



# ***User Manual***

---

## ***Cybersafety Application Tool***

Version 1.0  
October 3, 2020

**Prepared by:**  
Naseem Hamed  
Shaharyar Khan

---

This material is based, in part, upon research supported by the Department of Energy under Award Number DE-OE0000780, a seed grant from the MIT Energy Initiative (MITeI), and funds from the corporate members of Cybersecurity at MIT Sloan (CAMS): the Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity.

# ***Introduction***

**Cybersafety Application Tool (CAT)** is an online application that facilitates an integrated, holistic safety and security analysis using the **Cybersafety method [1] [2]**. The Cybersafety method [1][2] is based on the System-theoretic Accident Model and Processes (STAMP) [3] [4] accident-causality framework which is an alternative to the traditional Chain-of-events model. In the STAMP world view, accidents are considered to be a result of loss of a control and violation of safety and security constraints rather than individual component failures [3] [4].

The basic steps in the Cybersafety method are shown in Figure 1 below [1][2]; it consists of four steps:

**Step 1:** Define the basis of the analysis by identifying unacceptable losses for the system as well as high-level system hazards that could be exploited to result in those worst possible outcomes.

**Step 2:** Develop a model of the hierarchy of controllers and their interactions that together enforce safety and security constraints on system operation (Controllers include human operators, automated systems, management, and even government and regulatory entities)

**Step 3:** Identify control actions that could be hazardous and lead to system disruption or damage.

**Step 4:** Hypothesize scenarios and identify causal factors that would cause the constraints to be violated or cause the controlled to issue unsafe commands, given malicious actions of an attacker. The results are then used to identify new requirements that would prevent the worst possible outcomes identified in Step 1 of the analysis.

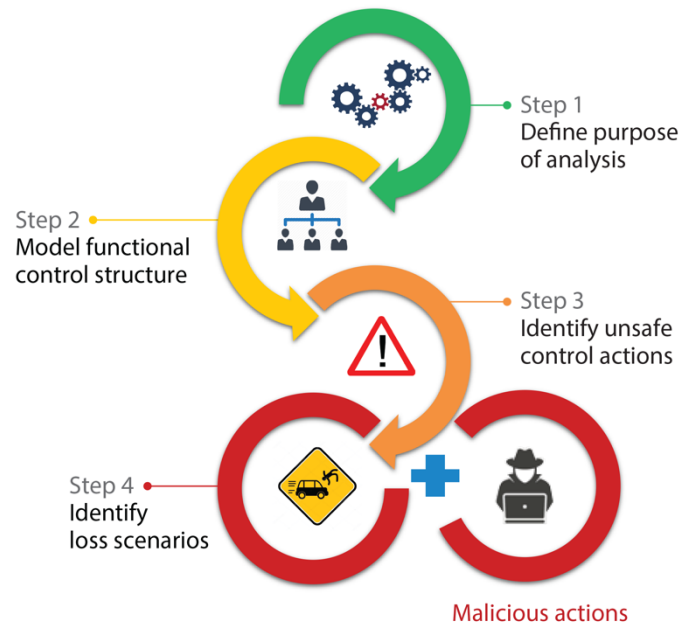


Figure 1 - Overview of Cybersafety Method [1]

The **Cybersafety Web Application Tool** was developed with a goal to improve efficiency of the analysis while reducing analyst workload. It was also developed with a goal to provide a superior user experience that integrates an advanced drawing tool while providing traceability throughout the analysis.

This document provides a step-by-step guide to use the tool and elaborates the many features the tool offers.

# Table of Contents

Introduction ..... 2

User Log In ..... 5

Project Homepage..... 7

Tool Layout..... 9

Step One – Basis of the Analysis..... 11

Step Two – Model the Functional Control Structure ..... 20

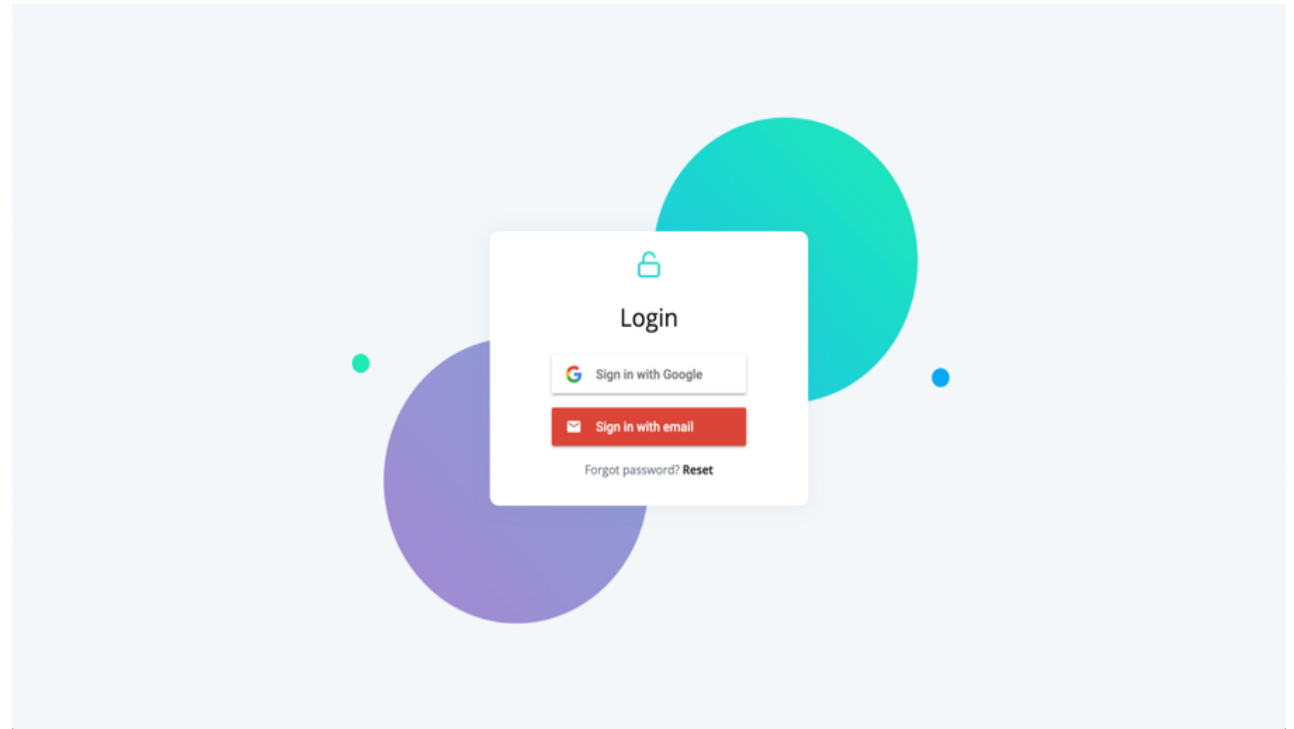
Step Three – Identify Unsafe Control Actions (UCA) ..... 29

Step Four – Generate Loss Scenarios ..... 34

References ..... 40

# User Log In

1. To open the Cybersafety web application, simply enter the following URL in a web browser:  
<https://stamp-webapp.web.app/>
2. First time users will be greeted with a login screen



3. The user can sign in either using a **Google** account or **creating a new account** using a valid email address
4. Fill out the small form and submit to enter the **Cybersafety Project Homepage**

