Pacific Northwest
NATIONAL LABORATORY

PNNL-33292

User Guide to the Facility Cybersecurity Architecture Generation (ArcGen) Tool

August 2022

Arcadio Vielma
Lisa Campbell
Amruth Gorantla
Chris Bonebrake

U.S. DEPARTMENT OF ENERGY

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

DISCLAIMER

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
email: orders@ntis.gov <https://www.ntis.gov/about>
Online ordering: http://www.ntis.gov

PNNL-33292

User Guide to the Facility Cybersecurity Architecture Generation (ArcGen) Tool

August 2022

Arcadio Vielma
Lisa Campbell
Amruth Gorantla
Chris Bonebrake

Prepared for
the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Version 2.0

Pacific Northwest National Laboratory
Richland, Washington 99354

List of Effective Pages

Dates of issue for latest changes are: Total number of pages in this publication is _____ consisting of the following:			
Page Number	**Change Number**	**Page Number**	**Change Number**

Table 1: Latest Changes

Revision History

Name	Date	Reason For Changes	Version
PNNL			

Table 2: Revision History

Acronyms and Abbreviations

ArcGen	Architecture Generation Tool
DMZ	Demilitarized Zone
FCF	Facility Cybersecurity Framework
HMI	Human-Machine Interfaces
IT	Information Technology
OT	Operational Technology
PLC	Programmable Logic Controller
QRA	Qualitative Risk Assessment
SCADA	Supervisory Control and Data Acquisition
XML	Extensible Markup Language

Contents

Figures

Tables

1.0 Introduction

The Architecture Generation (ArcGen) tool[1] is an interactive asset management tool that is based on the Purdue Reference Model to support vulnerability identification. The Purdue Reference Model[2] divides a network into 6 separate levels and stops at the edge of an enterprise's network. ArcGen considers external connections in addition to the different levels within an enterprise.

Levels 0 and 1 are combined in ArcGen and contain devices such as process control and instrumentation, like sensors, actuators, pumps, programmable logic controllers (PLCs), meters, lighting panels, and other devices that use serial networks and protocols. Level 2 is the portion of the facility that uses Internet Protocol (IP) but is not shared with any other system. It contains components that integrate process control networks with the Ethernet and TCP/IP components in the operations zone such as Human-Machine Interfaces (HMI), Supervisory Control and Data Acquisition (SCADA) systems, building level controllers, IP-based controllers, and other workstations and gateways. Level 3 contains components which connect the dedicated Level 2 IP networks with the Level 4 IP network. Level 3 contains operations devices such as production and application servers, database/historian servers, and engineering workstations. Between levels 3 and 4 there is an operations demilitarized zone (DMZ) that is designed to create a barrier between the information technology (IT) and operational technology (OT) networks and is represented as level 3.5 in ArcGen. This includes components that provide IT and security services for the operations zone including patching systems, antivirus and vulnerability scanning, network historians, remote access jump servers, and intrusion detection/prevention systems. Level 4 is for an organization's business systems. This includes desktops, workstations, servers (e.g., domain controllers, exchange/email, file shares, database/historian), corporate firewalls, and other devices that enable corporate network functionality. Level 4.5 is the Enterprise DMZ. Devices in this level are designed to serve as a buffer between external networks and the corporate network, including protection from external threats. Systems in this level include web servers, proxy servers, and internet facing firewalls. Level 5 represents devices and systems that are outside an enterprise's network but still may connect to their network in some way. Some examples include cloud infrastructure, vendor support connections, reporting services, and transaction and data exchange services.

ArcGen is part of the Facility Cybersecurity Framework (FCF) website[3] and is interconnected with the Qualitative Risk Assessment (QRA) tool[4]. Facility operators and owners can use ArcGen to identify and layer their assets, which will autonomously populate the QRA. If assets are defined in the QRA tool first then they will show up when moving over to ArcGen. In addition, facility owners and operators can subjectively define their impact and vulnerability grades to categorize the assets based on the risk level. The grades are reflected in ArcGen for contextual asset monitoring.

[1] https://facilitycyber.labworks.org/tools/arcgen/landing
[2] https://doi.org/10.1016/S1474-6670(17)48532-6
[3] https://facilitycyber.labworks.org/
[4] https://facilitycyber.labworks.org/tools/qra/landing

2.0 Accessing the ArcGen Tool and Landing Page

2.1 Accessing the ArcGen Tool

ArcGen is designed to give stakeholders a visual representation of their network to help them quicky identify gaps in protection and infrastructure, both internally and with external connections. To access the ArcGen tool, visit https://facilitycyber.labworks.org/. Next, navigate to the “Understand & Mitigate Gaps” tab and select “ArcGen” from the dropdown menu (*Figure 1*).

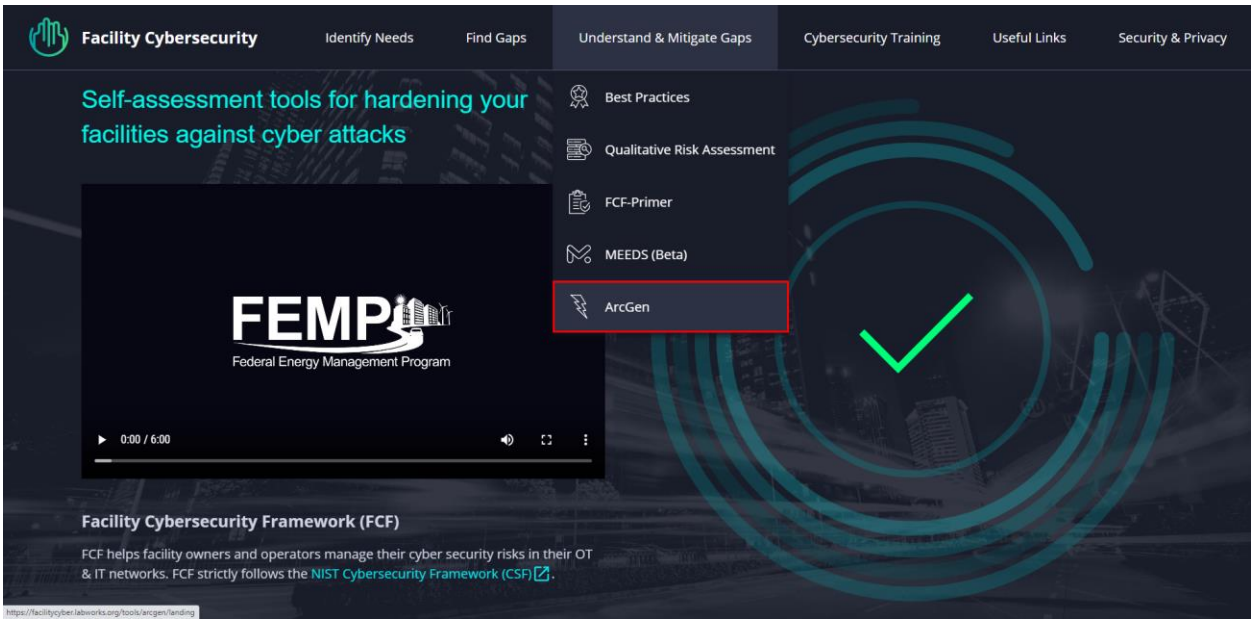

Figure 1: FCF Website – ArcGen

2.2 ArcGen Landing Page

The landing page offers a brief overview of the ArcGen tool and allows the user to (“A”) Get Started with a brand-new architecture or (“B”) Load an existing one (*Figure 2*). To learn how to start a new architecture, continue to the **Starting a New Architecture Diagram** section. To learn how to load a saved architecture, see the **Load** section.

When using the ArcGen tool, all user data entered will remain on the local cache of the workstation that the user is logged into, and no information is transmitted to the server. The information stored in the web browser cache can be used across multiple tools hosted on the FCF website, and the data is not transmitted outside the user’s control. However, clearing the cache will delete work that has been done in the tool.

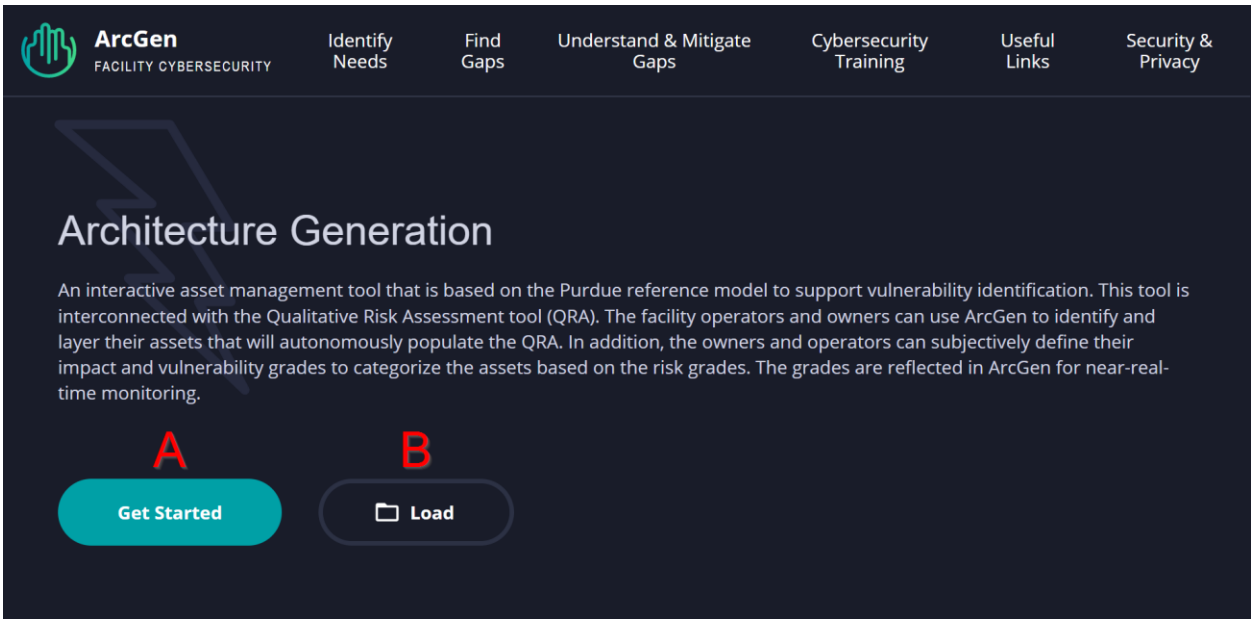

Figure 2: Getting Started – ArcGen Landing Page

2.3 ArcGen Landing Page for Returning User

Alternatively, if returning to the landing page after previously working on an architecture, the Get Started button will be replaced by two other buttons (“A”) Resume and (“B”) Restart (*Figure 3*). Resume will continue where the last cached session left off and Restart will clear the cache and start a new empty architecture and asset list.

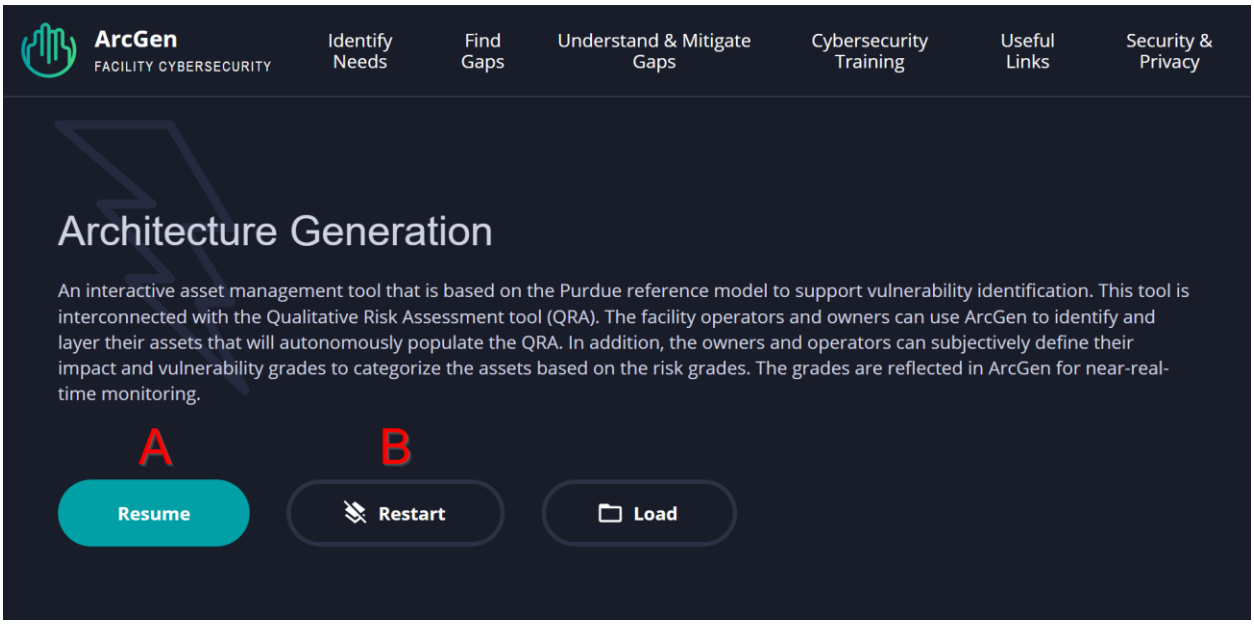

Figure 3: Returning User – ArcGen Landing Page

If the Restart option is selected the user will be prompted to confirm the reset and is notified of the loss of existing data (*Figure 4*). After confirmation, the user will be redirected to the **Getting Started – ArcGen Landing Page**.

