ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ

ПНСТ 120—2016/ МЭК 62646:2012

АТОМНЫЕ СТАНЦИИ

Пункты управления. Компьютеризированные процедуры

(IEC 62646:2012, IDT)

Издание официальное

Москва
Стандартинформ
2016

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Негосударственным образовательным частным учреждением «Новая Инженерная Школа» (НОЧУ «НИШ») на основе официального перевода на русский язык англоязычной версии указанного в пункте 4 стандарта, который выполнен Российской комиссией экспертов МЭК/ТК 45

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 322 «Атомная техника»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 09 июня 2016 г. № 42-пнст

4 Настоящий стандарт идентичен международному стандарту МЭК 62646:2012 «Атомные станции. Пункты управления. Компьютеризированные процедуры» (IEC 62646:2012 «Nuclear power plants — Control rooms — Computer based procedures, IDT»)

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов соответствующие им национальные и межгосударственные стандарты, сведения о которых приведены в дополнительном приложении ДА.

5 ВВЕДЕН ВПЕРВЫЕ

Правила применения настоящего стандарта и проведения его мониторинга установлены в ГОСТ Р 1.16—2011 (разделы 5 и 6).

Федеральное агентство по техническому регулированию и метрологии собирает сведения о практическом применении настоящего стандарта. Данные сведения, а также замечания и предложения по содержанию стандарта можно направить не позднее чем за 9 мес до истечения срока его действия разработчику настоящего стандарта по адресу: gost.e-ecolog.ru *и в Федеральное агентство по техническому регулированию и метрологии по адресу: Ленинский просп., д. 9, Москва В-49, ГСП-1, 119991.*

*В случае отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячном информационном указателе «Национальные стандарты» и журнале «Вестник технического регулирования». Уведомление будет размещено также на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (*gost.e-ecolog.ru

© Стандартинформ, 2016

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
1.1 Предмет 1
1.2 Краткий обзор компьютеризированных процедур 1
1.3 Исключения из настоящего стандарта 2
1.4 Структура настоящего стандарта 2
2 Нормативные ссылки 3
3 Термины и определения 3
4 Сокращения 5
5 Требования к методике компьютеризации процедур 5
5.1 Общие положения 5
5.2 Методика компьютеризации 5
5.3 Семейства компьютеризированных процедур 7
5.4 Краткий обзор средств компьютеризации 8
5.5 Выходная документация 9
6 Использование компьютеризированных процедур 10
6.1 Общие положения 10
6.2 Среда использования 10
6.3 Содействие деятельности операторов 11
6.4 Координация оператора 12
6.5 Выходная документация 12
7 Система компьютеризированных процедур 13
7.1 Общие положения 13
7.2 Требования безопасности 13
7.3 Интеграция системы компьютеризированных процедур в систему человекомашинного интерфейса 13
7.4 Система компьютеризированных процедур, независимая от системы человекомашинного интерфейса 13
7.5 Отказ системы компьютеризированных процедур 14
7.6 Выходная документация 15
8 Требования к рабочему проекту 15
8.1 Общие сведения 15
8.2 Основные функции компьютеризированных процедур 15
8.3 Информация, выдаваемая от компьютеризированных процедур 17
8.4 Навигация 18
8.5 Методические рекомендации по компьютеризированным процедурам 18
8.6 Автоматизация на основе процедур 19
8.7 Прочие средства компьютеризированных процедур 20
8.8 Выходная документация 20
9 Жизненный цикл компьютеризированных процедур 21
9.1 Общие сведения 21
9.2 Организация проекта 21
9.3 Проектная группа 21
9.4 Программа верификации и валидации 21
9.5 Программирование компьютеризированных процедур 22

9.6 Верификация и валидация компьютеризированных процедур 22
9.7 Внедрение компьютеризированных процедур 23
9.8 Выходная документация 24
9.9 Обслуживание компьютеризированных процедур и системы компьютеризированных процедур 24
9.10 Обучение оперативного персонала 24
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов национальным стандартам 25
Библиография 26

Введение

a) Технические положения, основные вопросы и организация стандарта

Настоящий стандарт рассматривает компьютеризированные процедуры, применяемые оперативным персоналом. Процедуры в значительной мере способствуют безопасности и готовности атомной станции (далее — АС), и в настоящее время все увеличивается и становится современной практикой применение компьютерных технологий, позволяющих расширить методическое руководство операторами АС. Настоящий стандарт приводит рекомендации для принятия решения о степени компьютеризации процедур.

Настоящий стандарт предназначен для проектировщиков АС, оперативного персонала энергетических компаний, экспертов-системотехников и инженеров по регулированию.

b) Место настоящего стандарта в структуре серии стандартов МЭК ПК 45А

МЭК 62646 является документом МЭК ПК 45А третьего уровня, касающимся характерных проблем компьютеризированных процедур.

МЭК 62646 рассматривают совместно с МЭК 60964 и с МЭК 61839. МЭК 60964 является надлежащим документом МЭК ПК 45А, дающим представление о средствах управления оператора, верификации и валидации проекта, применении устройств визуальной индикации в пункте управления, тогда как МЭК 61839 устанавливает функциональный анализ и рекомендации по распределению функций между операторами и системами.

Более подробное описание структуры серии стандартов МЭК ПК 45А см. в перечислении d) настоящего введения.

c) Рекомендации и ограничения относительно применения стандарта

Настоящий стандарт не устанавливает дополнительных функциональных требований к системам безопасности.

Настоящий стандарт рассматривает технические требования и проектирование с учетом человеческого фактора в отношении компьютеризированных процедур (КП). Однако в настоящем стандарте не приводятся подробные руководства ни по эргономичному проектированию центров управления, т. к. оно рассматривается в стандартах серии ИСО 11064, ни по распределению заданий между человеком и системами, рассматриваемому в МЭК 61839, ни по безопасности киберпространства, рассмотренной в МЭК 62645. Из настоящего стандарта также исключены вопросы организации поддержки процедур.

Аспекты, по отношению к которым в настоящем стандарте установлены требования и разработаны рекомендации:

- разработка методики для компьютеризации процедур, в которой особое внимание уделено принятию решений о том, какие типы процедур следует компьютеризировать и в какой степени. После чего устанавливают семейства КП с соответствующими функциями и рассматривают аспекты безопасности СВР:
- использование СВР внутри и вне блочного пункта управления (БПУ) возможно совместно с процедурами на бумажном носителе, а также помощь, оказываемая оператору, включая координацию пользователей;
- связанные и не связанные с безопасностью проектные требования к цифровой системе обработки СВР и рекомендации о действиях в случае отказа системы;
- подробные требования и рекомендации, связанные с функциональными свойствами СВР от базовых до усложненных, то есть информацией, навигацией, рекомендациями и управлением станцией;
- жизненный цикл СВР от разработки проекта до обслуживания СВР и обучения оператора посредством проектирования и реализации.

Для гарантии того, что настоящий стандарт останется актуальным в будущем, особое внимание уделено принципиальным вопросам, а не конкретным технологиям.

d) Описание структуры серии стандартов МЭК ПК 45А и их связи с другими документами МЭК и документами других организаций (МАГАТЭ, ИСО)

Стандартом высшего уровня в серии стандартов МЭК ПК 45А является МЭК 61513. Он содержит общие требования к системам и оборудованию контроля и управления, выполняющим функции, важные для безопасности на атомных электростанциях. МЭК 61513 формирует структуру серии стандартов МЭК ПК 45А.

МЭК 61513 содержит прямые ссылки на другие стандарты МЭК ПК 45А, рассматривающие общие темы, связанные с классификацией функций и классификацией систем, аттестацией, разделением систем, защитой от отказа по общей причине, аспектами программного обеспечения ЭВМ, аспектами ап-

паратных средств ЭВМ и проектированием пунктов управления. Стандарты второго уровня, на которые имеются ссылки, последовательно рассматривают вместе с МЭК 61513.

На третьем уровне стандарты МЭК ПК 45А, на которые нет прямых ссылок в МЭК 61513, — это стандарты, связанные с определенным оборудованием, техническими методами или определенной деятельностью. Как правило, документы, ссылающиеся на документы второго уровня (по общим темам), могут использоваться самостоятельно.

Четвертый уровень стандартов серии МЭК ПК 45А представляет собой Технические отчеты, которые не являются нормативными документами.

МЭК 61513 выполнен в том же формате изложения, что и основной документ по безопасности МЭК 61508, и содержит полную схему жизненного цикла безопасности и структуру жизненного цикла системы, а также предоставляет интерпретацию основных требований, изложенных в МЭК 61508-1, МЭК 61508-2 и МЭК 61508-4, применительно к ядерной отрасли. С этой точки зрения МЭК 60880 и МЭК 62138 соответствуют МЭК 61508-3 в части использования для ядерной отрасли. МЭК 61513 ссылается на стандарты ИСО, а также документ МАГАТЭ GS-R-3 и МАГАТЭ GS-G-3.1 по вопросам, связанным с обеспечением качества (ОК).

Стандарты серии МЭК ПК 45А последовательно внедряют и детализируют принципы и основные аспекты безопасности, предусмотренные в Руководствах МАГАТЭ по безопасности атомных станций и в других документах по безопасности МАГАТЭ, в частности, в Требованиях NS-R-1, устанавливающих требования к безопасности при проектировании атомных электростанций, и в Руководстве по безопасности NS-G-1.3, рассматривающем системы контроля и управления, важные для безопасности[1)] на атомных электростанциях. Терминология и определения, используемые в стандартах ПК 45А, соответствуют терминам и определениям, используемым в документах МАГАТЭ.