Lock icon

### Login

#### Create account

Email  
emailone@gmail.com

First & last name  
John Doe

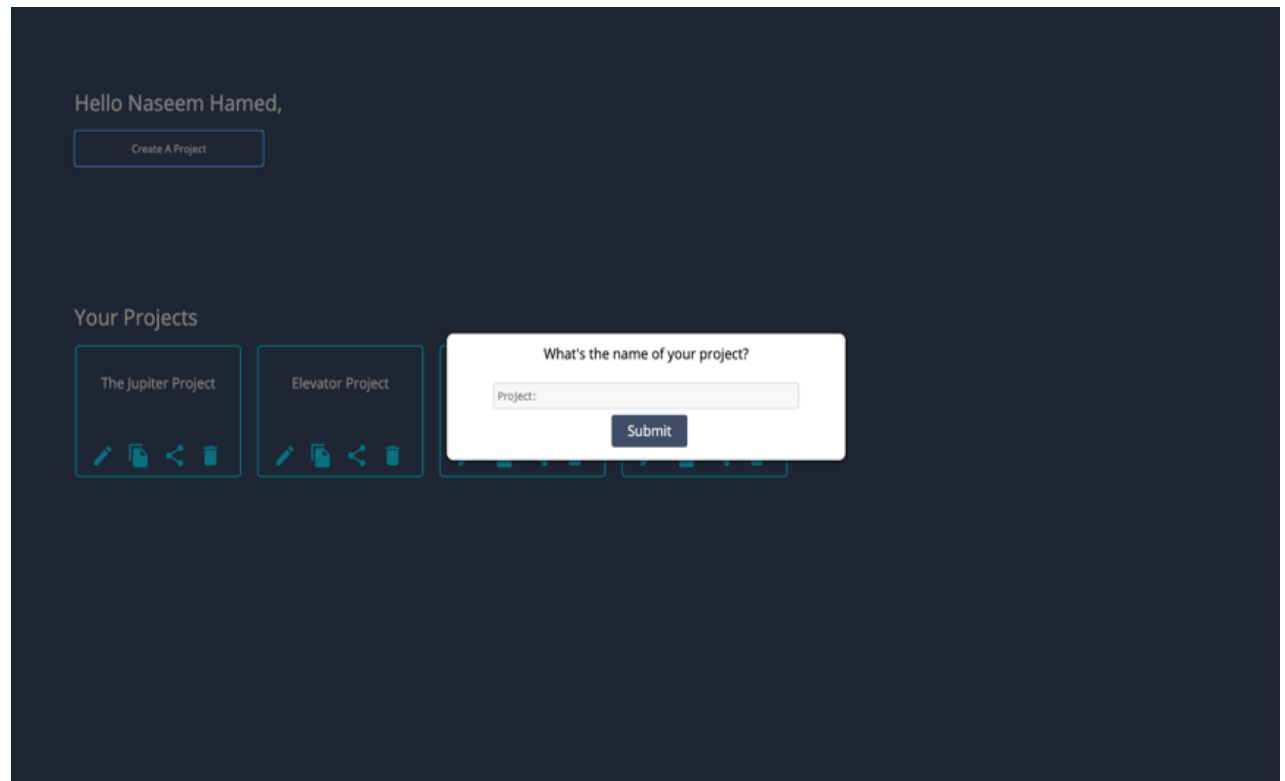
Choose password  
\*\*\*\*\*

CANCEL SAVE

Forgot password? Reset

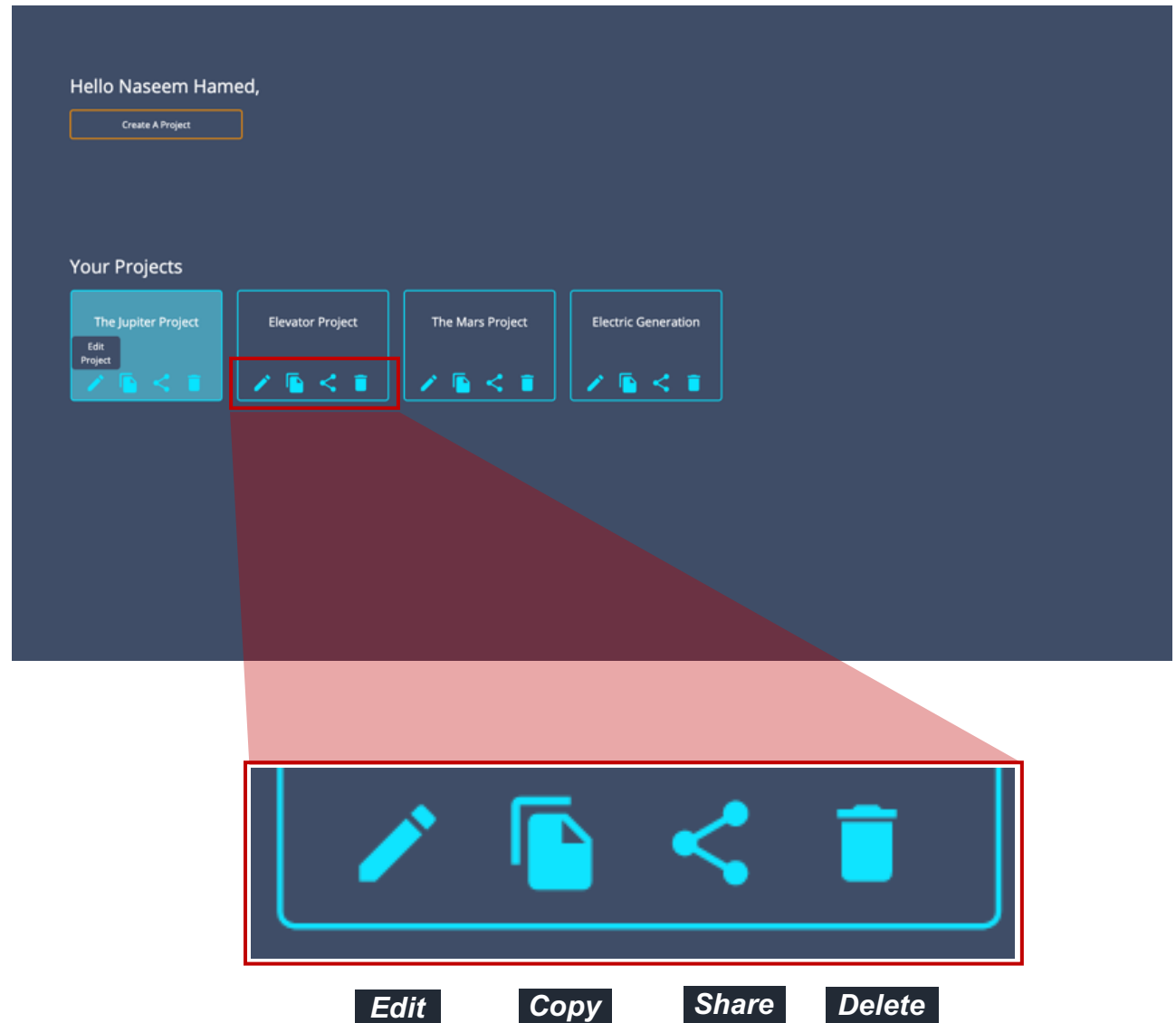
# *Project Homepage*

1. The Project Homepage enables the user to create a new project or enter an existing project
2. Click the **create project** button and choose a name for a new project **or** choose from the list of existing projects to get started



3. Note that each project has the following options:

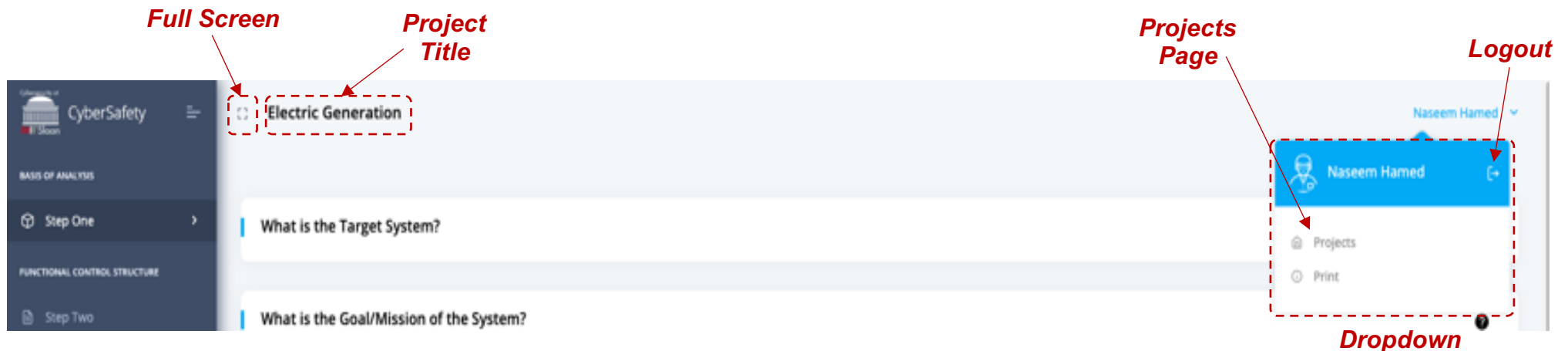
- a. **Edit:** Change project name
- b. **Copy:** Make a copy of this project
- c. **Share:** Click this icon to share the project with other team members by entering their email address
- d. **Delete:** Clicking this icon would delete the project; **NOTE** that a popup would ask for a user confirmation before deletion





# Tool Layout

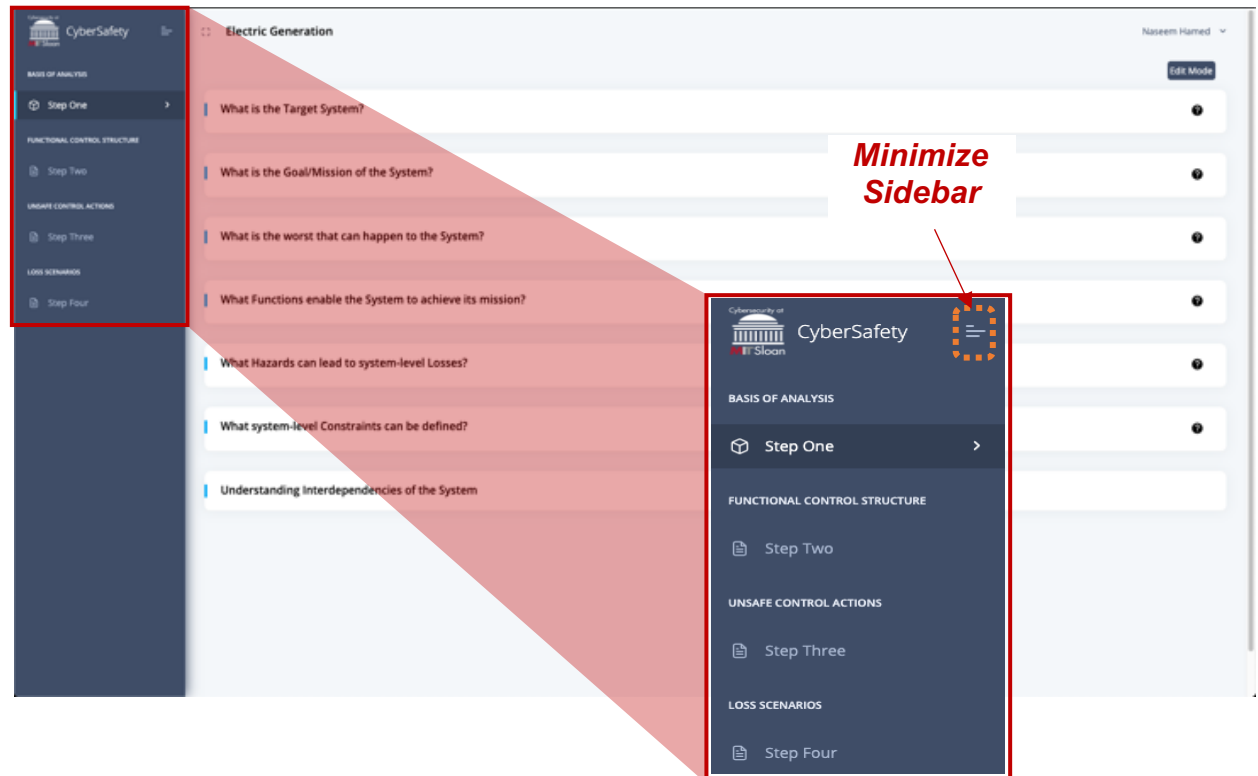
1. After creating a new project and clicking on it, the user enters the project space
2. The first thing to note is the navigation bar at the top of the screen. From left to right, there is button to enter **full screen mode**, the **project title** as well as a **dropdown menu**.
3. The dropdown menu provides options to go back to the **project homepage**, **print** the current page or **logout** of the web application



1. The **Sidebar** on the left of the page has links to the various **Steps** of the Cybersafety method. Note that the Cybersafety method consists of **four steps**:

- **STEP – 1:** Define Basis of the Analysis
- **STEP – 2:** Model the Functional Control Structure
- **STEP – 3:** Identify Unsafe Control Actions
- **STEP – 4:** Generate Loss Scenarios

2. To get additional screen real-estate click the **minimization button** at the top right of the sidebar



# Step One – Basis of the Analysis

1. **STEP-1** enables the user to define the foundation or **basis of the analysis** by posing several questions. This step includes identifying the:

- I. Target System
- II. System Mission
- III. System-Level Losses
- IV. Critical Functions
- V. System-level Hazards
- VI. System-Level Constraints
- VII. System Interdependencies

What is the Target System?

What is the Goal/Mission of the System?

What is the worst that can happen to the System?

What Functions enable the System to achieve its mission?


What Hazards can lead to system-level Losses?

What system-level Constraints can be defined?