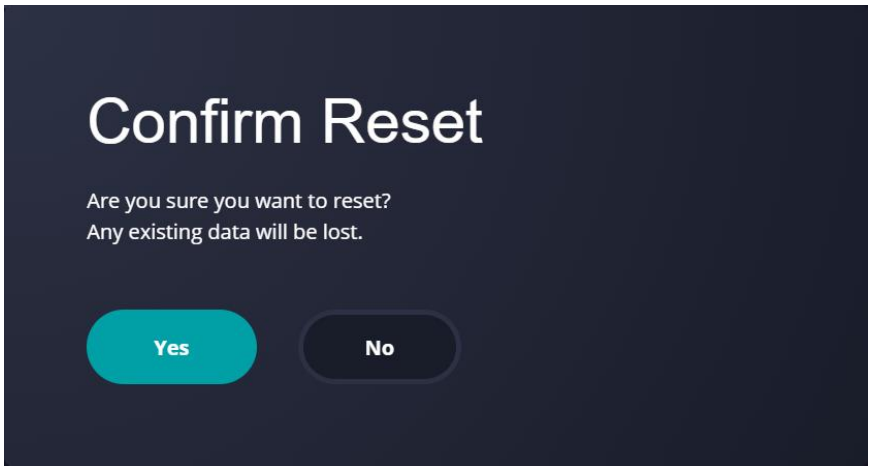

Figure 4: Confirmation Reset Message

3.0 Navigating the ArcGen Interface

The ArcGen interface has two main working areas (*Figure 5*):

(“A”) The ArcGen menu pane contains buttons that perform user functions. For detailed information, please view the **ArcGen Menu Pane** section.

(“B”) The architecture diagram area is aligned to the network layers defined by the Purdue Reference Model[1]. The scroll button just to the right of the architecture section allows a user to scroll up and down to view all the different levels. For more detailed information, please view the **Architecture Diagram** section.

Figure 5: ArcGen Interface

[1] https://doi.org/10.1016/S1474-6670(17)48532-6

4.0 ArcGen Menu Pane

Figure 6 displays the ArcGen menu pane with the top menu Task-Oriented Options labeled “A,” the View section labeled “B,” the Assets section labeled “C,” and the Collapse option labeled “D.”

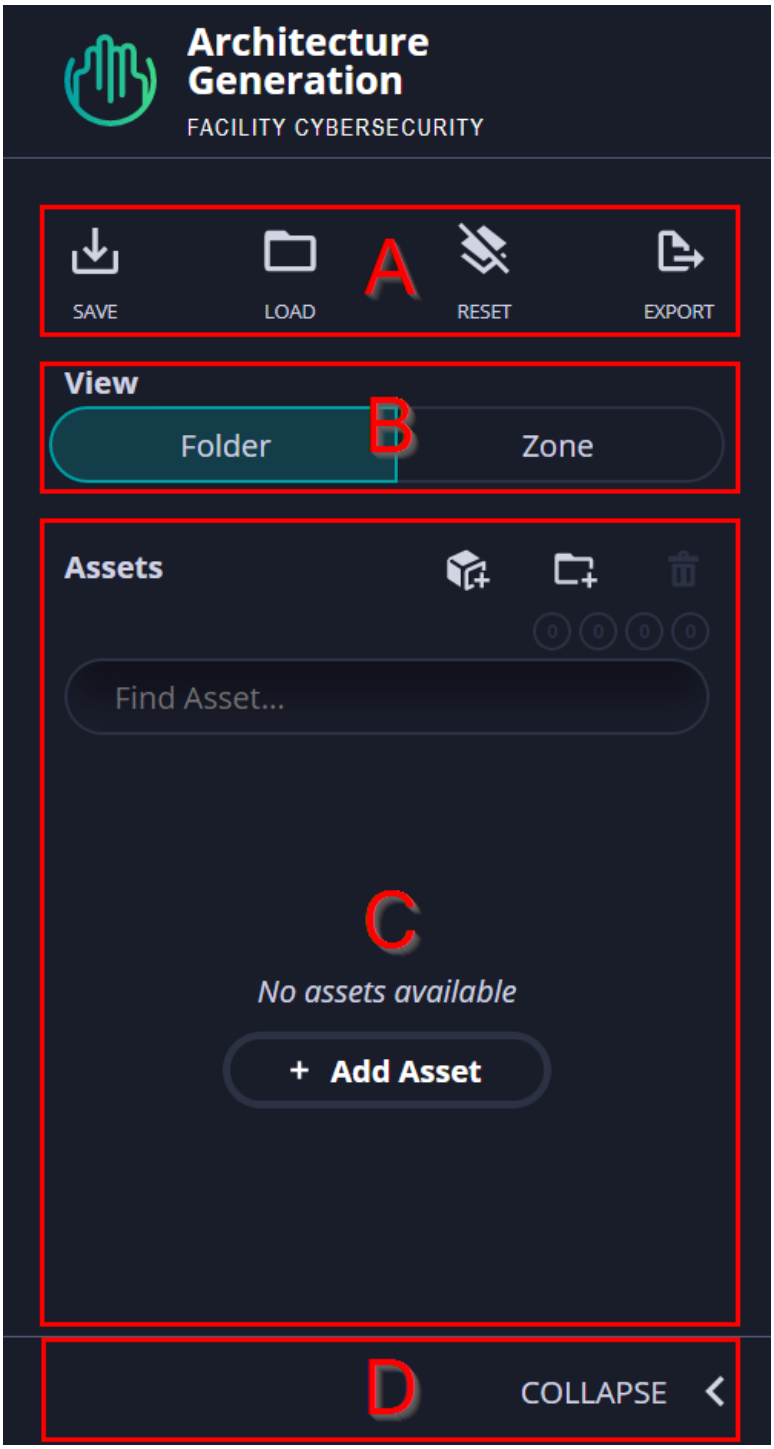

Figure 6: ArcGen Menu Pane

4.1 Task-Oriented Options

Figure 7 displays four top menu options with the Save button labeled “A,” Load button labeled “B,” Reset button labeled “C,” and the Export button labeled “D.”

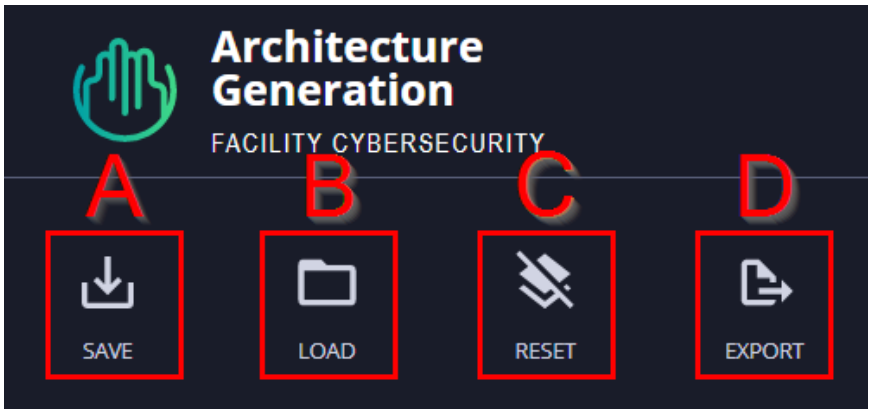

Figure 7: ArcGen Menu Pane – Task-Oriented Options

4.1.1 Save Button

The first button at the top left of the menu is the Save button labeled as “A.” Clicking the Save button opens a save progress dialogue window (*Figure 8*) that gives the user the choice of downloading the current architecture as a JSON file extension or copying the raw JSON formatted text into the clipboard so the user can paste the JSON into their choice of tools to read or save for future use.

Figure 8: Save Progress Dialogue

4.1.2 Load Button

The Load button labeled as “B.” Clicking the Load button will open a load progress dialogue window that gives the user the choice of uploading a JSON file extension or pasting a JSON

formatted text directly into the window to load an architecture (shown in *Figure 9*). This section is also applicable to the Load button on the main **ArcGen Landing Page**.

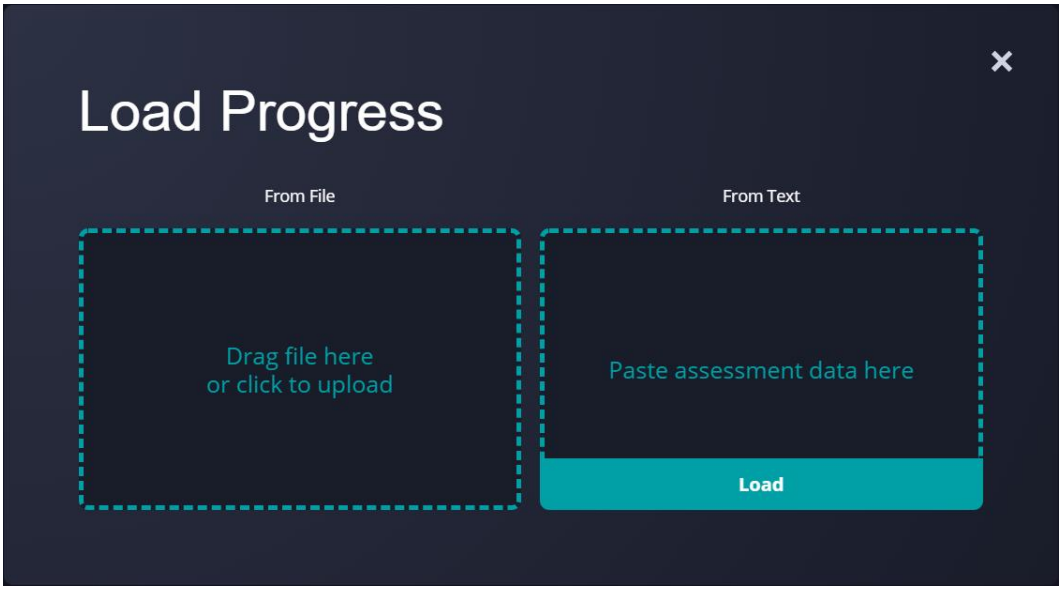

Figure 9: Load Dialogue

Once the preferred load option is selected, a confirmation load dialogue window will display along with a message informing the user that any existing data will be overwritten (*Figure 10*).

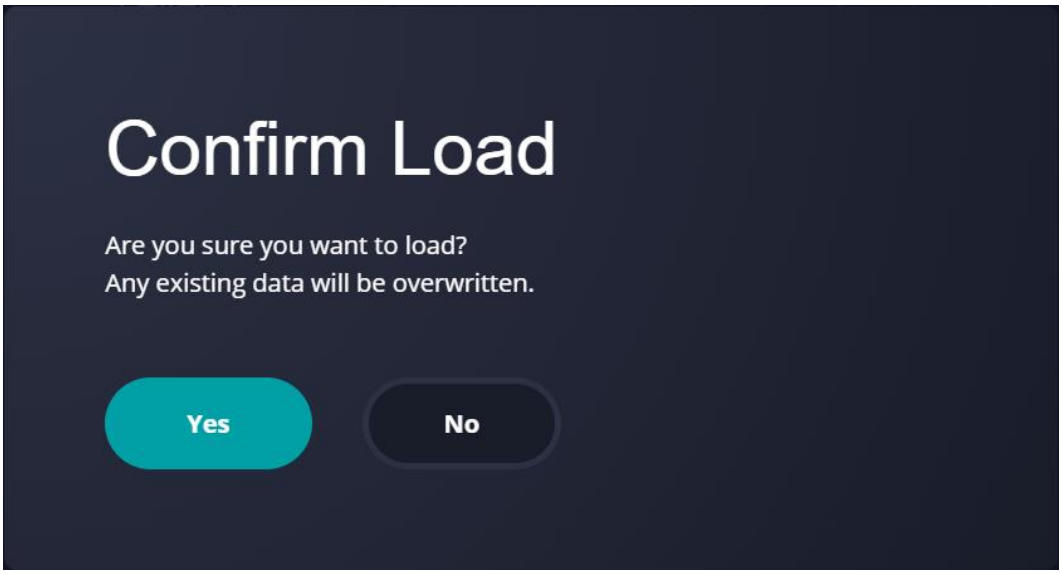

Figure 10: Confirmation Load Dialogue

4.1.3 Reset Button

The Reset button is labeled as “C.” Clicking the Reset button will open a confirmation reset dialogue window (*Figure 11*) to confirm with the user the reset and clearing of all QRA data.

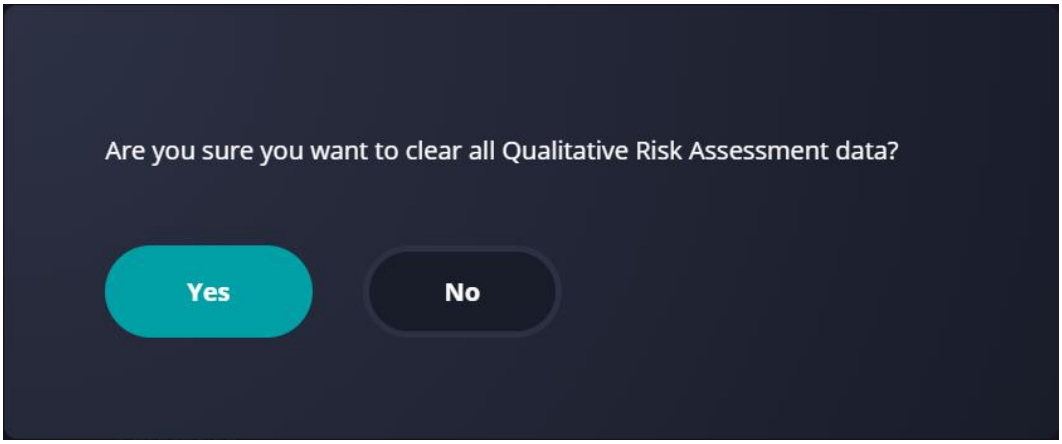

Figure 11: Confirm Reset Dialogue

4.1.4 Export Button

The Export button is labeled as “D.” Clicking the Export button downloads the current architecture to a user’s computer as an Extensible Markup Language (XML) file and an Excel-import instruction dialogue window will display with instructions on how to import the XML file into Microsoft Excel (shown in *Figure 12*).

