shock protection device or energy storage system to supply electrical power.
H005	Temperature Sensor	None	electrical shock, power cut or long time running makes device broken	Barrier ineffective / incorrectly designed	Temperature Sensor failure	B	● install the electrical shock protection device or energy storage system to supply electrical power.
H006	Lights	None	electrical shock, power cut or long time running makes device broken	Barrier ineffective / incorrectly designed	Lights	A	● install the electrical shock protection device or energy storage system to supply electrical power.
H007	Water Softener	Container to storage overflow water	too much water into softener	Barrier ineffective / incorrectly designed	Water Softener	B	● install a non-return valve before softener to protect the water softener from damage of too much water flow
H008	Steam Generator	Pressure Relief Valve	Pressure in stream generator device increase when perform faster than design limited	Barrier ineffective / failed completely	Steam Generator	B	● install a valve before generator to control the water flow based on the left water
H009	Steam Inlet Nozzle	Pressure Relief Valve	Flow / transfer unintended / too much / too little / none at all	Barrier degraded / failed completely	Steam Inlet Nozzle	C	● install a sensor to estimate the pressure situation inside of channel, then control the speed of steam generating.
H010	Mix / Selector Valve	None	water flow cause the damage the mix/select valve	Barrier degraded / failed completely	user	B	● install a drain before Mixer / Selector Valve to discharge the overflow water.
H011	Overhead / Body Jets	Jet has limited	water flow cause the damage the overhead body jets limited	Barrier degraded / failed completely	user	A	● Install a device which could reduce the speed of fluent water down to hurtles speed.
H012	Drain	None	too much water into in the enclosure	Barrier degraded	Enclosure.	D	● install a sensor which could monitor the height level of water in enclosure, to control the input water speed.
H012	Fragrance Pump	None	no fragrance in the tank, and cause pump no material to perform	Barrier degraded	fragrance tank	B	● install a sensor to estimate the left fragrance tank to advise user to add material.
H013	Overhead Jet	Support device	Support broken	Barrier too strong / weak	user or material	A	● Install extra support devices
H014	Moulded Seat	Support device	Support broken	Barrier too strong / weak	user or material	A	● Install extra support devices
H015	Domed Roof	Acrylic sheeting and Frame	Support broken	Barrier too strong / weak	user or material	A	● Install extra support devices

iii) Compare and comment on your results from parts (i) and (ii), considering (at least) the effectiveness of the techniques, their ease (or otherwise) of application and effort required.

Solution: For the result from part (i), the Q1-Hazard-Checklist-2014 provides the guidance to analysis the potential hazard in system by **causes** and **effects**. These threaten features in the work system would cause accident in the operation. This analysis is a systematic evaluation in **root cause** by pre-established standard. In the result of analysis, it includes **equipment issues** and **human factors issues**, and **conformance** and **non-conformance determinations**. As the result, analysis requires **balancing** of **technical definition** of hazard against need for sensible action/tracking, and would **contribute** to all kinds of area's safety management. This technique also takes care of **critical human errors** and **hardware failures** which is better the ETBA analysis. **However**, it **cannot** identify the hazard which caused by the energy conversation or release. For hazard identification **application** by generically checklist, it requires the users to analysis the root cause of hazard with equipment issues. As a result, this is **not** an **easy progress** in the system with many different or newly techniques. This activity requires the users or experts have the **background knowledge** or **experience** on this industry area. In the other words, the analysis's **effort** could be effect by the experts' abilities or training.

For the result from part (ii), the Q2-ETBA-Checklist-2014 provides the guidance to analysis the hazard in system by uncontrolled **energy conversation** or **release**, and energy effect on **vulnerable target**. These conversations would raise the problem which leads to unintended harm. Energy Trace and Barrier Analysis determines the effectiveness of countermeasures employed or proposed to mitigate the risk induced by energy conversation. As the result, this analysis could use **family** of **similar techniques**, and perform well in multiply energy source system or product. It is a **powerful** and **efficient** approach in discovery hazard associated with energy sources. Furthermore, its procedures produce **consistent, reasoned and objective judgements** on hazards. **However**, it will **miss** the hazard un-relative to energy source. For the **application** of ETBA, it requires the users or expert to have the **logically** way in operation in identify hazard. Fortunately, it provides a detailed procedure in analysis, which could make **user without** long time **training** or **experience** to perform well. However, the result's **effort** relative to the procedure's repeat situation and quality of procedures. In the other word, the effort of analysis depend on the user whether to perform process as guidance.

iv) Carry out a HAZOP study of the steam shower system.

In the Home Spa steam shower system, there are four flows includes electrical flow, hot water flow, cold water flow, and fragrance flow. Firstly of all, analysis the electrical flow by hazard and operability studies in the follow table 6.

Table 6: HAZOP

Guide Word	Deviation	Possible Causes	Consequences	Action Required
No or None	No flow	1. No electrical supply by Power Company 2. Mains power broken 3. Fuse in power supply melt because of devices short circuit	1. Steam cannot created in Steam Generator. 2. Air cannot be pumped into Fragrance system in Fragrance pump 3. The Control Unit cannot work 4. Temperature senor cannot monitor within enclosure 5. Control Panel cannot work 6. Lights cannot work	1. Install an electrical device, like uninterruptible power supply in the system 2. Install alarm light and speaker with battery to monitor loss of the electrical supply 3. Connect to this system with more than one Main Power which have different fuse protection system in house 3. Provide the guidance in installation of Home Spa System to make sure system not connect to undersigned power system
More	More flow	1. Thunder shock on the electrical supply system 2. Transformer cannot work cause the high-voltage electrical flow supply to the system 3. Other unknown high-voltage electrical flow connect to system	1. Steam Generator burnout 2. Fragrance Pump burnout 3. Control Unit cannot work or burnout 4. Control Panel cannot work burnout 5. Temperature Senor burnout 6. Lights become brighter or burnout	1. Install a device in main power to broken down connection to system when monitor the high-voltage electrical flow 2. Install alarm light and speak with battery to monitor voltage which higher than designed voltage 3. Install a device in Control Panel to stable the input voltage 4. Install a device in Lights to monitor high-voltage power, broken the power supply 5. Install a power system could provide designed voltage flow, and replace original power system when facing fault 6. Provide the guidance in installation of Home Spa System to make sure system not connect to undersigned power system
Less	Less flow	1. Transformer have problem in transform voltage and supply the low-voltage flow (A.C) 2. Power supply system provide the less voltage electrical flow (D.C)	1. Steam Generator cannot operate as designed speed, and cannot produce as much steam as user wish 2. Fragrance Pump cannot pump the enough air into the Fragrance system 3. Control Unit, Control Panel, Temperature Sensor cannot work 4. Lights cannot provide the designed lighting	1. Install a power supply system which could increase voltage in main power to avoid the damage caused by low voltage work environment 2. Install a battery connect to Control Unit, Control Panel and Temperature Sensor to make sure these devices work
More than or As well as	more little flow or as well as flow	1. Transformer have problem in transform voltage to the designed voltage (A.C) 2. Power supplier provides the flow with higher than system designed voltage	1. Steam Generator operators faster than design speed 2. Fragrance Pump operators faster than design speed 3. Control Unit, Control Panel would damage because the higher voltage than their designed	1. Install a device to modify the voltage reduce the normal voltage flow 2. Install a power supply system which could provide designed voltage electrical flow and supply power when monitor the high voltage flow has been provided by original power system 3. Provide the guidance in installation of Home Spa System to make sure system not connect to undersigned power system