Understanding Interdependencies of the System

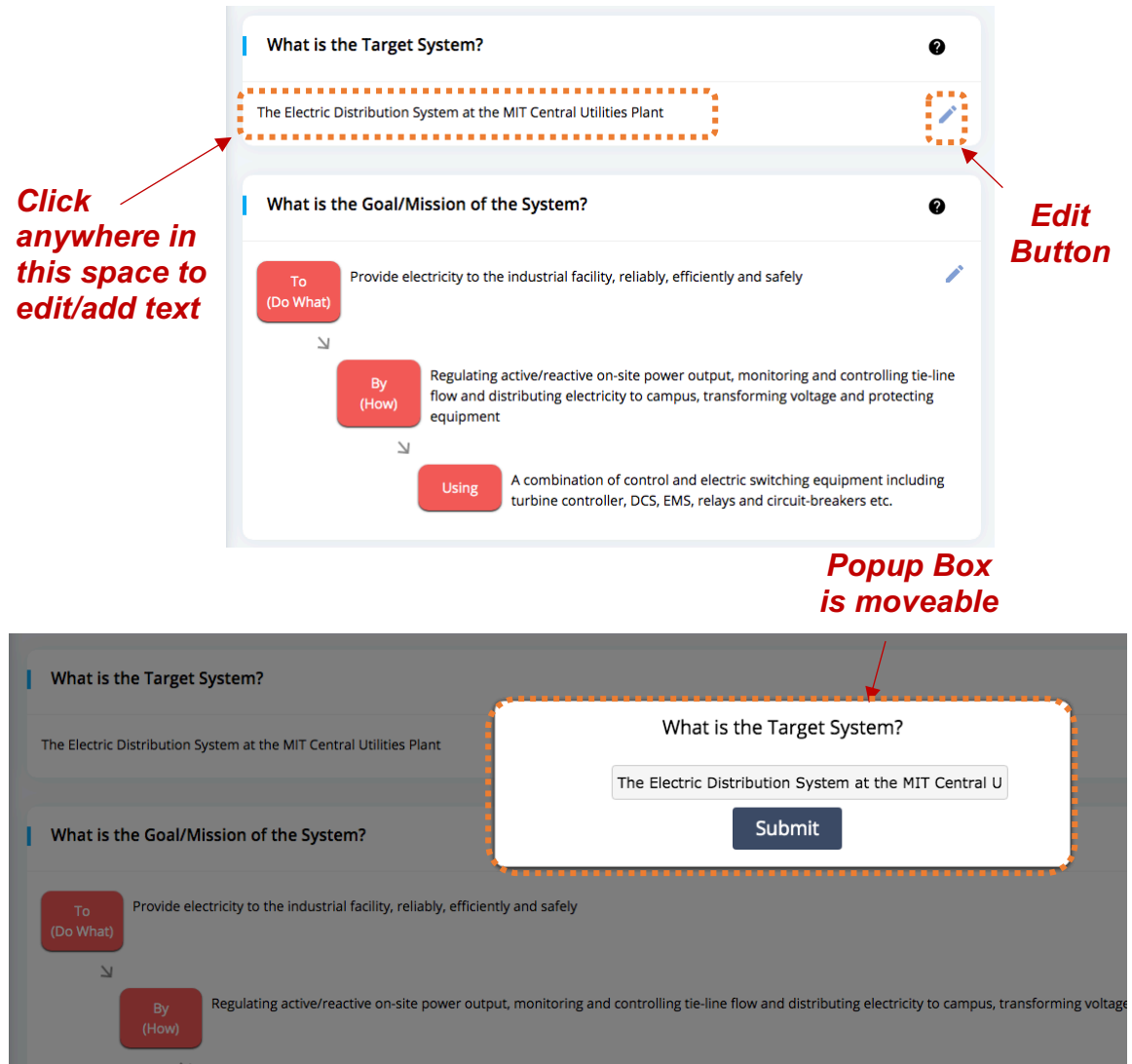
**Component  
Headers**

2. Clicking on each **component header** allows the user to view the component and **add** or **edit** data in it

3. To **add** or **edit** data simply click on the text (or blank space) in the dropdown component or click the edit button 

4. A popup will show up; simply complete the fields in the text box and hit Submit to update the database.

5. NOTE that all popup boxes are **moveable**; this enables uncovering obscured information on the screen



The image shows a screenshot of a web application interface for configuring a system. It consists of two main sections: "What is the Target System?" and "What is the Goal/Mission of the System?".

**Annotations:**

- Click anywhere in this space to edit/add text:** A red arrow points to the text "The Electric Distribution System at the MIT Central Utilities Plant" in the "What is the Target System?" section.
- Edit Button:** A red arrow points to a small blue pencil icon in the top right corner of the "What is the Target System?" section.
- Popup Box is moveable:** A red arrow points to a white popup box that appears over the "What is the Target System?" section. The popup box contains the same text as the section and a "Submit" button.

**Interface Details:**

- What is the Target System?:** Contains a text input field with the value "The Electric Distribution System at the MIT Central Utilities Plant" and a small blue pencil icon in the top right corner.
- What is the Goal/Mission of the System?:** Contains a flowchart with three steps: "To (Do What)", "By (How)", and "Using".
  - To (Do What):** Provide electricity to the industrial facility, reliably, efficiently and safely.
  - By (How):** Regulating active/reactive on-site power output, monitoring and controlling tie-line flow and distributing electricity to campus, transforming voltage and protecting equipment.
  - Using:** A combination of control and electric switching equipment including turbine controller, DCS, EMS, relays and circuit-breakers etc.

6. **CAUTION:** Clicking anywhere outside the popup box without hitting submit makes the box disappear without updating the database
7. **NOTE** that when entering information in the popup box, hitting **TAB** on the keyboard allows the user to create **multiple entries**.

The screenshot shows a web interface with a main form titled "What is the worst that can happen to the System?". Below the title is a section labeled "System-Level Losses" with a plus icon. It lists four categories: L-1: Death, dismemberment or injury to personnel; L-2: Physical damage to critical equipment; L-3: Loss of mission i.e. inability to deliver electricity to campus over an extended time period; and L-4: Economic loss due to an electrical event (including capital cost or operational cost). A popup form is overlaid on the main form, also titled "What is the worst that can happen to the System?". It contains two text input fields. The first field contains the text "Reputation Loss". The second field contains the text "Environmental Destruction". Below the input fields is a blue "Submit" button. Two red arrows point from the text "Multiple entries can be made by hitting the TAB key" to the end of the two input fields, indicating that pressing the TAB key moves the cursor to the next field to create multiple entries.

**Multiple entries can be made  
by hitting the **TAB** key**

8. This tool also provides the feature to enter subcategories for System-level functions, hazards and constraints.



9. Simply Click the downward arrow ↓ to define a subcomponent (hazard, constraint, function etc.)


10. Again, hitting **TAB** would enable the user to make multiple entries at the sub-component level within the popup box


The screenshot shows a web interface with a main form titled "What Functions enable the System to achieve its mission?". Below the title is a section labeled "System-Level Functions" with a plus icon. It contains a list of five items: 1. Regulation of on-site generation (active and reactive), 2. Monitoring and control of tie-line flow (i.e. synching), 3. Protection of individual components (generator, tra, 4. Load-shedding for system stability, and 5. Voltage transformation (transformer tap settings, if. A blue downward arrow points to the first item. A red arrow points from the text "Click to define subcomponent" to this arrow. A popup box is open over the first item, titled "What functions enable the System to achieve its mission?". It contains a list of two items: 1: Regulation of on-site generation and Active and Reactive Power Control. A button labeled "Click here to create a sub-form element" is positioned between the two items. A "Submit" button is at the bottom right of the popup. The main form also has a section titled "What Hazards can lead to system-level Losses?" at the bottom.


**Click to define  
subcomponent**




























11. Note that the tool automatically keeps track of **numbering** for components and subcomponents

12. The **order** or **numbering** for any loss, function, hazard etc., may be updated by clicking the up/down arrows   next to the item

13. Clicking the delete button  deletes the hazard, loss, constraint etc.; if the **'parent'** component is deleted, all associated **'children'** are automatically deleted and the list is automatically renumbered

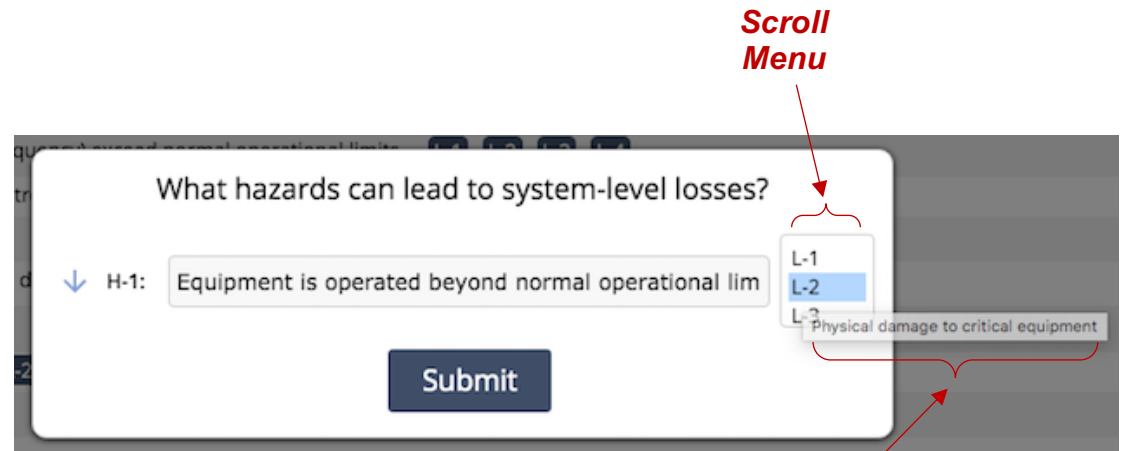
What Hazards can lead to system-level Losses? 

**System-Level Hazards** 

H-1: Equipment is operated beyond normal operational limits	 	   
— H-1.1: Mechanical parameters (speed, ramp-rates) exceed normal operational limits		   
— H-1.2: Electrical parameters (current, voltage, frequency) exceed operational limits		   
H-2: Active and reactive power is not adequately controlled	  	   
— H-2.1: Violation of power quality metrics		   

*Click to  
reorder*

14. When entering system-level hazards the user has the **option to associate** a system-level loss with the hazard
15. This is done by simply selecting the associated system-level loss from the **scroll menu** on the right
16. NOTE that multiple losses can be associated by pressing the **CTRL key** on the keyboard
17. NOTE that **hovering** over the losses in the scroll menu displays the description of the loss inside the scroll menu
18. Likewise, system-level hazards can be associated to system-level constraints by following the same approach



***Hovering over the 'loss numbers (L-1, L-2 etc.)' displays the description of the loss***



19. Once the **associations** between losses, hazards and constraints are defined, they appear as tags next to the associated hazard /constraint
20. Hovering over a tag reveals the associated item description (i.e. loss/hazard)
21. Note that the tool **does not require association** of any losses with hazards or hazards with constraints. The associations can be made at any time without impacting stability of the tool or progression to next steps
22. The associations can be made at any time i.e. at the time an item (hazard/ constraint) is initially defined or later by simply clicking a hazard or constraint and selecting the associated loss/hazard – it does not matter!

What Hazards can lead to system-level Losses?