Примечание — Предполагается, что для проектирования систем контроля и управления на атомных станциях, которые реализуют традиционные функции безопасности (например, для решения проблем безопасности работников, защиты имущества или ресурсов, химических опасных факторов, опасных факторов процессов получения, переработки и использования энергии) будут применены международные или национальные стандарты, основанные на требованиях стандарта, такого как МЭК 61508.

[1)] В ОПБ-88/97 используются следующие термины: «управляющие системы нормальной эксплуатации», «управляющие системы безопасности» и «управляющие системы, важные для безопасности».

ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ

АТОМНЫЕ СТАНЦИИ

Пункты управления.

Компьютеризированные процедуры

Nuclear power plants. Control rooms. Computer based procedures

**Срок действия — с 01—04—2017
по 31—03—2018**

1 Область применения

1.1 Предмет

Настоящий стандарт устанавливает требования к полному жизненному циклу эксплуатационных процедур, которые проектировщик планирует компьютеризировать. В настоящем стандарте также приведены рекомендации по принятию решений о том, какие типы процедур будут компьютеризированы и в какой степени. После компьютеризации процедуры определяют как компьютеризированные процедуры (далее — СВР).

Повышение безопасности и эксплуатационных характеристик АС всегда считались важными целями, достижению которых при эксплуатации АС в значительной степени способствуют оперативный персонал и эксплуатационные процедуры. В настоящее время применение цифровых технологий также способствует их достижению, оказывая эффективную помощь на уровне автоматизации.

Кроме того, увеличивается практика использования компьютерных технологий для выдачи форматов эксплуатационных процедур операторам станции[1)], в оперативном режиме и в режиме реального времени. Компьютеризированные процедуры можно использовать при нормальной эксплуатации, а также в качестве рекомендательных форматов для использования в нештатных ситуациях. При надлежащей реализации и своевременной актуализации компьютеризированные эксплуатационные процедуры могут способствовать повышению уровня безопасности АС и результативности оператора по сравнению с процедурами на бумажном носителе. Их подготовка требует большой тщательности и тесного взаимодействия с операторами и проектировщиками станции, а также тесного сотрудничества с проектировщиками систем контроля и управления.

У компьютеризированных процедур много общего с процедурами на бумажном носителе. В настоящем стандарте рассматривается только специфика компьютеризированных процедур.

1.2 Краткий обзор компьютеризированных процедур

Процедуры предоставляют операторам два типа высокоуровневых элементов:

- информацию, то есть отображаемые пояснения или данные, позволяющие оператору управлять процессом, оценивать ситуацию на станции, понимать эксплуатационные стратегии и принимать адекватные решения;
- методическое руководство, то есть ряд упорядоченных шагов для подсказки и помощи оператору в работе с технологическим процессом и оборудованием станции.

[1)] Операторами могут быть лица мужского или женского пола, поэтому в настоящем стандарте «он» является сокращением для «он/она», а «его» — сокращением для «его/ее».

Издание официальное

Информацию и методическое руководство комбинируют для минимизации ошибок операторов и оптимизации эффективности эксплуатации станции.

Данные элементы могут быть представлены на переменном уровне детализации в зависимости от методики процедуры, нацеленной на использование опыта оператора и определенных руководящих принципов.

Согласно указанной методике проектирования компьютеризация процедур может обеспечить:

- расширенную информацию о технологическом процессе и оборудовании станции;
- углубленное методическое руководство для оператора;
- автоматическое управление станцией.

Однако введение компьютеризированных процедур требует внимания к следующим проблемам:

- определение методики в области применения процедур, уровня методического руководства и возможного прямого управления процессом, например, с учетом опыта эксплуатации станции и человеческих возможностей, а также организационных и технологических проблем;
- проектирование безопасной и надежной системы компьютеризированных процедур, а также обеспечение адекватного резервирования, включая эксплуатационные процедуры, охватывающие предполагаемый отказ системы компьютеризированных процедур;
- валидация сочетания стратегий эксплуатации станции, представления форматов и человеческих возможностей, а также цифровых проблем;
- поддержка оператора в состоянии осведомленности, то есть обеспечение адекватного приоритета действия человека над компьютеризированными действиями и предотвращение потери знаний.

1.3 Исключения из настоящего стандарта

Для эффективного и адекватного проектирования СВР уже заранее должно быть принято решение о некоторых важных входных данных, которые лежат вне области применения настоящего стандарта:

- функциональный анализ и распределение функций.

В МЭК 61839 определены процедуры функционального анализа и распределения функций и установлены правила разработки критериев для распределения функций между операторами и системами;

- рекомендации по проектированию с учетом человеческого фактора.

В стандартах серии ИСО 11064 дано руководство по мероприятиям антропоцентрического проектирования на протяжении жизненного цикла компьютерной интерактивной системы.

Кроме того, для реализации компьютеризированных процедур на новых АС применяют МЭК 60964 и МЭК 60965, в которых приведены требования и рекомендации к блочному пункту управления и организации дополнительных пунктов управления. Дополнительные рекомендации по реализации компьютеризированных процедур в случае переоснащения блочного пункта управления приведены в 6.2.3.

Из настоящего стандарта также исключено рассмотрение следующих вопросов:

- компьютерная безопасность, необходимая для защиты жизненного цикла компьютеризированных процедур, но не ограничивающаяся компьютеризацией процедур. Данные вопросы рассматривают при компьютеризации средств эксплуатации. В МЭК 62645 рассматривают вопросы, связанные с безопасностью киберпространства;
- требования к реализации функций компьютеризированных процедур программного и аппаратного обеспечения компьютерных систем для компьютеризированных процедур необходимо реализовать в соответствии с его классом безопасности по МЭК 61513;
- организация поддержки процедур.

1.4 Структура настоящего стандарта

В разделе 2 приведены нормативные ссылки.

В разделе 3 приведены термины с соответствующими определениями.

В разделе 4 приведен перечень сокращений.

В разделе 5 приведен обзор компьютеризированных процедур. В данном разделе представлены рекомендации для разработки методики компьютеризации процедур исходя из типа реализуемой процедуры. Предложено три обобщенных типа (названных «семействами»), для которых даны общие и конкретные рекомендации. Также приведены рекомендации, связанные с требованиями к безопасности систем СВР.

В разделе 6 установлены требования к использованию в различных средах, внутри и вне блочного пункта управления и, возможно, совместно с процедурами на бумажном носителе. Затем рассмотрено содействие деятельности оператора и ее координация.

В разделе 7 рассмотрена цифровая система, обрабатывающая компьютеризированные процедуры. В данном разделе рассмотрены требования, связанные и не связанные с безопасностью, а также установлены требования противодействию отказам данной системы.

В разделе 8 рассмотрены подробные требования и рекомендации, связанные с функциональными свойствами компьютеризированных процедур, от базовых до усложненных, т. е. информацией, навигацией, руководством и управлением станцией. Также в данном разделе приведены иные опции, которые могут упростить использование компьютеризированных процедур.

В разделе 9 рассмотрен жизненный цикл компьютеризированных процедур от разработки проекта до обслуживания компьютеризированных процедур и обучения оператора посредством проектирования и реализации.

2 Нормативные ссылки

Для применения настоящего стандарта необходимы следующие документы. Для датированных ссылок применяют только указанное издание ссылочного документа. Для недатированных ссылок применяют последнее издание ссылочного документа (включая все его изменения).

IEC 60671, Nuclear power plants — Instrumentation and control systems important to safety — Surveillance testing (МЭК 60671 Атомные электростанции. Системы контроля и управления, важные для безопасности. Испытания для проверки работоспособности)

IEC 60880, Nuclear power plants — Instrumentation and control systems important to safety — Software aspects for computer-based systems performing category A functions (МЭК 60880 Атомные электростанции. Системы контроля и управления, важные для безопасности. Аспекты программного обеспечения компьютерных систем, выполняющих функции категории А)

IEC 60964:2009, Nuclear power plants — Control rooms — Design (МЭК 60964:2009 Атомные станции. Пункты управления. Проектирование)

IEC 60965:2009, Nuclear power plants — Control rooms — Supplementary control points for reactor shutdown without access to the main control room (МЭК 60965:2009 Атомные станции. Пункты управления. Дополнительные пункты управления для остановки реактора без доступа к главному пункту управления)

IEC 61513, Nuclear power plants — Instrumentation and control important to safety — General requirements for systems (МЭК 61513 Атомные станции. Системы контроля и управления, важные для безопасности. Общие требования)

IEC 61772, Nuclear power plants — Control rooms — Application of visual display units (VDUs) (МЭК 61772 Атомные станции. Пункты управления. Применение дисплеев)

IEC 61839, Nuclear power plants — Design of control rooms — Functional analysis and Assignment (МЭК 61839 Атомные станции. Проектирование пунктов управления. Функциональный анализ и распределение функций)

IEC 62138, Nuclear power plants — Instrumentation and control important for safety — Software aspects for computer-based systems performing category B or C functions (МЭК 62138 Атомные электростанции. Системы контроля и управления, важные для безопасности. Программное обеспечение компьютерных систем, выполняющих функции категорий В и С)

IEC 62241:2004, Nuclear power plants — Main control room — Alarm functions and Presentation (МЭК 62241:2004 Атомные станции. Блочный пункт управления. Функции и представление сигнализации)

ISO 11064 (all parts), Ergonomic design of control centres (ИСО 11064 (все части) Эргономическое проектирование центров управления)

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1 **резервная система** (back-up system): Альтернативное оборудование для управления и мониторинга станции, спроектированное для использования в случае отказа используемой в нормальных условиях системы человеко-машинный интерфейс.