Guide Word	Deviation	Possible Causes	Consequences	Action Required
Part of	Less flow	1. Transformer have problem in transform voltage and supply the low-voltage flow (A.C) 2. Power supply system provide the less voltage electrical flow (D.C)	1. Steam Generator cannot operate as designed speed, and cannot produce as much steam as user wish 2. Fragrance Pump cannot pump the enough air into the Fragrance system 3. Control Unit, Control Panel, Temperature Sensor cannot work 4. Lights cannot provide the designed lighting	1. Install a power supply system which could increase voltage in main power to avoid the damage caused by low voltage work environment 2. Install a battery connect to Control Unit, Control Panel and Temperature Sensor to make sure these devices work
Other than	Flow in undersigned component	1. Operation Component broken cause leakage 2. Main Power broken cause leakage 3. Unintended power system connect to Home Spa System cause flow	1. Electrical Flow may contain in water supply system 2. Mattel component or other kinds of electric conduction materials have electrical flow 3. Fragrance System contain electrical flow	1. Install a sensor to estimate the voltage situation in the component which undersigned to contain electricity 2. Install alarm system to remind user when get the leakage information from sensor 3. Provide the guidance in installation of Home Spa System to make sure system not connect to undersigned power system
Reverse	Reverse Flow	1. The wrong connect in socket 2. The wrong flow direction has been supplied in power supply system (D.C)	(if the Home Spa System work in Alternating Current environment, this situation would not cause problem) 1. Devices which require electrical supply cannot work	1. Install the devices which could transform Direct Current entry system in the right direction 2. Attached a notation on the socket to make sure connection is correctly 3. Change the Home Spa System electrical supply to Alternating Current

For this problem, there are other three flow which are hot water flow, cold water flow and frequency flow has been omission in the description. For these three flows, they all have the same guide word: no or none, other than, more, less, more than or as usual part of and reverse. These three flows are **liquid flow**, which would be effect by the **gravity**. As the result, the liquid may left on some component of system when facing the flow less than normal situation. These problems should be considered and take actions.

Question 2

i) Construct a fault tree for the event *Disease response centre unable to provide refrigerated vaccine storage* down to the level of detail provided in the description of the system and diagram above.

Construct a fault tree for **top event** *Refrigerated Storage Fail*, down to the level of components identified in Figure 1 and in the description above. Once the refrigerated storage fail, represent to the *main refrigerated storage fail and refrigerated shipping container fail*.

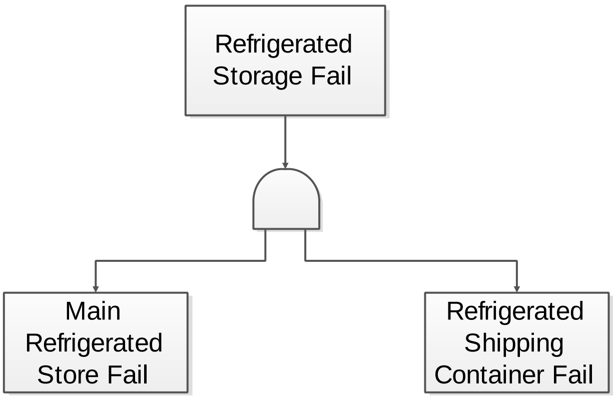
Refrigerated Storage Fail
Main Refrigerated Store Fail
Refrigerated Shipping Container Fail

Figure 1: Top Event

Main refrigerated store fail can be developed into four cases; *Power Supply Fail*, *Compressor Fail*, *Heater Exchange Fail* and *Thermostat Fail*. As main refrigerated store fail, one of these cases fail would effect on the refrigerated store, and cause failure. These four cases all implies some sort of failure. As the result, these event needs to development.

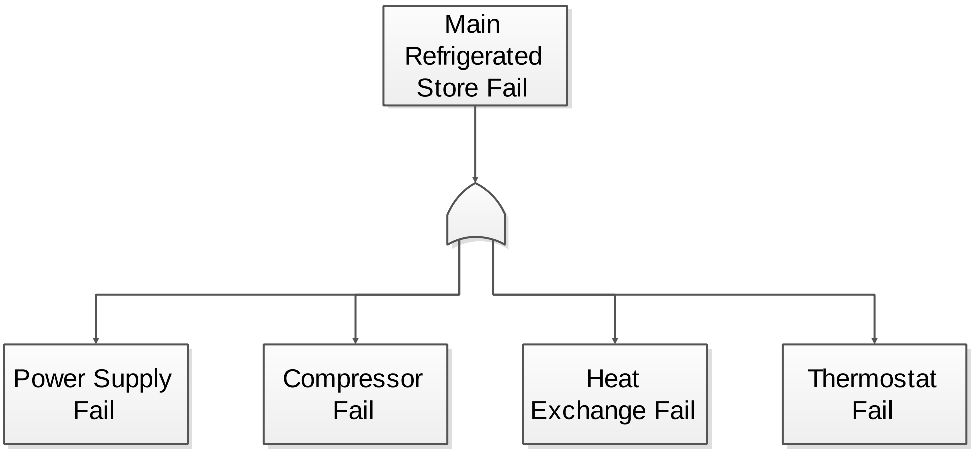

Figure 2: Top Event with Sub-event

Using *Power Supply Fail* event as the **example** to demonstrate the analysis process. According to question, the main refrigerated store system has two power system, which could be switch on or off based on the main power supply situation. As the result, the power supply fail event could develop to two case, *Main Electrical Supply Fail* and *Backup Electrical Supply Fail*.

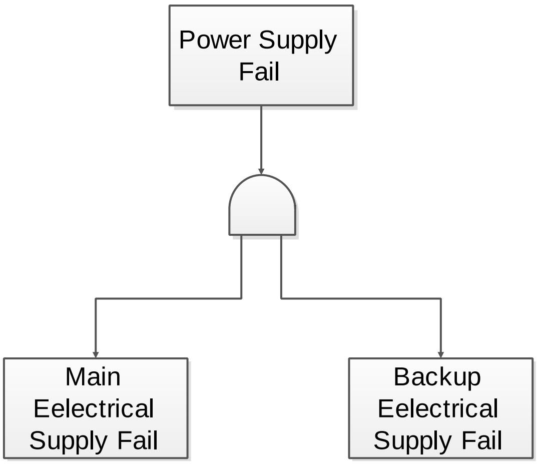

Figure 3: Power Supply Fail with Sub-events

The main electrical supply fail can be caused by two events, *No Power by Power Company* and *Supply Wire Broken*.

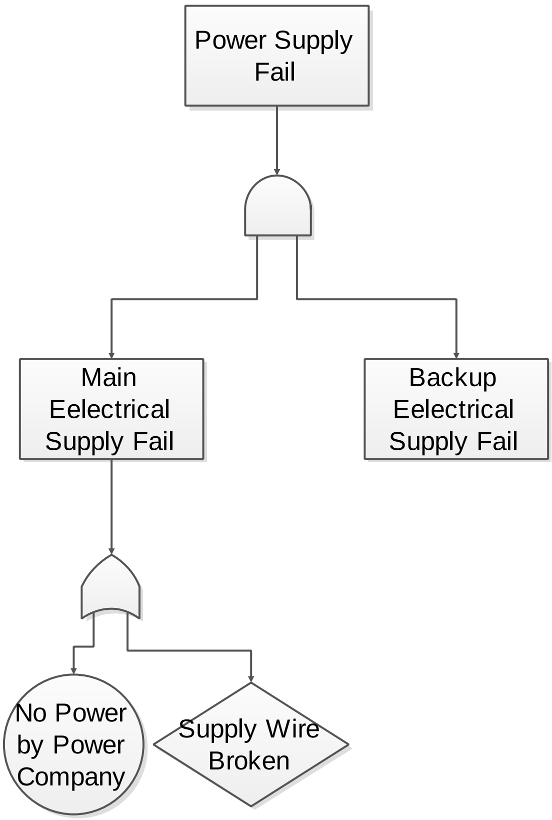
Power Supply Fail
Main Eelectrical Supply Fail
Backup Eelectrical Supply Fail
No Power by Power Company
Supply Wire Broken

Figure 4: Main Electrical Supply Fail Event

The No Power by Power Company is the initiating fault and there is no need to be further analysis in this fault tree analysis. The Supply Wire Broken, is the undeveloped event, which not developed further because it is considered unnecessary. The wire broken may cause by several situation, like burnout, cut, wrong connection. In this fault tree analysis, these kinds of tiny detail situation would be undeveloped, and assign the event to undeveloped event.

