

В. В. Скляр



ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ АСУТП

В СООТВЕТСТВИИ
С СОВРЕМЕННЫМИ СТАНДАРТАМИ



«Инфра-Инженерия»

В. В. Скляр

**Обеспечение безопасности АСУТП
в соответствии
с современными стандартами**

Методическое пособие

Инфра-Инженерия
Москва – Вологда
2018

УДК (665.6/7:681.5).002.2
ББК 35.514:32.965
С 43

ФЗ № 436-ФЗ	Издание не подлежит маркировке в соответствии с п. 1 ч. 4 ст. 11
----------------	---------------------------------------------------------------------

Скляр В. В.

С 43 Обеспечение безопасности АСУТП в соответствии
с современными стандартами: Методическое пособие./
В. В. Скляр. — М.: Инфра-Инженерия, 2018. — 384 с.

ISBN 978-5-9729-0230-9

Подробно рассмотрены требования к безопасности АСУТП международного стандарта МЭК 61508 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью», дана их интерпретация для практического воплощения. Последовательно раскрыты конкретные шаги, необходимые для получения сертификата соответствия МЭК 61508. Особое внимание уделено подготовке к сертификации, в том числе определению объекта сертификации, проектной инфраструктуры, плана и сметы затрат на выполнение работ. Рассмотрены требования стандарта, относящиеся к управлению безопасностью, предложены методы ее количественного оценивания и меры по ее обеспечению. Отдельно разобраны вопросы сертификации ПЛИС и применения методологии Assurance Case. Дан набор упражнений для закрепления навыков в области обеспечения и оценивания функциональной безопасности.

Для инженеров по АСУТП и специалистов в области IT, собирающихся сертифицировать системы управления и их компоненты на соответствие международным стандартам в области функциональной безопасности, а также для руководителей, желающих поднять безопасность АСУТП предприятия на новый уровень.

© Скляр В. В., автор, 2018

© Издательство «Инфра-Инженерия», 2018

ISBN 978-5-9729-0230-9

Содержание

ОБ АВТОРЕ	3
ВВЕДЕНИЕ	5
ГЛАВА 1.	
Изучаем МЭК 61508 и определяем структуру требований	11
1.1. Архитектуры компьютерных систем управления	11
1.2. Проблема обеспечения функциональной безопасности компьютерных систем управления	17
1.3. Стандарты, относящиеся к функциональной безопасности.....	22
1.4. Общие сведения о стандарте МЭК 61508	23
1.5. Термины в области функциональной безопасности согласно МЭК 61508-4	25
1.6. Структура требований к информационной и функциональной безопасности.....	35
1.7. Обзор содержания стандарта МЭК 61508	39
Выводы по разделу	47
Литература	48
Вопросы для самоконтроля	49
Практические задания.....	50
ГЛАВА 2.	
Запускаем проект сертификации	51
2.1. Общий алгоритм подготовительных работ по запуску проекта сертификации.....	51
2.2. Определение объекта сертификации и разработка концепции продукта	55
2.3. Управление проектом сертификации.....	60
2.4. Создание проектной инфраструктуры	63
2.5. Взаимодействие с сертифицирующим органом и внешним консалтингом.....	69
2.6. Разработка плана и бюджета проекта сертификации	71
Выводы по разделу	78
Литература	81
Вопросы для самоконтроля	81
Практические задания.....	82

ГЛАВА 3.

Формируем систему управления функциональной безопасностью

.....	83
3.1. План управления функциональной безопасностью	83
3.2. Управление персоналом	89
3.3. Управление конфигурацией	91
3.4. Выбор и оценивание инструментальных средств	97
3.5. Верификация и валидация	102
3.6. Управление документацией	103
3.7. Оценивание функциональной безопасности	106
Выводы по разделу	108
Литература	110
Вопросы для самоконтроля	110
Практические задания	111

ГЛАВА 4.

