SYSTEM THEORETIC PROCESS ANALYSIS FOR SECURITY (STPA-SEC)

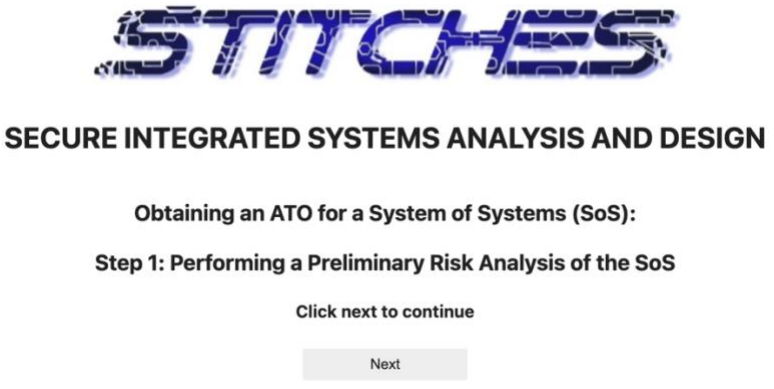
SPECIFICATION NOTEBOOK (SPEC-BOOKS)

PRELIMINARY RISK ANALYSIS INSTRUCTIONS (PRA)

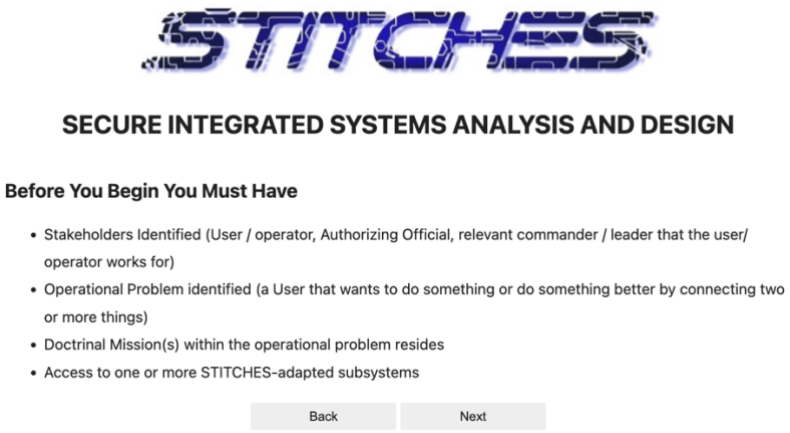
VERSION 1.0

This spec-book Preliminary Risk Analysis (PRA) is designed to facilitate obtaining the approvals necessary to begin subsystem adaptation. The stitches toolchain is hosted via the Gemini/Castor VM. The Gemini/Castor VM has already received an ATO for a generic application. However, the specific instance used to adapt the subsystem must be reviewed, understood, and tailored by the sponsoring organization. The spec-book PRA is meant to serve as an executive summary of the detailed risk analysis contained in the Gemini/Castor ATO. Although the toolchain is software, an ATO has been obtained and is made available to subsystem engineers conducting the adaptation.

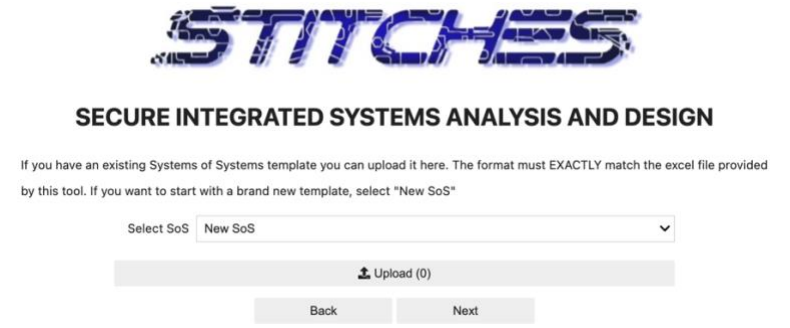
This version of spec-books 1.0 has terminology that confuses SoS preliminary risk analysis and a subsystem PRA. However, the next revision will correct that confusion. For now, any time SoS is referenced, the term subsystem is intended.



For the subsystem adaptation, the mission or purpose is to adapt and test a subsystem on a host network. The operational problem and doctrinal mission are generic and not necessarily needed. Before you begin, you must have stakeholders and “access” to one or more subsystem TO BE adapted.

