Функциональная безопасность

Санкт-Петербург, 2025

Функциональная безопасность

- часть общей безопасности, которая относится к системам управления объектами и зависит от правильности функционирования систем, связанных с обеспечение безопасности
(ГОСТ Р МЭК 61508-4-2012)

- способность системы управления и обеспечения безопасности движения поездов выполнять требуемые функции безопасности при всех предусмотренных условиях эксплуатации в течение заданного периода времени
(ГОСТ Р 33358-2015)

Функциональная безопасность

- способность системы в процессе жизненного цикла не подвергать опасности человека, экономику и окружающую среду при возникновении отказов аппаратуры или ошибочных действий человека при разработке (как аппаратного так и программного обеспечения) и эксплуатации.

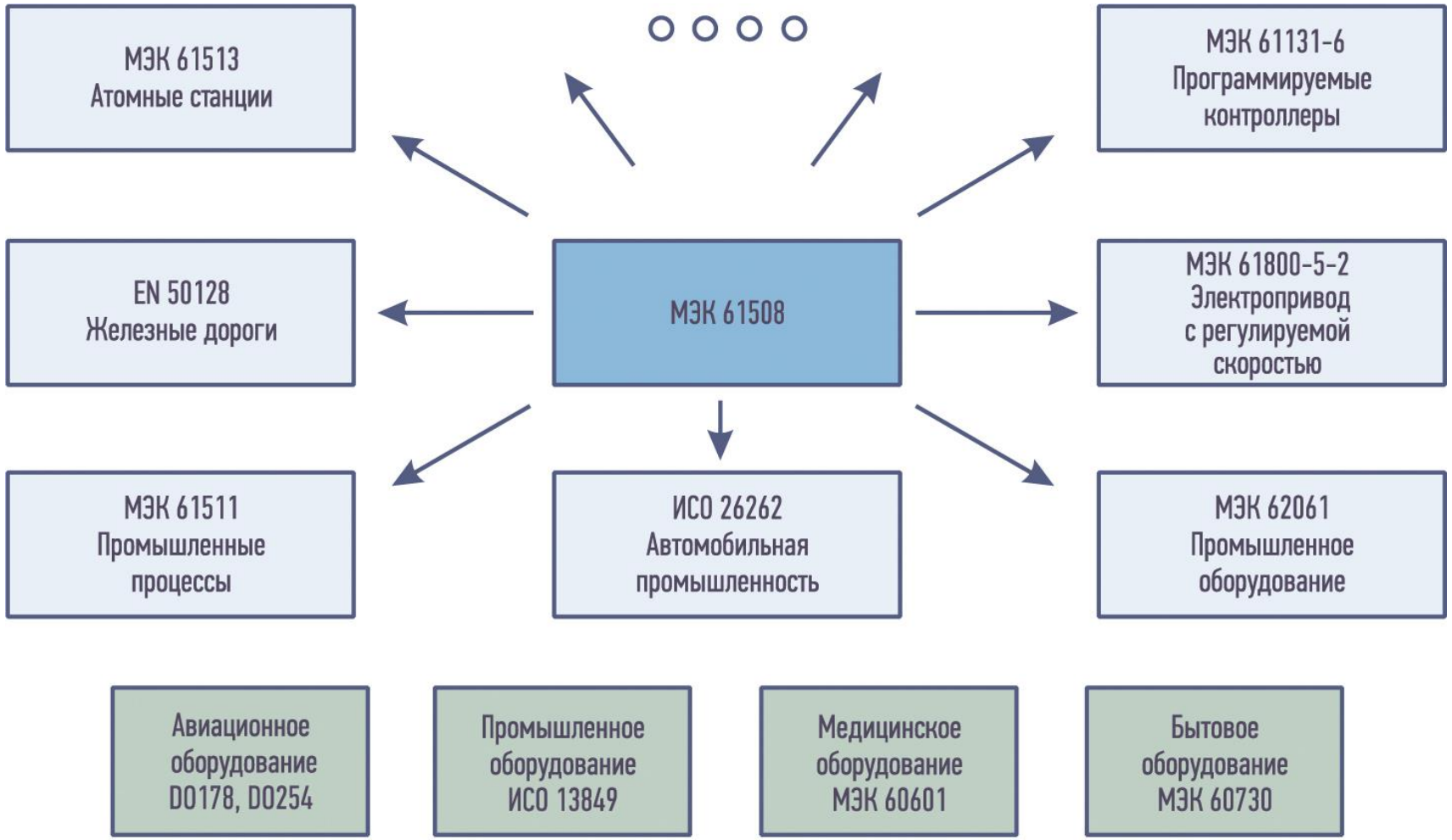
Характеризует:

- Надежность
- Отказоустойчивость АО
- Корректность ПО
- Защищенность от ошибок персонала

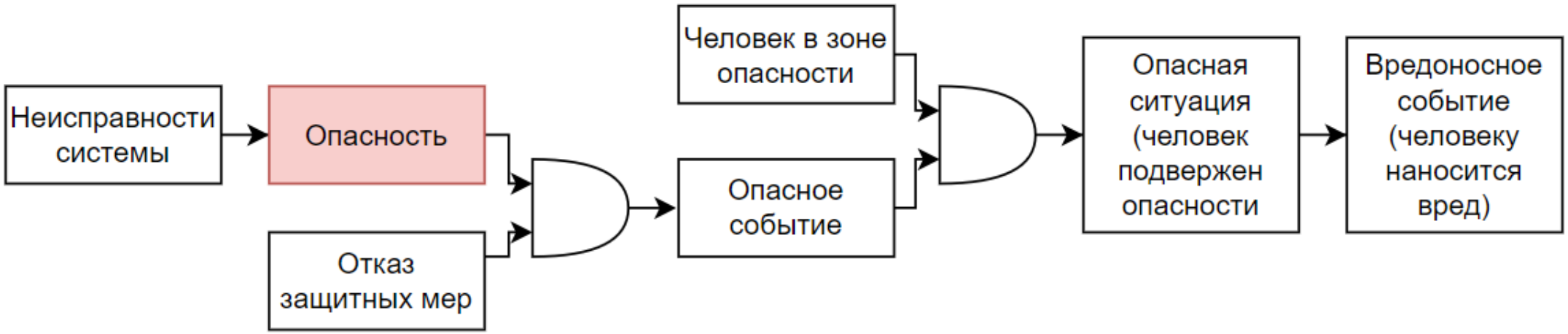
Разница?

Основы теории надежности	Функциональная безопасность
Цель	
Повышение общей надежности системы путем снижения вероятности отказов и увеличения времени безотказной работы	Предотвращение опасных ситуаций или снижение риска до приемлемого уровня в случае отказов системы
Подходы	
Предотвращение отказов	Реакция на отказ
Инструменты	
1. Статистический методы 2. Моделирование и испытания 3. Повышение надежности элементов	1. Методы анализа 2. Требования ФБ 3. Системные решения (реакция на отказ)

