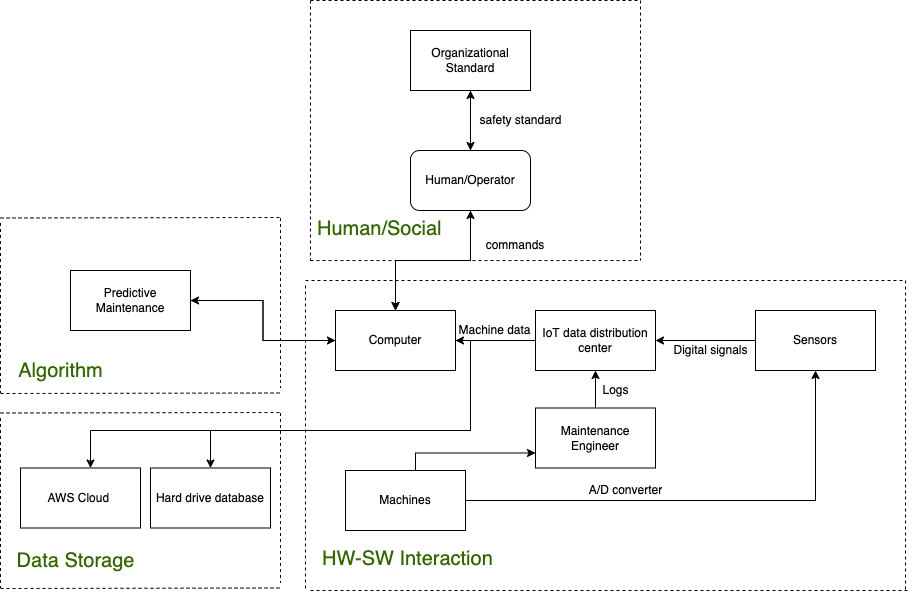
STAMP is an modern hazard analysis method which is used to identify or predict erroneous behavior. Instead of treating safety as a Reliability problem, STAMP treat as Control problem. As a result, it is able to identify the cause of failures that would have been difficult to extract with existing system design methods, especially those in the design phase. Control is broad, it can be human operators, system design, process or even through social controls such as governmental or regulatory. STAMP essentially has these steps as follows:

1. ***Identify system objectives, system hazard, hazard and safety constraint:***  
   Our project is a predictive maintenance system, which has multiple hazards that we discussed before. We pick hazard H1 to analyze, since it was the primary to the system.
2. ***Safety Constraint (SC):*** The prediction model is computed precisely and accurately.
3. ***Safety Requirements (SR):***

• Telemetry file is reachable by machines.  
• Machine IOT sensors are operating continuously and extracting accurate data.

• Machine timestamps are in correct format.  
• IOT sensors generate matching metric system.

1. ***Hierarchical control structure***



• **Organizational Standard**: these are safety standard and inspections necessary for the system.

• **Human/Machine Operator**: people who operates/interacts with the control computer.

•**Algorithm/Model**: it is installed in the control computer to predict the cycle and behavior of machines.

• **Computer**: main computer to act as a gateway between machines and operators. It receives telemetry data from sensors, manages sensor controllers through wire connectors.

• **IoT data distribution center:** send data to computer, receive logs file from maintenance engineer receive digital signals from sensors.

• **Maintenance engineer:** gather log files from machines

• **Machines:** machines that are need to be inspected.

• **AWS Cloud/hard drive database:** data storage for the system.

1. ***Control structure under normal conditions***

For a normal conditions, the operators initiate the computer using the GUI. The computer then connects to data storage, the algorithm and the sensor measurement controllers. The sensor measurement controller will control sensors and send feedback to the computer about its current working status. The sensors are attached to machines and records telemetry data. Some of the loops work as independent, in series or parallel with others.

1. ***Identifying potential Unsafe Control Actions (UCAs)***

The assessment of the hazard controls uses the fact that control actions can be hazardous in four ways:

1. A control action required for safety is not provided or is not followed.
2. An unsafe control action is provided that leads to a hazard.
3. A potentially safe control action is provided too late, too early, or out of sequence.
4. A safe control action is stopped too soon or applied too long (for a continuous or nondiscrete control action).

The table below shows as an example of identifying potential Unsafe Control Actions.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Control action | Not Providing Causes Hazard | Providing Causes Hazard | Wrong Timing or Order Causes Hazard | Stopped Too Soon or Applied Too Long |
| Sensors send signal to IoT data distribution center | Sensors did not send signal to data center when the center requires. | Not hazardous | Sensors take too long to send signal to data center. | Not applicable. |
| IoT center saves data to data storage. | IoT center did not save data to data storage. | Not hazardous | IoT center takes too long to save data to data storage. | IoT center stops sending data too soon, data is not fully saved in data storage. |

1. ***Identify hazard causal factors(HCFs****)*

Starting with hazardous control action identified in step 6, the analysis in this step involves identifying how it could happen. To gather information about how the hazard could occur, the parts of the control loop for each of the hazardous control actions identified in step 6 are examined to determine if they could cause or contribute to it.

The potential occurrence of the hazards is beyond the scope of this research, therefore, it can be recommended for further research using STAMP and CAST to do hazard analysis.