Для выполнения лабораторных работ необходимо выбрать систему (система, которая может нанести ущерб или травмирование человека / гибель), состоящую минимум из четырех компонентов. Эту систему можно использовать для выполнения трех лабораторных работ. Для выполнения лабораторных работ можно использовать ГОСТ 51901-5, 61511-3, 61508-5, 61508-6.

Лабораторная работа №2. Анализ дерева неисправностей (FTA)

Для выполнения этой лабораторной работы можно ознакомиться и пользоваться ГОСТ 51901-5, прим. страница 13 (Анализ дерева неисправностей). В дереве неисправностей конечным событием будет являться опасностью.

Лабораторная работа №4. Перечень угроз и опасностей

Перечень угроз и опасностей должен описывать характеристику каждой опасности системы (подсистемы), причины, которые могут вызвать опасность, опасные события и последствия их возникновения, а также методы и мероприятия, контролирующие правильность выполнения ответственных функций и переводящие систему в безопасное состояние.

Дополнительно для каждого опасного события можно описать метод нормирования (GAMAB, ALARP, MEM)., который будет применяться на следующем этапе жизненного цикла функциональной безопасности – анализ (оценка) рисков.

Анализируя деревья опасностей (FTA), которые проектировались в лабораторной работе №2, должны выделить опасности системы.

При не обнаружении опасностей наступает опасное событие, которое считается отказом защитных мер системы.

Необходимо учитывать связь с внешними системами (соседними подсистемами).

Программные ошибки также влияют на работу функций. Для проверки правильной работы программных компонентов необходимо использовать контролирующие функции, которые переводят систему в безопасное состояние в случае наступления отказа. Здесь необходимо определить, что будет являться для рассматриваемой системы безопасным состоянием.

Таблица 1 - Пример перечня угроз и опасностей

Опасность: Падение грузчика				
Угроза	Последствия	Причины возникновения	Контроль исполнения	Действия при возникновении отказа
Опрокидывание погрузчика и/или падение груза из-за превышения допустимого веса	1. Материальный ущерб; 2. Травмирование человека.	1. Превышение максимально допустимого веса груза; 2. Отсутствие или недостаточный контроль за весом груза перед погрузкой.	1. Самодиагностика компонентов системы; 2. Контроль наличия связи с внешними системами; 3. Диагностика работы программного обеспечения; 4. Вывод информации о полученной команде на дисплей оператора.	1. Отправление команды на торможение до полной остановки; 2. Проведение осмотра погрузчика на предмет повреждений.

Лабораторная работа №5. Анализ рисков

Анализ рисков необходим для идентификации возможных опасностей (неисправностей), возникающих во время работы системы, выявления последствий данных опасностей – оценки степени влияния возможных отказов на перевозочный процесс, а также вероятность наступления негативных последствий, касающихся жизни людей и материальных угроз, а также для определения уровней рисков, связанных с этими опасностями.

Под опасностью понимается потенциальный источник возникновения ущерба. Опасное событие – это событие, которое может причинить вред. Критерием опасного отказа является необнаруженная неисправность в работе системы. Неисправность в целом описывает любой отказ системы, который может быть связан с работой с недостоверными данными, систематическими или случайными ошибками программного или аппаратного обеспечения соответственно, а также работой других систем, результаты которых важны для корректной работы системы.

Задачей анализа риска является получение объективной информации о наличии, либо отсутствии необходимости принятия дополнительных мер, направленных на снижение или предотвращение ущерба инфраструктуре и травматизма людей от отказов системы.

Отчет должен состоять из следующих глав и подглав:

1 Определение области применения анализа рисков

1.1 Определение задач анализа рисков

1.2 Определение системы

2 Идентификация рисков и предварительная оценка последствий

Для решения поставленной задачи должны быть идентифицированы опасности, являющиеся причиной риска, а также пути, по которым возникают опасности. Для идентификации опасности применяются формальные методы.

Здесь нужно описать как идентифицируете опасности, как их обнаруживаете, какие используются методы и виды анализа

3.1 Анализ частоты

Анализ частоты используется для оценки вероятности каждого нежелательного события, идентифицированного на стадии идентификации опасностей. Для оценки частот происходящих событий применяется экспертный метод.

Уровни частот возникновения событий делятся следующим образом:

1. частое событие – постоянное наличие опасности;
2. вероятное событие – ожидается частое возникновения опасного события;
3. случайное событие – ожидается неоднократное возникновения опасного события;
4. редкое событие – возможное возникновения событие на протяжение жизненного цикла системы;
5. крайне редкое событие – возникновение опасного события в исключительных случаях;
6. маловероятное событие – опасное событие не возникает.

3.2 Анализ последствий

Анализ последствий используется для оценки вероятного воздействия, вызванного нежелательным событием.

Уровни тяжести последствий делятся следующим образом:

1. катастрофический – гибель более одного человека или повреждение объекта подвижного состава до степени исключения из парка;

2. критический – гибель одного человека, серьезные травмы нескольких людей, повреждение подвижного состава, требующее проведение капитального ремонта для восстановления его работоспособности;
3. несущественный – серьезное травмирование человека или повреждение подвижного состава, требующее проведения среднего ремонта для восстановления его работоспособности;
4. незначительный – легкий вред здоровью человека или повреждение подвижного состава, требующее проведение текущего ремонта для восстановления его работоспособности.

3.3 Расчет уровня риска

Сопоставляя результаты анализов частот и последствий, определяется уровень риска в зависимости от нахождения в ячейке матрицы рисков.

Таблица 2 – Матрица рисков

Уровень частоты	Уровни тяжести последствий			
	Незначительный	Несущественный	Критический	Катастрофический
Частое	Нежелательный	Недопустимый	Недопустимый	Недопустимый
Вероятное	Допустимый	Нежелательный	Недопустимый	Недопустимый
Случайное	Допустимый	Нежелательный	Нежелательный	Недопустимый
Редкое	Не принимаемый в расчет	Допустимый	Нежелательный	Нежелательный
Крайне редкое	Не принимаемый в расчет	Не принимаемый в расчет	Допустимый	Допустимый
Маловероятное	Не принимаемый в расчет	Не принимаемый в расчет	Не принимаемый в расчет	Допустимый

Вывод