**System-Level Hazards** +

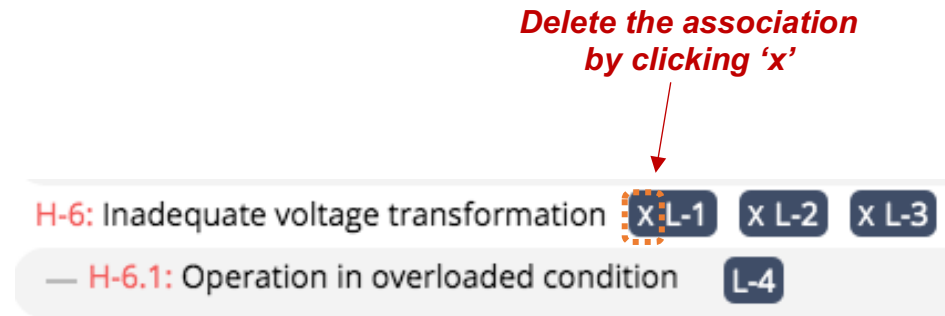
- H-1: Equipment is operated beyond normal operational limits **X L-1**
  - H-1.1: Mechanical parameters (speed, ramp-rates, temperature, vibration) exceed normal limits
  - H-1.2: Electrical parameters (current, voltage, frequency) exceed normal limits
- H-2: Active and reactive power is not adequately controlled **X L-2** **X L-3** **X L-4**

**Loss 'Tag'** points to the 'X L-1' tag.

**Loss Description** points to the tooltip for 'X L-1'.

**Tooltip for X L-1:** Death, dismemberment or injury to personnel

23. NOTE that if an associated loss is deleted, the tag automatically gets deleted from the hazard. The same is also true for a hazard associated with a constraint; this ensures **traceability** throughout the analysis



24. NOTE also that an associated tag can also be deleted by clicking the **'x'** on the tag

25. **Edit Mode** button: This button is located at the top-right of the page; clicking on it converts all the fields into editable textboxes for easy editing on the fly. The user can simply **TAB** through the textboxes to update any information.

26. To **SAVE** any text edit, press enter in the textbox after making the edit or click the **Edit Mode** button again.

**Electric Generation** Shaharyar Khan

**Edit Mode**

**What is the Target System?**

The Electric Distribution System at the MIT Central Utilities Plant

**What is the Goal/Mission of the System?**

**To (Do What)** Provide electricity to the industrial facility, reliably, efficiently and safely

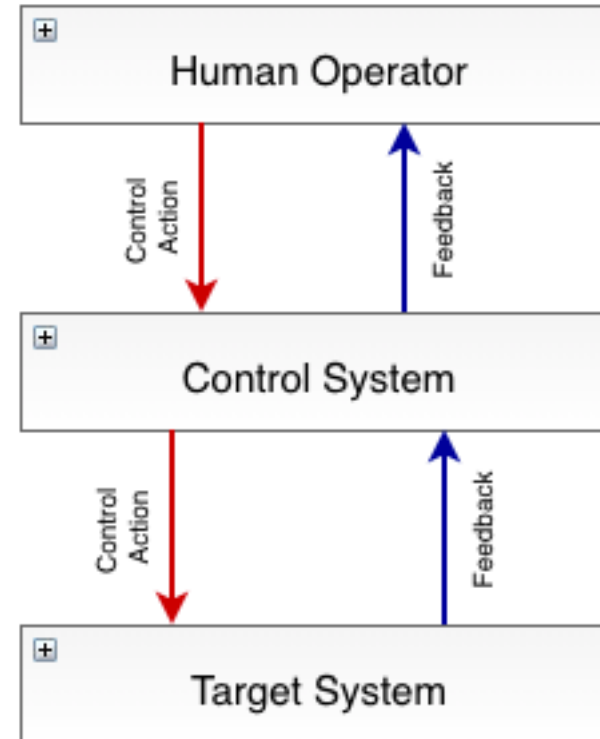
**By (How)** Regulating active/reactive on-site power output, monitoring and controlling tie-line flow and

**Using** A combination of control and electric switching equipment including turbine

*Gray boxes indicate they can be edited*

## ***Step Two – Model the Functional Control Structure***

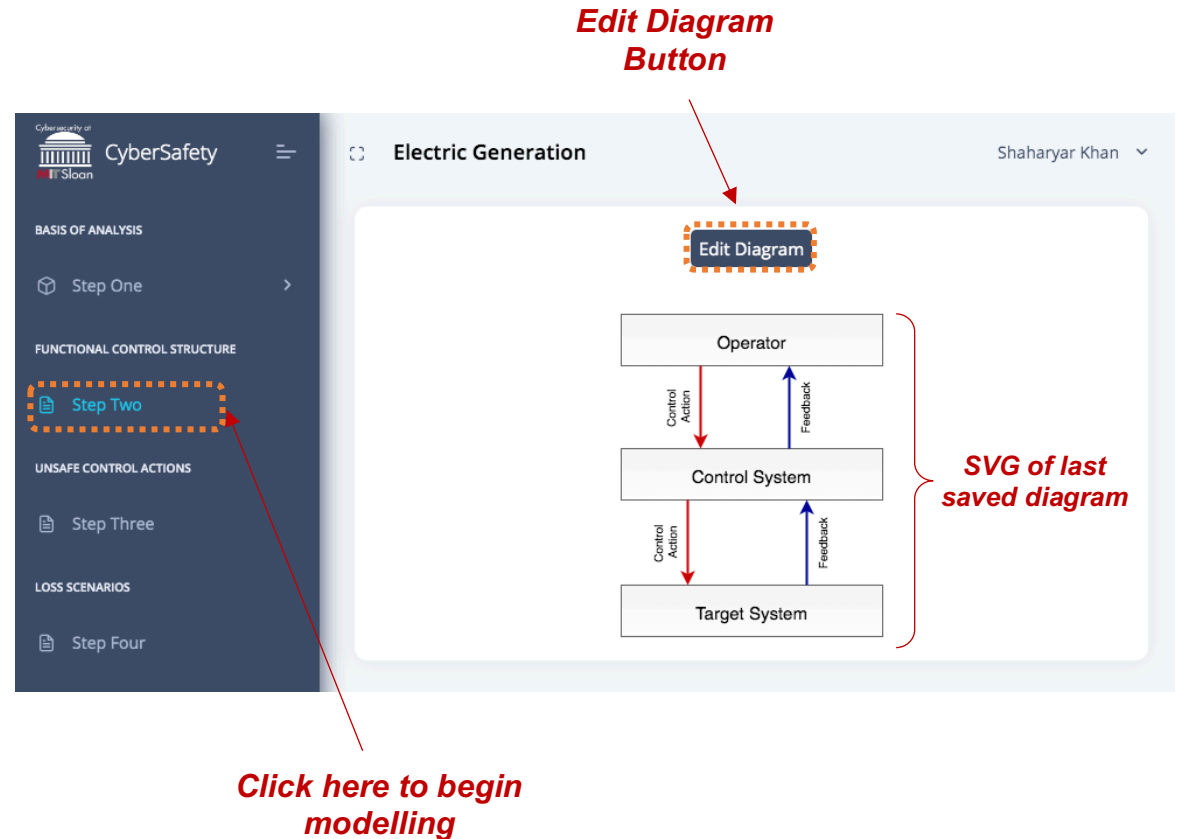
1. **STEP-2** enables the user to model the functional control structure. For increased flexibility and versatility, a [digrams.net](https://digrams.net) (formerly draw.io) frame is embedded inside the Cybersafety tool
2. Embedding the tool in such a way enables the user to perform the analysis in an integrated fashion in one place without keeping track of multiple files across different platforms (MS Excel, Visio, Word etc.)



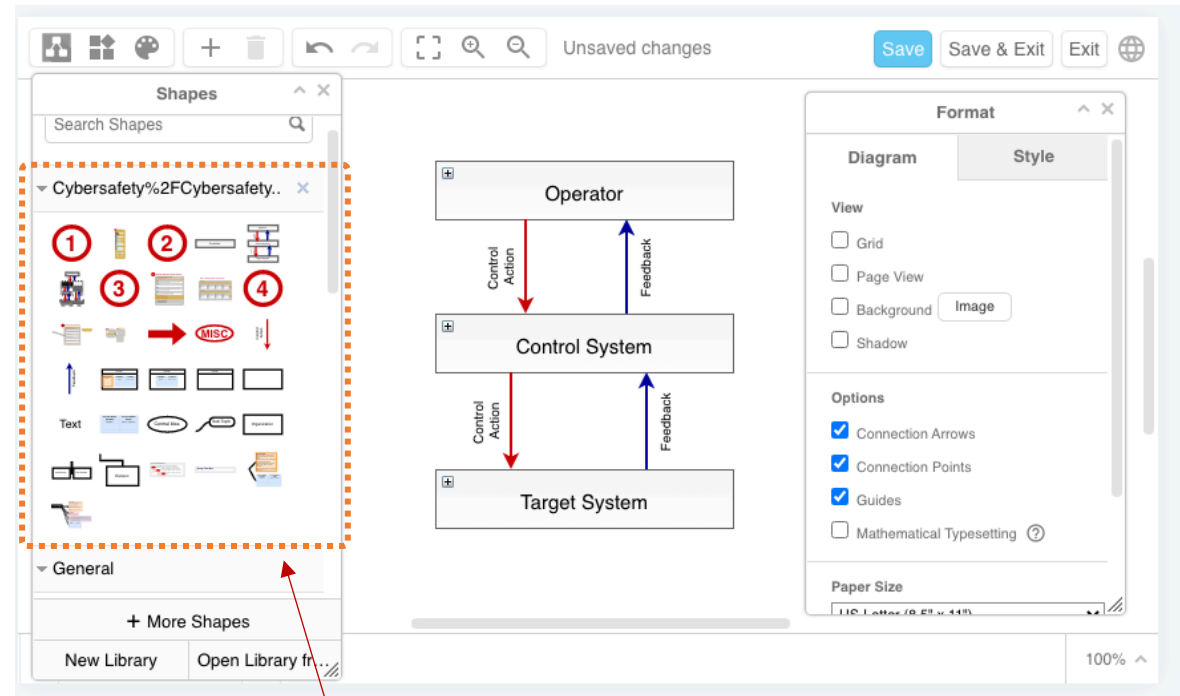
3. To begin modelling the functional control structure simply Click on **Step Two** from the Side bar

4. Step Two consists of an **Edit Diagram** button and an **SVG** of the last saved diagram

5. Clicking on the **Edit Diagram** button will open a diagrams.net (draw.io) window and allow the user to edit a diagram using the **custom** Cybersafety library.



