**Brainstorming Risks**

**Cornell Cup USA – Arm Enabled**

**Prof. David R. Schneider, Cornell Director of MEng Studies in Systems Engineering, drs44@cornell.edu**

This guide is designed to help you and your team brainstorm about potential concerns and risks that might be involved with your design. The value in this is to recognize these risks early on so you can help mitigate them or develop alternative back-up plans.

It is suggested that you read through this entire guide before you begin as you may find it helpful to do the steps in a different order. For example, you may decide it’s better to switch steps 2 and 3 around, i.e. do you like to think first about effects or causes? You may also want to only do a few steps and focus on the more obvious risks just to get a feel for the benefit of the overall process. For example, for a quick pass at this it can be worthwhile to do simply steps 0-2, and 4 maybe 5 and then go back to do the other steps for only those potential concerns that have been identified as being very risky or potentially harmful to your design or design process. However, the steps provided here are arranged to be very similar to those followed by NASA and many complex military projects to ensure the success of their designs and hence it is very good to at least complete all of them for your own professional development. For the purposes of the application, it is the largest risks that need to be highlighted in the main discussion.

A sample of part of following these steps, the Perpetual Motion Bicycle (PMB) is used as an example and part of a sample result of following these steps is provided in the file, SampleRiskBrainistormingPMB.xlsx. A discussion of this sample file is also provided at the end of this guideline’s steps and for many readers may be the key for understanding the value of brainstorming risks.

**Step 0:** Work out your design conceptually at least well enough that you have a good idea as to what is the main functionality your design must achieve to meet the challenge needs and what are all of main subsystems to your design.

**Step 0 is Complete When:** You and your team can easily describe how all of the subsystems work together in order to achieve the desired main functionality and handle all of the main use cases required by the challenge definition.

**Step 1:** Take a look at each one of your subsystems and make a list about how they could fail. The word “failure” is used a lot in risk analysis to generalize anything that doesn’t happen the way it’s supposed to. When starting to think about design failures, it’s best to think about what kinds of functionality would no longer be able to be performed properly, not what specific components fail. (Remember at this point of your design you are not expected to know what are all of or even many of your design’s specific components). For example, a functional failure for the PMB GUI subsystem could be that the GUI does not display the energy storage information. Likewise, a functional failure for the PMB IR Sensor Encoder subsystem could be an incorrect number of rotations is reported by the sensor.

Determining the causes for the loss of functionality will be delved into later at Step 3, but this focus on first listing out important potential losses of functionality or even potentially poor performance results is a great point to start risk brainstorming and sometimes is referred to professionally as identifying “Failure Modes”.

At this point of your design, potential failure can also come in the form of not being able to achieve a particular goal. For example, in the PMB sample application, not being able to create the very challenging control system would be one way that their overall design could “fail". Identifying these kinds of failures will also help your team to ascertain how important it is to achieve various goals and later steps will help you compare just how important one goal may be over another.

**Step 1 is Complete When**: You have created a list of possible failure modes. It is usually suggested that different team members examine different subsystems and then the lists are recombined. It is also okay to start out with just a few key ones and then come back to revisit and add to the list later once you have a better feel for the benefit of following these steps.

**Step 2:** For each functional failure mode identified, list all the effects it would have on the system. In some cases this is very specific. For example, one possible effect for a PMB’s Energy Storage failure mode of “energy storage system unable to store energy” could be “motors are not provided power”. Other effects can be somewhat more indirect. For example, the same PMB failure mode could also have a significant effect on the performance measure: “Energy Output from PMB Engine”. Effects like this one, such as any performance loss, additional budget cost, scheduling delays, equipment/parts damage, etc. are all worthwhile effects to list.

The reason for listing these effects is two-fold. First the effects might help to determine the possible causes for each identified failure mode & resulting effect pair. More so though, by listing the effects you can begin to determine the impact or severity of different kinds of failures and you will do so formally in step 5.