Figure 12: Excel Import Instructions Dialogue

4.2 View Section

The View section has two options: Folder labeled “A” and Zone labeled “B” (as shown in *Figure 13*). The Folder option is by default selected when beginning a new architecture and allows the user to view created folders under the Assets section. Alternatively, the user can select the Zone option to view created zones under the Assets section.

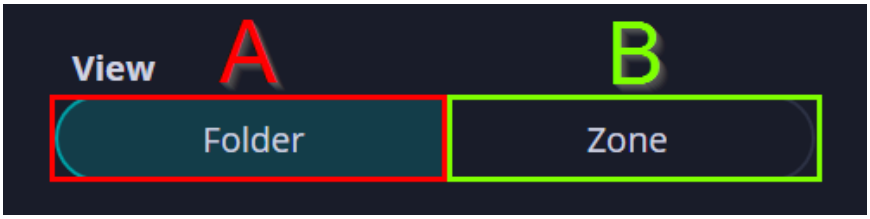

Figure 13: ArcGen Menu Pane – View Section

4.3 Assets Section

The Assets section will cover the user's options regarding creating, modifying, and deleting an asset, folder, and zone. Please note to view the zones, the user must select the Zone option in the **View Section**.

4.3.1 Asset

4.3.1.1 Create an Asset

The user can create an asset by clicking on the “Add an Asset” icon or “Add Asset” button highlighted in *Figure 14*.

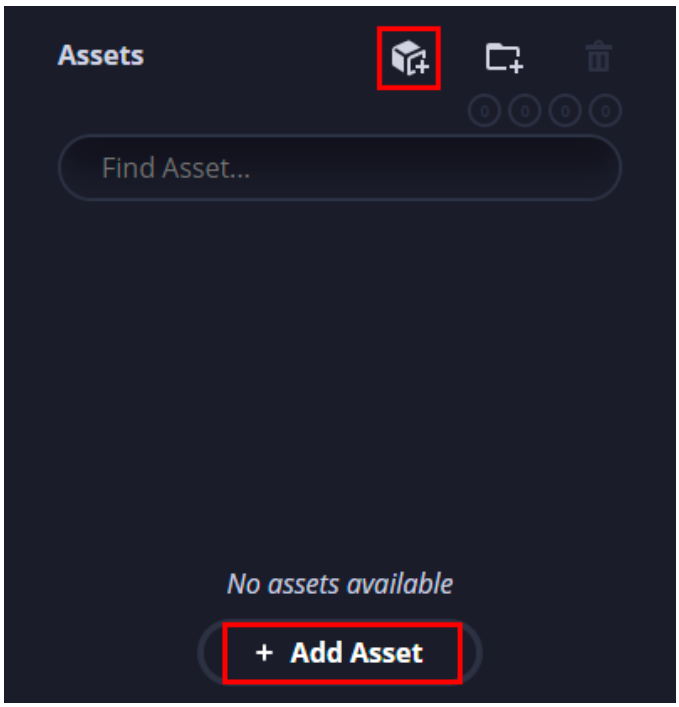

Figure 14: Add Asset Button

Alternatively, an asset can be created in the architecture diagram by right clicking on any level and selecting the “Add New Asset” option (*Figure 15*). This will populate the asset in the ArcGen menu pane under the Assets section and in the architecture diagram where right clicked.

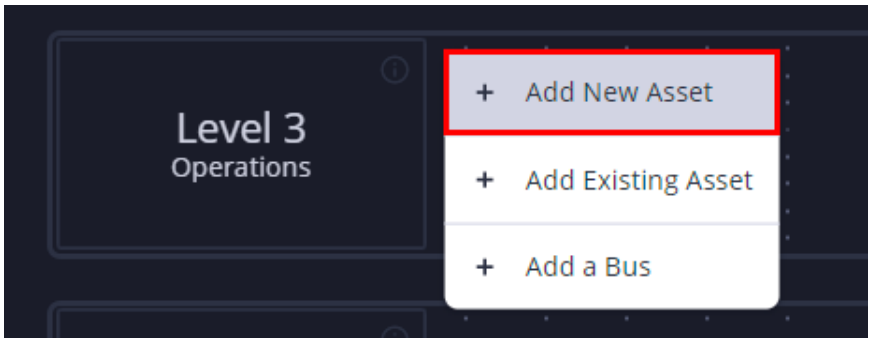

Figure 15: Alternative Method – Add New Asset

4.3.1.2 Entering Data for an Asset

Figure 16 presents an “Add Asset” dialogue window. The user should use this screen to enter details about the asset.

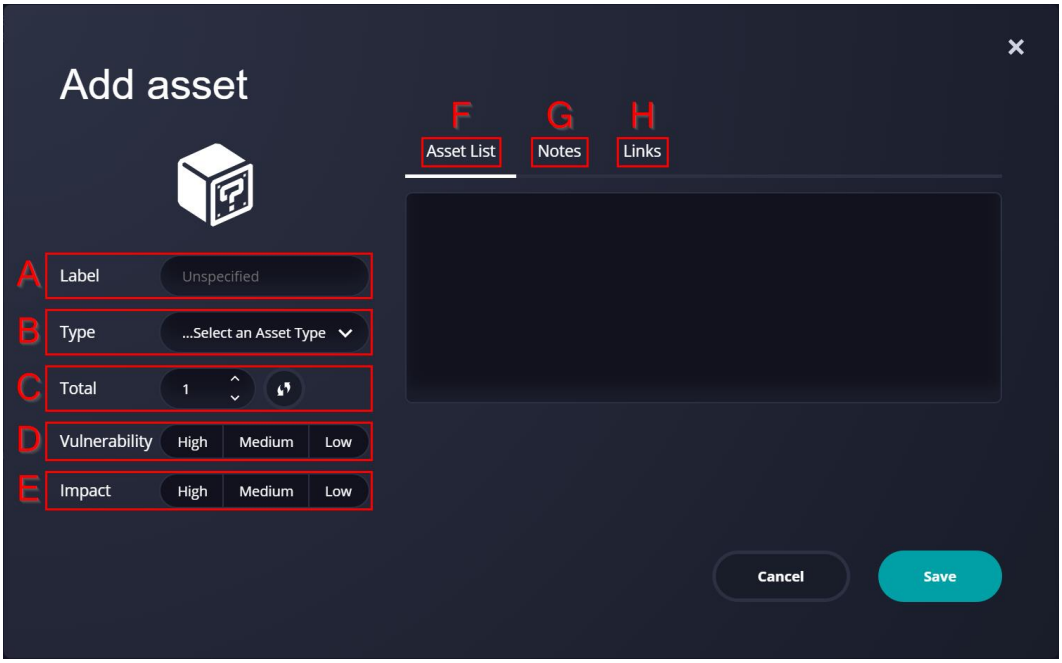

Figure 16: Add Asset Dialogue

Label

The Label option labeled “A” allows the user to name an asset.

Type

The Type option labeled “B” allows the user to select the type of asset from the “Select an Asset Type” drop-down menu. The user will have several types of options to choose from, as shown in *Figure 17*.

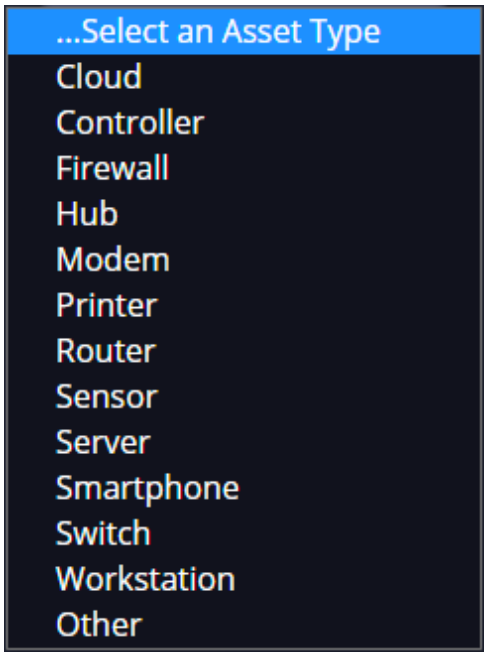

Figure 17: Asset Type Option

Total

The Total option labeled “C” allows the user to have multiple assets represented as a single icon in the architecture diagram.

Vulnerability

The Vulnerability option labeled “D” allows the user the ability to subjectively grade the asset based on high-, medium-, and low-severity. The grade should reflect the severity of the asset’s weakness that could potentially be exploited or triggered. The MITRE Common Vulnerabilities and Exposures framework[1] should be referenced when determining the vulnerability grade.

A Low grade is defined as a limited adverse effect, a Medium grade is defined as a serious adverse effect, and High grade is defined as a severe or catastrophic adverse effect.

The following is an example of a high vulnerability graded asset (*Figure 18*).

[1] https://cve.mitre.org/cve/search_cve_list.html

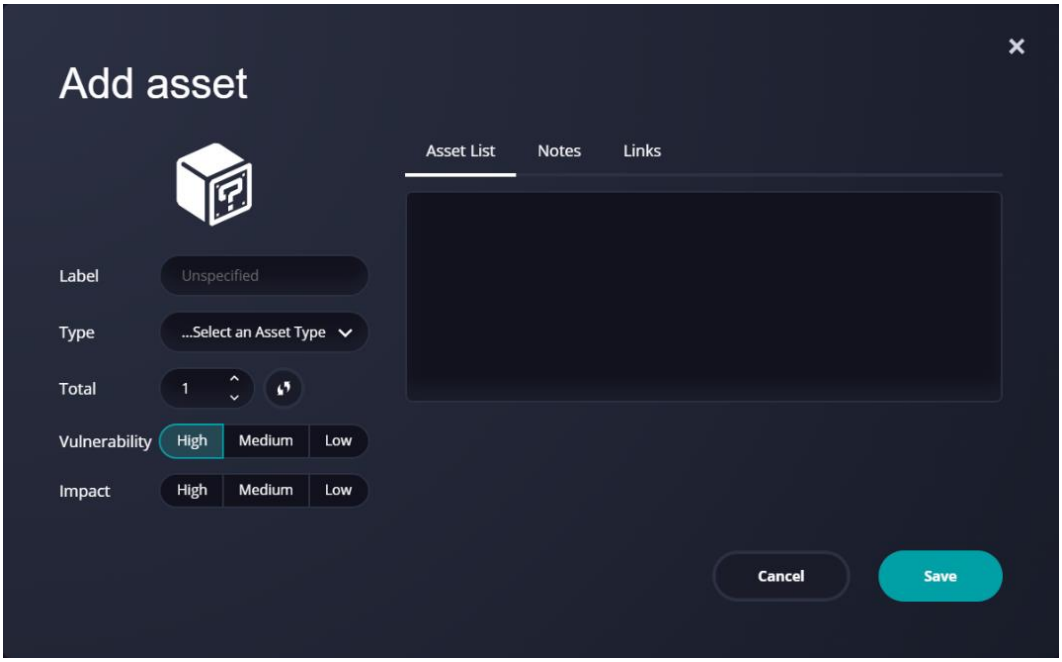

Figure 18: Example – High Vulnerability Selected

Once saved, the high vulnerability asset will be displayed in the ArcGen menu pane under the Assets section, with red representing the High grade (*Figure 19*). Oppositely, a Low grade would display the color green, and a Medium grade would show orange.

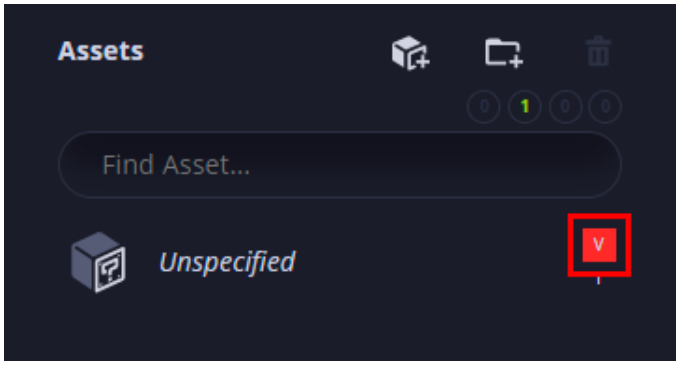

Figure 19: ArcGen Menu – High Vulnerability Display

Impact

The Impact option labeled “E” allows the user to subjectively categorize the asset based on a High, Medium, and Low grade. The grade should reflect the magnitude of an asset's impact due to a loss in confidentiality, integrity, or availability if the asset were exploited.

A Low grade is defined as a limited adverse effect, a Medium grade is defined as a serious adverse effect, and High grade is defined as a severe or catastrophic adverse effect.
The following is an example of a low impact graded asset (*Figure 20*).