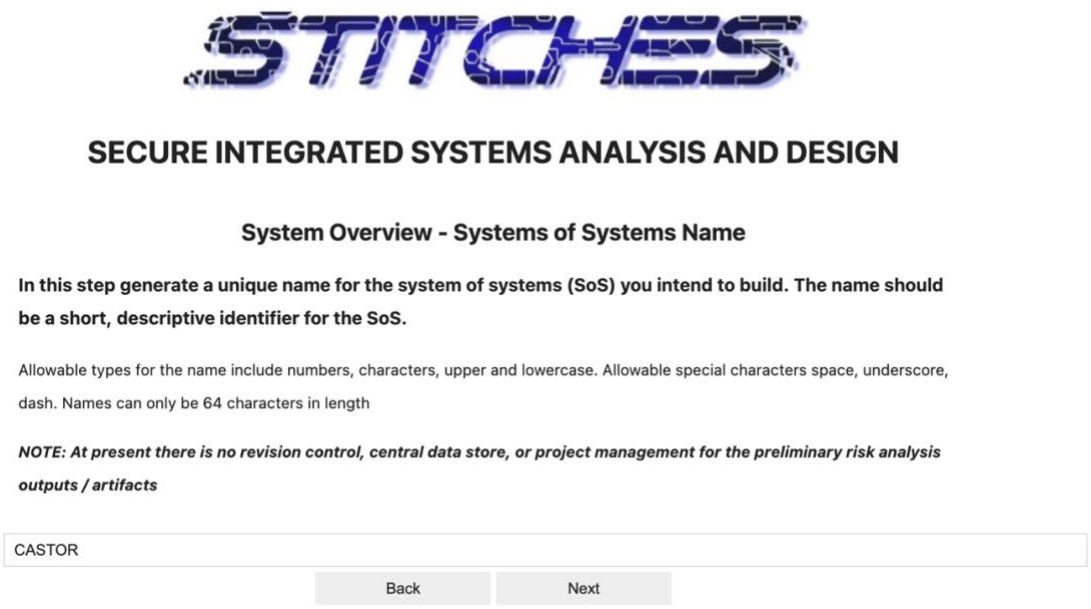


This is the name of the subsystem you plan on adapting (rather than New SoS). On this screen you can either import an existing PRA analysis spreadsheet or select “New SoS” to create a new one.



Step 1: In the future, this will be an incremental Preliminary Risk Analysis. We recommend you start by naming the project based on:

1. Bringing in the STITCHES tool chain via a CASTOR VM and establish a development environment on your host network.
2. Connecting the STITCHES integrated subsystem to your physical subsystem (i.e. Hardware based testing loop).
3. Connecting the STITCHES integrated subsystem to your physical subsystem via the host network (i.e. Hardware based testing loop on the host network rather than just stand alone).



STEP 2: This step is largely not applicable for the subsystem adaptation. Skip this step.

SECURE INTEGRATED SYSTEMS ANALYSIS AND DESIGN

Describe the PROBLEM to be developed in as much detail as possible

There is NO single best way to define a problem that is suitable for all circumstances. Likewise, there is no single format or framework that will ensure success.

STITCHES is inherently founded upon principles of both systems and design thinking. As a result, one useful way of thinking about a problem is to define it in terms of a GAP between what a user can currently do and what the user would LIKE TO BE ABLE TO DO. Another way of framing the gap is to describe some functionality that a user desires to accomplish some goal.

The Stanford Design school places great emphasis on the importance of having deep empathy of the user and the problem THEY are trying to address, rather than starting with a technology or solution and then trying to argue with the user or problem owner on how the technology will solve the user's problem.

If the SoS engineer cannot clearly articulate a user problem that is being addressed, then there is a need for further research.

Suggested Syntax:

[User/Operator] is currently incapable of doing [GAP](expressed a one or more VERBS), [STAKEHOLDERS] care about the [GAP] because [STAKE]. So we plan to develop CASTOR to help [User/Operator] to do [Action] by providing [FEATURE].

NOTE: If you aren't able to capture all of these items, that is ok, the next few steps will guide you on how and what each one of the [bracketed] content might be

STEP 3: Capture the intended stakeholders (typically):
1. The information system owner
2. The subsystem owner
3. The authorizing official
4. The current owner / owners of the missions that the subsystem currently supports
5. The adaptation engineers and the system users
6. The program office
7. The comm squadron or network owners

Each stakeholder has a stake. The stake is the summary of what they care about.