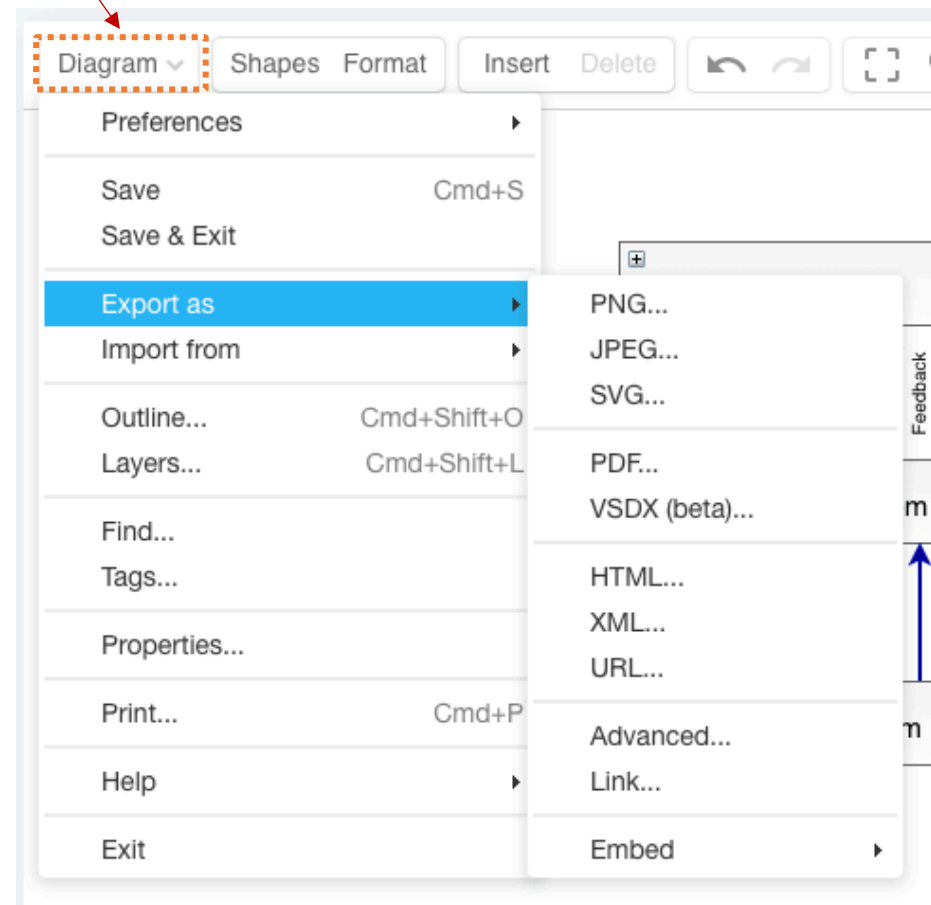
6. **Digrams.net** is equipped with a number of features to make all kinds of visually aesthetic diagrams.
7. Although there are too many features to exhaustively list in this manual, we will list some of the more important features that can improve modeling the functional control structure



**Cybersafety  
Custom Library**

8. Clicking on the **Diagrams** Icon, the user has the option to **import** a diagram made in a different application (Visio etc.)
9. The user also has the option to **export** a diagram into a number of different formats (PNG, JPEG etc.)

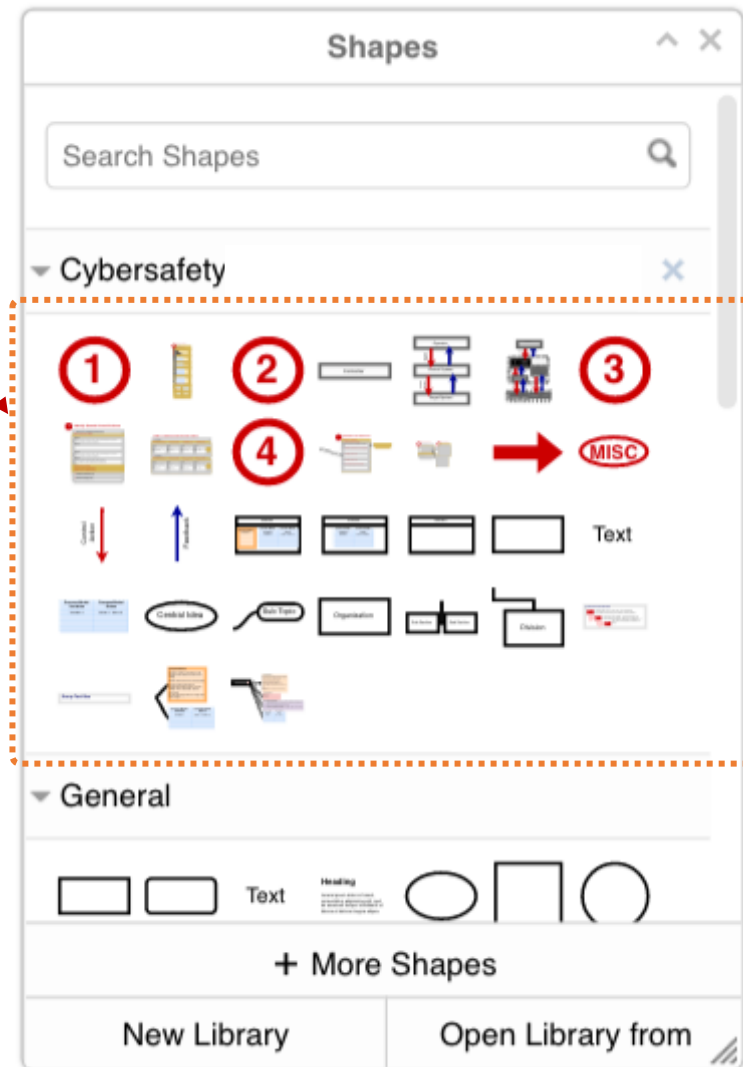
*Diagrams  
Icon*



10. The **custom** Cybersafety library has a number of shapes that are pre-formatted for modelling the function control structure.

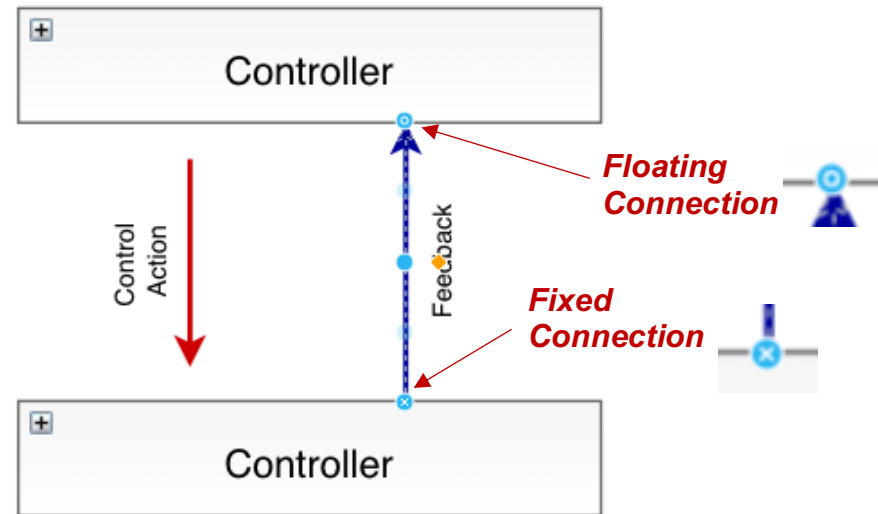
11. Simply Drag & Drop a shape onto the project page to get started

*Drag & Drop  
Shapes from  
the library on  
to the page*

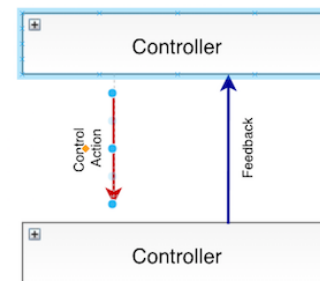




12. NOTE that two types of connections can be made between controllers; the **blue feedback arrow** is fixed in position (rep. by a 'x') with respect to the bottom controller and floating with respect to the top controller (rep. by a 'o'); using the 'floating connection' feature one can easily change the position of the various controllers

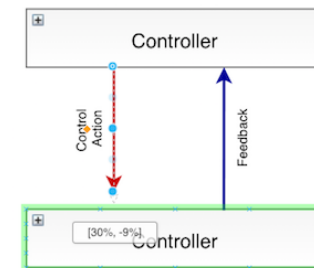


13. To make a floating connection, Drop the arrow point in the middle of the controller box when it is highlighted blue



**For floating point connection**

14. To make a fixed connection, Drop the arrow point at the boundary of the controller box when it is highlighted green



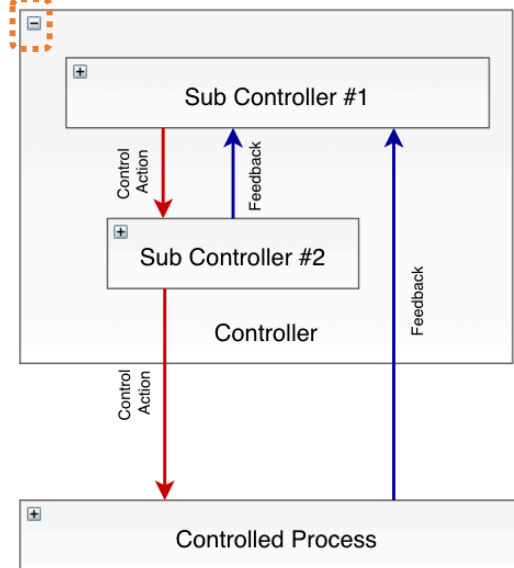
**For fixed point connection**

15. The Cybersafety app allows creating complex functional control diagrams at **different levels of abstraction**

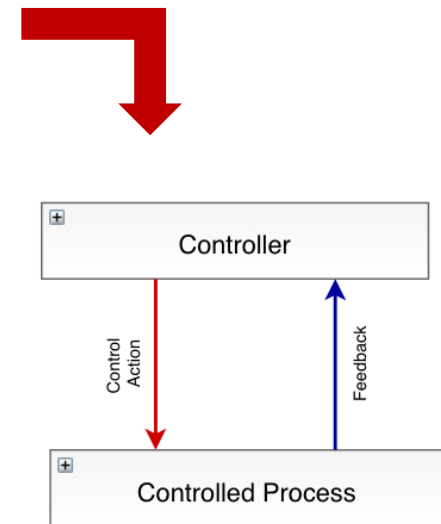
16. Simply click the **expand button '+'** in the top left corner of the controller box and **Drag and Drop** additional controllers/arrows inside the expanded box

17. When the box is **minimized**, all the detail inside the box is **automatically hidden** and the arrows become connected to the controller at the **higher-level of abstraction**