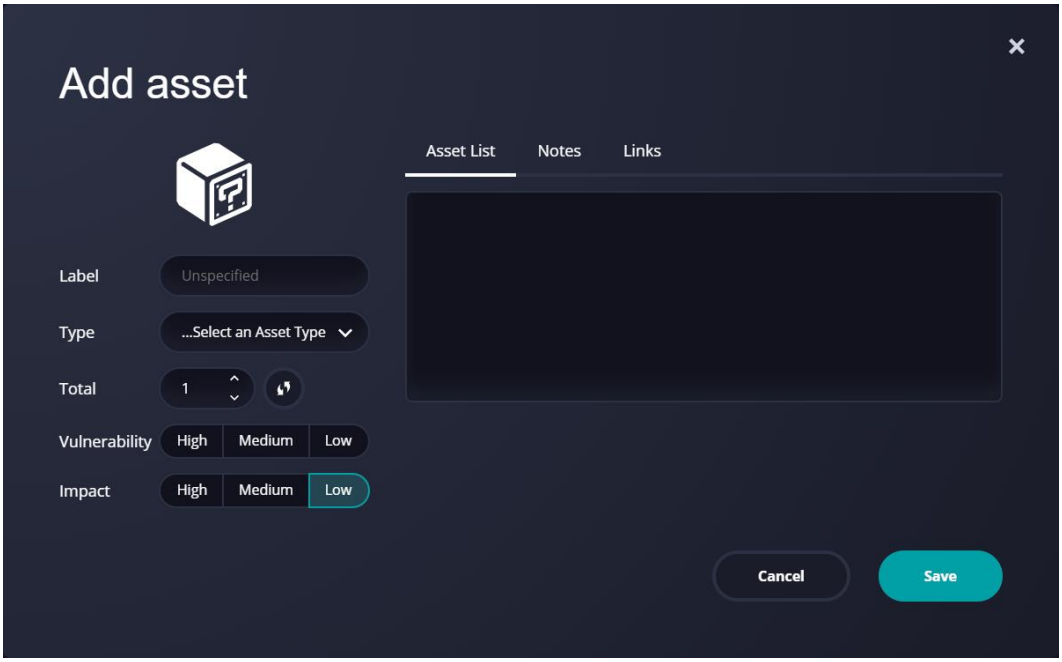

Figure 20: Example – Low Impact Selected

Once saved, the low impact asset will be displayed in the ArcGen menu pane under the Assets section, with green representing the Low grade (*Figure 21*). Oppositely, a High grade would display the color red, and a Medium grade would show orange.

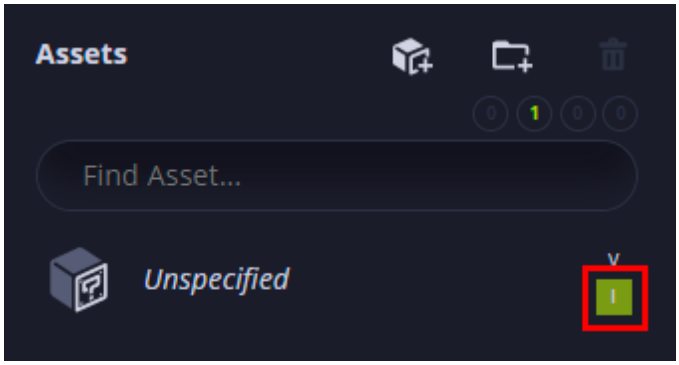

Figure 21: ArcGen Menu - Low Impact Display

Asset List

The Asset List section labeled “F” allows the user to list multiple assets that can be represented as a single asset in the architecture diagram. The user can add the assets, line by line, by clicking on the Asset List and then clicking into the textbox beneath it. After listing the multiple assets, the user can have the Total determined automatically by clicking on the “Auto Asset Calculation” button shown in example below (*Figure 22*).

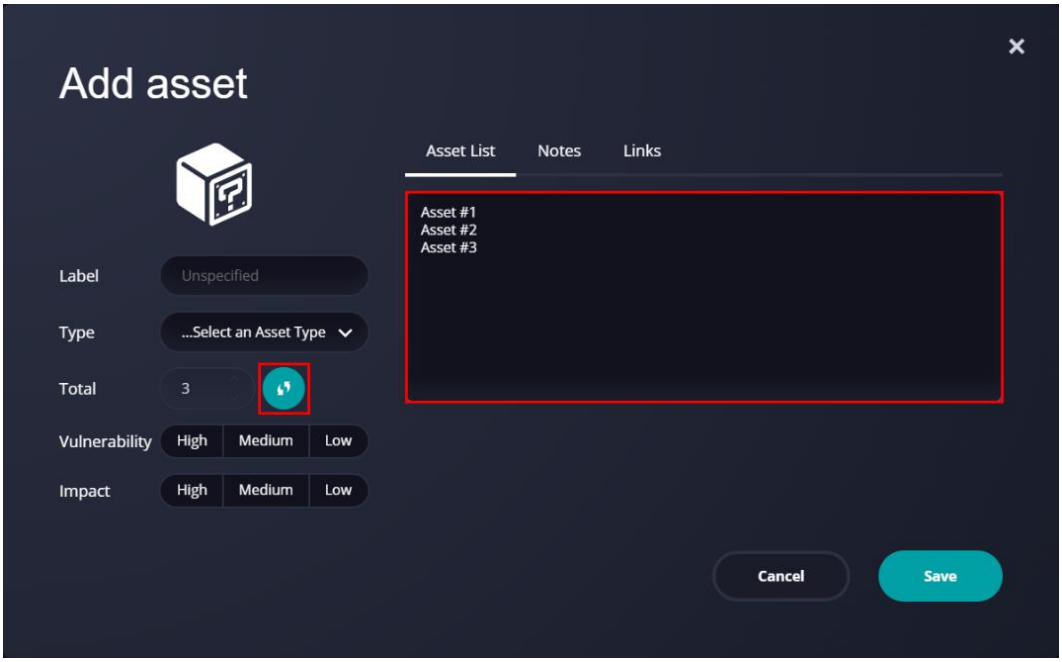

Figure 22: Example – Auto Asset Calculation

Notes

The Notes section labeled "G" allows the user to add details about the asset(s). To add a note the user must click on the “Add Note” button under the Notes section highlighted in *Figure 23*.

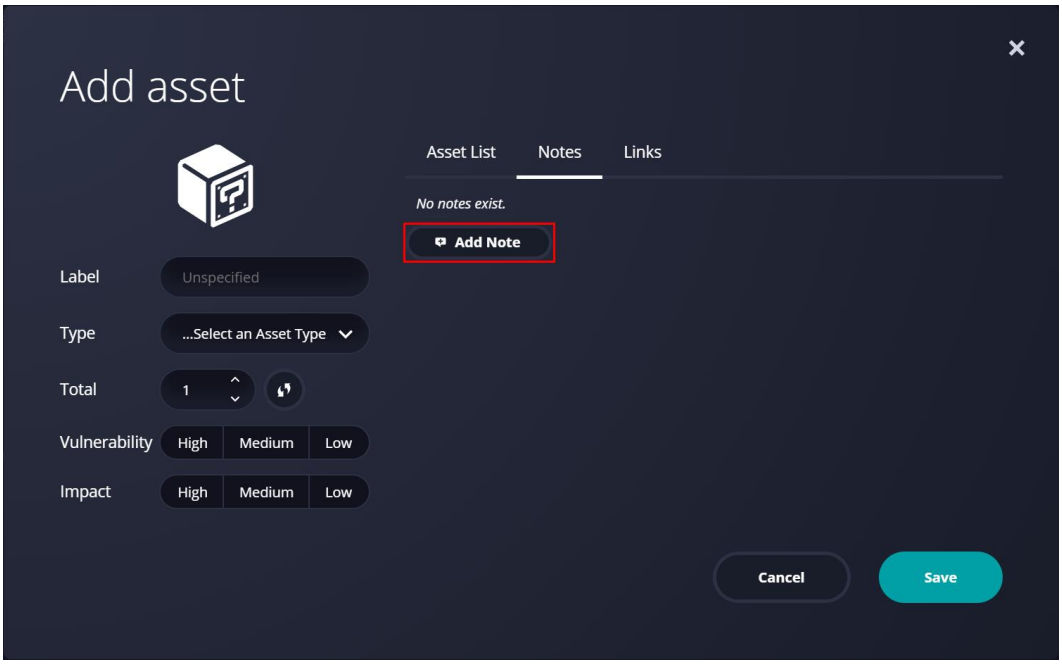

Figure 23: Add Note Button

Oppositely, the user can delete a note by clicking on the “trashcan” icon on the right side of the note under the Notes section, as shown below in *Figure 24*.

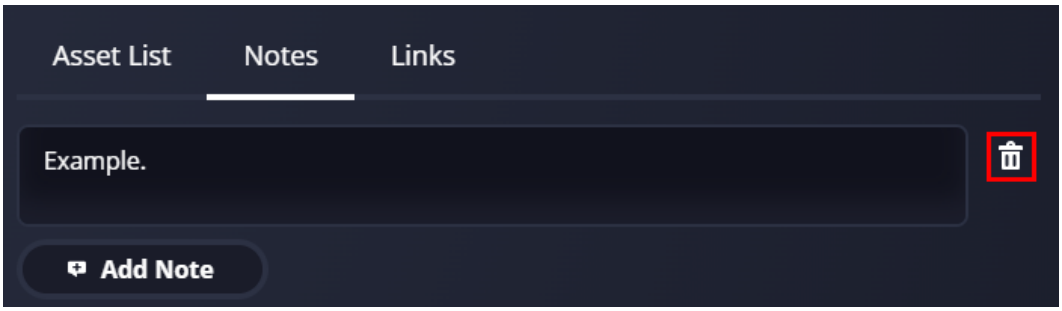

Figure 24: Delete Note Button

Links

The Links section labeled “H” displays any links that have been established between the asset being viewed and any other asset from within the architecture diagram. A link represents a connection between the two assets on a network. Once a link has been established, the user can revisit the Links section to provide details regarding the incoming and outgoing ports/data (*Figure 25*). Ports/data can describe the physical or logical connections and the associated service or process being run. Please see the **Data Link Assets** section for more information regarding linking two devices in the architecture diagram.

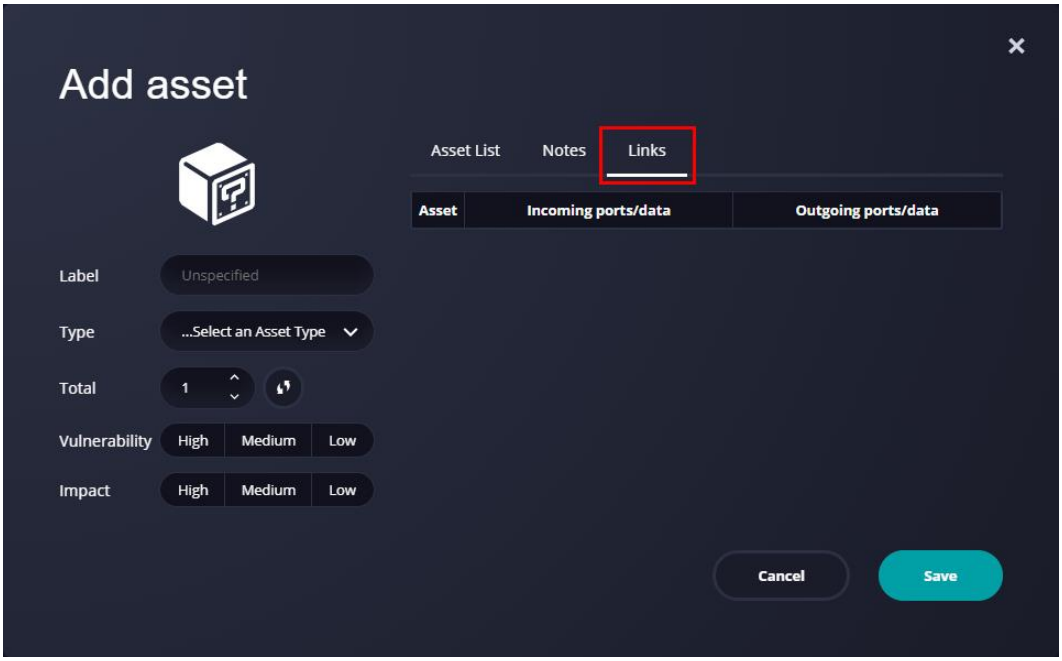

Figure 25: Links Section

The following is an example of how two linked assets would appear under the Links section (*Figure 26*).

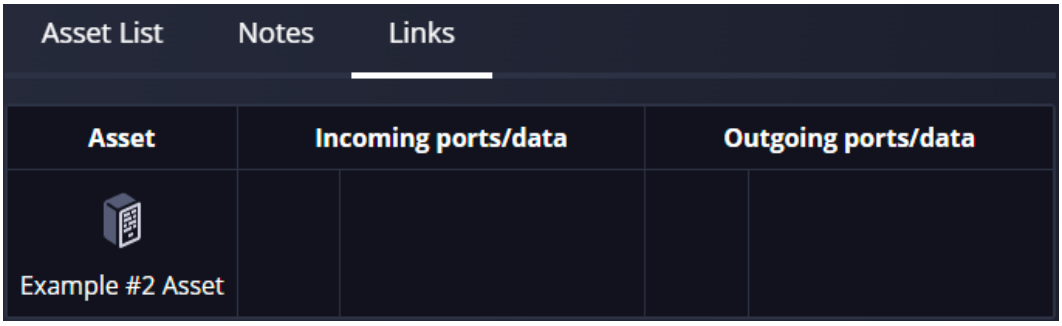

Figure 26: Example – Link Between Two Assets

4.3.1.3 Modify an Asset

Edit Asset

The user can edit an asset by right clicking on the asset listed in the ArcGen menu pane under the Assets section and selecting the “Edit” option (*Figure 27*). Alternatively, the user can edit an asset by right clicking on the asset and selecting the “Edit” option in the architecture diagram.

