



## ПРОГРАММА ОБУЧЕНИЯ 2024 г.

**Тема курса:** «Функциональная безопасность электронных / электронно-программируемых / электрических систем, связанных с безопасностью. ГОСТ Р МЭК 61508 и ГОСТ Р МЭК 61511, практическое применение. Проектирование систем противоаварийной автоматической защиты опасных производственных объектов».

Продолжительность: 36 часов.

Курс проводится для технологов ОПО, главных метрологов и специалистов по АСУ ТП эксплуатирующих организаций, проектных институтов, ПКО предприятий, компаний – системных интеграторов.

Курс разработан на основании многолетнего опыта проектирования и внедрения систем ПАЗ на Опасных Производственных Объектах в РФ и на основании требований ФЗ, ПБ, РД и ГОСТ:

- **116-ФЗ** «О промышленной безопасности опасных производственных объектов», в ред. 2015 г.
- **184-ФЗ** «О техническом регулировании», в ред. 2015 г.
- **Приказ Ростехнадзора № 533 от 25.12.2020** «Общие правила взрывопожаробезопасности для взрывопожароопасных химических, нефтеперерабатывающих, нефтехимических и нефтеперерабатывающих производств»
- **Приказ ФСТЭК России N 31 от 14.03.2014** «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»
- **РД 03-418-01** «Методические указания по проведению анализа риска опасных производственных объектов»
- **ГОСТ Р МЭК 61508** «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью»
- **ГОСТ Р МЭК 61511-1-2018** «Безопасность функциональная. Системы безопасности приборные для промышленных процессов»
- **ГОСТ Р МЭК 51901.11** «Менеджмент риска. Исследование опасности и работоспособности» (HAZOP). Принят в РФ в 2005 г.
- **ГОСТ Р 51901.12** «Менеджмент риска. Метод анализа видов и последствий отказов» (FMEA). Принят в РФ в 2001 г.
- **ГОСТ Р МЭК 61160** «Менеджмент риска. Формальный анализ проекта». Принят в РФ в 2006 г.
- **ГОСТ 34.602-89** «Техническое задание на создание автоматизированной системы»
- **РД 50-34.698-90** «Автоматизированные системы. Требования к содержанию документов»
- **ГОСТ 2.708-81** «Правила проектирования принципиальных электрических схем для цифровых вычислительных систем»

## Содержание курса:

### **Раздел I. Нормативная база в области промышленной безопасности (ПБ)**

- Структура (Федеральные законы, технические регламенты, ГОСТ, правила и рекомендации Ростехнадзор и МЧС, указы президента РФ, распоряжения правительства РФ).
- Взаимосвязь нормативных и технических документов в области ПБ.
- Требования НТД в области ПБ: 116-ФЗ, 225-ФЗ, 184-ФЗ 128-ФЗ, Общие правила взрывопожаробезопасности для взрывопожароопасных химических, нефтеперерабатывающих, нефтехимических и нефтеперерабатывающих производств - приказ РОСТЕХНАДЗОРА № 96, изменения, Приказ № 480 от 26.11.2015 г.)
- Допуск к деятельности, связанной с ПБ (аттестация, лицензирование, СРО).

### **Раздел II. Функциональная безопасность. Основы**

- Определение, потенциальные проблемы.
- Модель множественных слоёв защиты (LOPA). Слои предотвращения (снижения вероятности). Слои смягчения последствий (смягчение тяжести последствий).
- Приборные системы безопасности и виды отказов.
- История функциональной безопасности, основные стандарты, структура и назначение МЭК 61508 и 61511.
- Модель жизненного цикла, основы документирования (SRS, V&V, FSA).
- Гармонизация стандартов по созданию Автоматизированных Систем, ПБ и РБ Ростехнадзора и Жизненного цикла систем безопасности согласно ГОСТ Р МЭК 61508/61511.
- План безопасности (Safety Plan).
- План верификации и подтверждения соответствия - валидации (V&V Plan).