Измеряем показатели функциональной безопасности

.....	112
4.1. Атрибуты надежности, информационной и функциональной безопасности	112
4.2. Анализ рисков	119
4.3. Показатели надежности	121
4.4. Показатели функциональной безопасности	123
4.5. Примеры расчета показателей функциональной безопасности и надежности	128
4.6. Структурные схемы надежности	134
4.7. Анализ деревьев отказов	140
4.8. Марковские модели	144
4.9. Анализ видов, последствий и критичности отказов (ФМЕСА)	145
4.10. Модель отказов по общей причине	150
Выводы по разделу	151
Литература	153
Вопросы для самоконтроля	154
Практические задания	154

ГЛАВА 5.

Изучаем и выбираем методы обеспечения функциональной безопасности

.....	156
5.1. Обзор методов обеспечения функциональной безопасности	156
5.2. Организационные методы обеспечения информационной и функциональной безопасности	160

5.3. Технические методы обеспечения функциональной безопасности	163
5.4. Методы защиты от отказов аппаратных средств и систем согласно требованиям МЭК 61508-2	169
5.5. Методы защиты от отказов программного обеспечения согласно требованиям МЭК 61508-3.....	180
Выводы по разделу	194
Литература	195
Вопросы для самоконтроля	195
Практические задания.....	196
ГЛАВА 6.	
Проектируем и реализуем жизненный цикл информационной и функциональной безопасности	197
6.1. Общий жизненный цикл	197
6.2. Структура жизненного цикла информационной и функциональной безопасности.....	201
6.3. Трассировка требований	218
6.4. Общий алгоритм работ по выполнению проекта сертификации.....	221
6.5. Разработка и обзор спецификации требований по безопасности	226
6.6. Разработка и обзор проекта архитектуры системы	231
6.7. Разработка и обзор проекта аппаратных средств	236
6.8. Разработка и верификация программного обеспечения.....	241
6.9. Интеграция системы и интеграционное тестирование.....	243
6.10. Руководство пользователя по безопасности	248
6.11. Валидационное тестирование	250
Выводы по разделу	252
Литература	254
Вопросы для самоконтроля	254
Практические задания.....	255
ГЛАВА 7.	
Учитываем требования к информационной безопасности	256
7.1. Отличия компьютерных систем управления и других информационных (IT) систем.....	256
7.2. Стандарты в области информационной безопасности компьютерных систем управления	261

7.3. Структура требований к информационной безопасности.....	264
7.4. Система менеджмента информационной безопасности.....	268
7.5. Особенности обеспечения информационной безопасности компьютерных систем управления	271
Выводы по разделу	277
Литература	278
Вопросы для самоконтроля	279
Практические задания.....	279

ГЛАВА 8.

Учитываем особенности программируемых

логических интегральных схем..... 280

8.1. Особенности применения ПЛИС в компьютерных системах управления	280
8.2. Жизненный цикл информационной и функциональной безопасности для компьютерных систем управления на базе ПЛИС.....	285
8.3. Методы защиты от отказов ПЛИС согласно требованиям МЭК 61508-2.....	296
Выводы по разделу	305
Литература	306
Вопросы для самоконтроля	306
Практические задания.....	306

ГЛАВА 9.

Проводим квалификационные испытания оборудования

на устойчивость к внешним воздействующим факторам 307

9.1. Общий алгоритм работ по подготовке к проведению квалификационных испытаний оборудования.....	307
9.2. Состав и управляющая логика тестового образца и тестовой системы	310
9.3. План и процедуры квалификационных испытаний	324
9.4. Виды квалификационных испытаний: климатические, сейсмические и электромагнитные	327
Выводы по разделу	334
Литература	336
Вопросы для самоконтроля	336
Практические задания.....	336

ГЛАВА 10.**Оцениваем и обосновываем соответствие требованиям к информационной и функциональной безопасности**

при помощи методологии Assurance Case	338
10.1. Основы методологии Assurance Case	338
10.2. Нотация «Цель, аргумент и подтверждение» (Claim, Argument and Evidence, CAE)	342
10.3. Нотация структурированных целей (Goal Structuring Notation, GSN)	350
10.4. Инструментальные средства и база знаний Assurance Case	353
10.5. Критика неудачных применений Assurance Case и пути улучшения оценивания безопасности	359
Выводы по разделу	363
Литература	366
Вопросы для самоконтроля	367
Практические задания	367
Заключение	369
Перечень сокращений	370
ПРИЛОЖЕНИЕ.	
Онлайн-курс «Функциональная безопасность компьютерных систем»	372