

МЕТОДЫ ОБЕСПЕЧЕНИЯ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ ИННОВАЦИОННЫХ СИСТЕМ НА ПРАКТИЧЕСКОМ ПРИМЕРЕ

Родиманова Екатерина Сергеевна

Главный специалист сектора функциональной безопасности
СПбФ АО «НИИАС»

Актуальность доказательства безопасности систем технического зрения

Кадровый дефицит на сети железных дорог

Угроза стабильности и эффективности перевозок в средне- и долгосрочной перспективе

Автоматизация функций машиниста

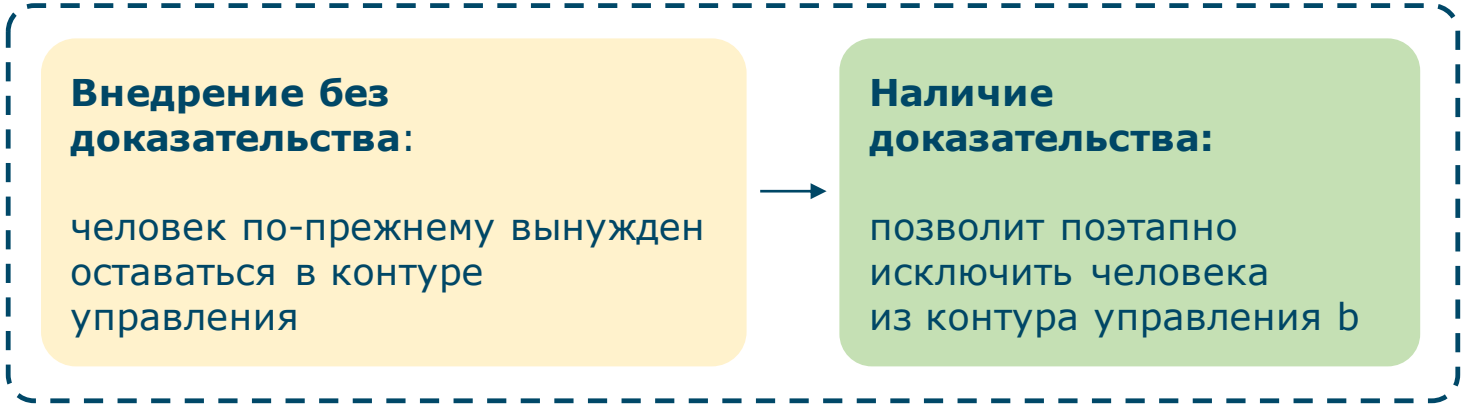
Необходима замена с воспроизведением функционала на достаточном уровне безопасности

Сложности верификации систем технического зрения

Низкая степень интерпретируемости и отсутствие формализованных подходов к верификации



Почему доказательство безопасности важно?



УПБ

Уровень полноты безопасности - дискретный уровень, соответствующий диапазону полноты безопасности

Полнота безопасности – степень уверенности в том, что система будет выполнять заданные функции безопасности при данных условиях эксплуатации в заданный период времени

Требования к системам технического зрения		
Функция	Уровень полноты безопасности по [11] ¹⁾	Средняя наработка до отказа ²⁾ по ГОСТ 27. 002, ч. не менее
Контроль свободности пути от препятствий системами технического зрения при автоматическом режиме управления железнодорожным подвижным составом ³⁾	[Значение 2 или 3 - в соответствии с приложением А (таблица А.2) настоящего стандарта]	50 000
ГОСТ 33435-2023, таблица А.1		

Уровень полноты безопасности	Средняя вероятность опасного отказа функции безопасности по запросу (PFD _{avg})
4	> 10 ⁻⁵ - < 10 ⁻⁴
3	> 10 ⁻⁴ - < 10 ⁻³
2	> 10 ⁻³ - < 10 ⁻²
1	> 10 ⁻² - < 10 ⁻¹
Уровень полноты безопасности	Средняя частота опасных отказов функции безопасности (PFH)
4	> 10 ⁻⁹ - < 10 ⁻⁸
3	> 10 ⁻⁸ - < 10 ⁻⁷
2	> 10 ⁻⁷ - < 10 ⁻⁶
1	> 10 ⁻⁶ - < 10 ⁻⁵
ГОСТ Р МЭК 61508-1-2012, таблица 2	