3.2 **компьютеризированные процедуры;** КП (Computer Based Procedures; CBP): Интерактивное компьютерное приложение, используемое для представления методического руководства операторам станции, которое может дополнительно содержать информацию о динамических процессах, включая доступ к органам управления пульта оператора.

Примечание — В отличие от процедур на бумажном носителе, которые являются фиксированным документом, CBP предлагают опции динамических показаний. Данные опции позволяют оператору перемещаться от одного шага к другому различными усовершенствованными способами, размещать закладки и использовать параллельную дисплейную индикацию.

3.3 **система компьютезированных процедур** (CBP system): Цифровая система, реализующая компьютеризированные процедуры.

Примечание — CBP можно реализовать в системе HMI совместно с прочими функциями управления станцией либо на отдельном компьютере CBP.

3.4

формат, дисплейный формат (format, display format): Наглядное отображение информации на экране дисплея в виде текстового сообщения, цифрового представления, условных обозначений, мнемосхем, гистограмм, графиков, указателей, многоугольного образа.

[IEC 60964:2009, статья 3.7]

3.5

абстрактное мышление (high-level mental processing): Акт обработки и/или интерпретации информации человеком с целью получения краткой абстрактной информации.

[IEC 60964:2009, статья 3.12]

3.6

человекомашинный интерфейс; ЧМИ (Human Machine Interface; HMI): Интерфейсы между оперативным персоналом, системой контроля и управления и вычислительными системами, обеспечивающими связь со станцией. Интерфейс включает в себя дисплеи, средства управления и интерфейс системы поддержки оператора.

[IEC 60964:2009, статья 3.13]

3.7

навигация (navigation): Функция поддержки операторов, позволяющая определять положение желательной информации в дисплейной информационной системе, а также регулировать выбор средств отображения информации.

[IEC 62241:2004, статья 3.29]

3.8

эксплуатационные процедуры; ЭП (Operating Procedures; OP): Набор документов, определяющий эксплуатационные задачи, которые необходимо выполнить для достижения функциональных целей.

[IEC 60964:2009, статья 3.19]

3.9 **процедуры на бумажном носителе** (paper based procedures): OP (см. 3.8), которые печатают на бумажных листах.

3.10

постулируемое исходное событие; ПИС (Postulated Initiating Event; PIE): Событие, определяемое на стадии проектирования как способное привести к ожидаемым при эксплуатации событиям или аварийным условиям.

[IAEA Safety Glossary, 2007 г.]

3.11 **последовательность, последовательность выполнения процедуры** (sequence, procedure sequence): Набор элементарных шагов в процедуре, которые необходимо полностью выполнить для достижения функциональной цели.

Примечание 1 — Частичное исполнение последовательности может либо привести к сбоям или отказам схем или оборудования, либо поставить под угрозу исполнение функции.

Примечание 2 — Обычно процедура охватывает несколько последовательностей для достижения своей глобальной функциональной цели.

Примечание 3 — Последовательность может состоять из одиночного шага.

3.12

дополнительный пункт управления; ДПУ (Supplementary Control Point; SCP): Помещение, из которого возможно ограниченное управление и/или мониторинг элементов станции с целью достижения функций безопасности, определенных при анализе безопасности, в соответствии с установленными требованиями в случае потери способности выполнять эти функции из помещения главного пункта управления.

Дополнительный пункт управления может представлять собой специальный зал управления, но во многих случаях он включает в себя ряд пультов управления и дисплеев в помещениях электрощитовых или подобных им зонах.

[IEC 60965:2009, статья 3.5]

3.13

дисплей (Visual Display Unit; VDU): Средство отображения информации, включающее в себя экран, на который выводится формируемое компьютером изображение.

[IEC 60964:2009, статья 3.31]

4 Сокращения

В настоящем стандарте применены следующие сокращения:

CBP — компьютеризированные процедуры;

HMI — человекомашинный интерфейс;

HVAC — отопление, вентиляция и кондиционирование воздуха;

MCR — блочный пункт управления;

OP — эксплуатационные процедуры;

PIE — постулируемое исходное событие;

SCP — дополнительный пункт управления;

VDU — дисплей.

5 Требования к методике компьютеризации процедур

5.1 Общие положения

В настоящем разделе приведен краткий обзор CBP. Представлены рекомендации по разработке методики компьютеризации процедур исходя из типа реализуемой процедуры. Предложено три обобщенных типа (названных «семействами»), для которых приведены общие и конкретные рекомендации. Также приведены методические рекомендации, связанные с нормами обеспечения безопасности систем CBP.

5.2 Методика компьютеризации

5.2.1 Общие положения

Компьютеризацию процедур необходимо включить в рамки определения концепции пункта управления, общей архитектуры контроля и управления, определения методики учета человеческого фактора и принципов работы энергетической компании (МЭК 60964:2009, раздел 5).

Данную деятельность следует поддерживать с помощью изучения опыта, концептуальных исследований, возможно, некоторого макетирования, выполненных либо в качестве входных данных к проекту, либо в качестве раннего этапа проектирования.

Проектировщик должен принять решение о типах процедур, подлежащих компьютеризации, и о степени данной компьютеризации.

Причины компьютеризации процедур необходимо привести в основном плане проекта, т. к. они будут сильно влиять на то, какие процедуры будут компьютеризированы и в какой степени. Реализация CBP не обязательно решит проблемы эксплуатационной стратегии или укомплектования персоналом, но проектная проработка CBP может помочь выявлению причины этих проблем и определении пути решения проблем на начальной стадии.

Примечание — Возможные последствия, влияющие на оперативный персонал организации, план помещения блочного пункта управления, эксплуатационные стратегии, область применения процедуры, уровень автоматизации и т. д. лежат вне области применения настоящего стандарта.

Примеры типов процедур, которые можно компьютеризировать:

- процедуры, обеспечивающие нормальную эксплуатацию станции при нормальных условиях (например, пуск станции), или процедуры, решающие элементарные задачи, прогрев трубопроводов или снижение нагрузки и возврат на мощность;
- процедуры при нарушении нормальной эксплуатации (включая проектные аварии, процедуры в случае возникновения запроектных аварий;
- процедуры реагирования на аварийные сигналы (аварийного оповещения, при достижении параметрами уставок и условий срабатывания АЗ);
- процедуры действий при пожаре;
- процедуры при потере электропитания и любые типы процедур, реализуемые в определенных условиях;
- процедуры, определяемые регламентом;
- процедуры проведения периодических испытаний, разработанные согласно МЭК 60671, например, посвященные калибровке плотности потока или останову реактора, или любые другие процедуры проведения периодических испытаний;
- руководства по эксплуатации, предлагающие простой доступ к данным конкретного устройства на экранном HMI.

5.2.2 Предварительная оценка

В дополнение к функциональному анализу, распределению функций и рекомендациям по антропоцентрическому проектированию, которые исключены из области применения настоящего стандарта подразделом 1.3, на начальной стадии проектирования необходимо учитывать некоторые другие основные вопросы, а именно:

- нормы действующего законодательства;
- стратегии эксплуатации

это функциональная проблема, независимая от компьютеризации, например, в случае аварии необходимо принять решение о выборе между стратегией на основе состояний и стратегией на основе событий;

- организация оперативного персонала

при строительстве новой АС и/или модернизации существующей проект СВР можно сделать неотъемлемой частью общего проекта пункта управления или его модернизации, что заставляет применять принятые методы проектирования с учетом человеческого фактора;

- обратная связь из опыта оперативного персонала следует определить хорошее, подлежащее улучшению, или отсутствующее в любой существующей СВР, или решении на бумажном носителе, кроме того, проектировщик может полагать, что следует компьютеризировать только стратегию эксплуатации, или напротив, только конкретизированную часть процедур;
- методика обучения операторов;
- данные, полученные от контрольно-измерительной аппаратуры станции;

Примечание — Уровень методического руководства СВР зависит от доступной контрольно-измерительной аппаратуры.

- интеграция обработки СВР в систему HMI, если она цифровая, или использование специализированной системы для обработки СВР, подключенной или не подключенной к цифровой системе HMI.

Исходя из данных положений следует определить предварительную методику СВР и типы процедур, которые можно компьютеризировать.

5.2.3 Окончательное решение о возможности использования СВР

Для принятия окончательного решения о типах компьютеризируемых процедур в проекте следует рассмотреть следующие вопросы:

- определение типов процедур, которые можно обрабатывать одновременно при нормальной эксплуатации, в случае пожара, в случае потери электропитания, в случае проведения периодического испытания, в случае PIE;
- оценка числа дисплеев, необходимых для данных процедур;
- оценка максимального числа процедур, которые может обрабатывать параллельно один оператор или весь оперативный персонал, для работы в случае возникновения наихудшего проектного сочетания событий;

- оценка максимального числа окон, которые можно отображать параллельно на одиночной рабочей станции или на всех рабочих станциях помещения;
- распределение задач оперативного персонала взаимодополняющим образом между СВР и процедурами на бумажном носителе.

Вышеуказанную оценку следует выполнять с учетом концепции пункта управления. Рассматривают следующие элементы:

- набор рабочих станций и рабочих мест, предназначенных для использования СВР, в блочном пункте управления и всех прочих пунктах управления;
- тот факт, что процедура может быть временно прекращена без завершения, например, в случае срабатывания сигнализации;
- максимальный объем информации, отображаемой в формате;
- характеристики системы СВР, в частности, дисплеев, емкости памяти, навигации;
- адекватный дополнительный запас с целью упрощения будущих модификаций.

Указанные положения могут усложнить аспекты методики реализации СВР, предложенного проекта системы СВР, его возможности и функционирования или сопутствующего обоснования рентабельности, а также организации сменной работы или стратегии эксплуатации.