**Expand  
button**



**When the controller  
is minimized, the  
internal controllers  
are hidden**

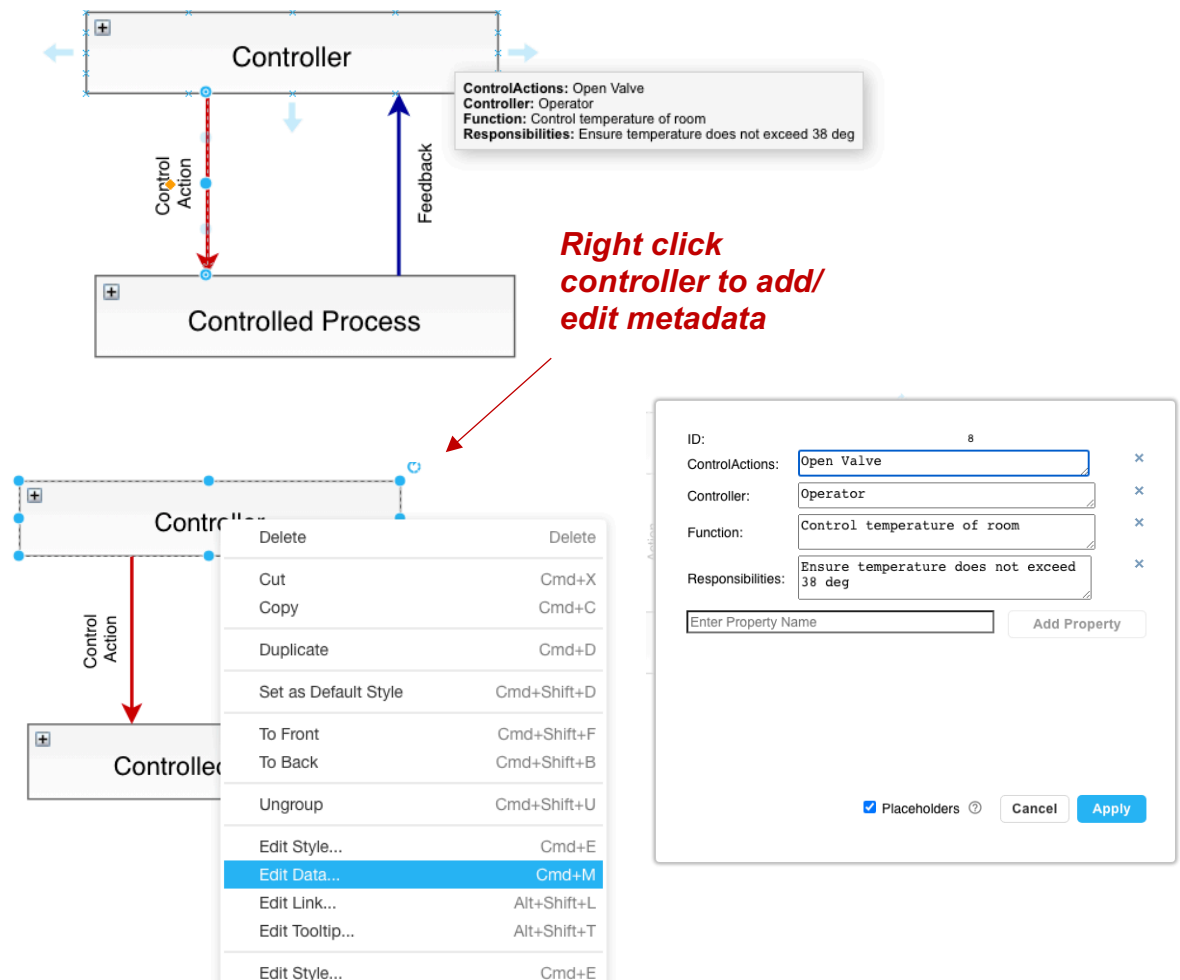


18. **Hovering** over any controller, displays important information about the controller, including:

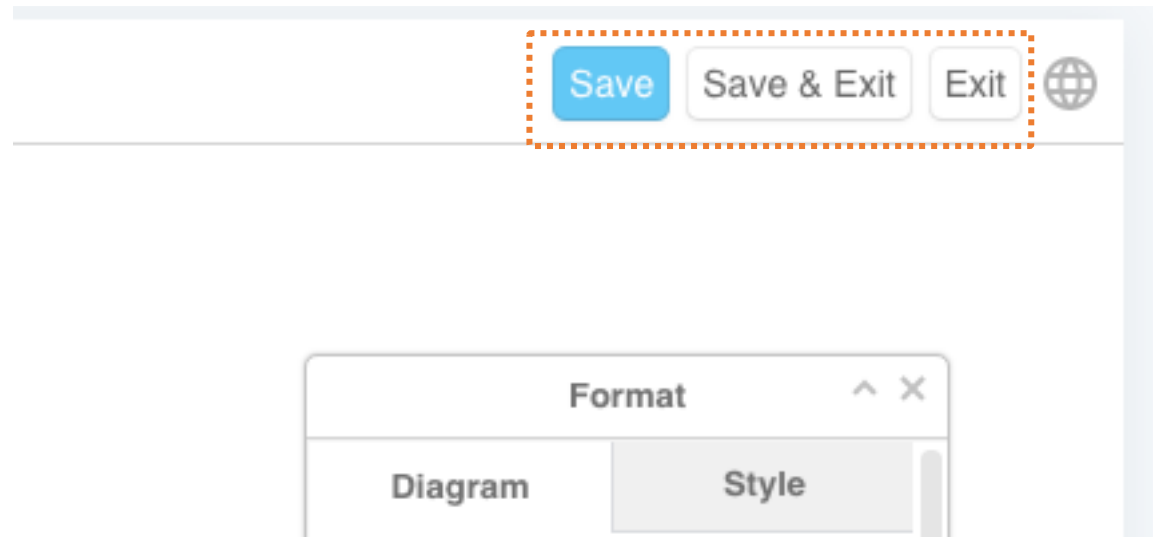
- Function/Goal of the Controller
- Safety & Security Responsibilities
- Control Actions

19. In order to enter this information, Select a Controller and Press **CTRL+M** or Right Click the controller and select **Edit Data**


20. Enter necessary information in the form and click Apply to save.

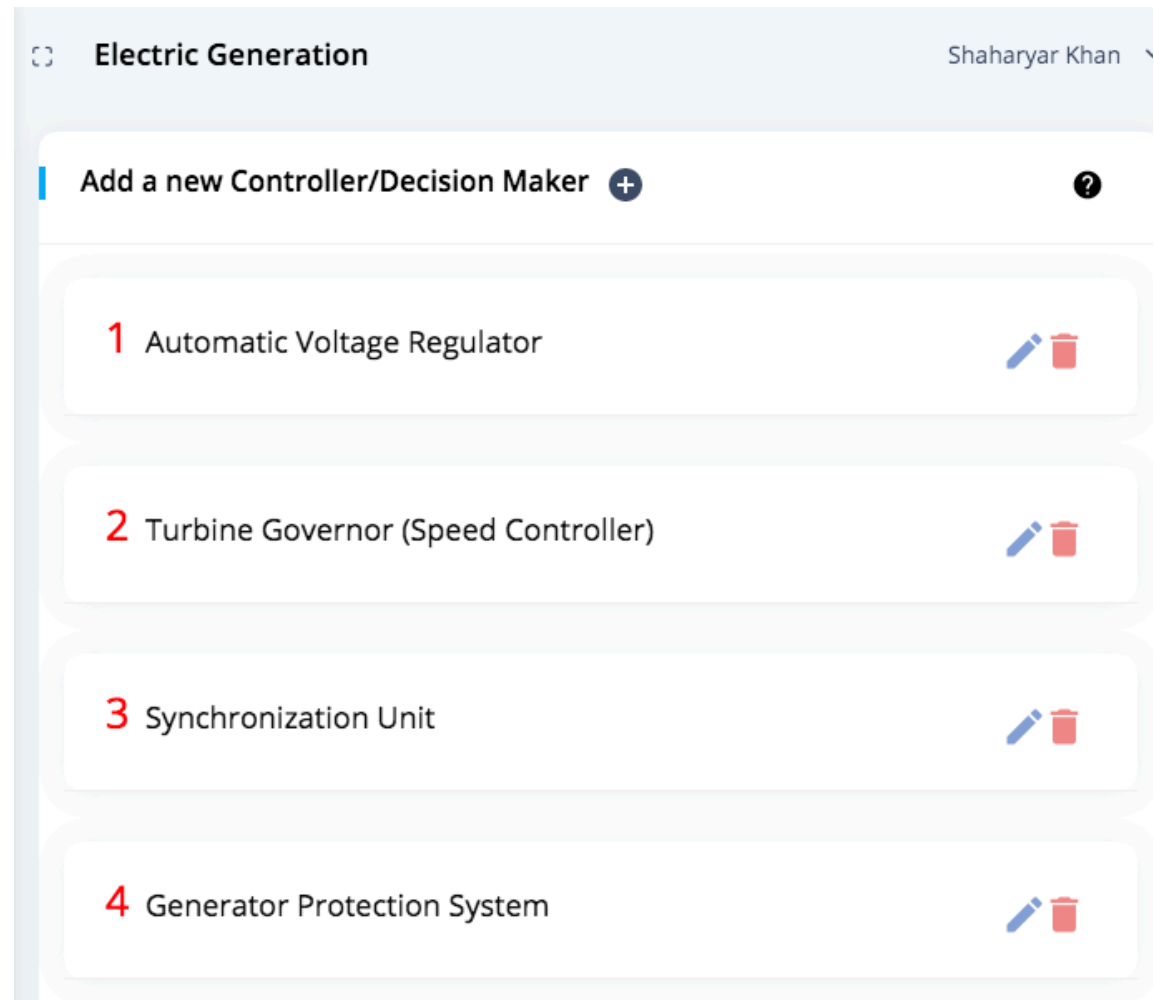


21. Once the modelling of the functional control diagram is complete, Click **Save and Exit** in the top right corner
22. NOTE that **inadvertently closing the webpage** or **clicking a menu bar** item would prompt the user to properly exit the application. Properly exiting the application requires the user to click on Exit (without saving) or Save and Exit; this feature prevents against loss of work due to inadvertently exiting the diagrams.net application




## Step Three – Identify Unsafe Control Actions (UCA)


1. **STEP-3** enables the user to identify hazardous control actions for each of the controllers
2. The layout for Step 3 presents each of the controllers as a 'collapsed card'
3. To define a new controller, simply click the plus icon  at the top of the page and enter the name of the controller