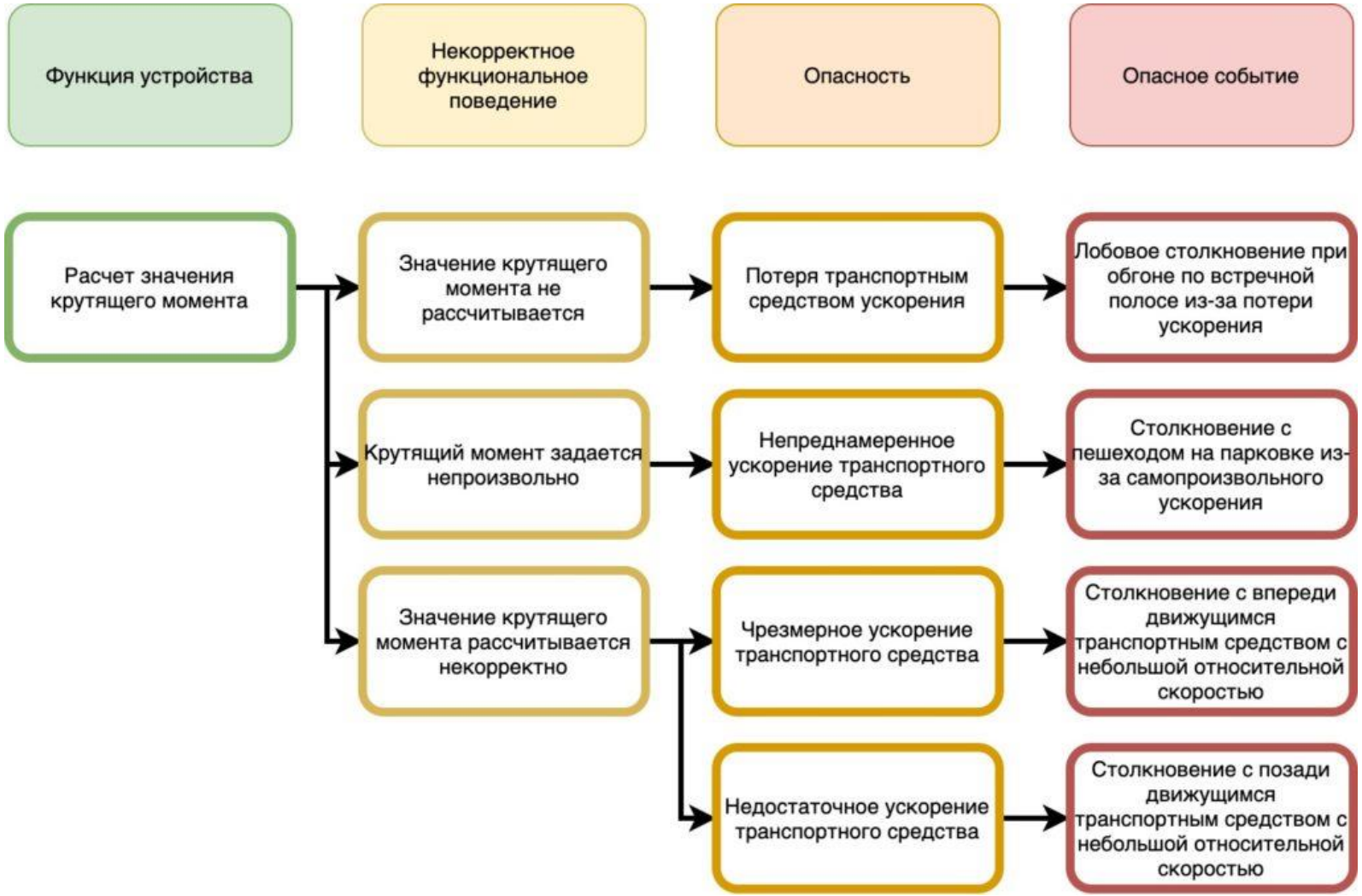
Стандарты и ГОСТ



Применение


Неисправности системы
Опасность
Отказ защитных мер
Человек в зоне опасности
Опасное событие
Опасная ситуация (человек подвержен опасности
Вредоносное событие (человеку наносится вред)

Хороший пример



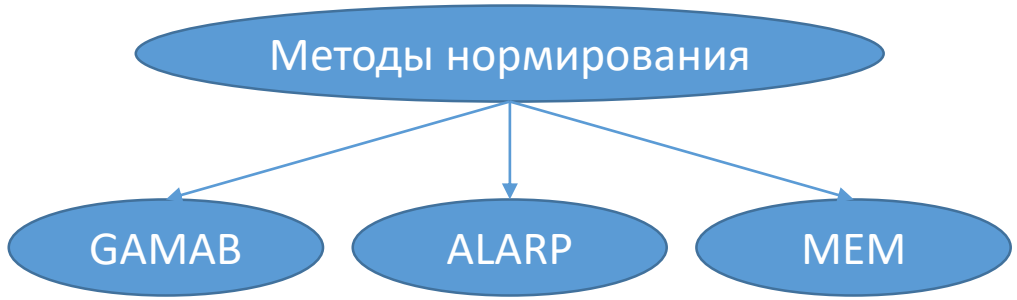
Как применять ФБ?

1. Знакомство с системой -> понимание системы
2. Ознакомиться со стандартами -> мат.часть
3. Идентификация опасностей -> выявление опасностей
4. Анализ рисков -> меры снижения, нормирование риска
5. Установить УПБ -> задача границы.
6. Внедрение -> макет, облик, образец, КД, ПД
7. Испытания -> ПМИ, обкатка, акты и протоколы
8. Доказательство безопасности -> ТР ТС, литера «О»

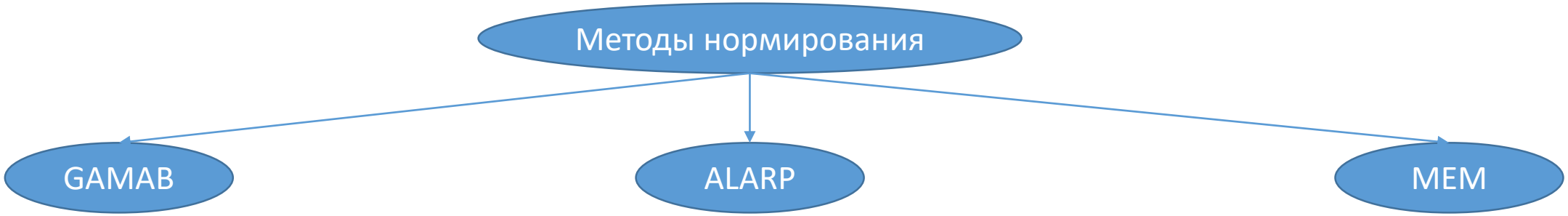
Этапы

1. **Перечень угроз и опасностей:** Угрозы, возможные последствия, влияние на внешние системы, причины возникновения, контроль правильности исполнения, действия при возникновении отказа, метод нормирования
2. **Анализ рисков:** FTA, уровни частоты, уровни последствий, матрица риска, меры и нормирование риска
3. **Установка УПБ**

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



Этапы



Globalement Au Moins Aussi Bon

Угроза, связанная с новой системой не должна повышать показатель минимальной эндогенной смертности для индивидуума

As Low As Reasonably Practicable

Minimum Endogenous Mortality

- Эндогенная смертность –это риск, учитывающий влияние технологических факторов на смертность в группе населения определенного возраста за год.
- Низкая величина смертности для возрастной группы от 5 до 15 пет.