Содержание и область рассмотрения человеческого фактора и организационных исследований следует определить в отношении:

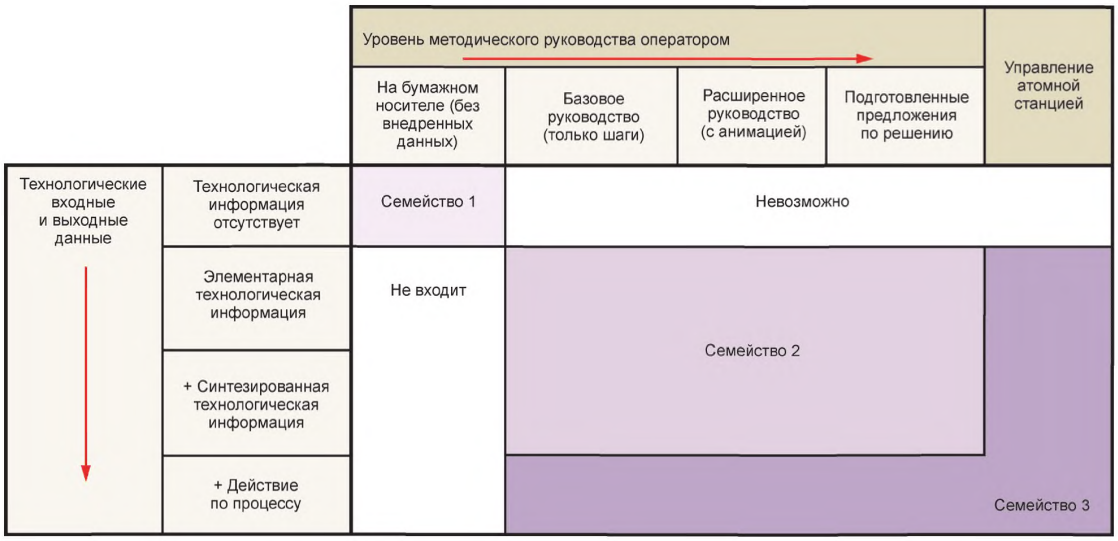
- идентификации кадровых ресурсов, необходимых для проекта, т. е. специалистов, включаемых в проектный коллектив, специалистов для верификации и валидации, организации поддержки СВР;
- использования конечного продукта, включая средства поддержки.

5.3 Семейства компьютеризированных процедур

Несмотря на то, что процедуры можно компьютеризировать многими способами согласно методике проектирования, реализацию следует рассматривать в виде одного из трех обобщенных семейств СВР согласно таблице 1. Данные семейства основаны на рассмотрении:

- предполагаемого уровня методического руководства;
- требуемых технологических входных и выходных данных.

Таблица 1 — Семейства СВР



В строках данной таблицы представлены различные виды технологических входных и выходных данных. В столбцах представлены различные уровни компьютеризации. Пересечения строк и столбцов представляют собой возможные опции СВР. Например, если проектировщик стремится поддержать оператора с помощью анимированного расширенного руководства или предложений по принятию ре-

шений, то необходимо предоставить и элементарную, и синтезированную технологическую информацию. Если проектировщик стремится поддержать оператора с помощью средств управления станции, то необходимо представить средства управления в дополнение к элементарной и синтезированной информации.

Указанные три семейства СВР характеризуют следующим образом:

- семейство 1: СВР, которые являются автономными заменами для процедур на бумажном носителе, представляющие собой связанные страницы статической информации и шагов перехода.

КП этого семейства не получают никакой технологической информации;

- семейство 2: СВР, обеспечивающие методическое руководство для оператора на основе информации, полученной системой СВР. Каждый элемент информации может быть интегрирован в представленные дисплейные форматы.

В семействе 2 различают три варианта согласно степени предоставляемого методического руководства:

- вариант 2.1 предоставляет оператору элементарные технологические параметры и состояния оборудования в форматах СВР. Доступ к СВР можно компьютеризировать (см. 8.5.2),

- вариант 2.2 в дополнение к элементарной информации предоставляет оператору синтезированную информацию. Примерами синтезированной информации являются уровень воды в компенсаторе давления, или запас до насыщения, или точка пуска реактора. Можно компьютеризировать пункт СВР (см. 8.5.2) и/или диагностическую помощь (см. 8.5.3),

- вариант 2.3 предоставляет оператору все виды средств предыдущих вариантов, дополненных содействием в принятии решения,

- опционально можно оповещать о возможных расхождениях между действиями операторов и предложенным решением;

- семейство 3: СВР, представляющие информацию и рабочие шаги с полной интеграцией оперативной информации, состояний и значений станции так, чтобы приводами можно было управлять с дисплея, к функциям автоматического управления можно было получить доступ, а автоматическое исполнение последовательностей мог инициализировать оператор с экранных форматов СВР.

Все семейства могут включать в себя некоторые средства, представленные в подразделе 8.7.

Для каждого типа процедуры, перечисленного в 5.2.1, можно выбрать различные семейства СВР.

5.4 Краткий обзор средств компьютеризации

5.4.1 Общие положения

Компьютеризация основана на глобальных факторах и на элементах, связанных с рекомендациями для оператора и с управлением станцией.

5.4.2 Глобальные требования к компьютеризации

Компьютеризация процедуры:

- гарантирует, что операторы легко понимают стратегию эксплуатации;
- оставляет полную ответственность за операторами;
- дает ясное определение функциональной цели;
- упрощает продвижение в ходе процедур и ограничивает вызовы между процедурами;
- дает возможность оператору пропустить шаги и последовательности, если они не относятся к данной ситуации;
- обеспечивает адекватную передачу информации между членами группы;
- применяется одинаково ко всем процедурам данного типа, например, ко всем аварийным процедурам или ко всем противопожарным процедурам;
- единообразна для различных видов процедур, которые можно обрабатывать параллельно.

СВР предоставляет средства отображения глобальной цели процедуры и краткий обзор ее последовательностей либо постоянно, либо по запросу оператора. По запросу оператора СВР отображает дополнительную информацию для шагов или последовательностей, таких как предварительные действия, аспекты технологического процесса и устройства.

Проектировщик должен проверить, что набор процедур и соответствующие им требования к вычислительной мощности соответствуют возможностям системы СВР.

5.4.3 Методическое руководство СВР

Методическое руководство со стороны СВР напоминает операторам о функциональной цели и способах ее достижения.

В дополнение к снабжению оператора элементарной технологической информацией может быть дана расширенная информация о технологическом процессе посредством доступа к СВР, диагностики или рекомендации по принятию решений.

Диагностика или рекомендации по принятию решения могут быть:

- автоматизированы: диагноз/решение предлагается оператору, который может затем запросить подробную информацию о нем;
- поддержаны: СВР отображает блок-схемы, помогающие оператору установить диагноз/решение. Информация, необходимая оператору для элементарного выбора, сделана легкодоступной или включена в блок-схемы для того, чтобы оператор мог последовательно утвердить каждый шаг.

Для разработки рекомендаций СВР следует рассмотреть:

- частоту событий или ситуаций. Например, следует организовать расширенное методическое руководство для редких событий по сравнению с руководством для ежедневной эксплуатации;
- операционная политика. Например, обеспечение высоких эксплуатационных характеристик станции может привести к повышению уровня компьютеризации и автоматизации;
- обратную связь с оперативным персоналом и требования.

Для определения методических рекомендаций проектировщик должен учесть собственные возможности системы СВР, то есть эксплуатационные характеристики, наглядность и восприятие.

Возможности оператора запрашивать элементарную информацию можно расширить до расчетов, ведущих к высокоуровневой обобщенной информации.

СВР предоставляет оператору синтезируемую информацию и возможно некоторую помощь в соответствии с 8.7.

5.4.4 Автоматизация на основе процедур

В случае, если система обработки СВР независима от системы HMI, управляющей станцией, необходимо реализовать условия, позволяющие избежать возможных расхождений между командами, отправленными обеими системами, или, как минимум, о таких расхождениях необходимо сообщить оператору.

СВР может управлять АС:

- автоматически запуская и выполняя последовательности СВР, например, последовательность сброса давления при достижении заранее определенных условий;
- автоматически выполняя последовательности, которые были запущены оператором.

Что касается процедур на бумажном носителе, СВР следует определить, рассматривая:

- распределение функций между оператором и цифровыми системами;
- тот факт, что набор процедур для резервной системы независим от системы HMI и от СВР;
- удобство для понимания оператором, особенно в аномальных условиях.

Дополнительно во внимание принимают:

- за исключением случаев проектирования в качестве резервных средств, дублирования функций между оператором и системой следует избегать, и следует вести поиск конструкций, в которых система СВР и оператор выполняют взаимодополняющие функции;
- дисплейные форматы СВР могут включать в себя возможности выдачи команды или могут направлять действия операторов на управление дисплейными форматами системы HMI. В качестве другого варианта можно санкционировать команды СВР, разрешая их выполнение из системы HMI.

Осведомленность оператора о ситуации необходимо расширить:

- отображая достоверную информацию, чтобы держать оператора в курсе происходящего.

Важные решения не автоматизируют, о конце автоматизированных последовательностей оповещают, а также сообщают о любых проблемах, возникающих во время автоматизированной последовательности, и о значениях технологических параметров, достигающих заданного порога;

- давая ему возможность принять на себя управление от СВР в любой момент;
- принимая во внимание координацию оперативной группы.

Последовательности, запущенные двумя операторами, могут обладать различными временами исполнения и не должны приводить к противоречащим или конкурирующим действиям.