**Step 2 is Complete When:** a list of all of the possible effects have been established for each identified failure mode.

**Step 3:** For each effect, create a list of possible causes. The causes tend to be more component or structurally design oriented and so through this brainstorming risk process we have gone from thinking very functionally and more high level to now being more detail and component oriented.

The causes however do not need to be only physical components. A very common check that professionals use to make sure they are considering all possible causes is to think of “***MMMME***” which stands for :

* ***M***an: human error
* ***M***achine: how the device operates, electrically, mechanically, etc.
* ***M***ethod: the procedure a device follows in performing its tasks
* ***M***aterial: how it was made
* ***E***nvironment: the context in which it is used, including interfacing with other devices

You can probably think of other causes and not all of these will apply to all failure modes and resulting effects but they offer a good starting point for the brainstorming.

**Step 3 is Complete When:** At least one possible cause has been listed for each identified effect. Multiple possible causes can be listed for each effect. Several effects may have the same possible cause as well, as is shown in the SampleRiskBrainistormingPMB.xlsx file for the first two effects listed.

**Step 4:** Determine how severe the impact of each of the identified effects & associated possible causes is on the overall project. In order to be fair, you need to first set up your own formal objective rating system. A sample rating system is provided in the Application Review Criteria document under the sheet tab labeled “RiskTable”. Taking a look at that sample, you can see that down the first column there are 4 severity categories that have been defined: “Catastrophic, Critical, Moderate, and Negligible”. Each category has listed underneath a set of criteria that define how severe the impact must be in order for an effect/cause to earn that category rating. For example, if an effect/cause would result in a 17% increase in the budget that effect/cause could get a critical severity rating.

The rule for assigning severity ratings however is that you assign the worst severity rating that had at least one of their criteria met by the effect/cause. For example, if an effect/cause would result in no damage to equipment / facilities, a 6% budget increase, an 18% increase to the timeline and a 62% negative impact on the end products performance, that effect/cause should be given a severity rating of catastrophic. Even though by themselves the “no damage to equipment / facilities” would earn a negligible rating, the “6% budget increase” would earn a moderate rating, and the “18% increase to the timeline” would earn a critical rating, because one of the criteria is met for the catastrophic rating, the final rating assigned to the effect/cause would be catastrophic as that this the worst severity rating that had at least one of their criteria met.

You are perfectly welcome to establish your own severity rating system, changing either the criteria for the various categories or even the number of categories. The important thing is that you have a formal objective means for quantifying the severity of all effects/causes across your entire project.

**Step 4 is Complete When:** Your severity rating system is complete and a severity rating is assigned to each effect/cause. Typically a number is given to each severity rating with the worst severity being associated with the highest number. The “RiskTable” sample shows the associated numbers in column B and the SampleRiskBrainistormingPMB.xlsx file uses these numbers to represent the severity category assigned to each of its effects/causes.

Please note if you have decided to skip Step 3 initially, you can base your severity ratings solely on the identified effects.

**Step 5:** Determine how “likely” each one of the identified effects & associated possible causes is for the overall project by assigning a probability or a “likelihood” rating to each one. Similar to the severity ratings, in order to be fair, you need to first set up your own formal objective likelihood rating system. A sample rating system is also provided in the Application Review Criteria document under the sheet tab labeled “RiskTable”. Taking a look at that sample, you can see that down row 2 that there are five likelihood categories that have been defined: “Likely, Probably, Maybe, Probably Not, and Unlikely”. Each category has listed underneath a range of probabilities that define how likely a cause must be in order for a cause to earn that category rating. The highest rating, “Likely” is set at greater than 15%.