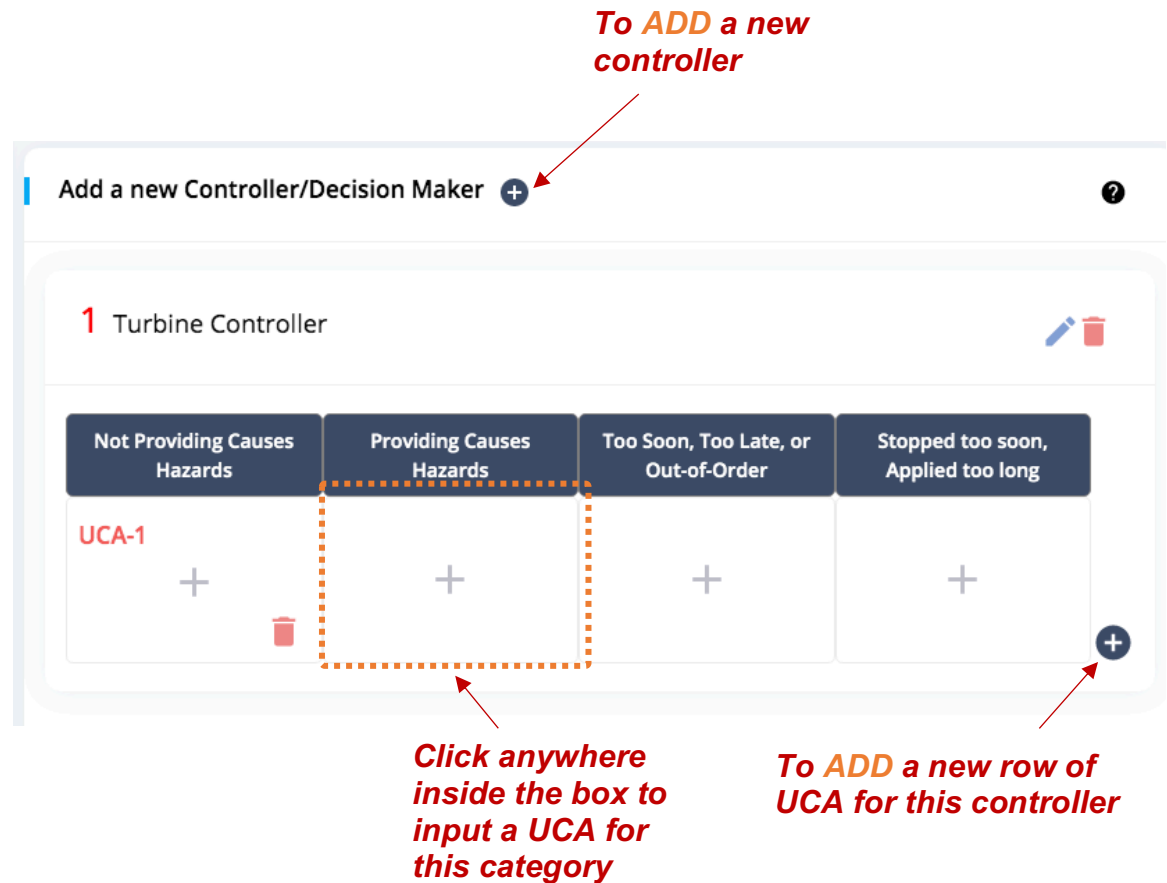


4. Clicking on the controller card expands its contents which shows a table with four types of UCAs:

- Not Providing (a control action) causes a hazard
- Providing (an incorrect) control action causes a hazard
- Providing a control action too soon, too late or out-of-order causes a hazard
- Stopping the control action too soon or applying it for too long causes a hazard





5. To **add a UCA** for this controller, simply click anywhere inside the box with the plus symbol  and enter the UCA

6. To **define a new row** of UCAs, simply click the plus icon  on the right of the table






**To ADD a new controller**

1 Turbine Controller

Not Providing Causes Hazards	Providing Causes Hazards	Too Soon, Too Late, or Out-of-Order	Stopped too soon, Applied too long
UCA-1 			

**Click anywhere inside the box to input a UCA for this category**

**To ADD a new row of UCA for this controller**

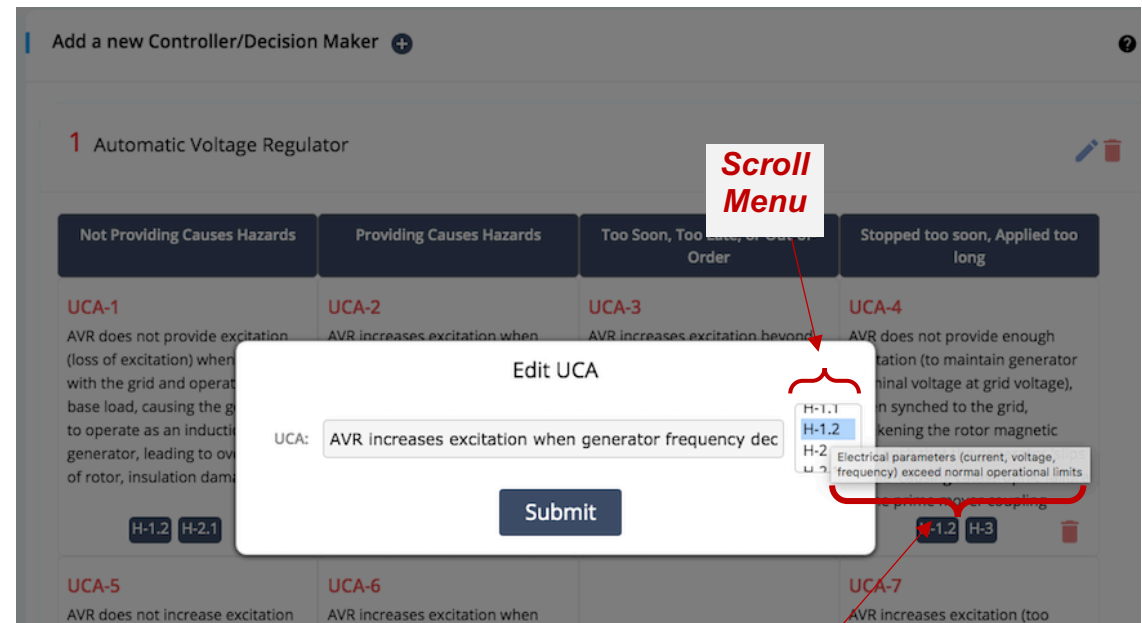
7. Clicking the delete button  inside the **UCA box**, deletes the individual UCA
8. Clicking the delete button  for the **controller card** deletes the controller along with ALL the UCAs contained within; the user is prompted for a confirmation when attempting this
9. The name of the controller can be edited anytime by clicking the **Edit Icon** 

**To DELETE the entire controller along with all the UCAs contained inside**

**To EDIT the name of the controller**

**To DELETE an individual UCA**

10. When identifying UCAs, the **Hazards associated with the UCA** can also be defined; similar to Step 1, the user has the option to select multiple associated hazards from the **Scroll Menu**
11. Multiple hazards can be selected by pressing the **CTRL** key
12. **Hovering** over the hazard reveals the **description** of the hazard
13. The associated hazards can be **updated** anytime by clicking anywhere **inside the UCA box** and selecting the correct associated hazards



**Hovering over the 'loss numbers (L-1, L-2 etc.)' displays the description of the loss**



14. After hazards are associated with UCA's, they appear as **tags** in the UCA table – hovering over the tags reveals the **description of the hazard**

15. Note that the UCA's are **automatically numbered**; If any UCA is **deleted**, the remaining UCA numbers are **automatically updated** – the location of the UCA in the table does not matter

Add a new Controller/Decision Maker + ?

1 Automatic Voltage Regulator

Not Providing Causes Hazards	Providing Causes Hazards	Too Soon, Too Late, or Out-of-Order	Stopped too soon, Applied too long
<p><b>UCA-1</b></p> <p>AVR does not provide excitation (loss of excitation) when coupled with the grid and operating at base load, causing the generator to operate as an induction generator, leading to overheating of rotor, insulation damage etc</p> <p>H-1.2 H-2.1</p>	<p><b>UCA-2</b></p> <p>AVR increases excitation when generator frequency decreases below synchronous speed leading to high V/Hz (overfluxing) during islanded or grid operation</p> <p>H-1.2</p>	<p><b>UCA-3</b></p> <p>AVR increases excitation beyond ampere field no-load (AFNL) condition before generator is synchronized to the grid leading to high V/Hz (overfluxing)</p> <p>H-1.2 H-3</p>	<p><b>UCA-4</b></p> <p>AVR does not provide enough excitation (to maintain generator terminal voltage at grid voltage), when synched to the grid, weakening the rotor magnetic field such that the generator 'slips a pole' causing catastrophic failure of the prime mover coupling</p> <p>H-1.2 H-3</p>
<p><b>UCA-5</b></p> <p>AVR does not increase excitation to match tie-line voltage preventing synchronization with the grid</p> <p>H-2.3</p>	<p><b>UCA-6</b></p> <p>AVR increases excitation when generator terminal voltage is above setpoint (overvoltage)</p> <p>H-1.2</p>	+	<p><b>UCA-7</b></p> <p>AVR increases excitation (too much) violating generator capability curve limits after synchronization with the grid, leading to rotor overheating</p> <p>H-1</p>

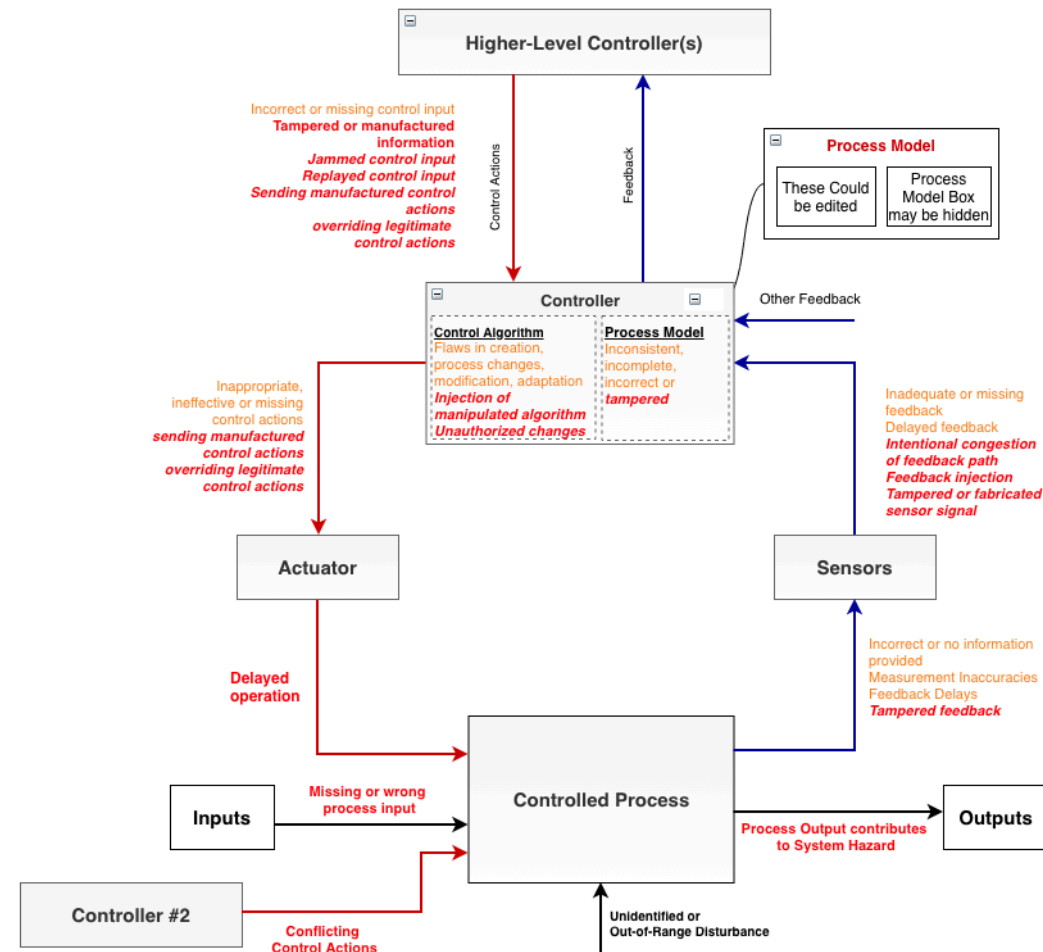
**Violation of power quality metrics**

**Hazard 'Tag'**

**Hazard Description**

# Step Four – Generate Loss Scenarios

1. **STEP-4** enables the user to generate loss scenarios. The basic idea is to go around each control loop and identify causal factors that would:
  - a. **Cause** the controller to issue unsafe commands or,
  - b. **Prevent** the execution of safe commands by the controller
2. The figure shows a generic control loop with sample attack scenarios superimposed around the control Structure