5.5 Выходная документация

В заключении к решению о реализации СВР необходимо привести следующие определения:

- тип СВР, их цели и область применения;
- реализация СВР с учетом системы HMI;

- опции методического руководства СВР, включая описание необходимой информации,
- опция автоматизации на основе процедур;
- политика энергетической компании по обучению операторов.

6 Использование компьютеризированных процедур

6.1 Общие положения

В данном разделе приведены требования к использованию СВР. Рассмотрены различные среды использования относительно MCR и возможного совместного использования с процедурами на бумажном носителе. Затем рассмотрены содействие и координация мероприятий оператора. В заключение приведена ожидаемая документация.

6.2 Среда использования

6.2.1 Общие положения

В данном подразделе рассмотрены различные среды, в которых возможно использование СВР, либо в новых компьютеризированных пунктах управления, либо для частичной модернизации обычных пунктов управления, совместно с процедурами на бумажном носителе или локальной операцией, выполняемой полевым оператором.

В общем случае, полную интеграцию СВР в MCR и прочие пункты управления необходимо выполнять на основе МЭК 60964 и МЭК 60965. Применение дисплеев согласуют с МЭК 61772.

6.2.2 Использование СВР в компьютеризированных пунктах управления

Необходимо наличие возможности раздельного управления дисплейными форматами системы СВР и прочими дисплейными форматами системы HMI.

Совместимость между форматами СВР и эксплуатационными форматами системы HMI обеспечивают:

- избегая расхождений при наличии ссылок на один и тот же объект, схему или оборудование в эксплуатационных форматах и форматах СВР;
- выполняя обновление без значительной разницы во времени сопутствующих форматов системы управления станцией и форматов СВР при одновременном отображении.

Например, надпись «задвижка открыта» отображается одновременно на сопутствующих эксплуатационных форматах и форматах СВР, если задвижка показана на обоих форматах.

6.2.3 Использование СВР в обычном или гибридном блочном пункте управления

«Обычный пункт управления» — это пункт, спроектированный без какого-либо цифрового оборудования. «Гибридный пункт управления» включает в себя цифровые устройства для контроля и управления элементами станции, но не всей станцией. Обычные пункты управления можно модернизировать до гибридных пунктов управления. Степень компьютеризации гибридного пункта управления, исключая управление всей станцией, может сильно варьироваться в зависимости от целей энергетической компании.

Для реализации СВР в обычном или гибридном пункте управления необходимо рассмотреть ограничения существующего MCR, т. е. в основном, свободное пространство и рабочие зоны оператора, в дополнение к приведенным в 5.2.3. Ввод устройств для отображения СВР в обычном MCR может потребовать перемещения существующих элементов, индикаторов, кнопок и т. п. с целью освобождения пространства для установки комплектов дисплеев и сопутствующего оборудования, такого как клавиатуры, панели, трекболы и т. п.

Также рассматривают возможности таких технических служб как HVAC.

В качестве особой задачи обычных и гибридных пунктов управления изучают одновременное использование СВР с дискретным оборудованием, таким как индикаторы, регистраторы, кнопки, полуавтоматические станции управления и т. п. Кроме того, необходимо ожидать одновременного использования СВР и процедур на бумажном носителе и проанализировать его.

Принимая во внимание, что компьютеризация управления станцией ограничена, СВР проектируют с расчетом на выдачу информации и рекомендаций, т. е. с принадлежностью к семейству 1 или семейству 2 с соблюдением требований, связанных с этими семействами.

Кроме того, предусматривают особые условия для:

- проектирования HMI СВР таким образом, что при отображении информации на дисплеях оператор не перепутает СВР с любыми иными отображаемыми форматами, особенно в аварийных условиях,

- возможности операторам читать СВР из своих рабочих зон, либо перед дисплеем, либо с некоторого расстояния от дисплея.

6.2.4 Использование СВР совместно с процедурами на бумажном носителе

КП можно использовать совместно с процедурами на бумажном носителе либо по конструктивным соображениям, либо по временным причинам в зависимости от опций, определенных согласно 5.2.3.

Примечание 1 — Например, подробная эксплуатация остается на бумажном носителе, тогда как стратегия эксплуатации компьютеризирована.

Примечание 2 — Например, особые комплекты процедур на бумажном носителе, используемых, к примеру, в период простоя, используемых по причине обнаружения ошибки в компьютеризированной процедуре, и комплект процедур на бумажном носителе используется до тех пор, пока не будет подготовлена правильная новая компьютеризированная версия.

Такие ситуации необходимо разрабатывать так, чтобы:

- отсутствовал разрыв между СВР и процедурами на бумажном носителе;
- возможные наложения между СВР и процедурами на бумажном носителе были функционально обоснованы;
- ссылки и наименование СВР и процедур на бумажном носителе были согласованы и не приводили к ошибкам оператора;
- передача между СВР и процедурами на бумажном носителе была ясна;
- была гарантирована отслеживаемость действий, выполненных как с помощью СВР, так и процедур на бумажном носителе;
- ситуация оставалась легко объяснимой при смене персонала.

6.2.5 Использование СВР вне помещения блочного пункта управления

В случае если некоторые локальные пункты управления, например, SCP, компьютеризированы и эксплуатируются с помощью СВР, то последние необходимо адаптировать к задачам оператора.

При эксплуатации с локальных пунктов управления, если они компьютеризированы, или с любых типов переносных устройств необходимо соблюдать требования, приведенные в 6.4.

6.3 Содействие деятельности операторов

6.3.1 Общие положения

При разработке СВР необходимо учесть реагирование операторов на условия, принимая во внимание реальную ситуацию на станции, контролируя технологический процесс и обнаруживая события.

Примечание — Процедуры предназначены для помощи оператору путем предложения стратегий эксплуатации и подготовки возможных действий относительно состояния станции. Однако могут случиться неожиданные ситуации, и оператор должен быть в состоянии достигнуть цели высшего уровня, установленной процедурой, даже если некоторые ее части стали неприменимы.

В целях настоящего стандарта выполняемые СВР функции разделены на основные функции (например, предоставление информации оператору) и вторичные функции (например, управление окнами и задачи навигации по требуемой информации).

6.3.2 Содействие основной деятельности оператора

На этапе проектирования необходимо рассмотреть следующие концепции СВР с документальным обоснованием проектных решений по отношению к каждой концепции:

- совместимость с представлением оператора

аспекты HMI совместимы с мышлением оператора, т. е. с пониманием, опытом и ожиданием оператора о состоянии и развитии электростанции и способа функционирования СВР;

- представление ситуации

отображаемую информацию легко идентифицировать и понять, а точность отображенных значений согласуется с точностью измеренных значений, таким образом, чтобы это помогало абстрактному мышлению и продвижению оператора к функциональной цели процедуры. Следует отобразить обоснованность данных;

- структура HMI

аспекты HMI основаны на логических и непротиворечивых правилах. Основными аспектами HMI являются представление информации, иерархия последовательностей в рамках процедуры, терминология, вспомогательные формулировки, структуры списков и т. д.;

- совместимость с деятельностью

отображаемая информация относится к ситуации на станции;

- возможности оператора

объем отображаемой информации позволяет оператору понимать ее, и для принятия надлежащих решений оператору дано достаточно времени.

Можно отобразить контекстную информацию для усиления актуальности информации и содействия пониманию оператора.

6.3.3 Содействие вторичной деятельности оператора

Для того чтобы упростить задачи оператора и позволить ему сосредоточиться на первостепенных задачах, при проектировании необходимо рассмотреть следующие аспекты. Основные проектные решения по каждому аспекту документально фиксируют, включая обоснование:

- умственной нагрузки оператора

минимизируют запоминание элементов, таких как списки кодов, коды операций, информация для запоминания при переходе с одной страницы на другую;

- действий оператора

действие выполнить легко, а любых избыточных действий избегают.

Вторичная деятельность по СВР должна выполняться легко и надежно, чтобы выполнение основной деятельности не пострадало.

6.4 Координация оператора

СВР явно выражает информационную связь относительно последовательностей, назначенных отдельным членам эксплуатационной группы, то есть связь, необходимую в связи с распределением задач между операторами и начальниками смен. Такую координацию можно реализовать посредством точек приостановки в процедурах, запросом устных диалогов и компьютеризированных подтверждений.

Примечание — Например, начальник является единственным пользователем СВР и затем координирует остальных операторов, либо и начальнику, и первому и второму операторам предоставляют СВР.

Если несколько операторов могут одновременно получить доступ к одной и той же СВР, то необходимо установить правила управления одновременным доступом к одной процедуре. Необходимо определить следующие темы:

- кто может получить к ней доступ, относительно уровня авторизации;
- какой вид доступа позволен, только чтение или полное использование;
- как получают доступ к СВР с учетом обрабатываемой в настоящее время СВР;
- как предотвратить повтор или остановку оператором действия, уже запущенного другим оператором, особенно когда СВР предназначены для управления станцией. Этого можно достигнуть резервацией процедур, таким образом гарантируя, что одновременно только один оператор может использовать СВР для управления станцией, тогда как остальным операторам предоставляют доступ только на чтение.

Резервация процедуры требует определения методики в отношении возможных вызовов другой процедуры или подпроцедуры;

- какие сигналы СВР предоставлены, то есть сигналы предупреждения о том, что СВР в настоящее время используется, сигналы, указывающие, что СВР зарезервирована в течение долгого времени без использования.

Все или только конкретные процедуры можно назначить на конкретные рабочие станции.

Необходимо, чтобы в СВР была обеспечена координация операторов для параллельного использования СВР в помещении блочного пункта управления и в локальных пунктах управления.