Continue to analysis the fault tree like above approach, and the following four figures are the complete fault tree for Refrigerated Storage Store Fail.

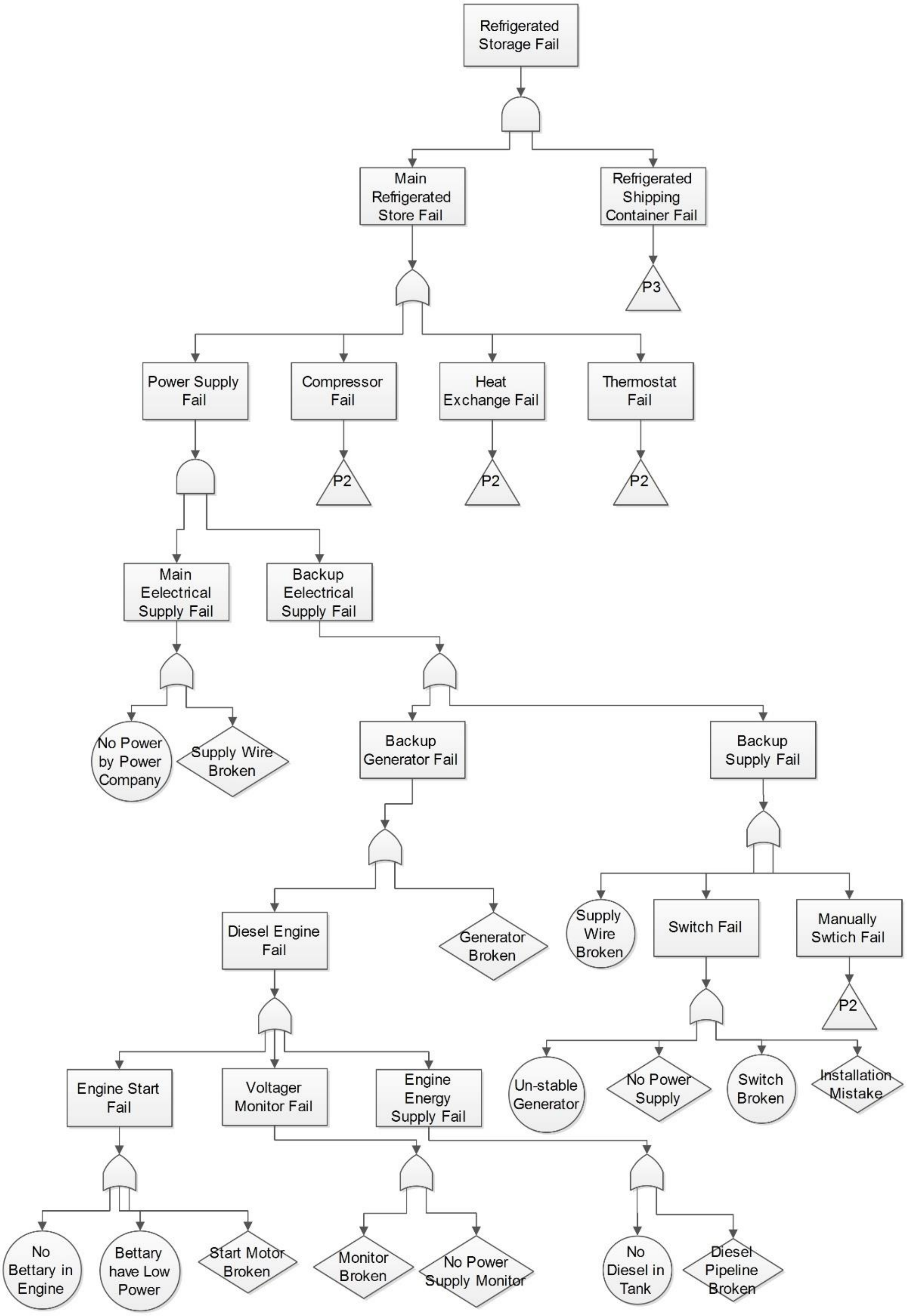

Figure 5: Fault Tree of Refrigerated Storage Store Fail - P1

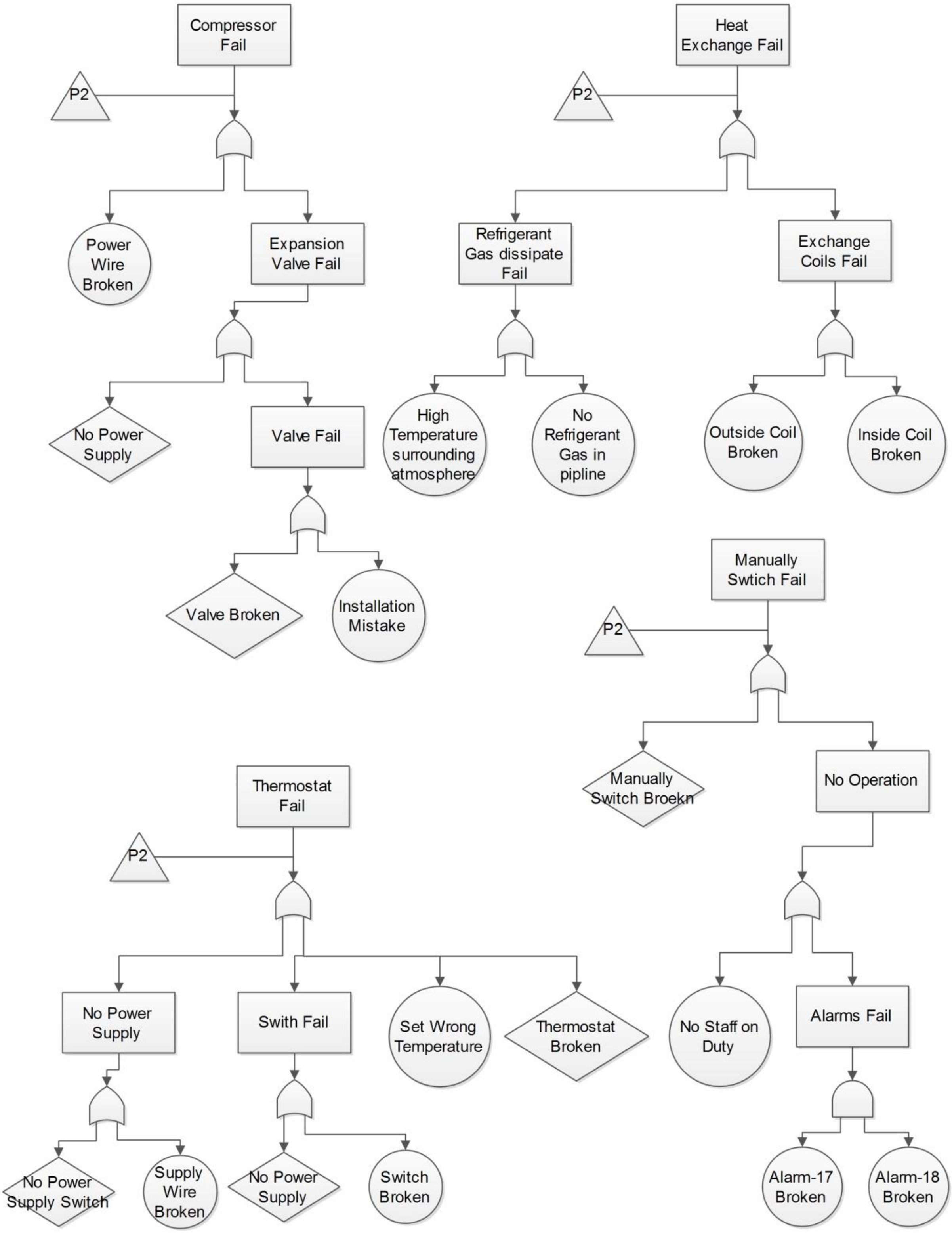

Figure 6: Fault Tree of Refrigerated Storage Store Fail - P2

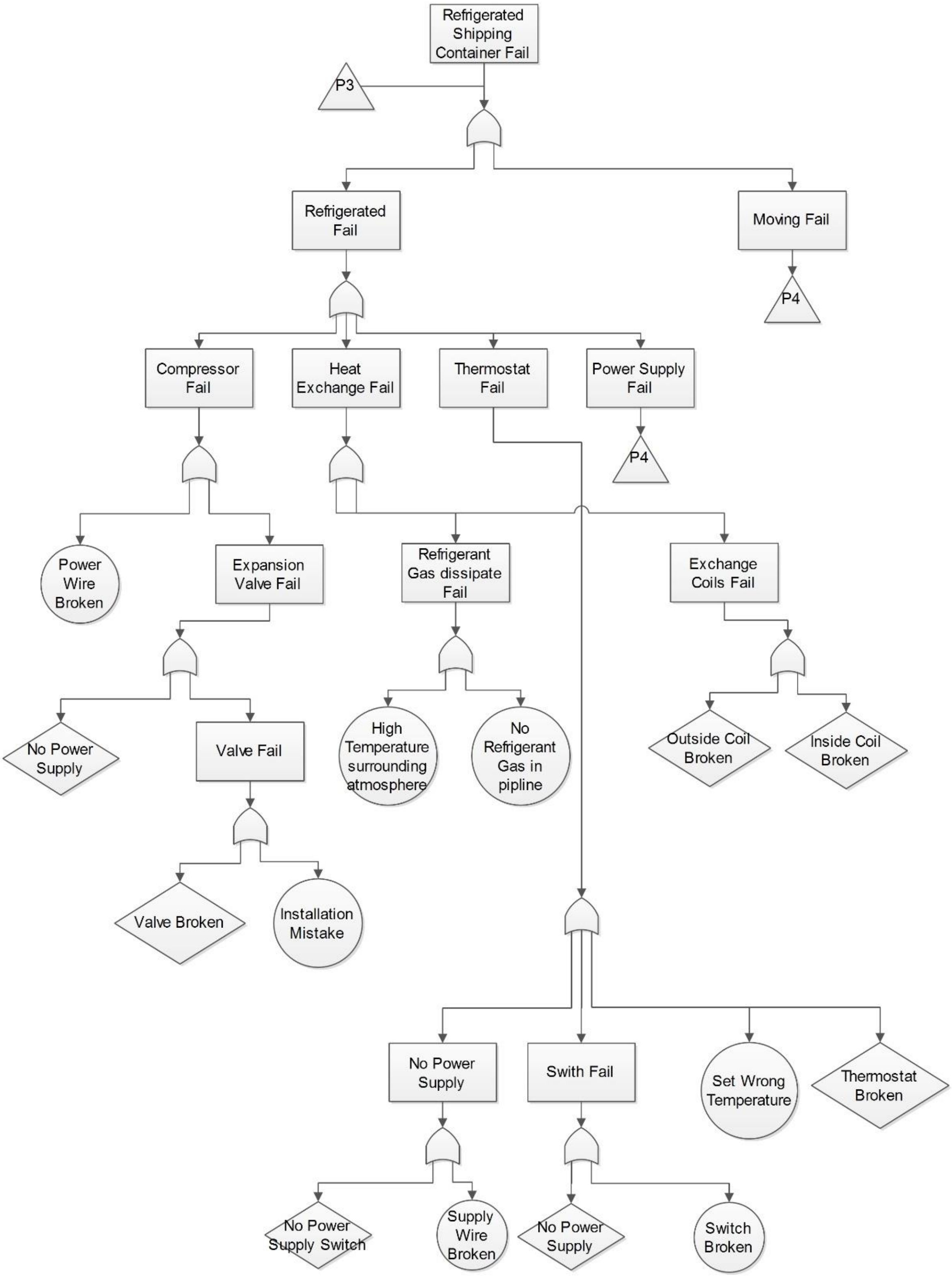

Figure 7: Fault Tree of Refrigerated Storage Store Fail - P3

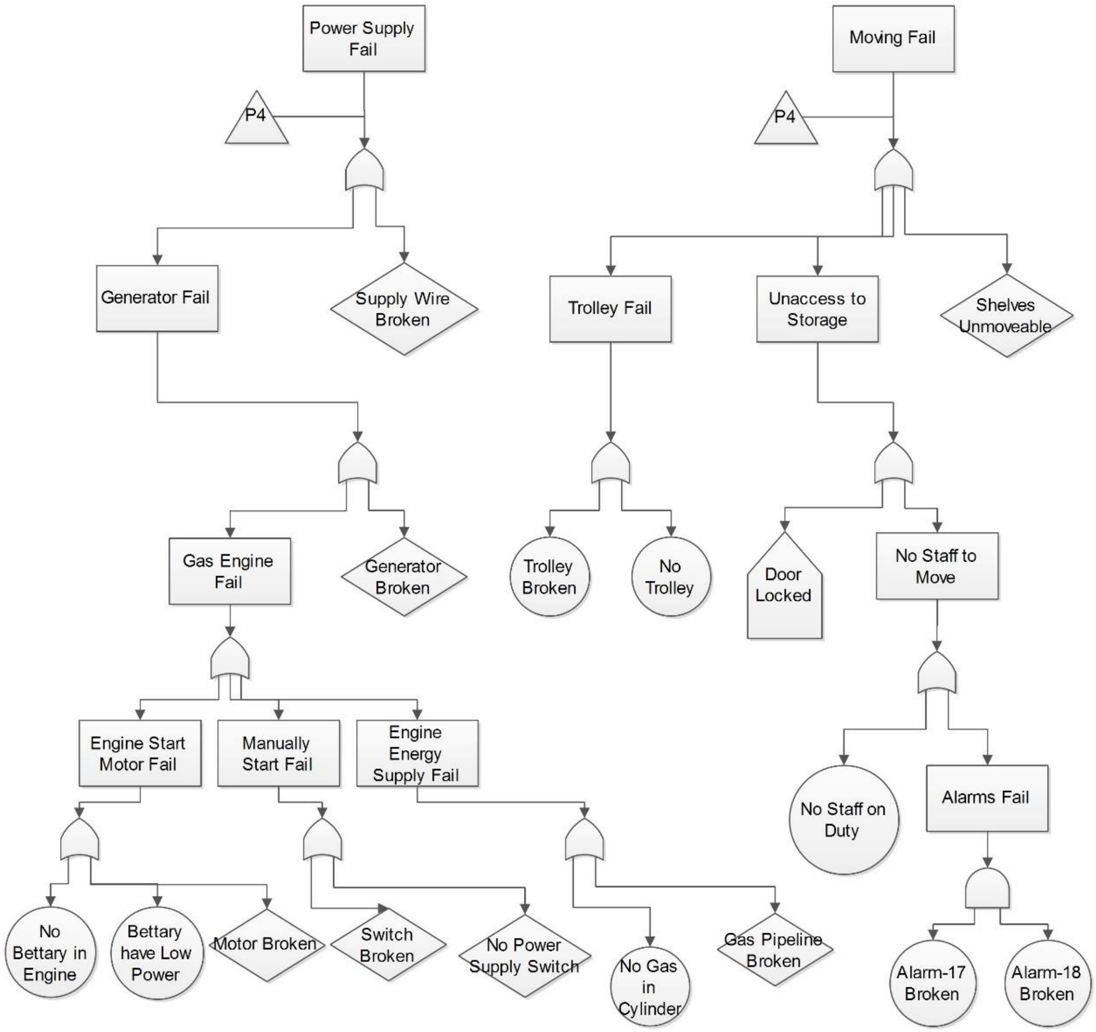

Figure 8: Fault Tree of Refrigerated Storage Store Fail - P4

ii) Identify which events in your tree represent potential dormant failures

Solution: A fault tree is a model that logically and graphically represents the various combinations of possible events, both fault and normal, occurring in a system that lead to an undesired event or state. As the result, **the potential dormant failures** in the fault tree analysis is the event which occurrence of these **indirect system effect**, for example, the **redundant system** / **item automatic takes** / **backup item** / **emergency state** over or when the failure only is **problematic during specific mission** or system **states**. As the result, in this fault tree, these actions should be analysis as potential dormant failures.

Event - 1: **Door Locked** in page 4, which come from *procedures prohibit staff from opening the door unless the refrigeration system in working*. According to this statement, it is easy to understand if refrigeration system fail, the door access to storage would be locked. As the result, when there is a failure happened on the main refrigeration system, the door would be locked and **stop** staff to **access**. In the other words, this action event would be one potential format failure.

Event - 2: **Un-stable Generator** in page 1, which come from the *once the generator has stabilized, switch will switch over automatically so that the backup supply powers the refrigeration system*. According to this statement, it is easy to find that the backup supply system would be switch on to supply refrigeration system. However, for the situation which the generator would not stable, the backup supply power system would not perform.

Event – 3: **Installation Mistake** in page 1, which come from the *switch will switch over automatically so that the backup supply powers the refrigeration system*. For this automation switch, once it has been installation in the wrong direction, the main supply and backup supply system would be connect together, and raise failure.