### **Раздел III. Анализ опасностей и рисков**

#### **Этап 1. Планирование анализа опасностей и рисков**

- Риск. Менеджмент риска. Составляющие риска. Уровни риска, приемлемый риск.
- Методы оценки риска. Уровни риска, принципы ALARP. Уровни полноты безопасности (УПБ/SIL).

#### **Этап 2. Идентификация опасностей (HAZID)**

- Этапы проектирования технологических объектов.
- Идентификация факторов опасности, метод проверочных листов (Check list).

#### **Этап 3. Оценка риска (HAZAN, HAZOP)**

- Методики анализа риска: дерево событий (ETA), дерево неисправностей (FTA).
- Исследование опасности и работоспособности (HAZOP): цель проведения, HAZOP на разных стадиях жизненного цикла опасного объекта, подготовка HAZOP, требуемые исходные данные, состав и функции членов рабочей группы, документирование, анализ результатов и практические выводы.

#### **Этап 4. Установления степени опасности аварий на ОПО, наиболее опасных частей ОПО**

#### **Этап 5. Разработка рекомендаций по уменьшению риска**

- Распределение требований к безопасности.
- Назначение Уровня Полноты Безопасности (УПБ/SIL) для приборных систем безопасности как слоя защиты (методы Графа рисков, матрицы рисков, LOPA).

### **Раздел IV. Техническое задание (ТЗ) на систему безопасности**

- Спецификация требований к системе безопасности (SRS).
- Состав исходных данных, требуемых для выполнения рабочего проектирования по системе ПАЗ.
- Кнопки аварийного останова.
- Полнота автоматических функций.

## Раздел V Выбор технических средств

- Основные концепции средств ПАЗ (ETS/DTS, низкая/высокая частота запросов, безопасность/ложные срабатывания), основные архитектуры (MoN).
- Архитектурные ограничения системы безопасности (HFT). Избыточность.
- Обзор типовых структур контроллеров ПАЗ.
- Оптимальный диапазон применимости контроллеров ПАЗ.
- Обзор способов самодиагностики контроллеров ПАЗ.

## Раздел VI. Подтверждение соответствия УПБ/SIL

(согласно Приказу Ростехнадзора № 96 п.6.3.4)

- Пример анализа соответствия контроллера уровню безопасности.
- Расчёт показателей надёжности МТТФ, PFD (методы FMEA, Марковские модели, блок-диаграммы RBD), глубина диагностики (SFF), интервалы проверочных испытаний.
- Тестирование клапанов с неполным ходом (PST).
- Сертификация технических средств по МЭК 61508/61511.

## Раздел VII. Требования к программированию систем ПАЗ

- Типовые проблемы, виды ПО, типы языков программирования, ограничения в зависимости от УПБ/SIL.
- Получение исходных данных, правила проектирования логических схем блокировок (ГОСТ 2.708-81, ГОСТ 2.743-82).
- Концепция байпасов (отключения защиты).

## Раздел VIII. Передача системы в эксплуатацию. Эксплуатация

- Заводские приёмочные испытания (FAT).
- Подтверждение соответствия безопасности (Validation) - приёмо-сдаточные испытания на объекте (SAT).
- Эксплуатация, обслуживание и ремонт.
- Модификация и изменение.
- Вывод из эксплуатации или ликвидация.

## Раздел IX. Кибербезопасность

- Требования к передаче данных.
- Уровни безопасности (SL – security level) по ГОСТ Р 56205-2014 - МЭК 62443-2-1:2009.
- Требования ФСТЭК, приказ № 31, по обеспечению кибернетической безопасности систем АСУ ТП.
- Типовые структурные схемы АСУ ТП для обеспечения функциональной и кибернетической безопасности.

## Лектор:

**В.А. Потехин** – Ген. директор ООО «СПБ-Экспертиза», эксперт по функциональной безопасности