Существующие проблемы доказательства безопасности систем технического зрения



1

Отсутствие четких требований стандартов

ГОСТ Р МЭК 61508 и ГОСТ Р МЭК 62279 не подходят для систем технического зрения

11

таблиц требований

29

требований обязательны для УПБ2

63

требования обязательны для УПБ3

Нейронные сети как «чёрный ящик»: поведение сложно объяснить и предсказать

Нет прослеживаемости между слоями сети и требованиями

Обучение нейронных сетей стохастично: результаты нестабильны

Качество работы зависит от обучающей выборки

ГОСТ Р МЭК 61508-3-2018, таблица А.4

Пример таблицы с методами, которые необходимо применять на этапе детального проектирования

Метод / средство <1>	Ссылка	УПБ1	УПБ2	УПБ3	УПБ4
1a Методы структурных диаграмм <2>	С.2.1	HR	HR	HR	HR
1a Методы структурных диаграмм <2>	Таблица В.7	R	R	HR	HR
1c Формальные методы проектирования и усовершенствования <2>	В.2.2, С.2.4	-	R	R	HR
2 Средства автоматизированного проектирования	В.3.5	R	R	HR	HR
3 Программирование с защитой	С.2.5	-	R	HR	HR
4 Модульный подход	Таблица В.9	HR	HR	HR	HR
5 Стандарты для проектирования и кодирования	С.2.6, таблица В.1	R	HR	HR	HR
6 Структурное программирование	С.2.7	HR	HR	HR	HR
7 Использование доверительных/проверенных программных модулей и компонентов (по возможности)	С.2.10	R	HR	HR	HR

Существующие проблемы доказательства безопасности систем технического зрения

2

Безграничность возможных сценариев

Для оценки требуются наборы данных, покрывающие все возможные ситуации

Тестирование в реальных условиях
небезопасно, дорого и долго

Тестирование с применением симулятора:
требует подтверждения соответствия
реальным условиям и сертификации
используемого инструмента



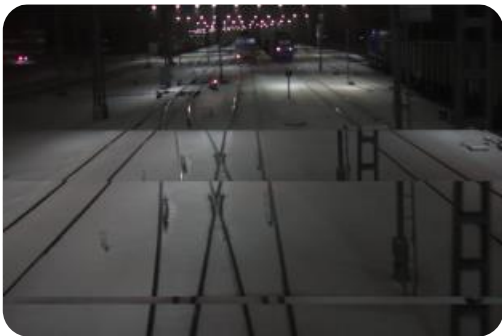
Существующие проблемы доказательства безопасности систем технического зрения

3

Входные данные влияют на работу

Даже незначительные отклонения во входной информации могут радикально повлиять на поведение алгоритма