Event – 4: **High Temperature Surrounding Atmosphere** in page 2, which come from *…and dissipate heat to the surrounding atmosphere*. According to the general physical knowledge, the process of heat dissipate to surrounding atmosphere require the atmosphere temperature lower than the exchange coil outside of the store. However, for the situation which outside temperature is high enough, and it would effect on the heat dissipate process of outside coil. As the result, this is a potential failure of system because it would effect on refrigeration system and without respond approach.

Event – 5: Battery Has Low Power in page 1, which come from *starting the diesel engine requires that the battery is well charged*. According to the question description, the backup power supply system keep closed situation when the main power supply is stable. As the result, these failure was dormant in the normal operation process, and would trigger failure when backup system started.

Question 3

i) Examine the computer system outputs

Solution: According to the question, the **controlled (real world) variables** in this computer system includes: data on active Ringing **Alarm Bell** or not, data on active **Relay Locked** or not and data on active **Light** of Segment 1 – 10 lights or not. For the **Ringing Alarm Bell**, its actual outputs from the computer is Alarm variable set be true, which is a binary data and represent the actual load weight close to limited load weight. Once the actual load exceed load limits, the alarm variables would be set to true and activate built-in alarm sounder in panel. For the **Relay Locked**, its actual outputs from the computer is Relay variables set be true, which is a binary data and control the control function interlock relays. Once the device in a dangerous situation, its value set to ‘0’, and stop operation. As the result, when relay variables is ‘1’, the operation could be operated, and fail stopped. For the **Lights of Segments**, their actual output from the computer is Segment variables set be true, which are binary data and control the lights on the panel which could represent the performance situation. These lights could be make user know the device performance situation obviously.

The **Alarm** Variable is the **critical safety information** because once this variable become true, the software would interlock control function. Furthermore, this variables would raise the alarm user by unable operate, and inform user the crane was load the materials which close to its limited load weight. This is a main part of safety approach on protection overload operation. Furthermore, the **hazardous failure modes** focus