3. The layout for Step 4 is similar to Step 3 in that each of the controllers identified in Step 3 are listed
4. Clicking on any Controller card lists the UCAs as a 'sub-card' shown in the Figure (as opposed to a UCA Table shown in Step 3)
5. Clicking on UCA sub-card allows the user to input **Scenarios**, **Causal Factors** and **Mitigation requirements** in the form of Safety/Security Constraints

**Click on the Controller Card to list UCAs**

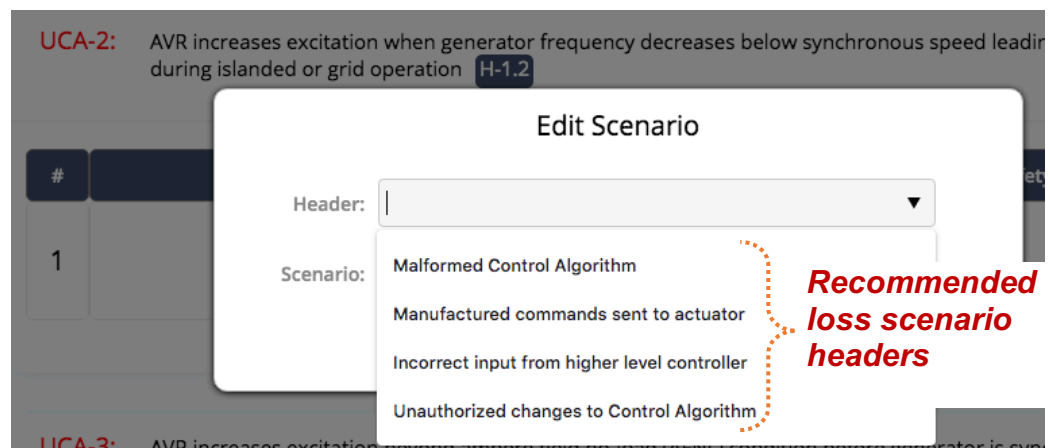
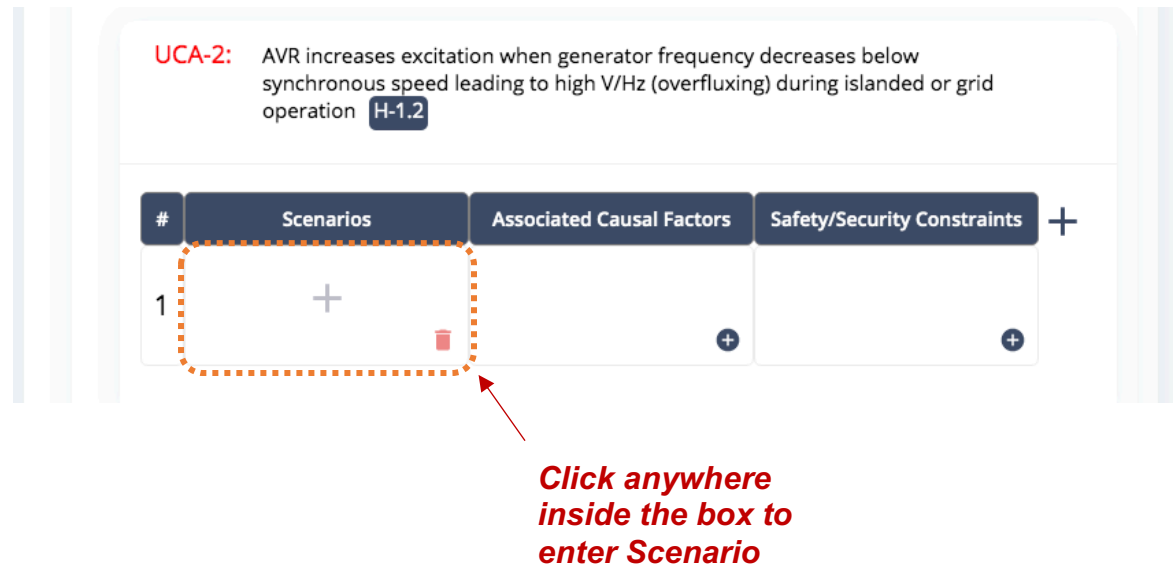
The screenshot shows a web interface titled 'List of Loss Scenarios'. A red arrow points to a dashed orange box containing the title '1 Automatic Voltage Regulator'. Below this, two UCA entries are listed: 'UCA-1: AVR does not provide excitation (loss of excitation) when coupled with the grid and operating at base load, causing the generator to operate as an induction generator, leading to overheating of rotor, insulation damage etc' with tags 'H-1.2' and 'H-2.1'; and 'UCA-2: AVR increases excitation when generator frequency decreases below synchronous speed leading to high V/Hz (overfluxing) during islanded or grid operation' with tag 'H-1.2'. A red arrow points to a dashed orange box around the UCA-2 entry. Below the UCA entries is a table with columns: '#', 'Scenarios', 'Associated Causal Factors', and 'Safety/Security Constraints'. The table has one row with the number '1' in the first column, a plus sign in the second, a trash icon in the third, and a plus sign in the fourth. A red arrow points to the table area.

**Click on the UCA Sub-card to ADD/EDIT Scenarios**

6. The Scenarios have a **1-to-many** relationship with Causal Factors

7. To **add** a scenario, click anywhere inside the scenario box with the plus symbol **+**; a popup would show up which enables the user to define a Scenario header/category along with the Scenario;

8. NOTE that the header comes **pre-filled** with **recommended** loss scenario headers; the user also has the option to define their own scenario header



9. To **delete** a scenario, click the delete icon; NOTE that **deleting** a scenario, deletes ALL associated causal factors and constraints


10. **Multiple Scenarios** can be defined for each UCA; click the plus icon + on the right of the table to add another row of scenarios

UCA-2: AVR increases excitation when generator frequency decreases below synchronous speed leading to high V/Hz (overfluxing) during islanded or grid operation **H-1.2**

#	Scenarios	Associated Causal Factors	Safety/Security Constraints
1	<div><div>+</div><div>🗑️</div></div>	<div>+</div>	<div>+</div>

**Deleting a Scenario would delete all Causal Factors and Mitigation constraints**

**Additional scenarios can be defined by clicking here**

11. Causal factors and mitigation constraints can be added by clicking the plus icon  inside the respective boxes; NOTE that pressing the **TAB** key allows addition of **multiple entries** in one go

12. NOTE that the scenarios, causal factors and constraints are **automatically numbered** by the tool

UCA-3: AVR increases excitation beyond ampere field no-load (AFNL) condition before generator is synchronized to the grid leading to high V/Hz (overfluxing) H-1.2 H-3

#	Scenarios	Associated Causal Factors	Safety/Security Constraints
1	<b>No feedback or incorrect feedback</b> AVR does not know the actual state of the generator's terminal voltage; it continues to increase field excitation to achieve AFNL condition	1. Feedback path from the sensors (PT) is maliciously congested; AVR assumes previous state: a) delayed feedback b) no feedback received 2. Fabricated feedback signal is injected from the sensors (PT) to the	1. AVR excitation signal must be interlocked with out-of-band feedback signal, such as turbine speed to prevent excitation beyond AFNL condition 2. AVR must alarm the operator, if at any time feedback is not received 3. Overflux Relay ANSI 24 must be installed with separate PT 1. AVR must have physical interlock with generator breaker 2. Overflux Relay ANSI 24 must be installed - Same as SC-AVR-03-01-03 3. Overvoltage relay ANSI 59 must be installed (Already installed)

Add a new Causal Factor ?

Feedback path from the sensors (PT) is maliciously congest

Fabricated feedback signal is injected from the sensors to t


Factor:

Factor:

Submit

**Pressing TAB allows multiple entries**

**Add Causal Factors & Constraints**

13. To make any edits to any scenario, causal factor or constraint, simply click on the item that requires changes or click the Edit Icon 

14. This concludes the step-by-step guide for using the **Cybersafety Web Application Tool**

**UCA-3:** AVR increases excitation beyond ampere field no-load (AFNL) condition before generator is synchronized to the grid leading to high V/Hz (overfluxing) **H-1.2** **H-3**

#	Scenarios	Associated Causal Factors	Safety/Security Constraints
1	<b>No feedback or incorrect feedback</b> AVR does not know the actual state of the generator's terminal voltage; it continues to increase field excitation to achieve AFNL condition	1. Feedback path from the sensors (PT) is maliciously congested; AVR assumes previous state: a) delayed feedback b) no feedback received 2. Fabricated feedback signal is injected from the sensors (PT) to the AVR	1. AVR excitation signal must be interlocked with out-of-band feedback signal, such as turbine speed to prevent excitation beyond AFNL condition 2. AVR must alarm the operator, if at any time feedback is not received 3. Overflux Relay ANSI 24 must be installed with separate PT
2	<b>Malformed process model as a result of wrong info</b> AVR believes synchronization has already occurred and increases reference excitation signal to attain VAR/PF setpoint	1. Malicious feedback injection about status of generator breaker - AVR believes it to be closed when it is not	1. AVR must have physical interlock with generator breaker 2. Overflux Relay ANSI 24 must be installed - Same as SC-AVR-03-01-03 3. Overvoltage relay ANSI 59 must be installed (Already installed)

\*Please email Shaharyar Khan ([shkhan@mit.edu](mailto:shkhan@mit.edu)) or Dr. Stuart Madnick ([smadnick@mit.edu](mailto:smadnick@mit.edu)) for more information

# References

1. S. Khan and S. Madnick, Working Paper, Cybersafety: A System-theoretic Approach to Identify Cyber-vulnerabilities & Mitigations in Industrial Control Systems, <http://web.mit.edu/smadnick/www/wp/2019-22.pdf>, 2019
2. N. Stauffer, Energy Futures, Spring 2019 Issue, Protecting our Energy Infrastructure, <http://energy.mit.edu/news/protecting-our-energy-infrastructure/> (accessed Oct 5, 2020)
3. N.G. Leveson, J.P. Thomas, STPA Handbook, 2018. <http://psas.scripts.mit.edu/home/> (accessed Oct 5, 2020).
4. N. Leveson, Engineering a Safer World: Systems Thinking Applied to Safety, The MIT Press, 2012