Технические сбои



Физические явления

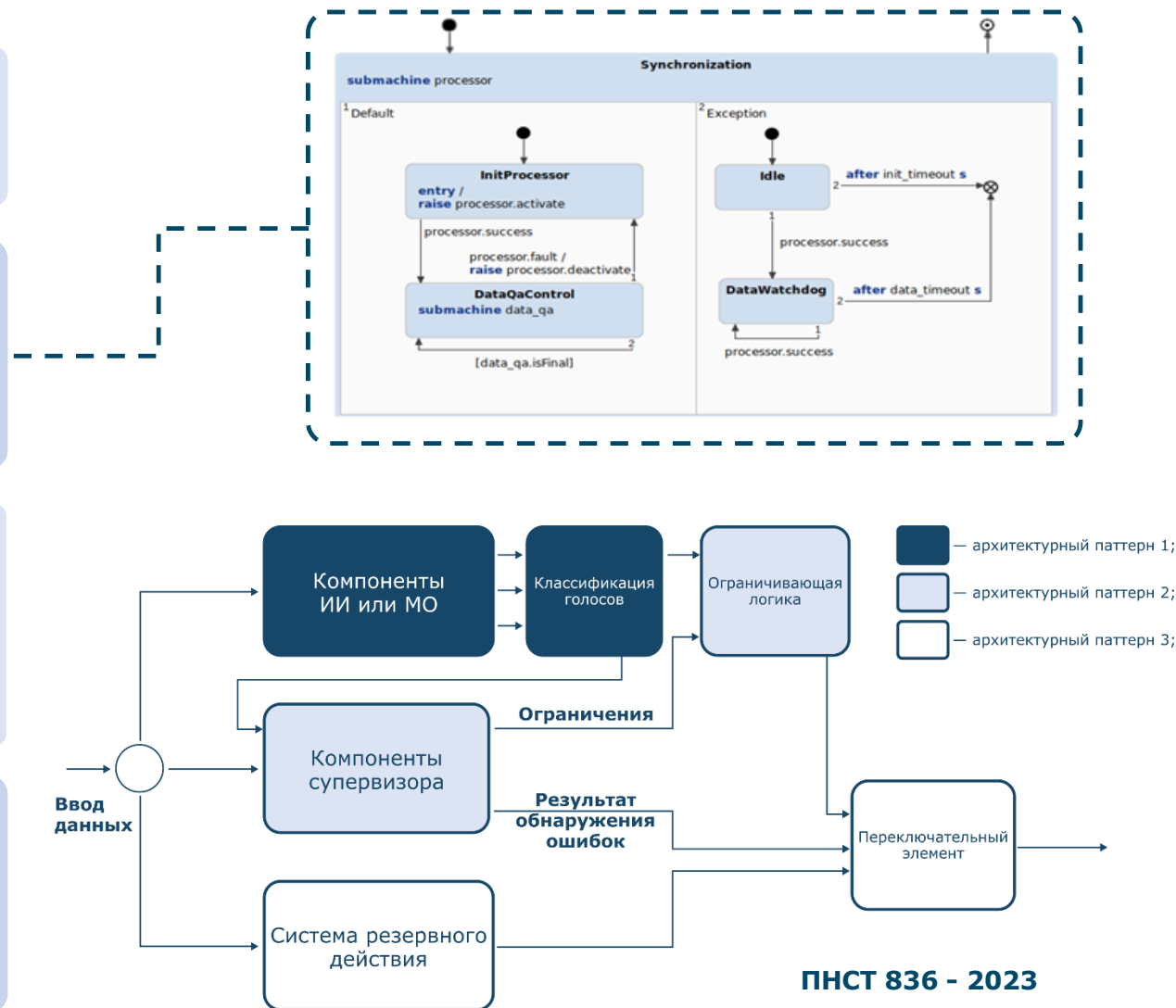


Ошибки алгоритмов обработки



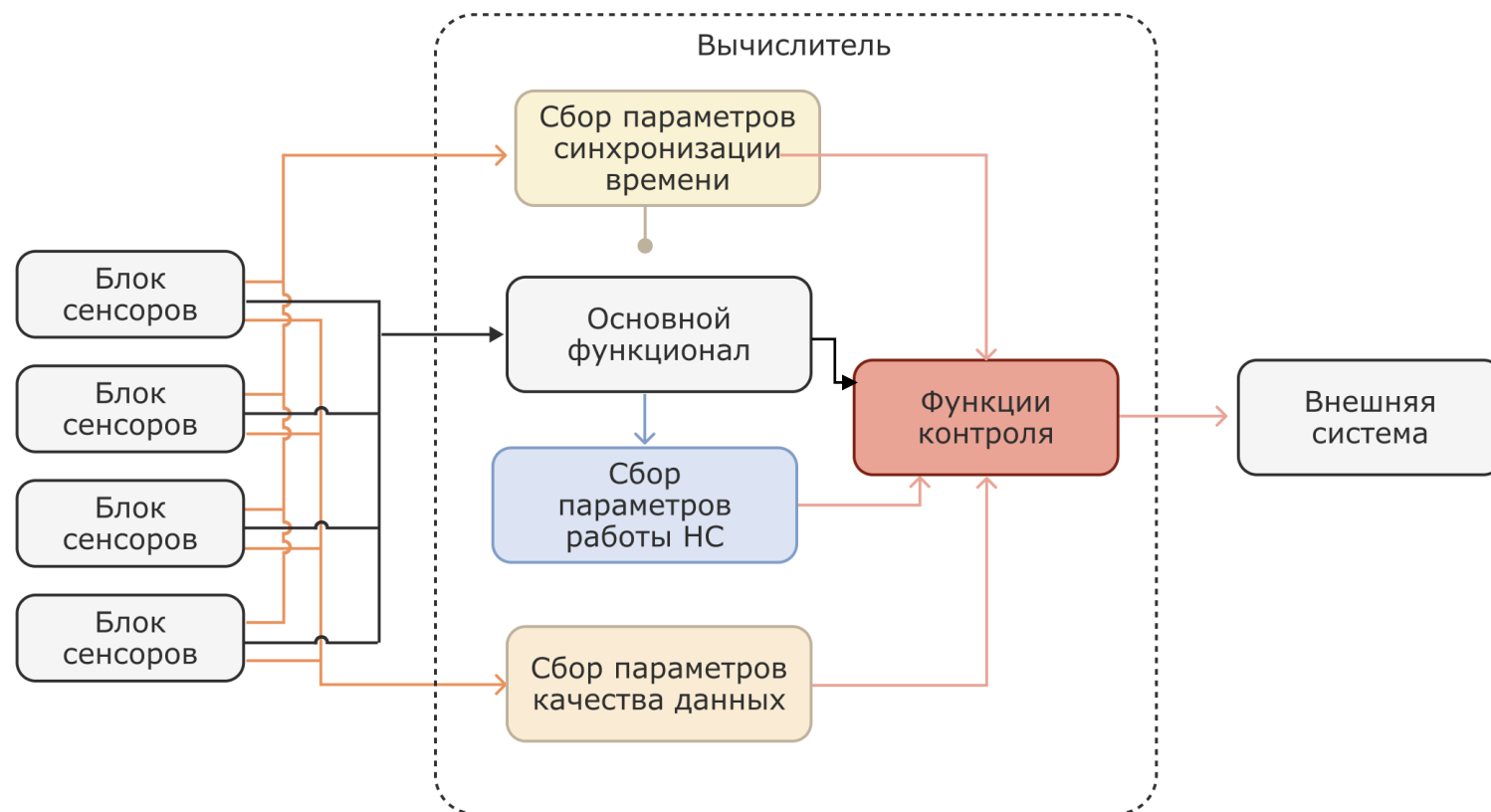
Предлагаемый подход для обеспечения безопасности систем технического зрения

- 1 Вынести функции безопасности в отдельный программный модуль**
- 2 Функции безопасности спроектировать в виде вложенной машины состояний с использованием сертифицированных инструментов кодогенерации**