on identify failure modes that would adversely affect overall system reliability. As the result, for the Relay Locked, once the variables are not set to low at the same time because of loss of output, the whole control functions in the crane would not enable at the same time, which would effect on the stable of crane performance. At the same time, for the Alarm Bell, once the variables are not set to true when facing the overload situation because out of tolerance, the bell would not ring and the staff would not realize the overload situation. Moreover, the **Relay Variables** would be transform at the highest **priorities** in the computer system, because of its importance on protection of dangerous operation. The Relay Variables were a serious output, and go to set the relative control function to lock. Once the output is not continuous, or leak on the transform, not all control function would be locked. This kind of situation would effect on the crane effectively because of this asynchronous interlock actions.

ii) Consider the computer system inputs

Solution: According to the question, the **monitored (real world) variables** is in the environment that system observes and respond to. As the result, in this system, the **monitored variables** in computer system inputs include: data of **Jib Length**, **Jib Elevation Angle**, **Hydraulic Ram Pressure**, **Cable Under-Wind or not**, **Cable Wound Out**, **Load Weight**, **Active Outrigger 1 – 4 Deployed or not, Fly Jib Rigged, Active Button 1 – 4 Input** and **Active Override Button Holding**. For **Jib**

Length, the jib length would be measured by drum and cable mechanism on side of jib, and converted to digital by input circuitry. For **Jib Elevation Angle**, it would be measured by gear-driven potentiometer from jib pivot, and converted to digital by input circuitry. For **Ram Pressure**, it will measured by pressure transducer in hydraulic system, and converted to digital by input circuitry. For **Cable Under-Wind or not**, it will set the Two Block to 0 to represent cable under-wind is true. For **Cable Wound Out**, the condition sensed by micro switch activated by follower on threaded rod driven from drum. The variable would be set to 0 to represent to cable out is true. For **Load Weight**, it will measured by load cell, and converted to digital by input circuitry. For **Outrigger 1- 4**, they would be sensed by micros witch in outrigger leg mechanism. For **Fly Jib Rigged**, it would sense by micro switch on fly jib mounting plate. For **Button 1-4** and **Override Button**, they would get the input data from panel.