Возможные отказы цифровой связи не должны снизить надежность и готовность СВР в MCR и в локальных пунктах управления. О существенной разнице в продвижении между операторами, применяющими одинаковый набор СВР, следует оповещать, чтобы избежать нескоординированного управления технологическим процессом.

6.5 Выходная документация

Все опции, определенные согласно 6.3 и 6.4, документально фиксируют в различных документах:

- краткое изложение опций и рациональные обоснования конструкции, разработки, этапов валидации или лицензирования;
- краткое изложение для операторов. Оно служит памяткой и легко применимо в нештатных ситуациях на станции;

- подробный документ в качестве руководства для проектирования и поддержки СВР.

Данную документацию необходимо обновлять вместе с дальнейшими изменениями СВР для гарантии полноты и согласованности.

7 Система компьютеризированных процедур

7.1 Общие положения

Данный раздел касается цифровой системы обработки СВР либо интегрируемой в систему HMI, управляющую станцией, либо независимой от нее. Рассмотрены связанные и не связанные с безопасностью требования.

Затем приведены требования к обращению с отказами системы СВР. В заключение рассмотрена выходная документация.

Безотносительно принятого решения, нельзя использовать экранные заставки (скринсейверы).

7.2 Требования безопасности

Процедуры, независимо от того, бумажные они или компьютеризированные и безотносительно их указательного уровня, предназначены для использования оператором и не могут управлять технологическим процессом без действий оператора. От оператора ожидают интеллектуальных действий, без их автоматического применения, и оператор остается единственно ответственным за их адекватное использование.

Классификацию безопасности системы СВР необходимо определить согласно МЭК 61513, принимая во внимание возможное влияние на безопасность в случае:

– потери СВР;

- ошибочной рекомендации операторам или случайных управляющих сигналов;
- готовности разнообразной информации, доступной оператору, позволяющей подтвердить информацию, отображаемую СВР. Следует обучить оператора предпринимать такие сравнения, см. 9.10.

В классификации также следует рассмотреть:

- функциональное покрытие СВР;
- семейство СВР.

Примечание — Различные виды СВР перечислены в 5.3.

КП можно реализовать в нескольких подсистемах с различными классификациями безопасности.

Требования и рекомендации, приведенные в МЭК 61513, МЭК 60880 и МЭК 62138, необходимо применять к проектированию и реализации систем СВР, в зависимости от применимости для класса безопасности системы СВР. Уровень резервирования системы СВР необходимо согласовать с классом безопасности системы СВР.

Особое внимание на этапах разработки и верификации следует уделить гарантии того, что потенциальные неисправности или отказы системы СВР не смогут блокировать, запретить или запустить ручные и автоматические функции.

7.3 Интеграция системы компьютеризированных процедур в систему человекомашинного интерфейса

С целью интеграции обработки СВР в систему HMI необходимо проверить, что:

- класс безопасности системы HMI в состоянии справиться с классом безопасности СВР согласно факторам, изложенным в 7.2;
- функции системы HMI соответствуют требованиям 5.2.3;
- Функции системы HMI соответствуют требованиям раздела 8.

7.4 Система компьютеризированных процедур, независимая от системы человекомашинного интерфейса

7.4.1 Общие положения

В данном подразделе дополнены требования безопасности, изложенные в 7.2, а затем рассмотрены связи между системой СВР и системой HMI.

7.4.2 Требования, не связанные с безопасностью

В дополнение к требованиям безопасности рассматривают дополнительные области:

- обязательно соответствие СВР требованиям 5.2.3;
- необходимо указать требования к надежности и готовности;
- необходимо определить возможности самопроверки;
- необходимо определить резервные возможности для расширения, рассмотрев такие элементы, как память, производительность процессора, объем ЗУ, пропускная способность сети, число подключенных рабочих станций.

7.4.3 Связи между системой СВР и системой HMI

Некоторые переменные, выдаваемые технологическим процессом или оборудованием, могут использоваться системой СВР и системой HMI. Если СВР предназначены для управления станцией, то система СВР и система HMI могут дополнительно быть способны отправлять команды на одни и те же приводы.

Следует предпринять меры для минимизации разности по времени при обновлении динамических частей отображений для одного и того же объекта. Можно считать приемлемым значение в диапазоне 2 с.

Не следует подвергать систему СВР опасности из-за возможных отказов системы HMI. Она оповещает об отказах своих интерфейсов с системой HMI и об отказах, блокирующих доступ к приводу.

7.4.4 Техническое обслуживание системы СВР

Необходимо рассмотреть техническое обслуживание системы СВР, то есть необходимо наличие спецификаций для испытаний, для ремонтов, для запасных частей и для специфичных инструментов. Необходимо принять меры по соблюдению требуемой продолжительности ремонта.

7.5 Отказ системы компьютеризированных процедур

Операторы должны быть обучены ставить под сомнение эксплуатационные характеристики СВР. В их поддержку в системе СВР необходимо реализовать условия самоконтроля и самопроверки для обнаружения и оповещения о неисправностях. Рассматривая возможные последствия неправильного руководства оператором, следует обеспечить как можно большее покрытие самоконтроля. Для принудительного обнаружения неисправностей СВР, часть эксплуатационной группы может использовать процедуры на бумажном носителе.

Примечание 1 — В настоящее время основными способами обнаружения неисправностей являются самоконтроль, реализованный согласно МЭК 60671, независимые механизмы мониторинга и периодическое наблюдение, выполняемое персоналом.

Если оператор подозревает о неисправности СВР, не обнаруженной или не объявленной системой, например, неожиданные отклонения параметра, то система СВР, ее части или базовые подсистемы контроля и управления можно считать недоступными.

В случае неисправности или отказа СВР или системы СВР необходимо использовать разнообразные средства резервирования и набор адаптированных процедур. Этот набор процедур резервирования должен быть совместим с системой HMI, если последняя будет все еще доступна и будет использоваться для эксплуатации станции.

Примечание 2 — В общем случае диапазон средств резервирования и сопутствующих процедур, как правило, ограничен набором функций, необходимых для поддержания станции в безопасном состоянии и минимизации влияния на эксплуатацию станции до восстановления системы СВР или основной системы HMI.

В разнообразном наборе процедур, разработанных для резервирования системы СВР, необходимо учесть, что эта ситуация редкая и напряженная, и необходимо стремиться избегать ошибок или недопонимания оператора посредством:

- независимости от системы СВР, как с технической, так и с функциональной точки зрения, то есть, отсутствие ссылок на информацию, существующую только в системе СВР;
- расчета на стратегии эксплуатации, подобные стратегиям СВР;
- предназначенности для одного и того же оперативного персонала;
- использования в максимально возможной степени одинаковых команд и графических элементов, а также представления процедуры, совместимого с представлением СВР.

Необходимо, чтобы набор процедур резервирования, а также любая сопутствующая система резервирования, были легкодоступными. Необходимо, чтобы система резервирования и набор процедур

резервирования, если они компьютеризированы, была спроектирована, разработана и утверждена согласно ее классу безопасности.

Примечание 3 — Выбор в качестве резерва второго набора СВР является сложной проблемой, поскольку подразумевает разнообразную систему СВР, характеризуемую обнаружением неисправностей, более сложным техническим обслуживанием и обучением оператора, по этой причине обычно более предпочтительны процедуры на бумажном носителе. Для принятия такого решения рассматривают также экономические аспекты.

Если СВР реализованы как отдельная от HMI система, то применяют следующее:

- система HMI отслеживает СВР и оповещает персонал пункта управления об обнаруженных отказах;
- система HMI не блокируется в случае отказа системы СВР.

7.6 Выходная документация

Требования и проектные решения системы СВР необходимо документально фиксировать в соответствии с требованиями МЭК 61513.

8 Требования к рабочему проекту

8.1 Общие сведения

В данном разделе поясняется, как компьютеризировать функции СВР, от основных до самых сложных, то есть информация, навигация, рекомендации и управление электростанцией. Также приведены разные опции, которые могут упростить использование СВР.

8.2 Основные функции компьютеризированных процедур

8.2.1 Общие положения

Для того чтобы координировать разработку, избежать неверного истолкования при использовании СВР и упростить их техническое обслуживание, необходимо определить основные функции СВР в самом начале проекта и использовать на протяжении всего жизненного цикла СВР. Их необходимо использовать для проектирования, разработки и поддержки набора СВР.

Примечание — Обновлять СВР могут лица, отличные от лиц, изначально их разработавших.

Данную деятельность ведет объединенная группа, представленная в 9.3. Учитывают данные обратной связи на основе опыта использования процедур на бумажном носителе и известных других случаев использования СВР.

Для проектирования и отображения форматов СВР используют МЭК 61772 и ИСО 11064. Форматы СВР и рабочие форматы, отображаемые в MCR, должны быть совместимы. Данная совместимость затрагивает такие функции HMI, как графическое представление, имена переменных, схема формата, навигация и т. д.

КП реализуют с помощью дисплейных форматов согласно 5.2.3, включая форматы для отображения на местных станциях управления при необходимости.

Любые последующие изменения функций, определенных согласно данному подпункту, обосновывают, формально принимают и документируют.

8.2.2 Основные свойства, необходимые для СВР

Следующие основные свойства СВР следует определить точным и однозначным образом:

- все технические термины, обозначения и графические элементы;
- глоссарий, содержащий значение и использование каждого элемента формата;
- обозначения или рисунки, представляющие элементарные шаги СВР, а также связи между ними.

Каждый тип элементарного шага СВР обрабатывают таким же образом, но он может запустить различные действия из-за своего содержимого. Например, схема принятия решения запускает выполнение формулы, которую содержит, и может предложить дальнейшие действия в зависимости от ее результата;

- правила обработки содержимого шагов СВР;
- правила назначения имен между расчетными или внутренними переменными;

Примечание — Имена переменных помогают оператору понять тип и использование расчетной переменной.