STEP 4: Each stakeholder would have a role (Typically):

1. User
2. Developer
3. Assessor
4. Approver
5. Mission Owner

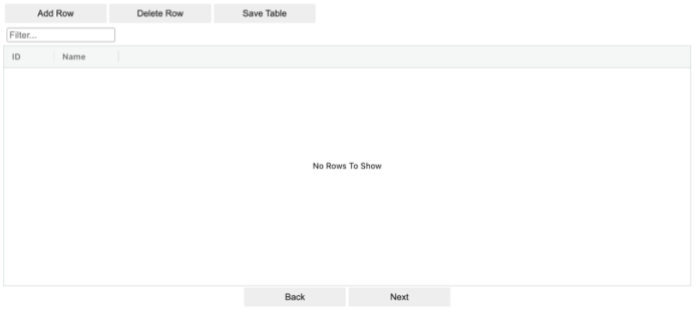
STEP 5: If your subsystem was a black box define the subsystem's functionality in the form of input and output relationships. For **Output** the function will be a <verb> <noun> pair where the verb is an action from the subsystem that does something to an external entity by providing information, producing a physical effect (matter), or an electronic effect (energy). For **Input** the function will be a noun that is "received" by an external entity. The input will be in the form of information, a physical effect (matter), or an electronic effect (energy).

STEP 6: In step 3, you defined the stakeholder and their stake.

STITCHES

SECURE INTEGRATED SYSTEMS ANALYSIS AND DESIGN

Step 6 - Identify the losses



Using the stakes defined earlier, map the stakes to the asset class description and loss protection criteria in NIST 800-160 volume 1. The syntax should follow the STPA Handbook, page 16-17.

Table 1. Common Asset Classes

ASSET CLASS	DESCRIPTION	LOSS PROTECTION CRITERIA
MATERIAL RESOURCES AND INFRASTRUCTURE	This asset class includes physical property (e.g., buildings, facilities, equipment) and physical resources (e.g., water, fuel). It also includes the basic physical and organizational structures and facilities (i.e., infrastructure) needed for an activity or the operation of an enterprise or society.[29] An infrastructure may be comprised of assets in other classes. For example, the National Airspace System (NAS) may be considered infrastructure that itself is a system and contains other elements that are forms of systems and infrastructures, such as Air Traffic Control, navigational aids, weather aids, airports, and the aircraft that maneuver within the NAS.	*Material resources* are protected from loss if they are not stolen, damaged, or destroyed or are able to function or be used as intended, as needed, and when needed. *Infrastructure* is protected from loss if it meets performance expectations while delivering only the authorized and intended capability and producing only the authorized and intended outcomes.
SYSTEM CAPABILITY	This asset class is the set of capabilities or services provided by the system. Generally, system capability is determined by (1) the nature of the system (e.g., entertainment, vehicular, medical, financial, industrial, or recreational) and (2) the use of the system to achieve mission or business objectives.	*System capability* is protected from loss if the system meets its performance expectations while delivering only the authorized and intended capability and producing only the authorized and intended outcomes.
HUMAN RESOURCES	This asset class includes personnel who are part of the system and are directly or indirectly involved with or affected by the system. The consequences of loss associated with the system may significantly change the importance of this asset class (e.g., the effect on personnel due to a failure of a guidance system in an aircraft is significantly different from the effect on personnel due to the breach of a system that compromises individual credit card information).	*Human resources* are protected from loss if they are not injured, suffer illness, or killed.
INTELLECTUAL PROPERTY[30]	This asset class includes trade secrets, recipes, technology,[31] and other items that constitute an advantage over competitors. The advantage is domain-specific and may be referred to as a competitive advantage, technological advantage, or combative advantage.	*Intellectual property* is protected from loss if it is not stolen, corrupted, destroyed, copied, substituted in an unauthorized manner, or reverse-engineered in an unauthorized manner.
DATA AND INFORMATION	This asset class includes all types of data and information (aggregations of data) and all encodings and representations of data and information (e.g., digital, optical, audio, visual). There are general sensitivity classes of data and information that do not fall within the above categories, such as classified information, Controlled Unclassified Information (CUI), and unclassified data and information.	*Data and information* are protected from loss due to unauthorized alteration, exfiltration, infiltration, and destruction.
DERIVATIVE NON-TANGIBLES	This asset class is comprised of derivative, non-tangible assets, such as image, reputation, and trust. These assets are defined, assessed, and affected – positively and negatively – by the success or failure to provide adequate protection for assets in the other classes.	*Non-tangible assets* are protected from loss by ensuring the adequate protection of assets in the other classes.