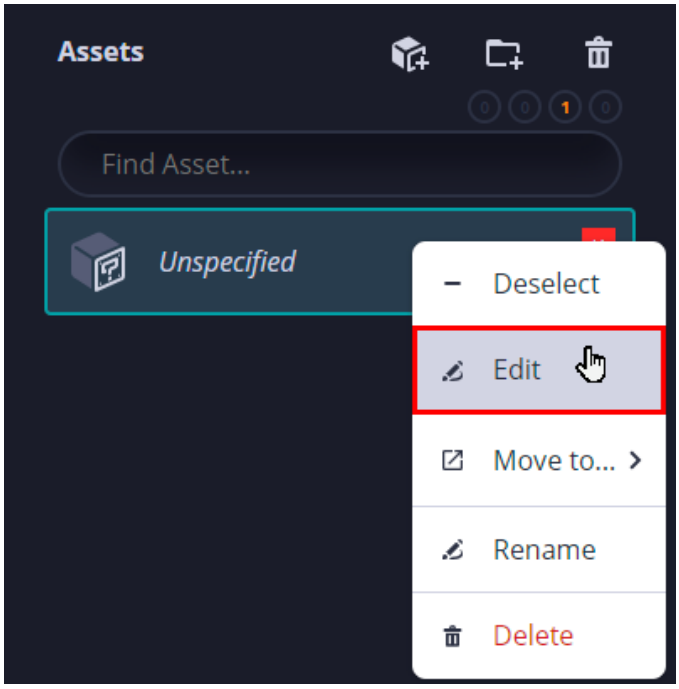

Figure 27: Edit Asset Selection

Rename Asset

The user can rename an asset by right clicking on the asset in the ArcGen menu pane under the Assets section and selecting the “Rename” option (*Figure 28*). Alternatively, the user can rename an asset when editing.

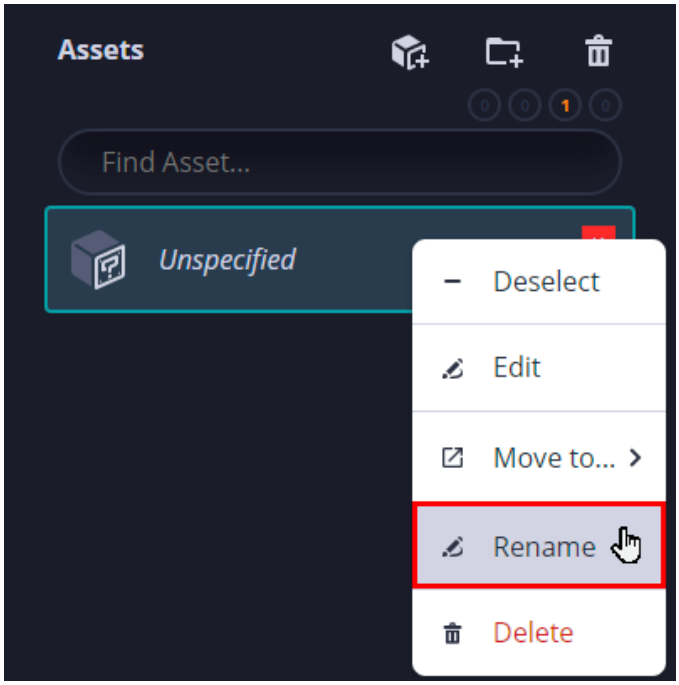

Figure 28: Rename Asset Selection

4.3.1.4 Delete an Asset

The user can delete an asset by right clicking on the asset in either the ArcGen menu pane under the Assets section or from within the architecture diagram and then selecting the “Delete” option (*Figure 29*). Alternatively, the user can click on the asset they wish to delete and then click on the “trashcan” icon located under the Assets section in the ArcGen menu pane.

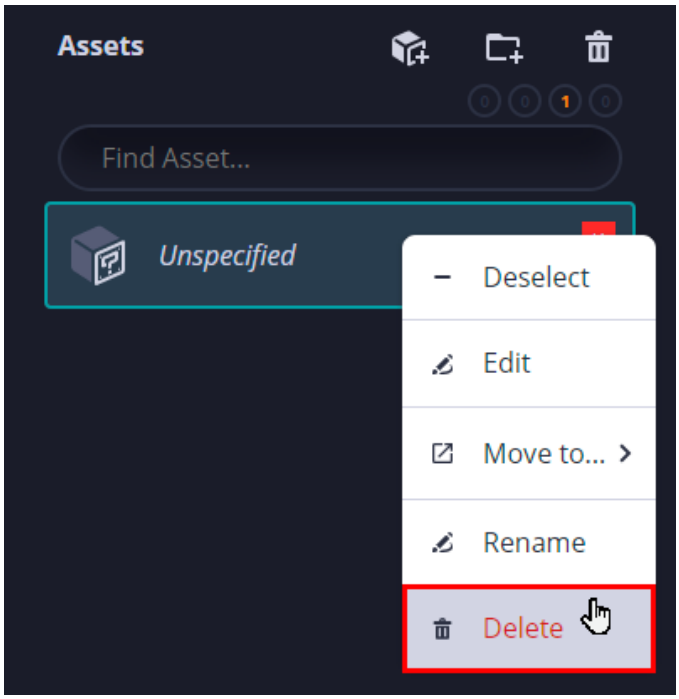

Figure 29: Delete Asset Selection

The user will then be prompted with a delete confirmation message (*Figure 30*).

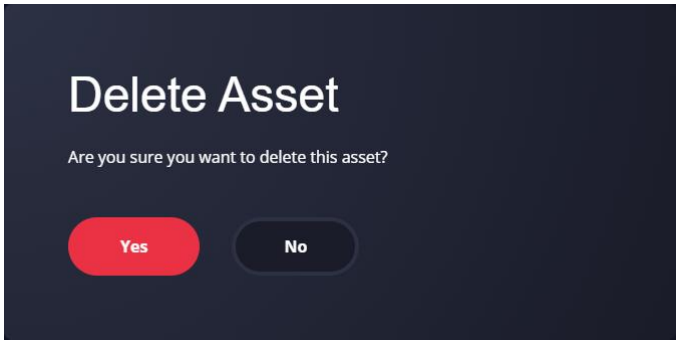

Figure 30: Delete Asset Confirmation Message

4.3.2 Folder

Before creating, renaming, or deleting a folder, the user must make sure the “Folder” option is selected in the **View Section**.

4.3.2.1 Create a Folder

The user can create a folder by clicking on the “Add a Folder” icon highlighted in *Figure 31*.

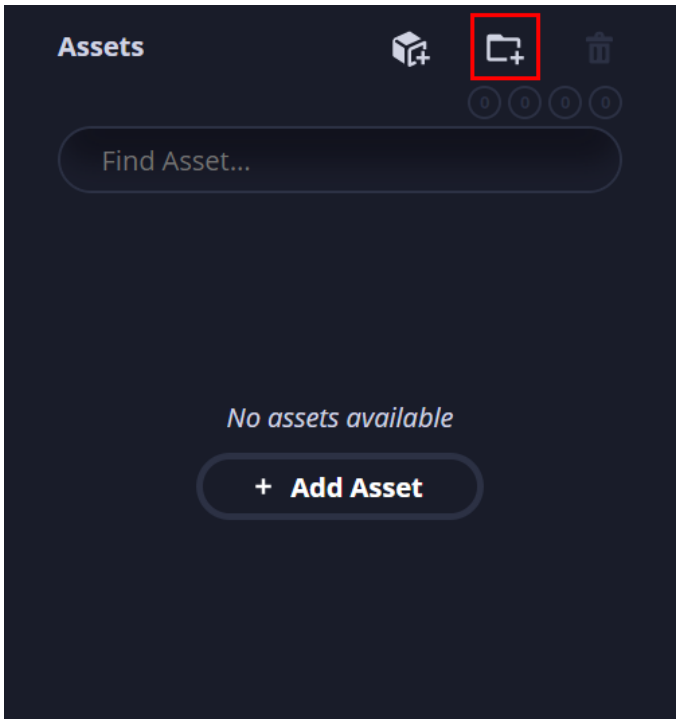

Figure 31: Create a Folder Button

The following is an example of a folder created and populated under the **Assets Section** (*Figure 32*).

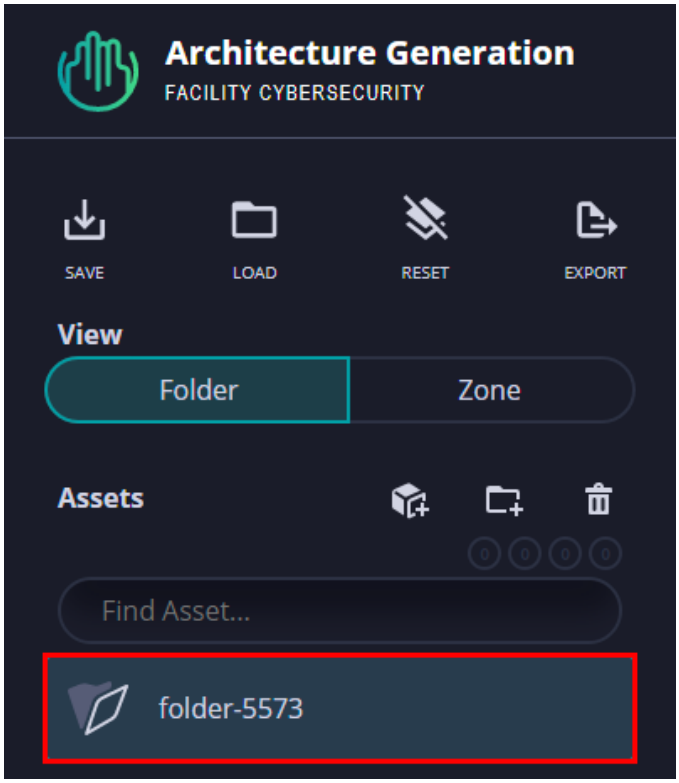

Figure 32: Example – Created Folder

4.3.2.2 Rename a Folder

The user can rename a folder by right clicking on the folder and selecting the “Rename” option (*Figure 33*).

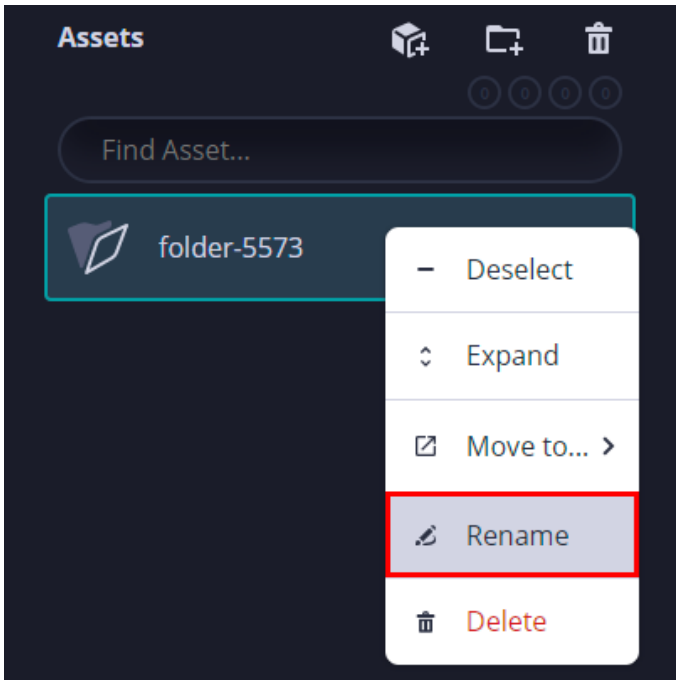

Figure 33: Rename a Folder

4.3.2.3 Add an Asset to a Folder

To add an asset to a folder, the user can right click on the asset and select “Move to” option then select the appropriate folder (*Figure 34*). Alternatively, the user can drag and drop the asset into the desired folder.

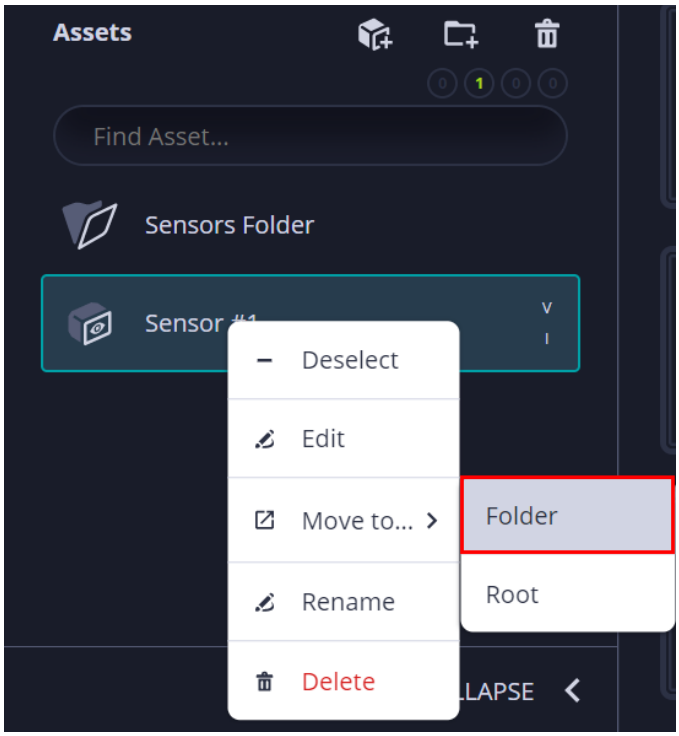

Figure 34: Add Asset to Folder

After selecting the appropriate folder, the user will be prompted with a “Move Asset” dialogue box. Next, the user must choose the folder once more they want the asset to move to, as shown in *Figure 35*.

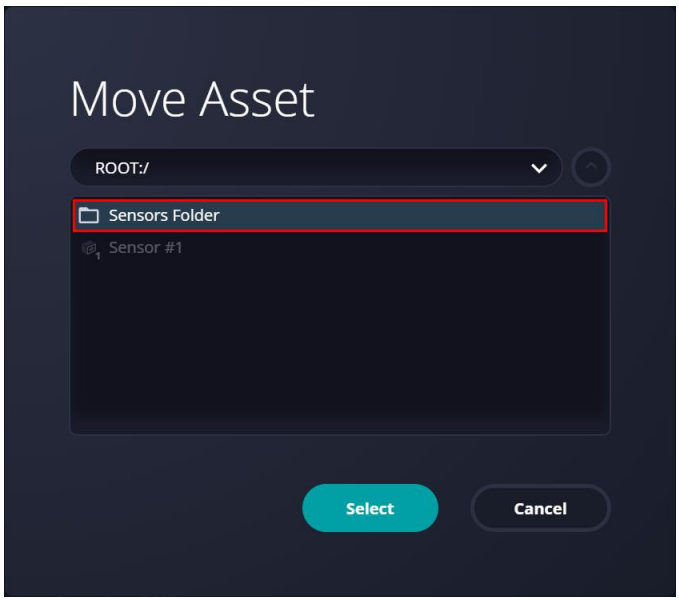

Figure 35: Move Asset Dialogue

4.3.2.4 Remove an Asset from a Folder

To remove an asset from a folder, the user can right click on the asset within the folder and select “Move to” option then select the “Root” folder (*Figure 36*). Alternatively, the user can drag and drop the asset into a different folder.