- правила навигации между элементарными шагами, страницами или последовательностями одной СВР или между разными СВР.

Такие элементы, как «шаги», «индикаторы», «блоки принятия решений», а также их сочетания, которые предназначены для обобщенного использования, следует определить в качестве элементов многократного использования с набором параметров, подлежащих уточнению.

8.2.3 Правила представления

С целью минимизации умственной нагрузки оператора и согласованности с обобщенными требованиями 5.4.2 представление СВР следует разработать так, чтобы:

- местные действия были четко идентифицированы;
- оператору был предоставлен обзор выполняемых в данный момент процедур и прерванных в данный момент процедур;
- представление процедуры согласовалось со всеми СВР и с парадигмами представления системы HMI;
- была минимизирована возможность ошибок оператора с помощью и СВР, и цифровой системы HMI для управления станцией;
- информацию, необходимую для выполнения процедуры, можно было прочитать из рабочего положения оператора;
- всегда отображалась самая новая утвержденная и выпущенная версия процедуры.

Для минимизации ошибок оператора содержимое формата:

- отображает идентификацию текущей процедуры и текущей последовательности в рамках этой процедуры;
- четко идентифицирует достигнутые шаги, активный шаг и возможные следующие шаги;
- минимизирует число дискретных действий для доступа к требуемому отображению формата;
- упрощает диалог между оператором и процедурой.

8.2.4 Схема дисплейного формата СВР

Схему дисплейного формата СВР разрабатывают таким образом, чтобы

- идентификатор процедуры, т. е. название и функциональный код, а также функциональные цели процедуры были постоянно видны в виде части формата процедуры и имели свое постоянное местоположение в формате;
- распределение информации подчинялось одному и тому же методу во всех процедурах;
- деление процедуры на последовательности выполнялось согласно единообразным правилам;
- важность шагов отображалась явно выраженным образом;
- предупреждения, предостережения и прочая информация, связанная с одиночным шагом, была видна при каждом отображении этого шага;
- любые предупреждения, предостережения и информация такого рода были представлены таким образом, что их нужно читать, например, при помощи всплывающих меню, которые должны быть подтверждены оператором, прежде чем оператор начнет выполнять этот шаг.

8.2.5 Требования к представлению отдельных дисплейных элементов

Правила представления отдельных элементов следующие:

- информация и фрагменты шага должны выглядеть различным образом;
- представление схем принятия решений с сопутствующими вариантами выбора (например, «да» или «нет») единообразно независимо от процедуры;
- в случае если необходим отклик оператора, автоматическое исполнение не продолжается без отклика оператора.

При наличии в форматах процедур повторяющихся элементов информации, таких как набор элементов станции, набор аналогичных действий и т. д., представление данных элементов информации выполняют в виде списков. Проектом предусмотрено, что:

- список выделяется из прочих фрагментов процедуры;
- приоритет элементов списка ясно обозначен;
- во всех списках присутствует заголовок;
- к списку привлекают внимание оператора.

8.3 Информация, выдаваемая от компьютеризированных процедур

8.3.1 Общие положения

КП выдают информацию, связанную с ними самими, например, назначение, версию, дату выпуска, номер страницы. Элементы данного описания отображаются либо систематически, либо по запросу оператора.

Все семейства СВР представляют данный тип информации:

- чтобы оператор мог правильным образом использовать рекомендации СВР;
- чтобы держать оператора в курсе происходящего.

Сигнализации и сообщения, генерируемые неким технологическим процессом или ошибкой при установке, необходимо адаптировать к этапу эксплуатации, на котором они могут отображаться, чтобы не вводить в заблуждение оператора и не вызывать у него сомнений.

Генерируемые в СВР сигнализации необходимо отображать таким же образом, как и сигнализации, генерируемые событиями технологического процесса или оборудования. В качестве справочного материала по проектированию используют МЭК 62241.

8.3.2 Информация для СВР семейства 1

КП семейства 1 аналогичны процедурам на бумажном носителе, они указывают отслеживаемые значения для технологического процесса или оборудования, но не отображают динамической информации от станции.

8.3.3 Информация для СВР семейства 2

В целях адекватного понимания эксплуатации, в информацию СВР необходимо включить все показания и входные данные от технологического процесса или оборудования:

- необходимые для понимания и выполнения стратегий эксплуатации;
- необходимые для понимания контекста, состояния станции и отображаемых сообщений, связанных с процедурой.

Качество информации СВР обеспечивают:

- адаптацией частоты обновлений к потребностям процедуры;
- незамедлительным представлением возможного конфликта между введенными данными оператора и поступившими или вычисленными значениями.

Организуют простой доступ оператора к информации по перекрестным ссылкам. Шаги процедур на бумажном носителе, связанные с перекрестной проверкой данных, переносят на решение СВР.

Для пользователя обеспечивают индикацию доступности информации. В общем смысле, обеспечивают доступность статуса информации, например: доступна, доступ запрещен из-за тестирования, доступ запрещен из-за технического обслуживания, недоступна, не согласуется с прочими входными данными.

Применение методики проектирования приводит к решениям об отображении:

- итоговой информации;
- информации, связанной с состоянием станции;
- информации, выбранной оператором.

Данные опции могут потребовать, чтобы дополнительные значения были рассчитаны системой СВР на основе входных данных или иных внутренних значений. Также это может привести к требованию дополнить необработанные входные данные индикацией их надежности, получаемой, к примеру, в ходе перекрестных проверок различных значений.

Следует обеспечить, чтобы дополнительные расчетные значения:

- были доступны оператору как любые иные получаемые полевые сигналы;
- были легко идентифицируемы при отображении на дисплее, например, с помощью особого кодирования или особого цвета.

Свойства информации могут отличаться в зависимости от типов процедур, перечисленных в 5.2, при условии, что форматы HMI остаются единообразными.

Методика руководства может потребовать оповещения о возможных расхождениях между действиями оператора и предложенным решением.

8.3.4 Информация для СВР семейства 3

Для автоматического управления станцией необходимо предоставить для СВР семейства 3 все типы информации СВР семейства 2, как обязательной, так и факультативной.

8.4 Навигация

8.4.1 Общие положения

Наряду с методиками HMI и СВР следует реализовать возможности навигации.

8.4.2 Навигация для СВР семейства 1

Навигация для СВР семейства 1 охватывает возможности выборки страниц или последовательностей, чтобы переходить непосредственно к страницам, проглядывать страницы и выбирать термины на страницах.

Можно реализовать расширенные возможности выборки страниц или последовательностей, такие как закладки, всплывающие окна или миниатюры. Всплывающие окна должны появляться в предопределенных частях форматов, не скрывая слишком большой части формата, и должны легко перемещаться с одного места на другое.

Можно предоставить ссылки на соответствующие процедуры, например, на регламент или на процедуру реагирования на пожарную тревогу. Их не следует путать с отдельными шагами.

В случае если одновременно активны несколько процедур, то следует предусмотреть возможность перейти от одной к другой, даже если она в настоящий момент не отображается.

8.4.3 Навигация для СВР семейства 2 и семейства 3

Навигация для СВР семейства 2 и семейства 3 расширяет функции навигации СВР семейства 1 на последовательности и отдельные шаги внутри процедуры.

Кроме того, можно изучить процедуры согласно типам шагов, например, для поиска следующего этапа принятия решений в отношении давления в первом контуре реактора.

Следует предусмотреть возможность отслеживать путь, пройденный оператором до текущей ситуации. Данные хронологические форматы не следует путать с форматами, связанными с текущей ситуацией.

8.5 Методические рекомендации по компьютеризированным процедурам

8.5.1 Общие положения

Методические рекомендации по СВР опираются на те же основы, что и процедуры на бумажном носителе, но расширяются с целью выполнения методики компьютеризации. Данные рекомендации варьируются от элементарной информации о технологическом процессе до расширенной помощи в отношении:

- доступа СВР;
- диагностики;
- принятия решений.

Примечание — Подробности рекомендаций различаются, частично из-за природы процедур, например, аварийные процедуры содержат больше рекомендаций, чем процедуры нормальной эксплуатации, и частично из-за ожидаемого уровня знаний оператора, который опирается на методику обучения.

8.5.2 Доступ к СВР

Доступ к процедурам на бумажном носителе происходит в зависимости от их природы:

- в случае изменения состояния станции, например, пуска или простоя;
- в случае тревожной сигнализации или сигнала от технологического процесса или оборудования;
- периодически, например, процедуры надзора вводят при каждой передаче смены.

В случае СВР события станции или периодические события могут автоматически оповещать о том, к какому типу СВР будет произведен доступ. Можно рекомендовать или автоматически выбрать конкретную процедуру.

Доступ к нужной процедуре следует сделать как можно более прямым, т. е. следует избегать слишком сложных путей выбора.

СВР могут также позволить оператору автоматически контролировать показатели технологического процесса или оборудования и определять пороги этих значений. При достижении порога может выдаваться сигнал, и, при условии, что ни необходимая информация, ни требуемые заранее действия и сигналы предупреждения не обойдены, можно получить прямой доступ и отобразить соответствующий шаг СВР.

В СВР следует сохранить ручной доступ, а инициирующее событие следует отображать по запросу оператора.

8.5.3 Помощь в диагностике

Некоторые конкретные ситуации на станции, например, аварии или любое событие, о котором свидетельствует отклонение параметров безопасности, которые может четко идентифицировать проектировщик, можно идентифицировать и формализовать, чтобы об их возникновении при эксплуатации можно было оповещать.