For this system, the **Jib Elevation Angle, Jib Length, Fly Jib Position Override Button Holding** and **Load Weight** are the **critical** safety **input information**. For the former three variables, they could be used to calculate to the **effective radius** of crane, which it is an extremely signification parameter to alarm user. Furthermore, the Load Weight is also a critical information which could be compare with the crane limited load weight, and feedback the alarm information to user or not. This input relative to the core safety software function, and should be monitored all the time. In general, it is better the make these **input** could be **respond** by software in real time. However, it is hard to respond to asynchronous event and data all the time. As the result, the **response time parameter** setting determines the maximum reaction time based on the crane work situation. Consider of the computer system performance, several input should be response immediately after getting. At the same time, several characters which would display on the screen would also effect on the work performance of the crane. For the **Load Weight** and **Override Button Holding** (relative to critical safety input), they should be reflect immediate when test the overload, and the reaction time should be greater than 100 revolutions per minute, which could make sure the load weight input would be get immediately. For the **Jib Elevation Angle**, **Jib Length**, **Fly Jib Position**, the change of these parameters are based on the crane operation, and always *slow*. As the result, the reaction time should be greater than 10 revolutions per minute. For the rest input parameters, which not relative to the critical safe, their reaction time should be greater than 5 revolutions per minute.

For the input event, it may possible to have **fault** on **input operation**. The **mistake** on **operation** would active **buttons** on the inappropriate situation. At the same time, the **errors** on **measurement devices** may raise problem on input fault. For the **errors** on **measurement devices**, these errors may be detected when the overflow in range of data. For example, the Jib Elevation Angle become negative. As the result, the measurement devices should **test** by a monitor in its measurement range before performance in real world. For the mistake on operation button, it would be detected by button pressure period time from monitors. For example, the **Hold Button** would active load over limited weight on holding this button by monitor device, and enable critical outputs. As the result, these fault could be detected. When these fault has been detected, the software will not change the input data variables.

In the computer system, the **Load Weight** information input should be transform prioritise when consider of the crane performance situation. The crane's main task is load materials, however, load over limited weight would cause damage on crane, and effect on the quality of performance. As the result, the load weight information input should be input prioritise to avoid damage.

iii) Represent principal modes of operation either as a mode table, or as a state transition diagram.

Solution: In this problem, Check-Weight 2000 change its states during performance by user operations. The processes of state situation changing will be represented by state transition diagram. **State transition diagram** is a directed graph representation of system states, transitions between states, and transition rates. These diagrams contain sufficient information for developing the state equations, which are used for probability calculations. The state transition diagram is the backbone of the technique. In the Check-Weight case, it will only be represented with the relationship between state of system and user's action.

Firstly, **define the system**, which includes examine the system and define the system boundaries, subsystems, and interfaces. In this case, the system **starts with** load weight, **end with** crane stop working. In its performance, it has an **interface** on user to **operation holding button** action to continue or end performance. The next task is **identify the system states**, which aims to establish the goals of the system and determine the system and component states of interest. In this case, it has state includes: **Crane Working (Green Lights Light)** (Guard: load weight, less than warning limited), **Crane Working (Amber Lights Light)** (Guard: load weight, greater than warning limited and less than limited), **Control Locked** (Guard: Amber Lights Light) and **Fully Locked**. Finally, construct the state diagram for all of the identified system states. The following figure 9 is the state transition diagram (in this case, assume the limited weight load would cause crane stop working).

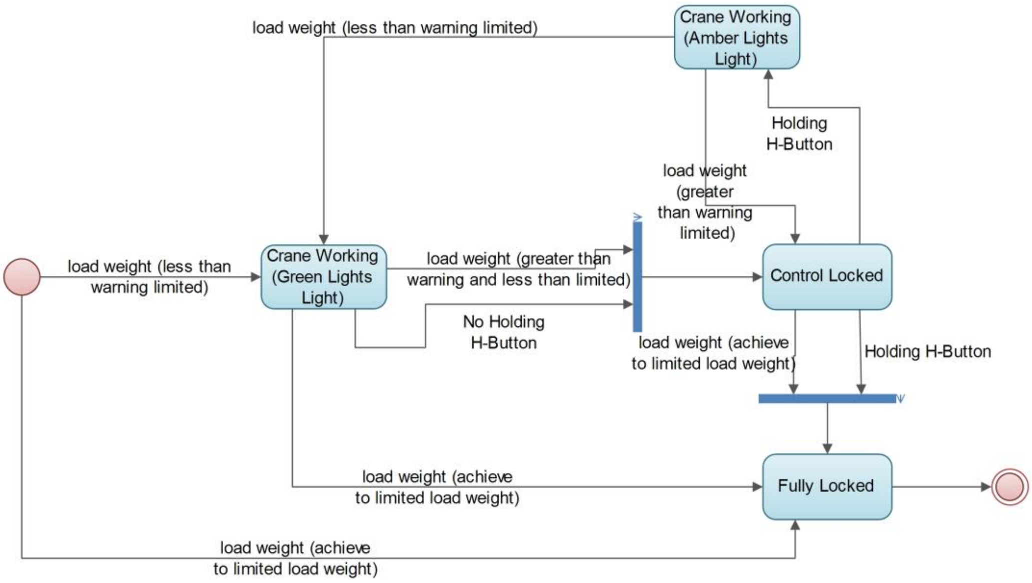
load weight (less than warning limited)
Crane Working (Amber Lights Light)
Holding H-Button
load weight (greater than warning limited)
load weight (less than warning limited)
Crane Working (Green Lights Light)
load weight (greater than warning and less than limited)
Control Locked
No Holding H-Button
load weight (achieve to limited load weight)
Holding H-Button
load weight (achieve to limited load weight)
Fully Locked
load weight (achieve to limited load weight)

Figure 9: State Transition Diagram of Crane

The load weight (less than warning limited), load weight (greater than warning and less than limited), Holding holding-button and No Holding holding-button are **normal operations** if the system. The load weight (achieve to limited load weight) represent **failure detection**, and make the system to stop perform.

iv) What are the positives and negatives of these choices? Do you think these are reasonable decisions for this system?

Solution: According to the question description, the Coyote Technology’s software engineers propose to implement the controller software primarily in MISRA C, with code written in assembly language. At the same time, put all the functions to be called in a single main loop. Moreover, the functional code could be reused by add a hardware abstraction layer.

This design have **positive** characters in the system, on **hardware** and **software cost**. In the design, the user only need to buy hardware devices, which **not** require **high property device** to run operation system, to fulfil the requirement of system. At the same time, the **hardware abstraction layers** plays the role of **interface of program**, which increase the code reused on different hardware without modification. However, this kind of design still have **negative** part. Firstly of all, all functions will run in a **main loop**, which means all functions will run one by one. If one **a function** in the first location **failed**, then **other functions** will **not perform**. As the result, once one method cannot perform, the rest will be effect on. Moreover, this kind of program performance based on the **correction of code** and **correction** of hardware device **installation**. Once the hardware devices have mistaken, the programs will not perform correctly.

In my mind, the design on **implement interface** code for some of the **hardware devices** and **adding abstraction layer** (isolate from details of computing hardware)

are the effective and reasonable approach for this system design. However, run all methods in a **main loop** is a bad design approach, because it **increase** the **probability** of functions **fail** in the programs, and make user **hard** to **detect** the **failure** on the devices.

v) What are the implications of the decision to separate the code from the configuration data? Is this a sensible decision for this system?