Этапы

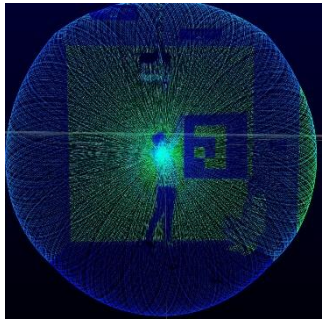
Полнота безопасности - степень уверенности в том, что система управления и обеспечения безопасности движения поездов будет выполнять заданные функции безопасности при данных условиях эксплуатации в заданный период времени.

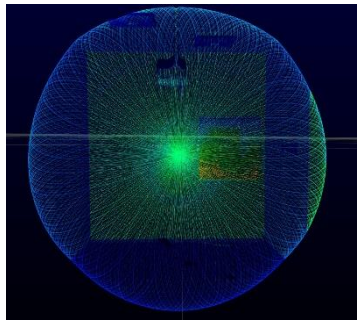
Уровень полноты безопасности	Целевое сокращение риска	PFDavg: средняя вероятность отказа выполнения по запросу	PFH: средняя частота отказов в час
УБП 4	100,000-10,000	$>=10^{-5}$ -$<10^{-4}$	$>=10^{-9}$ -$<10^{-8}$
УБП 3	10,000-1,000	$>=10^{-4}$ -$<10^{-3}$	$>=10^{-8}$ -$<10^{-7}$
УБП 2	1,000-100	$>=10^{-3}$ -$<10^{-2}$	$>=10^{-7}$ -$<10^{-6}$
УБП 1	100-10	$>=10^{-2}$ -$<10^{-1}$	$>=10^{-6}$ -$<10^{-5}$

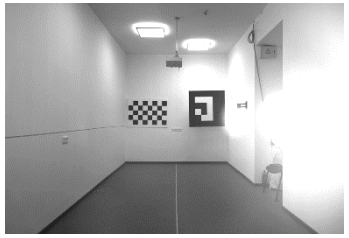
Уровень частоты, 1/год		Уровень тяжести последствий				
		1 и более пострадавших средней тяжести	1 пострадавший с причинением тяжкого вреда	1 погибший или от 2 до 10 пострадавших с причинением тяжкого вреда	От 2 до 5 погибших	Более 5 погибших
		Незначительный	Серьезный	Критический	Катастрофический	Бедственный
$\lambda >= 10^{-1}$	Частое	УПБ3	УПБ3	УПБ4	УПБ4	АСУ недостаточно
$10^{-2}<= \lambda < 10^{-1}$	Вероятное	УПБ2	УПБ3	УПБ3	УПБ4	УПБ4
$10^{-3}<= \lambda < 10^{-2}$	Случайное	УПБ2	УПБ2	УПБ3	УПБ3	УПБ4
$10^{-4}<= \lambda < 10^{-3}$	Редкое	УПБ1	УПБ2	УПБ2	УПБ3	УПБ3
$10^{-5}<= \lambda < 10^{-4}$	Крайне редкое	НСБ	УПБ1	УПБ2	УПБ2	УПБ3
$\lambda < 10^{-5}$	Маловероятное	НСБ	НСБ	УПБ1	УПБ2	УПБ2

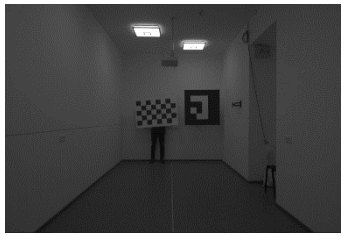
Этапы

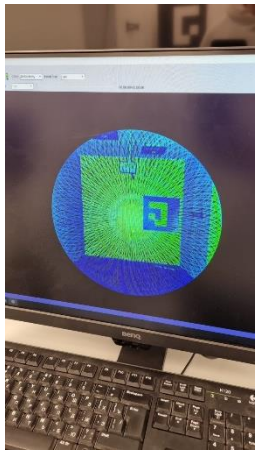
Моделирование или испытания?











Этапы

Доказательство безопасности - это итог всех мероприятий по ФБ, который показывает, соответствует ли система требованиям при ее проектировании, реализации и тестировании в соответствии со стандартами.