Although 15% might not initially seem very likely at first, overall the likelihood rating system provided is a bit generous and many likelihood rating systems used professionally are far more stringent. This step will probably require the largest estimations on your part and it is common that people underestimate the likelihood associated with a potential cause. Having a seemingly lower percentage threshold for your most likely likelihood category, like 15%, can also help your team treat their more probable causes more seriously as they often should be. You are again perfectly welcome to establish your own likelihood rating system, changing either the criteria for the various categories or even the number of categories. The important thing is that you have a formal objective means for quantifying the likelihood of all effects/causes.

**Step 5 is Complete When**: Your likelihood rating system is complete and a likelihood rating is assigned to each cause. Typically a number is given to each likelihood rating with the most likely category being associated with the highest number. The “RiskTable” sample shows the associated numbers in row 4 and the SampleRiskBrainistormingPMB.xlsx file uses these numbers to represent the likelihood category assigned to each of its causes.

**Step 6:** Combine the severity rating and the likelihood rating to determine the overall risk associated with each effect/cause. Although there are many ways to quantify risk, a simple and objective means for doing so given your previous steps is to simply multiply the severity rating number with the likelihood rating number. The larger the resulting product, the more risk associated with the possible cause. This product is sometimes referred to as a Risk Priority Number or RPN.

Typically risk is also characterized in terms of a risk rating, similar to the way severity and likelihood rating systems were established earlier. RPN can be useful for determining the risk rating criteria and this was done in the “RiskTable” sample as well. In Column L, RPN thresholds have been created for 5 risk rating categories “High Risk, Medium High Risk, Medium Risk, Medium Low Risk, and Low Risk”. These risk ratings are sometimes also referred to as Risk Criticality or Corrective Action Priority categories. Each category is also assigned a color to represent itself as is shown in Column J of the “RiskTable”

In combining the severity and the likelihood rating categories into a matrix, each one of the cells can also be assigned its own RPN as is shown in the “RiskTable” sample. Then each cell can be colored according to its risk rating to produce the gradient-like view of that ranges from Negligible & Unlikely effect/causes being low risk up to Catastrophic & Likely effect/causes being high risk.

Matrices colored like this are sometimes referred to as a “Gradient Chart” or because the matrix was colored with primarily red, yellow, and green colors it could also be referred to as a “Stoplight Chart”.

**Step 6 is Complete When:** A risk rating system has been established and all of the effect/causes have been assigned a risk rating.

**Step 7:** For each possible cause, list potential corrective action(s) to address that cause. Corrective actions commonly are:

* changes to the design or project plan to prevent a failure
* actions that lessen the severity of the effect/cause should it be realized
* actions that lessen the likelihood of a possible cause
* alternative plans should the original concern be realized

Short phrases are often acceptable when writing these in a spreadsheet format. However, in order to make the spreadsheet easier to read, sometimes the column entry may simply be a reference to another document, i.e. “Please see the timeline alternative plan B”.

Many times the effects/causes that are associated with the highest risk are dealt with first or given the most attention. However, it is not uncommon that by going through this process that simple corrective actions can be identified to eliminate a number of medium or lower risks fairly easily and hence allow you to produce a far more robust design with relatively minimal effort.

**Step 7 is Complete When:** Corrective actions are attempted to be created for at least all high and almost all medium high risk potential concerns. An overview of these risks and associated mitigation/alternative plans should be included in the application.

**Step 8:** Create new columns for Adjusted Severity, Adjusted Likelihood, and Adjusted Risk Ratings. These “Adjusted” columns represent what the new severity, likelihood and resulting risk would be now that you have come up with your corrective actions.

An obvious benefit to doing this is that it can help you decided which corrective actions would be most worthwhile. More so however it can be a very useful tool to communicate to other teammates or your boss the importance of the corrective actions. Similarly it is also useful for demonstrating to outsiders that you have taken identifying risks very seriously and that you have effective means for dealing with these risks.

**Step 8 is Complete When**: Adjusted severity, adjusted likelihood, and adjusted RPN and/or risk ratings have been assigned to all effect/causes that have corrective actions associated with them.