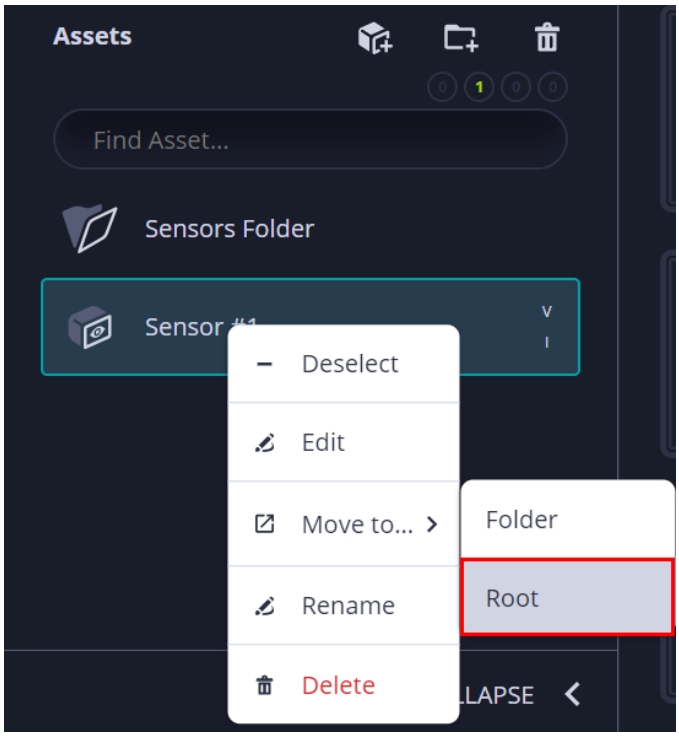

Figure 36: Remove Asset from Folder

4.3.2.5 Delete a Folder

The user can delete a folder by right clicking on the folder and selecting the “Delete” option (*Figure 37*).

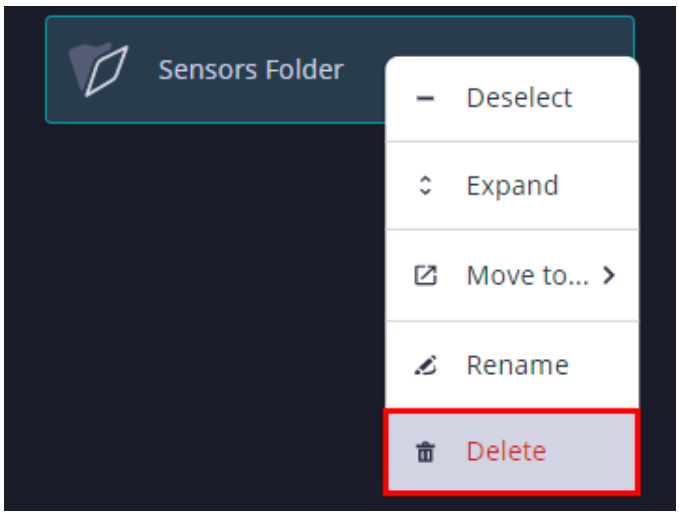

Figure 37: Delete a Folder

4.3.3 Zone

Before creating, renaming, or deleting a zone, the user must make sure the “Zone” option is selected in the **View Section**.

4.3.3.1 Create a Zone

The user can create a zone by clicking on the “Add a Zone” icon highlighted in *Figure 38*. Alternatively, the user can create a zone while in the architecture diagram by right clicking on an asset in any level and selecting the “Zones” option then “Add to a New Zone.”

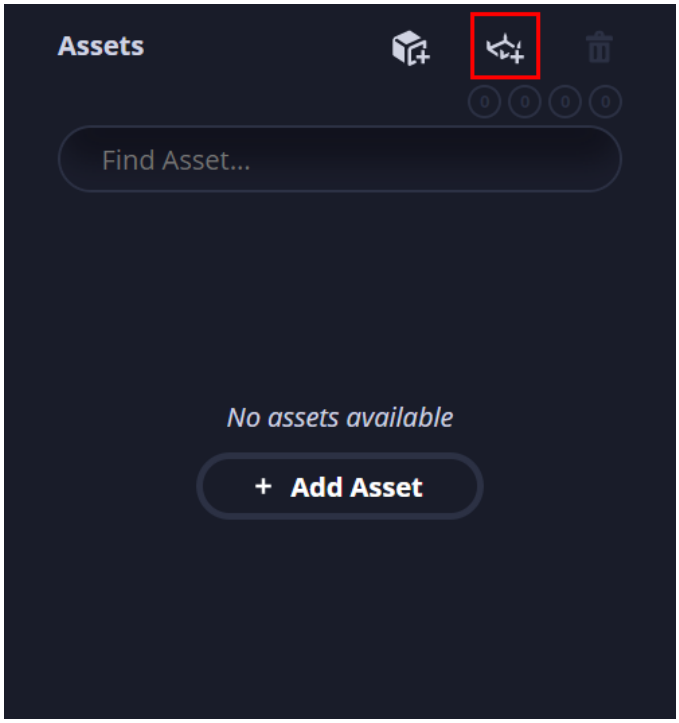

Figure 38: Create a Zone

The user will then be prompted with a zone creation dialogue window to title and color code the zone, as shown in *Figure 39*.

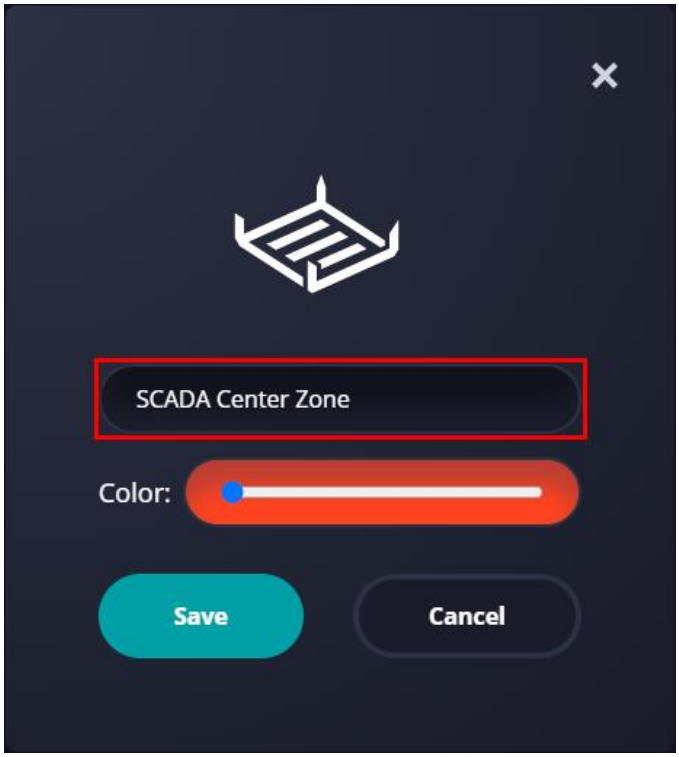

Figure 39: Zone Creation Dialogue

4.3.3.2 Edit a Zone

The user can edit a zone by right clicking on the desired zone and selecting the “Edit” option (*Figure 40*).

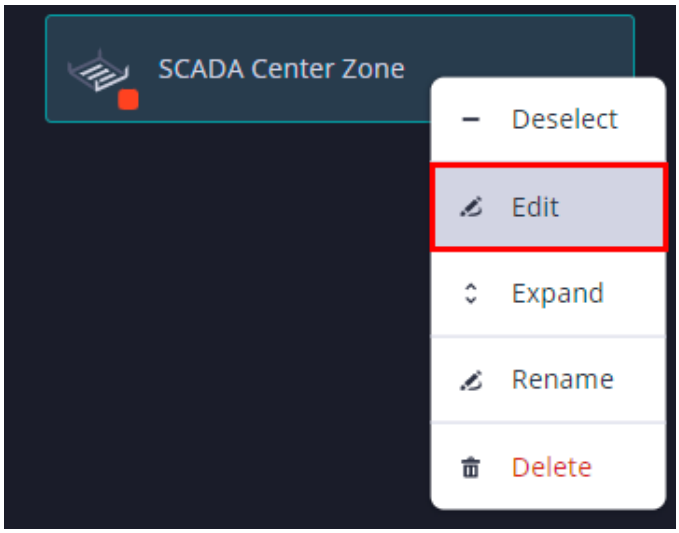

Figure 40: Edit a Zone

4.3.3.3 Rename a Zone

The user can rename a zone by right clicking on the zone and selecting the “Rename” option (*Figure 41*).

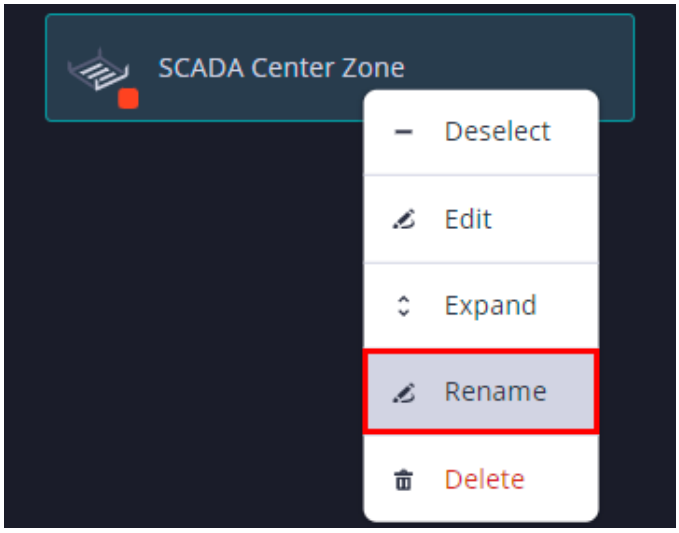

Figure 41: Rename a Zone

4.3.3.4 Add an Asset to a Zone

To add an asset to a zone, the user can right click on the asset and select “Move to” option then select “Existing Zone” (*Figure 42*). Alternatively, the user can add an asset to a zone while in the architecture diagram by righting click on an asset and selecting the “Zones” option then “Add to Existing Zone.”

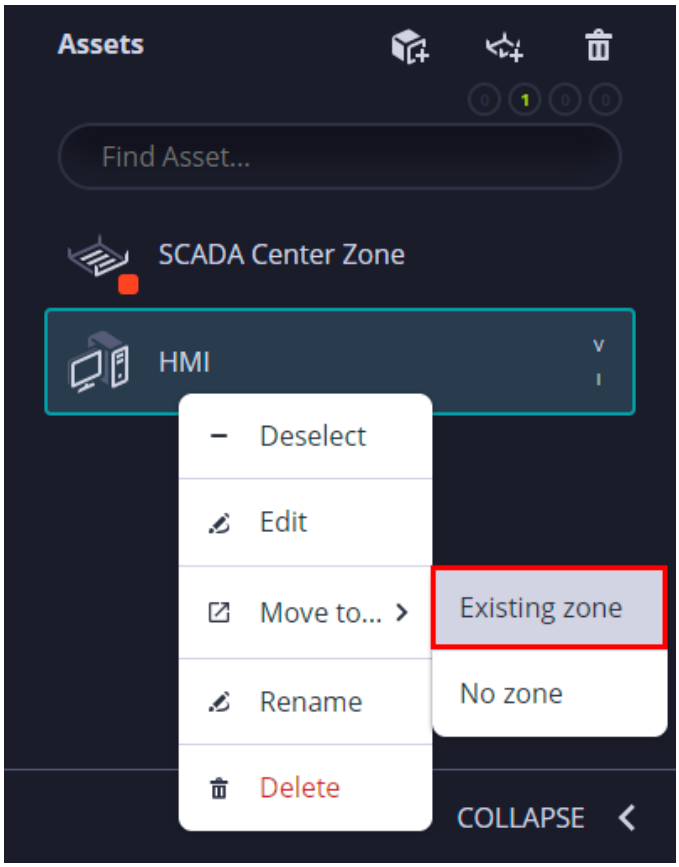

Figure 42: Move Asset to a Zone

The user will be prompted to select the desired zone to add an asset highlighted in *Figure 43*.

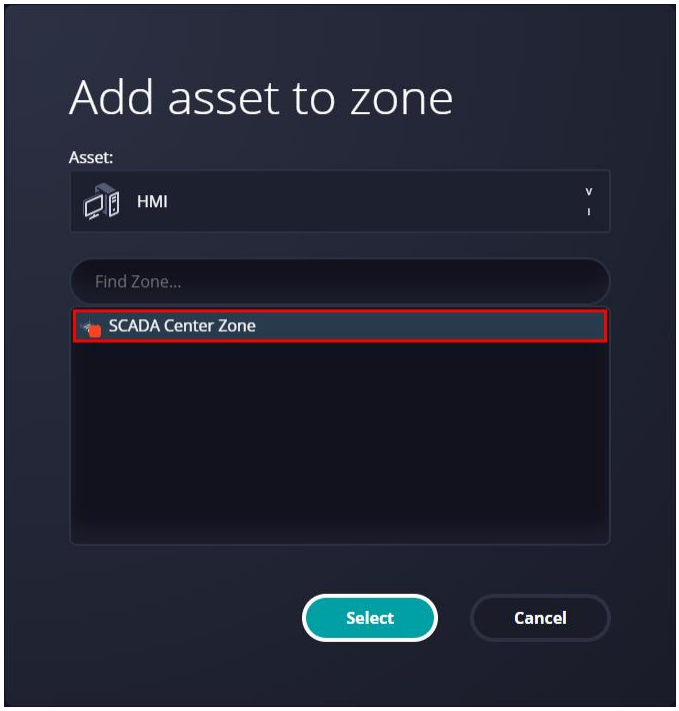

Figure 43: Add Asset to Zone

The zone can be viewed in the ArcGen menu pane (*Figure 44*) and within the architecture diagram (*Figure 45*).