STEP 7: In future versions, a new table will be displayed that will pivot Functions vs Losses. For this version it will be helpful to do this prior to identifying your hazards. Make a table that has Functions on the vertical access and the Losses on the horizontal axis. The subsystem can do all the functions. You must describe how each function within the subsystem could plausibly misbehave in a manner that could result in the loss under the worst-case environmental conditions. Plausible miss behavior generally consists of one of three things:
1. The functionality is not invoked when needed / desired or expected.
2. The functionality is invoked under the wrong condition
3. The functionality is invoked in the wrong way or the wrong manner
Once you have this filled out, then translate it into the STPA Hazard syntax: <Subsystem><Misbehavior><Associated Loss or Losses> and the <Concern> associated with each hazard. (Page 17-20 of the STPA Handbook)

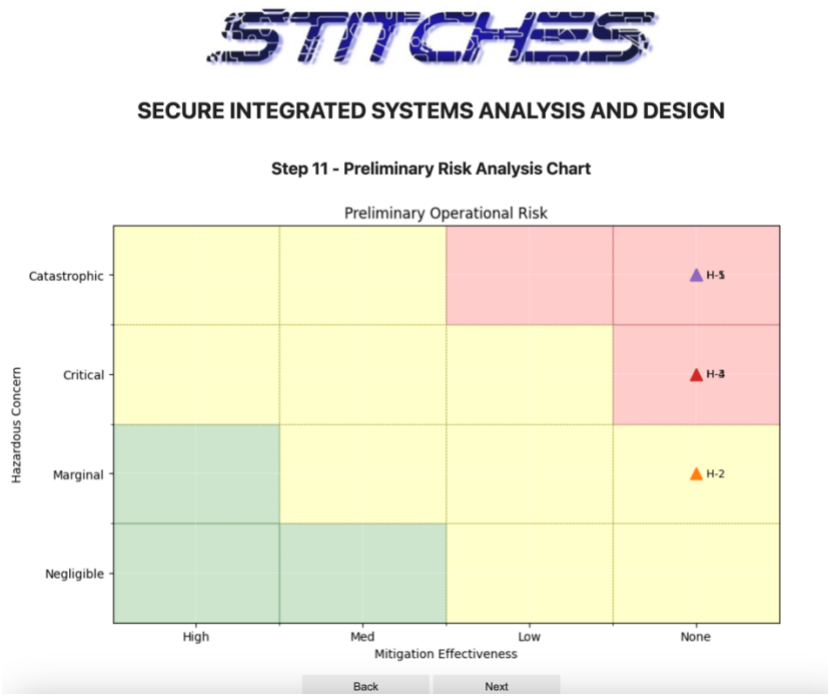
Tips to prevent common mistakes when identifying hazards

- Hazards should not refer to individual components of the system
- All hazards should refer to the overall system and system state
- Hazards should refer to factors that can be controlled or managed by the system designers and operators
- All hazards should describe system-level conditions to be prevented
- The number of hazards should be relatively small, usually no more than 7 to 10
- Hazards should not include ambiguous or recursive words like “unsafe”, “unintended”, “accidental”, etc.

STEP 8: Explicitly define the linkage between the Hazards and Losses. This should be directly applied to the following table.