**Step 9:** (optional) Assign an estimate on the additional effort and resources required to implement the corrective actions. This can be a very useful step in deciding which corrective actions should be implemented. It is usually best to have developed a timeline or an objective means of quantifying effort before attempting this step.

**Step 9 is Complete When:** Effort and resources required have been added for all of the corrective actions. Separate columns may be added for the effort and the resources required.

**Step 10:** (optional) Add a Troubleshooting Actions column. This step is usually completed towards the end of the design implementation phase of your project. From completing the earlier steps you have already listed potential losses of functionality that a user may notice and you have a list of possible causes associated with the losses of functionality. For each failure modes possible cause, list the troubleshooting actions that should take place.

Sometimes in order to make the spreadsheet easier to read, the column entry may simply be a reference to another document, i.e. “Please see the Motor Calibration Section of the Final Report”.

**Step 10 is Complete When:** troubleshooting actions have been listed for at least all of the Likely and Probably likelihood causes.

**SampleRiskBrainistormingPMB.xlsx Discussion**

The file SampleRiskBrainistormingPMB.xlsx provides a small but worthwhile example of the brainstorming risk process for the IR Sensor Encoder subsystem. When first thinking about just this one small sensor failing, initially you may think, “Big deal if the simple IR encoder sensor fails. Things just won’t work right.” but this example provides a good demonstration on how this process can be valuable.

In a first attempt at creating the chart, the failure mode and associated potential effect might look something like the one below. Notice that the failure mode is listed as “Reported number of rotations from the IR sensor is incorrect” and does not specify whether the error is in reporting more or less rotations. The reason it isn’t specified at the beginning is because at this early attempt the author doesn’t believe it would make a difference. In fact, the author may even feel that there is little to be gained from this and feel if there’s some problem with the sensor again it will be “no big deal” and the author when simply deal with whatever problems might show up.

|  |  |
| --- | --- |
| **Failure Mode** | **Failure Effects** |
| Reported number of rotations from the IR sensor is incorrect | Demand incorrectly calculated.  Energy storage is used (more, less? … |

The notion that there may be more to this failure mode begins to become clear when the author began listing out the effects. Tracing through the subsystems, if the reported number of rotations is incorrect, this would cause the calculated demand to be incorrect as well. Then if the demand is incorrect, it would cause the controllers to use more or perhaps less stored energy depending on whether the demand was reported as being higher or lower than it should be. The demand error however is either higher or lower depending on whether the reported rotations are lower or higher.

This lack of detail in the failure mode that leads to uncertainty in the effects tells the author that it is worthwhile to split the failure mode into 2 cases, one where the reported number of rotations is less than it should be and one where it’s more. This is also shown in sample file, an excerpt of which is shown below.

|  |  |
| --- | --- |
| **Failure Mode** | **Failure Effects** |
| Reported number of rotations from the IR sensor is too few | Demand incorrectly larger than necessary, Energy usage is larger than necessary, Bicycle goes far faster than desired |
| Reported number of rotations from the IR sensor is too many | Demand incorrectly as smaller than necessary, Energy storage is conserved or even increased more than it should be, Bicycle goes far slower than desired |

Now the failure modes have been refined to make the effects clear and precise. However the effects do not stop at just the stored energy usage. Examining the failure mode where the number of rotations is higher, this would mean that the perceived speed would be higher and hence the demand is lower. This in turn would cause the energy storage use to be actually lower, and the bicycle acceleration would be lower as well. This might affect some of the performance measure results but ultimately the system still runs and so the severity of this effect is probably fairly low, i.e. “no big deal” just like the author originally thought. But at least the author has some documentation to show that they investigated this potential failure.

However, looking at the other failure mode, where the number of rotations is lower, this means that the perceived speed would be lower and hence the demand would be higher. This in turn would cause the energy storage use to be actually higher, and the bicycle acceleration would be higher as well. In fact, it’s now not hard to imagine that if this reported rotations failure continued, the bike could continue to accelerate out of control (to potentially its maximum capability!). This is dangerous; especially dangerous considering one of the test cases is city street driving.