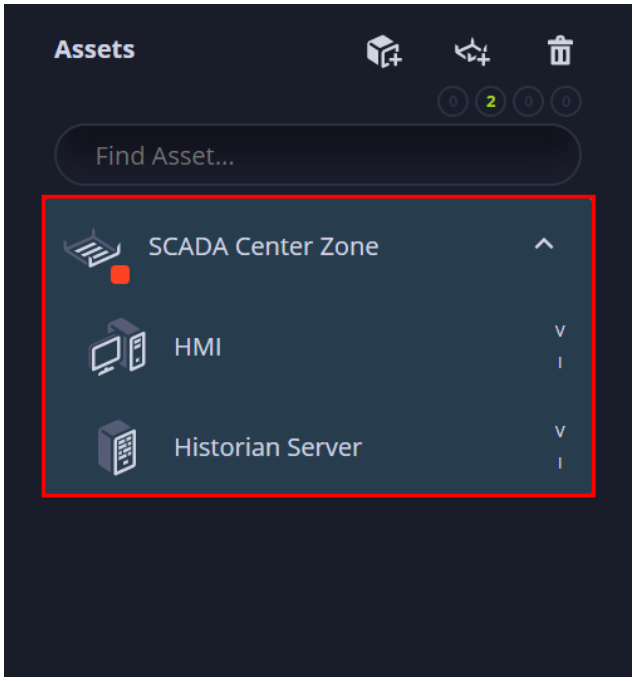

Figure 44: Assets Added to a Zone in ArcGen Menu Pane View

Figure 45: Assets Added to a Zone in Architecture Diagram View

4.3.3.5 Remove an Asset from a Zone

To remove an asset from a zone, the user can right click on the asset within a given zone under the Assets section and select “Move to” option then “No Zone” (*Figure 46*). Alternatively, an asset can be removed from a zone within the architecture diagram by right clicking on an asset and selecting the “Zones” option then “Remove from current zone.”

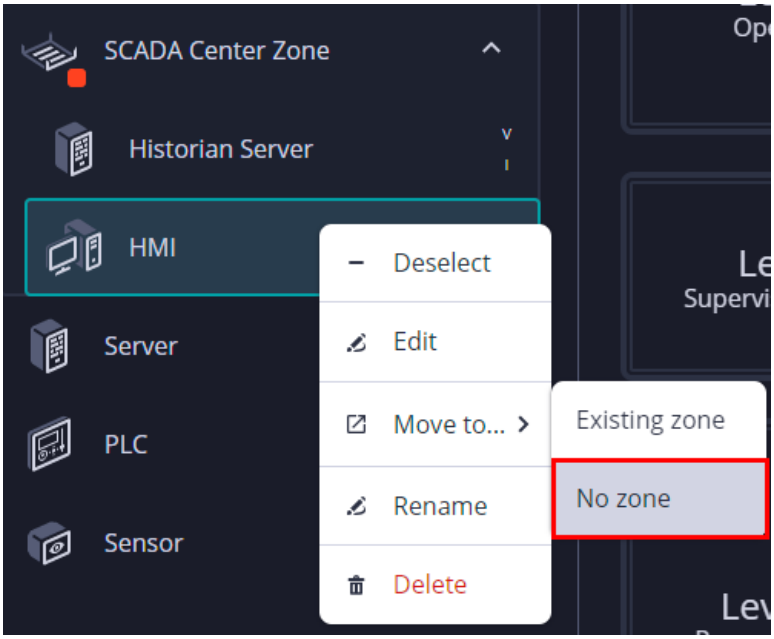

Figure 46: Asset Removal from Zone

4.3.3.6 Delete a Zone

The user can delete a zone by right clicking on the zone and selecting the “Delete” option (*Figure 47*). Alternatively, a zone can be deleted by clicking on the desired zone and then clicking on the “trashcan” button found in the Assets section.

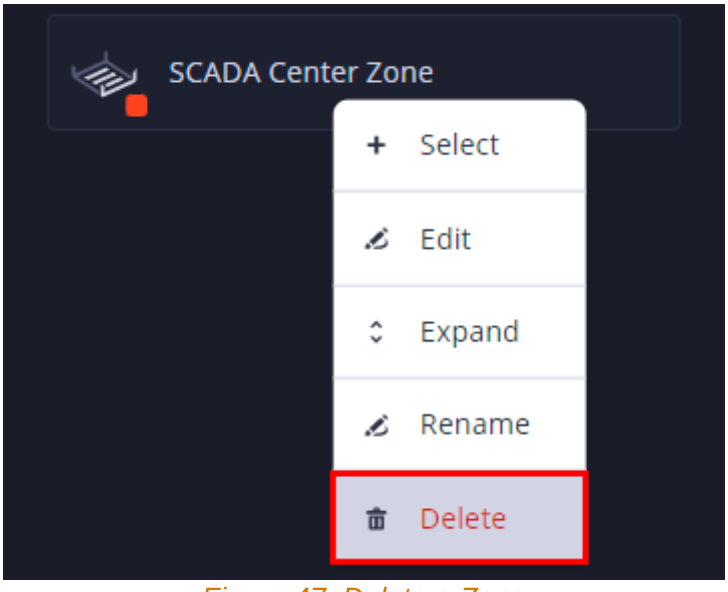

Figure 47: Delete a Zone

4.4 Collapse Option

The ArcGen menu pane can be collapsed to the left and reopened to the right by clicking the “Collapse” option found below the “Assets” section, as shown in *Figure 48* and *Figure 49*.

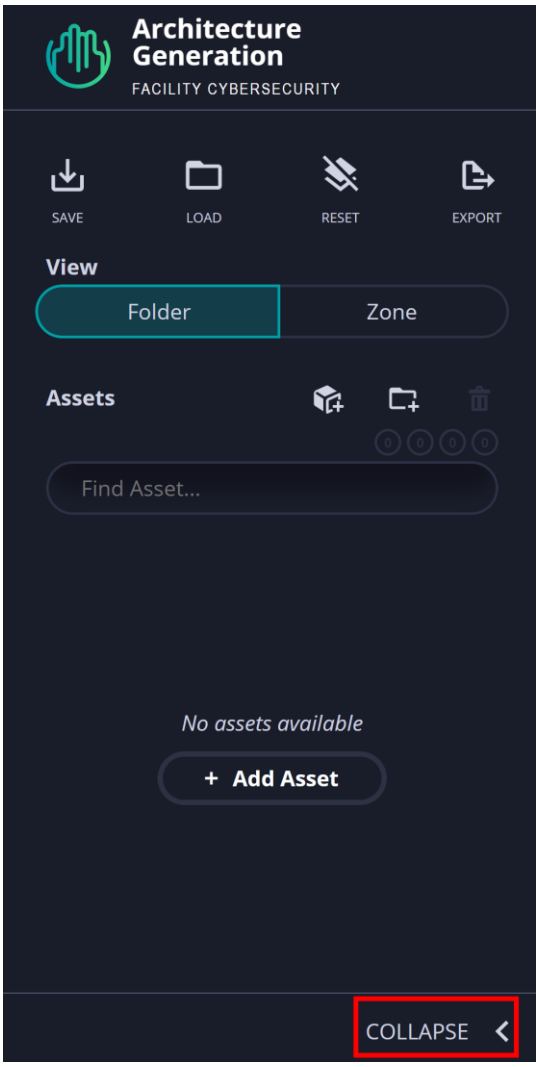

Figure 48: Collapse Menu Toggled Off

Figure 49: Collapse Menu Toggled On

5.0 Architecture Diagram

This section will cover creating an architecture diagram.

5.1 Starting a New Architecture Diagram

To start a new architecture, click the “Get Started” button shown in *Figure 2*. A new page with a blank architecture diagram will load. There will be no assets or zones defined in either the menu or in the architecture, as shown in *Figure 50*.

Figure 50: Blank Architecture

5.2 Purdue Reference Model Level Information

For every level in the architecture diagram, the user can obtain information regarding components found within a given level by left clicking on the “information” button highlighted in *Figure 51*.

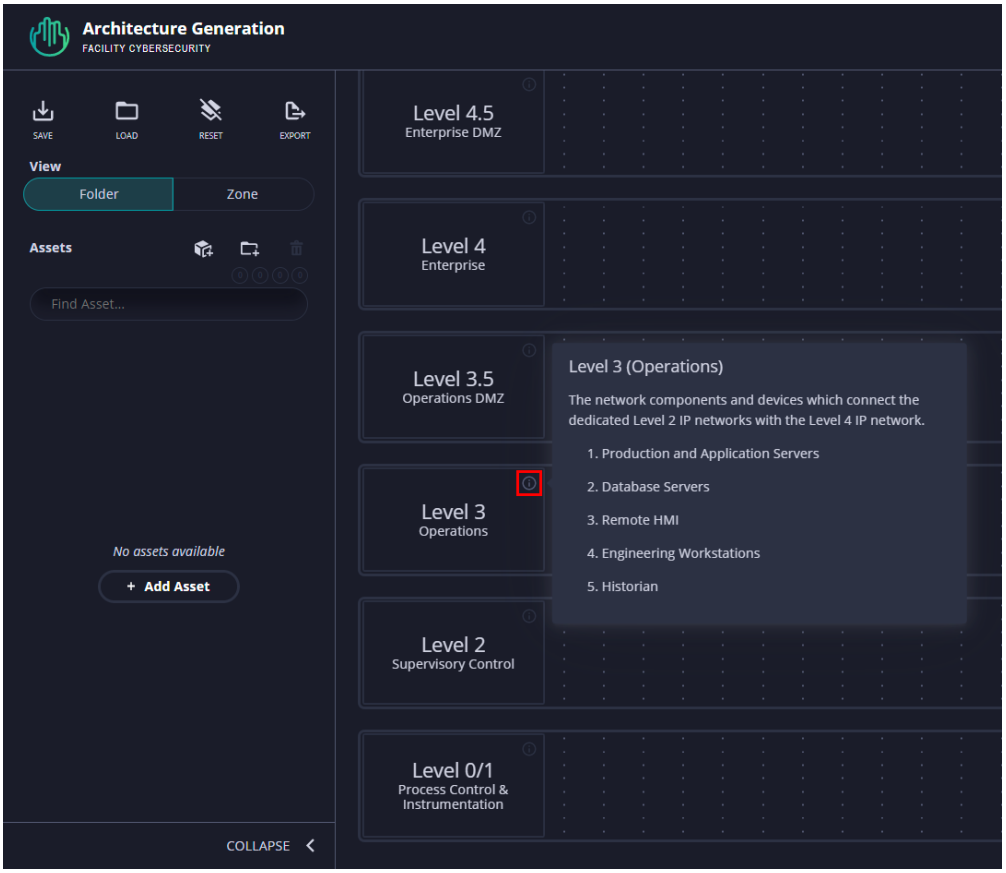

Figure 51: Purdue Reference Model – Level 3 Information

5.3 Drag and Drop Asset

The user can drag and drop assets (*Figure 52*) into any level of the architecture diagram that can then be represented as an asset widget.

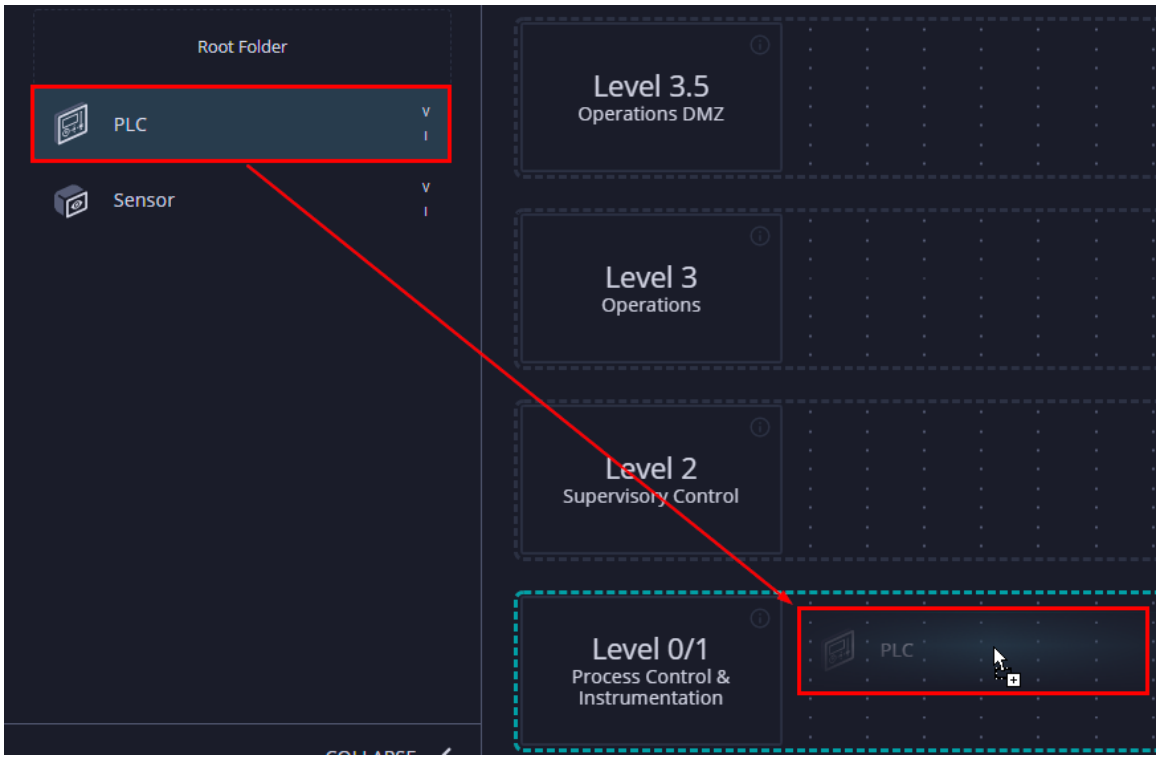

Figure 52: Drag and Drop an Asset

The following is an example of an asset widget that has been dragged and dropped into the architecture diagram (*Figure 53*).