Solution: In this system's design, it separate the code from configuration data, which refers to the arrangement of components to form a system. In the configuration item in computer software, it **aggregates** of software that **satisfies** and **end-use function** and is designated for **separate** configuration management by the **developer** or **acquirer**. The configuration date are selected based on **trade-offs** among software function, size, host or target computers, developer, support concept, plans for reuse, criticality, interface considerations, need to be separately documented and controlled, and other factors. As the result, it should modified based on the requirements. In this case, the *company's intention is that the core software should never change; customisation for each model of crane to which the system is fitted will be achieved by changing the calibration parameters (mostly look-up tables mapping sensor values to engineering units) in the configuration EPROM*. Therefore, separate the code from configuration could separate the core function and configuration information, and there is no need to modify core software when configure software. For the **developer**, they could focus on the **core software development**. For installation software on **different platform**, the **project engineers** could focus on the **data configuration** based on customer's requirement.

In this system, it is a **sensible** because it **fulfil** the **requirement** of company intention. According to the development of this company, the managers pay attention to selling the safety management software to different devices. As the result, the software should adopt to different kind of hardware platform. After separate the core software code from data configuration, the core software development and update could be separate from project performance. For example, once the core software should update, the engineer only need to update the core software code, ignore the configuration data. This **reduce** the **probability** of software **failure** in **updating** and **improve** the **stability** of software.

Question 4

i) Sketch out the structure of a suitable safety argument for this software, making best use of the evidence identified in points 1-12 above. Ideally, this argument structure should be presented in GSN, although there will be no penalty if you are unfamiliar with GSN and choose to use another method provided that the argument is clear.

Solution: In order to present argument structure in Goal Structuring Notation, identify goals to be supported. In this question, its **goal** is *Coyote Software is acceptably safe within Tokushima Product*. In this goal, it could be solved by one **strategy**, which is *Argument over product and process of the calibration data*. In order to perform this approach, the two **sub goals**, which are *G2 Software does not raise hazard on Tokushima Product* and *G2 Software does not have hazard in itself*. For the Goal 2, the software performance situation should be assess. For the Goal 3, the software should be perform hazard analysis to make sure the software have no hazards. At the same time, this goal has four **contexts**, which are *Coyote Software*, *Tokushima Product*, *Safety Standard of Software* and *Software Running*, act as the states to Goal 1 and Goal 3. As the result, the **top** part of Goal Structuring Notation could be diagram as following:

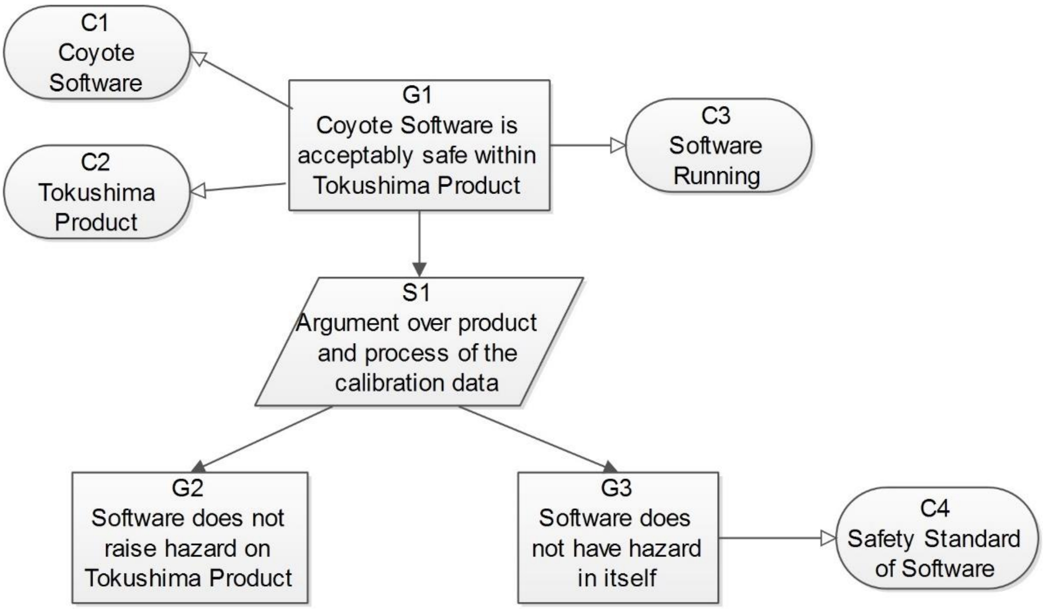
C1
Coyote Software
G1
Coyote Software is acceptably safe within Tokushima Product
C3
Software Running
C2
Tokushima Product
S1
Argument over product and process of the calibration data
G2
Software does not raise hazard on Tokushima Product
G3
Software does not have hazard in itself
C4
Safety Standard of Software

Figure 10: Top Part of GSN on Coyote Software

According to the same approach to develop argument diagram, continue to define basis on goals states and strategy, than identify new goals until identify basic solution. The following two figures are the whole result of a goal structuring notation figure which represents to the argument structure (Some goals lock of evidence to support).

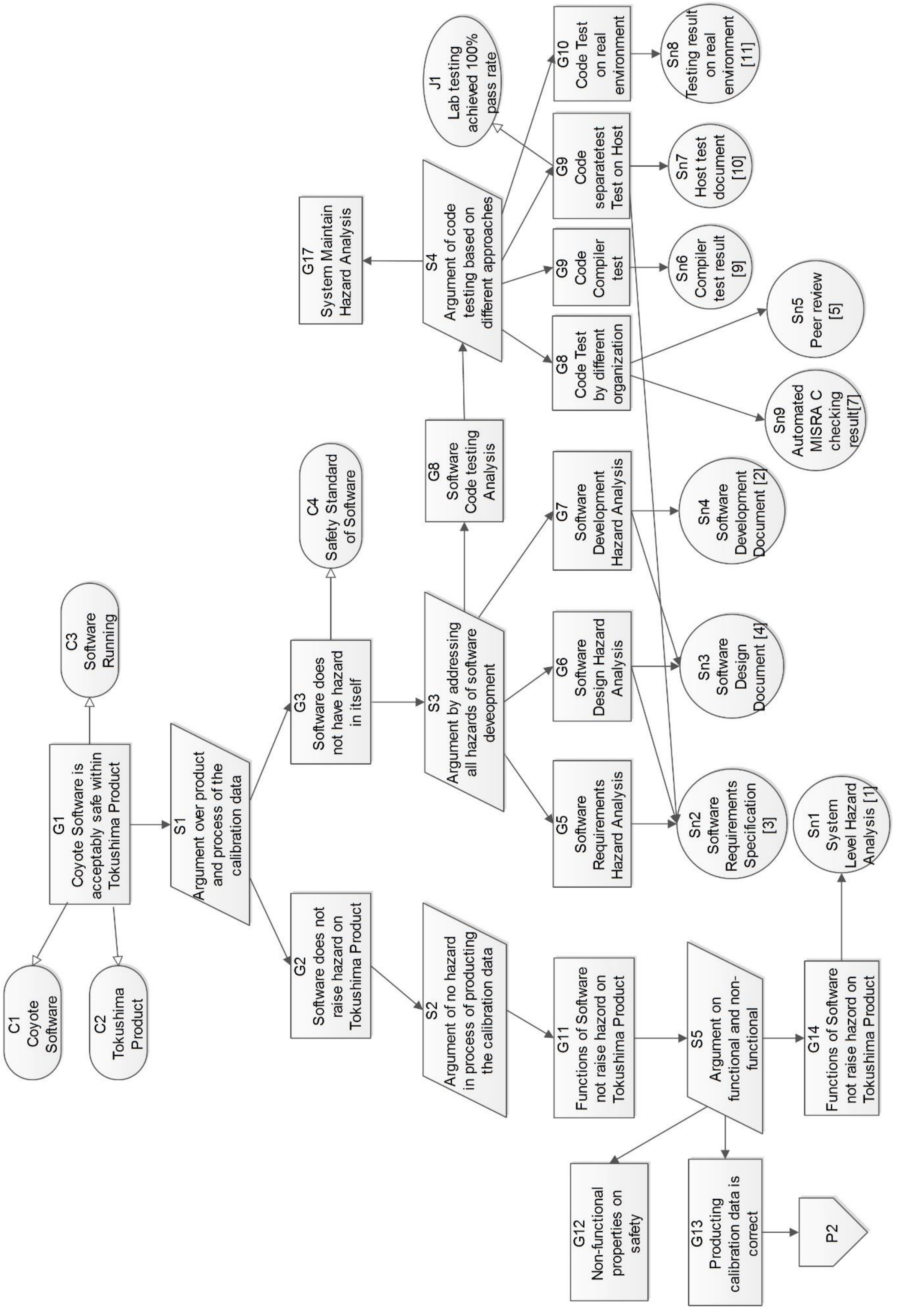
G1
Coyote Software is acceptably safe within Tokushima Product
C1
Coyote Software
C2
Tokushima Product
C3
Software Running
S1
Argument over product and process of the calibration data
G2
Software does not raise hazard on Tokushima Product
G3
Software does not have hazard in itself
C4
Safety Standard of Software
S2
Argument of no hazard in process of producting the calibration data
S3
Argument by addressing all hazards of software deveopment
G8
Software Code testing Analysis
S4
Argument of code testing based on different approaches
G17
System Maintain Hazard Analysis
J1
Lab testing achieved 100% pass rate
G11
Functions of Software not raise hazord on Tokushima Product
G5
Software Requirements Hazard Analysis
G6
Software Design Hazard Analysis
G7
Software Development Hazard Analysis
G8
Code Test by different organization
G9
Code Compiler test
G9
Code separatetest Test on Host
G10
Code Test on real environment
S5
Argument on functional and non-functional
G14
Functions of Software not raise hazord on Tokushima Product
Sn1
System Level Hazard Analysis [1]
Sn2
Software Requirements Specification [3]
Sn3
Software Design Document [4]
Sn4
Software Development Document [2]
Sn9
Automated MISRA C checking result[7]
Sn5
Peer review [5]
Sn6
Compiler test result [9]
Sn7
Host test document [10]
Sn8
Testing result on real environment [11]
G12
Non-functional properties on safety
G13
Producting calibration data is correct
P2