You could say, “yeah they can just go into manual override mode and disconnect the PMB” and yes it is good that you have already thought about having a manual override mode as a bicycle going out of control in city streets could be quite dangerous. However, the manual override mode is hardly the desired mode of operation and whenever possible its best not to have to rely on quick thinking from the operator, particularly a panicked one whose bike is out of control.

Overall this seemingly simple failure mode has now been identified as a source of significantly severe impact and is given a high (catastrophic) severity rating. The author is suddenly motivated to list potential causes for this error and determines that either the emitter or the receiver could become easily partially covered from dust on the road and so the author lists this as one potential cause with a high probability rating. Another cause is determined from looking at the potential component’s data sheet, which reveals that whenever these sensors begin to go bad, they often exhibit this kind of failure. This second cause is also listed, but given a medium likelihood rating as the author finds enough information on the data sheet about their reliability to justify it. Now since the 2 possible causes have different likelihoods (and might also have different corrective actions later on) the two causes are split into two different rows as highlighted in the table excerpt below.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure Mode** | **Failure Effects** | **Possible Cause** | **Severity** | **Likelihood** | **Risk Priority Number** | **Risk Level** |
| Reported number of rotations from the IR sensor is too few | Demand incorrectly larger than necessary, Energy usage is larger than necessary, Bicycle goes far faster than desired | sensor detector or emitter is partially blocked or damaged, | 4 | 5 | 20 | HIGH |
| sensor detector or emitter is damaged | 4 | 2 | 8 | MEDIUM |

Combining the high severity and likelihood, it becomes clear that this is a high risk problem and it is marked as such. This then leads the author to consider potential corrective actions. A number are generated but one of the most promising may be the inclusion of a second IR encoder sensor. This is redundant but redundancy in this case may be able to significantly lower the likelihood of the failure mode because both will need to fail at the same time to happen.

This does come at the cost of paying for and building 2 IR sensor encoders and it also effects the requirements of what the Sensor Filter subsystem will have to handle. Now the Sensor Filter subsystem will have to do additional tasks such as resolve the two different sensors readings into one and detect whether there is an error occurring with one and perhaps prompt user intervention if there is. Ultimately this results in significant additional effort for at least the IR Sensor Encoder subsystem and the Sensor Filter subsystem, but it is good that it is determined early so that the overall project plan and the designs can be adjusted to take into account these additional efforts.

The possibility of using a COTS encoder or a pair of COTS encoders is also considered as an alternative plan, as can be seen farther down the row of this failure mode in the sample file. Although this option is lower risk, there are also the rest of the performance measures to consider as well and these COTS encoders will certainly cost more. So a decision will have to be made to weigh what options are better given the various risks and performance measure considerations. Timelines may be updated to determine when a decision must be made by and additional tests may be created before then to more accurately ascertain the likelihood or severity of various risks.

There is not always a clear answer but far more times than not this brainstorming risk process can help lead you to a more confident direction. In fact you might have already formed your own opinion as to what option you would pursue in this case and feel that you could justify your decision as a result of what was explored through this brainstorming risk process.

The format for this process shown here is sometimes referred to as a kind of Failure Modes and Effects Analysis (FMEA, and sometimes pronounced FEE-Ma). You may not determine all of all possible failure modes, effects, and/or causes especially as you are doing this for the first time but try your best to capture the failure modes, effects and causes that will lead to the greatest risks. Even if you don’t catch all of the important ones and one of these important risks is realized, it is still very valuable to think back as to maybe how you could have caught that risk, or maybe you’ll realize there wasn’t enough information for you to make that assessment at that point. Either way, reflecting on process can help you develop this key analysis skill and be all the better prepared for the next challenge you take on.