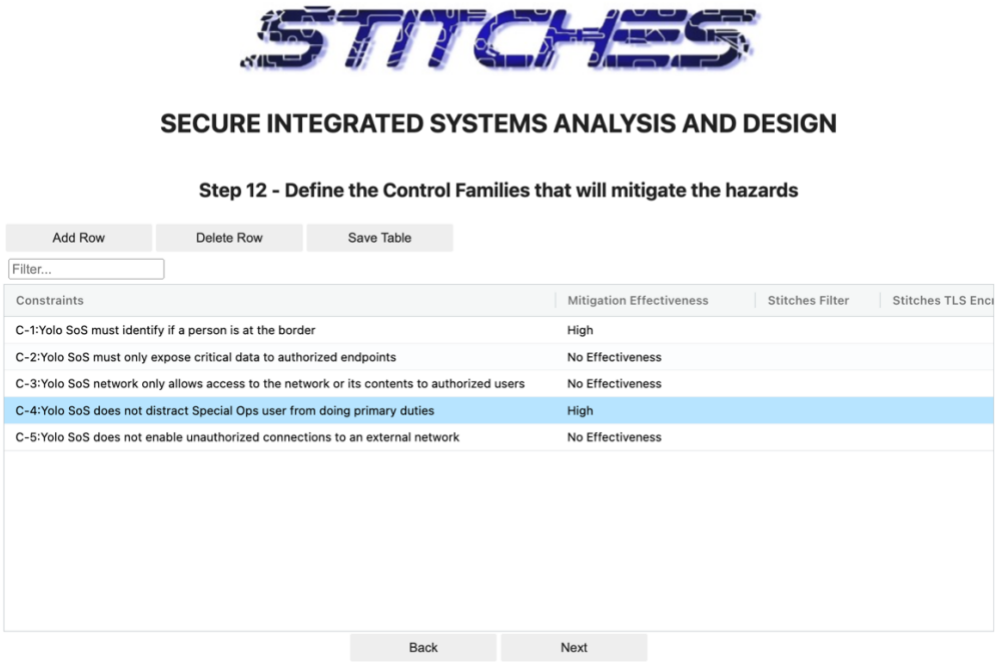
STEP 9: Translate the hazards to constraints using the STPA handbook pages 20-21.

STEP 11: The next to final step is a visualization step. This step simply shows how the hazards map to a current risk matrix. The only difference is that probability has been replaced by mitigation effectiveness. See "Improving the standard risk matrix part 1"

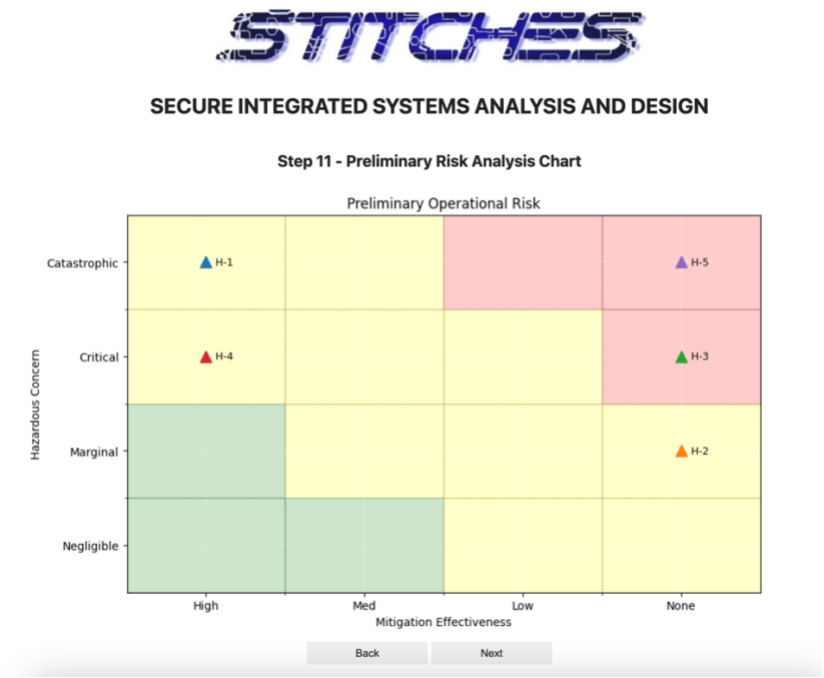


STEP 11: Import the previously generated constraints and identify what controls will be used to enforce the constraint. The enforcement of the constraints results in an effective method to mitigate the hazards that were identified. This table assumes the “standard” control families are included in the CASTOR Virtual Machine. However, the future version of this step will include those families, specific controls included in each family, and custom controls based on STITCHES applications.

In the future version of the Preliminary Risk Analysis, this step will be broken into three steps. First, the constraints will be mapped to the appropriate control families that are required to enforce that constraint. The next step will be to identify the controls that are required to satisfy the control family constraint enforcement. The last step will be to justify the mitigation effectiveness based on the controls applied.



STEP 12: By identifying the mitigation effectiveness and the justification, a new Preliminary Risk Chart will be generated.



STEP 13: Finally, the last step is to download the presentation and the source excel database that the entire process is stored.