Figure 53: Example – Asset Widget in Architecture Diagram

Alternatively, the user can right click in the architecture diagram on any level and select the "Add Existing Asset" option (*Figure 54*).

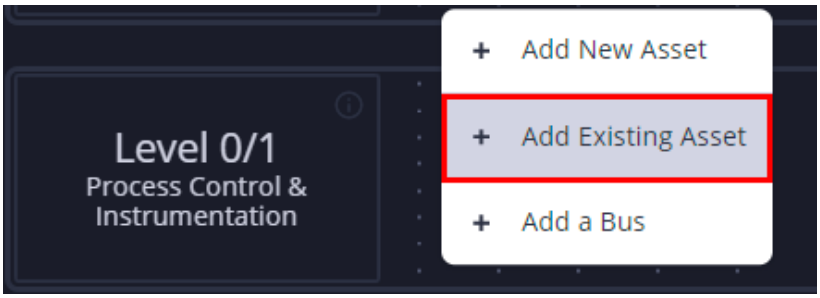

Figure 54: Alternative Method – Add Asset to Level

5.4 Data Link Assets

Data links provide a way for the user to model relationships between assets. To create a data link, the user can click on the top or bottom point of an asset and then click on another asset to link, as shown in *Figure 55*.

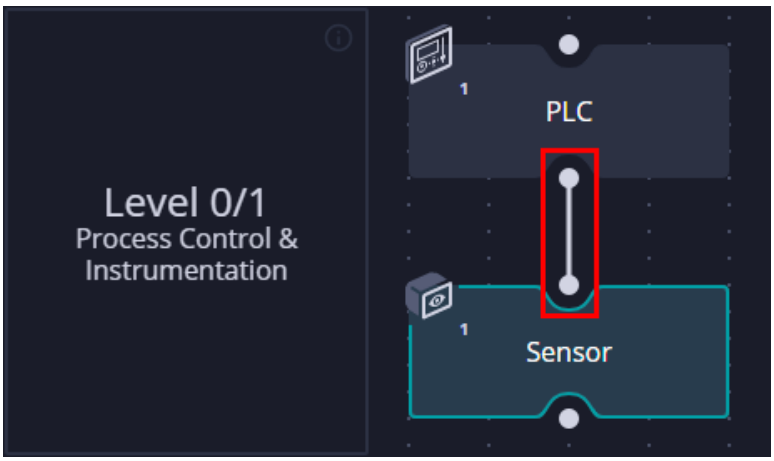

Figure 55: Data Linking Assets

5.4.1 Edit Data Link

Once a data link connection has been established between two assets, the user can right click on the link and select “Edit Data” (*Figure 56*).

Figure 56: Edit Data Link

The user would then be able to add/edit the ports and data communication between the two assets represented by the link (*Figure 57*). Please see the **Links** section for more information regarding Link Data.

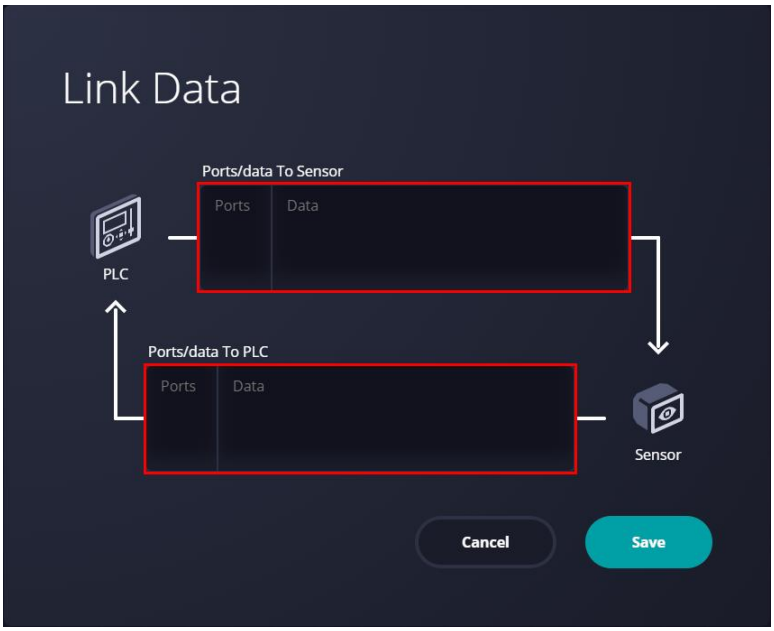

Figure 57: Edit Link Data

5.5 Bus

5.5.1 Add a Bus

The user can add a bus to the architecture diagram by right clicking on any level and selecting the “Add a Bus” option (*Figure 58*).

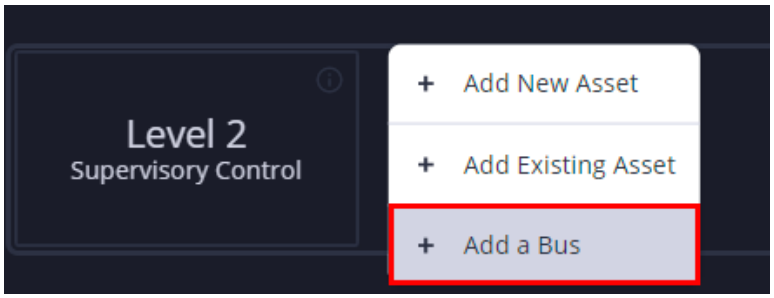

Figure 58: Add a Bus Option

The user can link assets to the bus by clicking on the top or bottom points of an asset then clicking on either ends of the bus (*Figure 59*).

Figure 59: Example – Added Bus in Architecture Diagram

5.5.2 Delete a Bus

The user can delete a bus by right clicking on the bus and selecting the “Delete Bus” option (*Figure 60*).

Figure 60: Delete Bus Option

5.6 Architecture Diagram Controls

Several controls are located on the lower right side next to the architecture diagram working area. The minimize/maximize button (*Figure 61*) allows the user to increase and decrease the size of the assets in the architecture diagram. The zoom-in button (*Figure 62*) has three levels that would enable the user to zoom further into the architecture diagram. Oppositely, the zoom-out button (*Figure 63*) has three levels that allow the user to zoom further out of the architecture diagram.

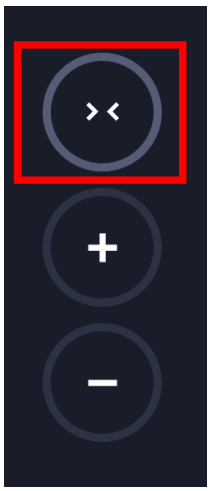

Figure 61: Minimize/Maximize Assets Button

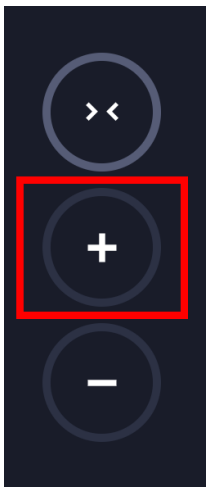

Figure 62: Zoom-in Button

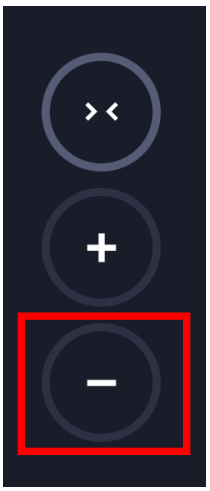

Figure 63: Zoom-out Button

5.6.1 Minimize/Maximize Assets Button

When creating an architecture diagram, the user has the ability to minimize (*Figure 64*) and maximize (*Figure 65*) the diagram by using the “Minimize/Maximize Assets” button.

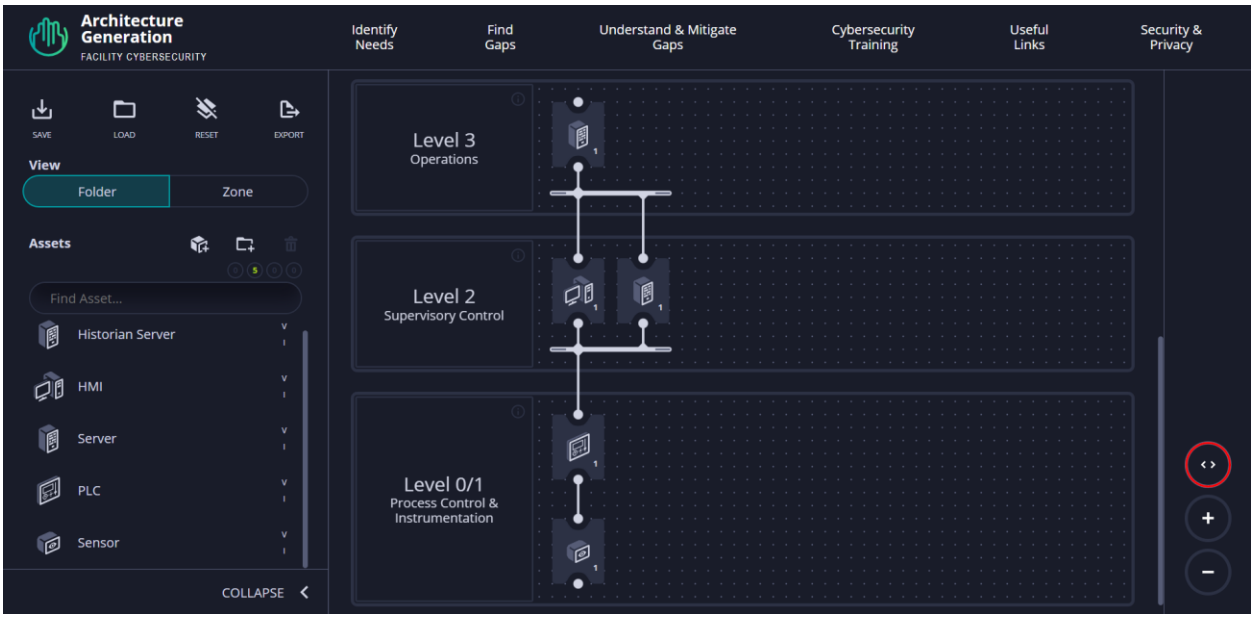

Figure 64: Minimize in Architecture Diagram

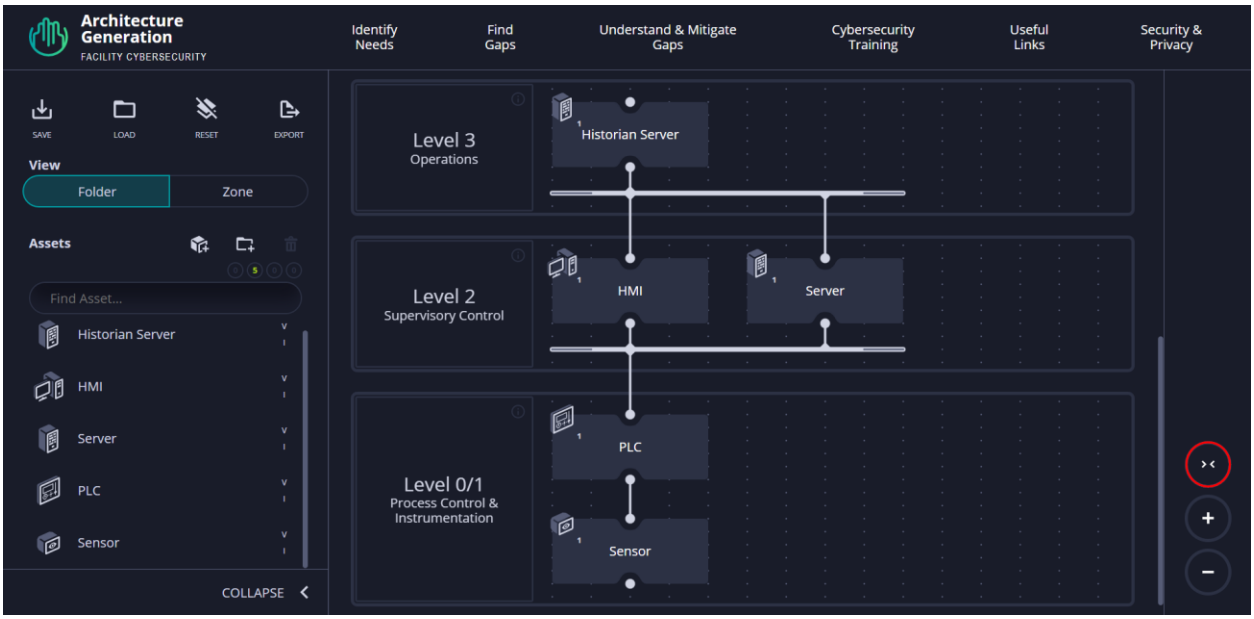

Figure 65: Maximize in Architecture Diagram

Pacific Northwest National Laboratory

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99354

1-888-375-PNNL (7665)

www.pnnl.gov