Figure 11: The Complete GSN on Coyote Software – P1

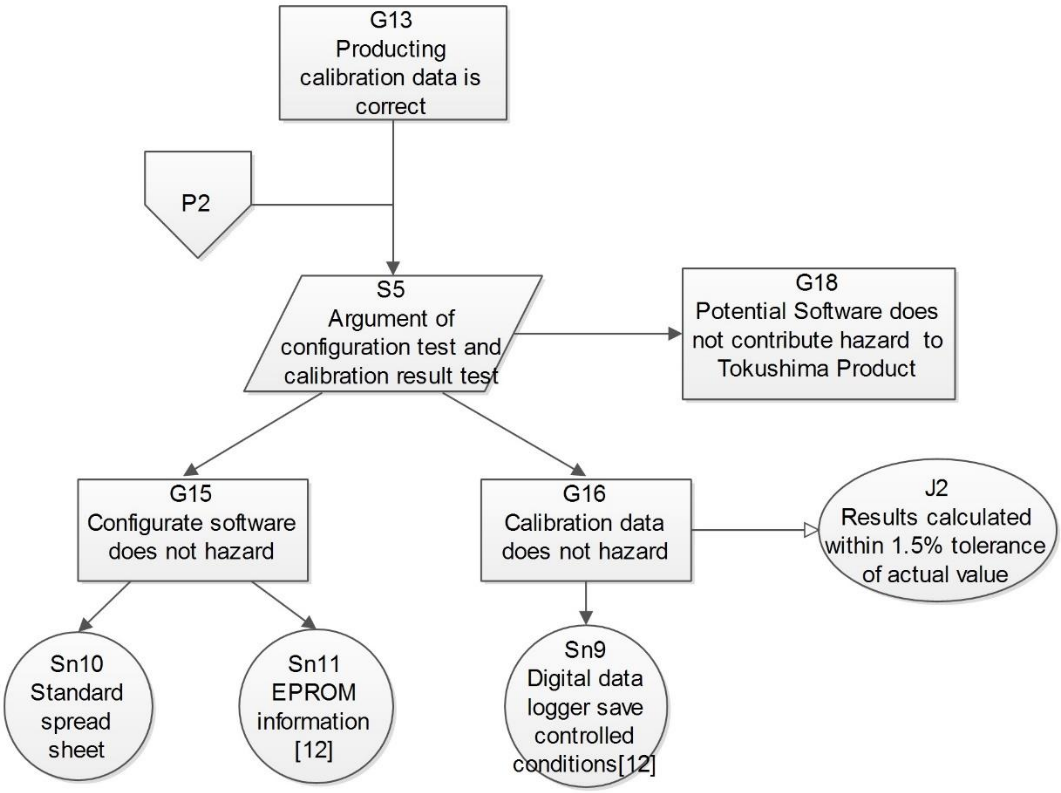
G13
Producting calibration data is correct
P2
S5
Argument of configuration test and calibration result test
G18
Potential Software does not contribute hazard to Tokushima Product
G15
Configurate software does not hazard
G16
Calibration data does not hazard
J2
Results calculated within 1.5% tolerance of actual value
Sn10
Standard spread sheet
Sn11
EPROM information [12]
Sn9
Digital data logger save controlled conditions[12]

Figure 12: The Complete GSN on Coyote Software – P2

The Figure and are the structure of a suitable safety argument for this software, which presented in GSN.

ii) Is there sufficient evidence available to make a compelling argument? If not, identify what else you believe is needed, and explain why. Is any of the evidence identified in points 1-12 above of no use in supporting your argument?

Solution: In this argument, the **evidence** is **not sufficient** because there are some part of sub-goal **lock of** evidence to support. This situation could be easy to find from the **figure** and **figure**. For *Goal 12- Non-functional properties on safety*, the Coyote Company did not provide evidence to analysis the non-functional hazard. For the *Goal 17- System Maintain Hazard Analysis*, the Coyote Company did not provide evidence to analysis the hazards in their product maintain process. Moreover, the *Goal 18 – Potential Software does not contribute hazard to Tokushima Product*, the Coyote Company did not provide the system level hazard identification and risk analysis to the in the compatibility between software from Coyote and crane from Tokushima. At the same time, several evidence have the **defect** on **completeness** or **effectiveness** of document, and effect on the argument. For the *Sn4 – Software Development Document*, did not follow the form style like safety integrity level or Development Assurance Level, which are only record brief from the team members. This kind of evidence could not be used to demonstrate the development process.

As the result, the Coyote Company should provide the evidence relative to s*ystem non-functional hazard analysis to support* to support *Non-functional properties on safety, system maintain hazard analysis* to support *System Maintain Hazard Analysis*, *system level hazard identification and risk analysis based on Coyote functi*on to support *Potential Software does not contribute hazard to Tokushima Product*. These evidences would use to support argument, and make it compelling. At the same time, Coyote Company should provide the **formal documents** which in standard software project development management style on **development process** of software to act as the evidence to support *Software Development Analysis*.

There are several evidences does not used to support to my argument. There are the **comments** in the codes which could trace back to Software Requirement Specification. The **code** which **subjected** to automated MISRA C conformance checking, which is useless, unless get the feedback report from official organization.