- 3 Определить набор метрик и собрать статистику для дальнейшего принятия решений о правильности функционирования системы на каждом этапе обработки данных**
- 4 Спроектировать переход в защитное состояние при обнаружении выхода параметров за пределы граничных значений**



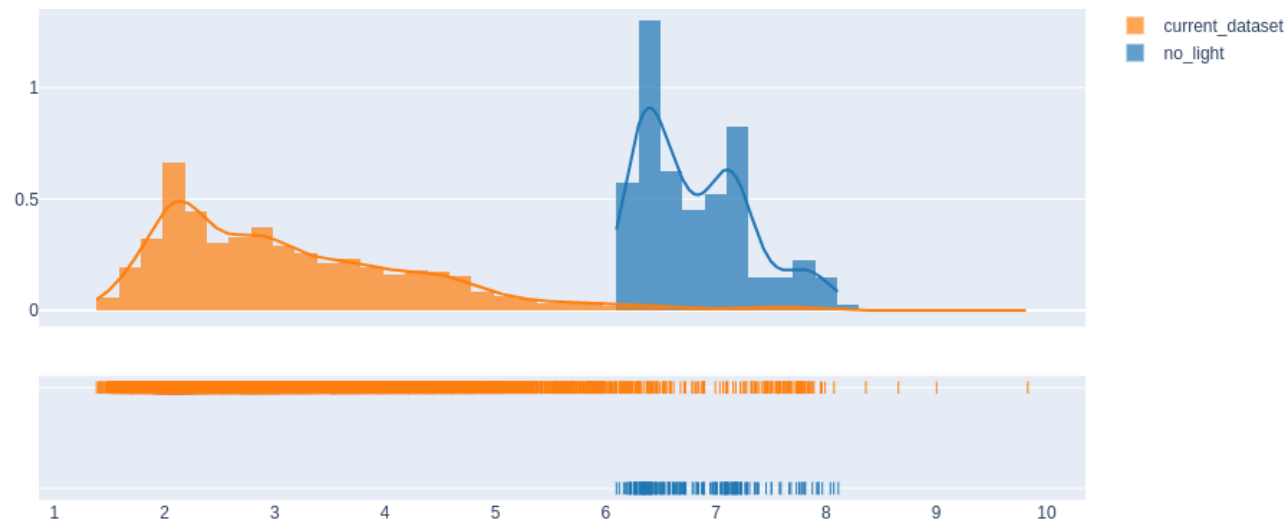
Модули ПО делятся на:

- **нейронные сети**
- алгоритмы, поведение которых не явно, полностью задается обучающими данными
- **классическое ПО**
- алгоритмы с четкой логикой, не привязанные к входным данным
- **data-driven алгоритмы**
- алгоритмы с четкой логикой, построенной на базе статистики

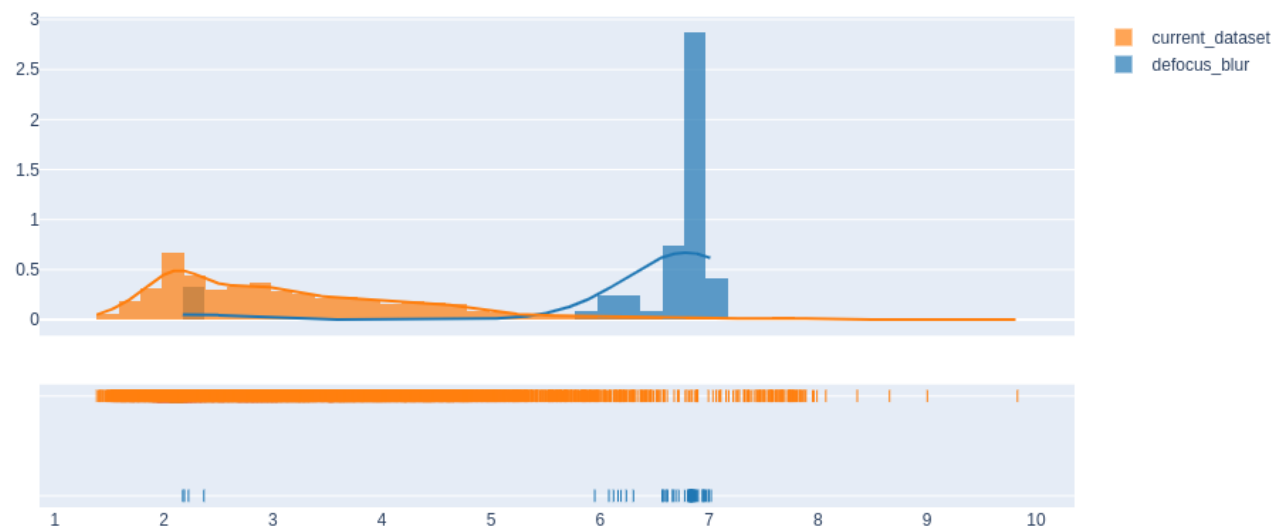


Фактическая реализация метода оценки качества ВХОДНЫХ ДАННЫХ

Отсутствие освещенности



Расфокусировка



Фактическая реализация метода оценки работы нейронных сетей

Прожектор локомотива



**Пиксели в зоне
локомотива имеют
высокую
неопределенность**

**Нейронной сети сложно
отличить класс «Фон»
и класс «Вагон»**

*чем больше неопределенность,
тем более синий цвет для наглядности*

Эффективность функции безопасности уже сейчас

Обнаружение ошибок НС,
потенциально опасных
с точки зрения безопасности



по метрикам объект обнаруживается
во всех случаях



нейронная сеть ошибочно определяет
людей как неизвестный объект



с другой камеры нейронная сеть
не видит объекты на пути

Эффективность функции безопасности уже сейчас

Улучшение процесса поиска и обработки ложных срабатываний на этапах отладки системы



переход в защитное состояние
показан фиолетовым цветом

Пример перехода в защитное состояние
при ошибках нейронной сети

Нейронная сеть считает «гуляющую»
тень на путях объектом в красной зоне





Спасибо за внимание!