### **Nội dung gốc (tiếng Nga):**

**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.

**Bài thực hành số 4. Danh sách các mối đe dọa và nguy hiểm**

Danh sách các mối đe dọa và nguy hiểm phải mô tả đặc điểm của từng mối nguy trong hệ thống (hoặc phân hệ), các nguyên nhân có thể gây ra mối nguy hiểm, các sự kiện nguy hiểm và hậu quả của chúng, cũng như các phương pháp và biện pháp kiểm soát để đảm bảo các chức năng quan trọng được thực hiện đúng cách và đưa hệ thống về trạng thái an toàn.

Ngoài ra, đối với mỗi sự kiện nguy hiểm, có thể mô tả phương pháp tiêu chuẩn hóa (GAMAB, ALARP, MEM), sẽ được áp dụng ở giai đoạn tiếp theo trong vòng đời an toàn chức năng – phân tích (đánh giá) rủi ro.

Phân tích cây nguy hiểm (FTA), được thiết kế trong bài thực hành số 2, cần xác định các mối nguy của hệ thống.

Nếu không phát hiện ra mối nguy hiểm, một sự kiện nguy hiểm sẽ xảy ra, được coi là sự thất bại của các biện pháp bảo vệ hệ thống.

Cần tính đến sự kết nối với các hệ thống bên ngoài (các phân hệ lân cận).

Lỗi phần mềm cũng ảnh hưởng đến hoạt động của các chức năng. Để kiểm tra tính đúng đắn của các thành phần phần mềm, cần sử dụng các chức năng kiểm soát giúp đưa hệ thống về trạng thái an toàn trong trường hợp xảy ra lỗi. Ở đây, cần xác định trạng thái nào được coi là an toàn đối với hệ thống đang xem xét.

**Таблица 1 - Пример перечня угроз и опасностей**

**Опасность:** Падение груза

| **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. |

**Bảng 1 - Ví dụ về danh sách các mối đe dọa và nguy hiểm**

**Nguy hiểm:** Rơi hàng hóa

| **Mối đe dọa** | **Hậu quả** | **Nguyên nhân phát sinh** | **Kiểm soát thực hiện** | **Hành động khi xảy ra lỗi** |
| --- | --- | --- | --- | --- |
| Lật xe nâng và/hoặc rơi hàng do vượt quá trọng lượng cho phép | 1. Thiệt hại vật chất; 2. Chấn thương con người. | 1. Vượt quá trọng lượng hàng hóa tối đa cho phép; 2. Thiếu hoặc kiểm soát không đầy đủ trọng lượng hàng trước khi xếp. | 1. Tự động chẩn đoán các thành phần hệ thống; 2. Kiểm soát kết nối với các hệ thống bên ngoài; 3. Chẩn đoán hoạt động của phần mềm; 4. Hiển thị thông tin về lệnh nhận được trên màn hình điều khiển. | 1. Gửi lệnh phanh cho đến khi dừng hoàn toàn; 2. Kiểm tra xe nâng để phát hiện hư hỏng. |

### **Bài thực hành số 4: Danh sách các mối đe dọa và nguy hiểm**

#### **1. Mô tả hệ thống và sơ đồ FTA**

Hệ thống đang được phân tích là một hệ thống chiếu sáng đơn giản, trong đó đèn có thể ngừng hoạt động do nhiều nguyên nhân khác nhau. Sơ đồ FTA (Fault Tree Analysis) được sử dụng để phân tích các nguyên nhân gốc rễ dẫn đến sự cố "ĐÈN KHÔNG SÁNG".

Sơ đồ bao gồm bốn nhóm nguyên nhân chính:

* **G1 - Mất nguồn điện**
* **G2 - Lỗi bộ chuyển đổi**
* **G3 - Hỏng dây dẫn**
* **G4 - Hỏng chính bóng đèn**

Mỗi nhóm nguyên nhân có thể bao gồm nhiều sự kiện con và nguyên nhân gốc rễ khác nhau.

#### **2. Danh sách các mối đe dọa và nguy hiểm**

| **Mối đe dọa** | **Hậu quả** | **Nguyên nhân phát sinh** | **Kiểm soát thực hiện** | **Hành động khi xảy ra lỗi** |
| --- | --- | --- | --- | --- |
| Mất nguồn điện (G1) | Đèn không sáng | 1. Mất điện tổng (BE1.1)2. Hỏng rơ-le chính (BE1.2)3. Cháy cầu chì (BE1.3) | 1. Kiểm tra định kỳ hệ thống điện2. Bổ sung bộ nguồn dự phòng (UPS)3. Giám sát điện áp đầu vào | 1. Kích hoạt nguồn dự phòng2. Kiểm tra lại trạm biến áp và rơ-le |
| Lỗi bộ chuyển đổi (G2) | Đèn không sáng | 1. Hỏng công tắc (BE2.1)2. Lỗi bộ nguồn phụ (BE2.2) | 1. Định kỳ kiểm tra thiết bị chuyển đổi2. Cảnh báo sự cố trên hệ thống giám sát | 1. Thay thế công tắc lỗi2. Kiểm tra lại bộ chuyển đổi |
| Hỏng dây dẫn (G3) | Đèn không sáng | 1. Đứt dây (BE3.1, BE3.2)2. Ngắn mạch do nước (BE4.1)3. Hỏng dây do động vật gặm nhấm (BE4.2) | 1. Sử dụng dây dẫn cách điện chất lượng cao2. Kiểm tra định kỳ để phát hiện sự cố | 1. Kiểm tra hệ thống dây dẫn2. Cách ly vùng bị ảnh hưởng |
| Hỏng bóng đèn (G4) | Đèn không sáng | 1. Bóng đèn cháy (BE5)2. Đui đèn không phù hợp (BE5.1)3. Đứt dây tóc bóng đèn (BE6) | 1. Kiểm tra chất lượng bóng đèn trước khi lắp đặt2. Sử dụng bóng đèn tiêu chuẩn | 1. Thay bóng đèn mới2. Kiểm tra lại đui đèn |

#### **3. Phân tích các biện pháp an toàn và giảm thiểu rủi ro**

Dựa trên sơ đồ và danh sách trên, các biện pháp sau được đề xuất để cải thiện độ an toàn và giảm nguy cơ lỗi hệ thống:

* **Đối với nguồn điện (G1):** Cần có bộ nguồn dự phòng và hệ thống giám sát nguồn điện.
* **Đối với bộ chuyển đổi (G2):** Kiểm tra và bảo trì công tắc, bộ đổi nguồn định kỳ.
* **Đối với dây dẫn (G3):** Dùng dây chống thấm nước, kiểm tra hư hỏng vật lý thường xuyên.
* **Đối với bóng đèn (G4):** Sử dụng bóng đèn chất lượng cao, kiểm tra đui đèn trước khi lắp đặt.

### **Kết luận**

Bài thực hành đã phân tích chi tiết nguyên nhân dẫn đến sự cố "đèn không sáng" bằng sơ đồ cây lỗi FTA, liệt kê các mối nguy hiểm, nguyên nhân, biện pháp kiểm soát và các hành động khắc phục. Đây là cách tiếp cận hữu ích để đánh giá rủi ro và đảm bảo hệ thống hoạt động ổn định.