Оператор остается ответственным за приемку результатов диагностики и доступ к предложенной процедуре.

Подробности диагностики следует отображать по запросу оператора.

8.5.4 Помощь в принятии решений

Помощь в принятии решений следует ограничить шагами, требующими принятия решения. Необходимо, чтобы такая информация, как входные данные, тревожные сигнализации, графики, синтезируемые значения и т. п., которые затем необходимы, были доступны и легко отображались.

Оператор остается ответственным за принятие любого решения.

С целью расширения помощи в принятии решений СВР оповещает о том, что:

- предложенная процедура запущена;
- каждый шаг утвержден оператором;
- каждый шаг получил положительный сигнал обратной связи;
- выбор оператора в случае этапа принятия решения совпадает с предложением;
- цели рассматриваемой процедуры были достигнуты.

Для подтверждения того, что действия оператора соответствуют шагам СВР, можно использовать ответные контрольные сигналы от приводов, например, в сложных ситуациях. В случае этой опции о несоответствиях следует оповещать, но они не должны препятствовать действиям оператора.

8.5.5 Компьютеризация методического руководства СВР

Независимо от типа и уровня руководства СВР необходимо компьютеризировать таким образом, чтобы:

- они отображали все необходимые элементы, позволяющие оператору понимать и управлять станцией в любой ситуации;
- они предоставляли разумный и уместный уровень информированности, чтобы оператор мог ее усваивать, не отвлекаясь и не приходя в замешательство от неадекватной помощи;
- они оставляли за оператором ответственность за его действия, запрашивая от него либо утверждения предложений, либо выбора курса действий, отличных от предложенных действий;
- они выдавали по запросу оператора отображение обоснований для предложений;
- они проводили различие между предложениями и шагами или информацией;
- они не скрывали важную часть отображаемого формата менее важной информацией;
- легко обнаруживалось прекращение обновления информации, например, обусловленное отказом оборудования.

Помощь отображается по запросу оператора, а оператор в состоянии ее отключить в любое время.

Оператору предоставляют средства временного запрета отображения предупредительных сообщений, которые могут выдаваться благодаря функциям помощи.

Может быть предложено использование иных процедур и предоставлены ссылки на них.

8.6 Автоматизация на основе процедур

8.6.1 Общие положения

СВР могут предназначаться для автоматической обработки некоторых эксплуатационных задач под управлением оператора.

8.6.2 Взаимодействия между операторами и автоматизацией на основе процедур

Распределять задачи между операторами и цифровыми системами необходимо на основе МЭК 61839, возможно, с обоснованием по критериям, связанным с конкретным проектом. СВР необходимо разработать так, чтобы они:

- информировали оператора о том, что обрабатывается;
- позволяли оператору выполнять ручное управление в любое время;
- информировали оператора о состоянии СВР, например, только чтение, автоматическое выполнение и т. п.;
- позволяли оператору возобновить автоматическое выполнение после ручного прерывания последовательности;

- сигналом тревоги привлекали внимание оператора к неожиданному событию, которое может помешать правильной обработке процедуры. Оператору предоставляют средства отображения причины такого сигнала тревоги.

Следует изучить дополнительные возможности, например, СВР могут позволить операторам выбирать части СВР для их автоматической обработки.

8.6.3 Проектирование СВР для управления станцией

С целью управления станцией СВР необходимо проектировать таким образом, чтобы:

- последовательности начинались и заканчивались в одной и той же процедуре;
- между управляющими воздействиями от управляющих последовательностей СВР и прочими управляющими воздействиями устанавливался согласно правилам назначения приоритет для ручных и автоматических функций;
- последовательности были предопределены и фиксированы. Они могут включать в себя точки приостановки, требующие подтверждения от операторов;
- сначала проверялась доступность оборудования или схемы, в случае необходимости для обработки шага;
- автоматические действия получали метки времени и заносились в архив, так же как и ручные команды операторов.

В случае если некоторые процедуры нельзя отобразить на дисплее, либо потому, что их слишком много, либо из-за ограниченных возможностей дисплея, следует предусмотреть возможность для скрытых процедур:

- оповещать или выдавать сигнал тревоги о значимых событиях;
- периодические признаки жизни, чтобы показать, что обработка еще продолжается. Как вариант, некоторые процедуры можно автоматически останавливать или «замораживать» в зависимости от спецификации проектировщика;
- отображения по запросу оператора.

На этапе проектирования следует провести анализ и показать, что эксплуатация не подвергается угрозе, даже если некоторые процедуры не отображаются на дисплее постоянно.

8.7 Прочие средства компьютеризированных процедур

Для каждого типа процедуры рассматривают различны опции:

- может быть предоставлена возможность включения записей оператора в СВР. Это соответствует привычной работе оператора с бумажными процедурами. Названные записи можно использовать, например, для указания потребности во временном отклонении от СВР при особых условиях, которые подлежат уточнению;
- оператору может быть предоставлена возможность выбора конкретных отслеживаемых технологических значений;
- могут быть предоставлены средства отслеживания и архивирования.

В случае нечастых ситуаций на станции может быть принято решение регистрировать и архивировать управление ситуацией посредством использования СВР с целью проанализировать его позже;

- регистрация мероприятий.

Может представлять ценность автоматическая регистрация мероприятий, проводимых в ответ на шаги СВР;

- можно предоставить возможность адаптации методического руководства к ситуации с целью позволить оператору выбирать уровень руководства, адаптированный к его навыкам относительно конкретных СВР или последовательностей.

8.8 Выходная документация

Все опции, определенные согласно разделу 8, следует фиксировать в разных документах:

- краткое изложение опций и обоснований для этапов проектирования, разработки, валидации или лицензирования;
- краткое изложение для операторов. Его следует воспринимать как памятку, которую легко использовать при нештатных ситуациях на станции;
- подробный документ, предназначенный для использования в качестве руководства по проектированию и обслуживанию СВР.

Указанную документацию необходимо обновлять вместе с последующими модификациями СВР для гарантии полноты.

9 Жизненный цикл компьютеризированных процедур

9.1 Общие сведения

В данном пункте установлены требования и рекомендации для всего жизненного цикла СВР от организации проекта до обслуживания СВР и обучения оператора, при этом особое внимание уделено верификации и валидации СВР.

9.2 Организация проекта

Проект компьютеризации процедуры аккумулирует аспекты HMI, стратегий эксплуатации и технологии программирования. Организационные аспекты HMI и стратегий эксплуатации аналогичны аспектам процедур на бумажном носителе. Если система СВР классифицирована по классу безопасности, то аспекты программного обеспечения следует устанавливать на основе МЭК 61513, учитывая, что она аналогична любой другой разработке программного обеспечения и рассматривает СВР, классифицированные или не классифицированные по классу безопасности.

Затем первой задачей является организация проектной группы, обладающей всеми необходимыми компетенциями, и определение полномочной комиссии.

На основе методики СВР, проектная группа несет ответственность за:

- проектирование процедур;
- разработку процедур;
- верификацию и валидацию;
- экспертизу и утверждение процедур;
- пересмотр процедур.

Для гарантии качества и контролепригодности в ходе типичных этапов жизненного цикла процедуры следует использовать технические средства. На всех этапах проекта компьютеризация обладает потенциальным преимуществом и может облегчить выполняемую работу, особенно отслеживаемость и архивирование различных версий.

Следует организовать формальные экспертизы и архивировать заключения.

9.3 Проектная группа

В целях проектирования, разработки, испытаний и особенно валидации СВР объединяют различные виды участников:

- проектировщиков процедур;
- специалистов по проблемам человеческого фактора;
- специалистов по компьютерам, при необходимости;
- все категории конечных пользователей, т. е. начальников смен, операторов, возможно, полевых операторов.

Опыт и потребности операторов, а также гибкость и емкость отображений учитывают при проектировании наглядности и восприятия СВР для более быстрого усвоения СВР оператором.

Названных специалистов включают в группу, и они начинают совместную работу с начала проекта.

9.4 Программа верификации и валидации

Необходимо учредить программу верификации и валидации для гарантии того, что на протяжении всего этапа разработки соблюдаются требования разделов 6 и 8, и для подготовки заключительной верификации и валидации законченного продукта.

При верификации СВР необходимо рассмотреть как соответствие визуальных дисплейных форматов спецификациям HMI, так и технические аспекты, которые анимируют процедуры.

При валидации СВР необходимо рассмотреть и функциональные, и эргономические аспекты для гарантии того, что состоящая из операторов эксплуатационная группа преуспеет в достижении целей безопасности и работоспособности при использовании СВР.

Стратегию верификации и валидации следует определить на ранней стадии проекта, чтобы запланировать необходимые ресурсы, т. е. операторский и цифровой инструментарий. Также следует запланировать адекватные средства регистрации.

9.5 Программирование компьютеризированных процедур

Опции, определенные в 6.3 и 6.4, следует оценить на ранней стадии проекта на макете, чтобы не усомниться при разработке СВР.

Необходимо определить программу обеспечения качества, учитывающую классификацию СВР по безопасности, для проверки того, что:

- требования разделов 6—8 учтены правильным образом;
- обеспечена отслеживаемость разработки;
- архивирование разработанного программного обеспечения выполняется регулярно, а резервные файлы доступны и надежны;
- покрытие тестов оптимально, и обеспечена отслеживаемость и архивирование тестов;
- управление версиями выполняется правильно.

Могут применяться требования МЭК 61513, МЭК 60880 и МЭК 62138 в зависимости от класса безопасности СВР системы СВР.

9.6 Верификация и валидация компьютеризированных процедур

9.6.1 Общие положения

В данном подразделе рассмотрены верификация и валидация и технических, и эргономических аспектов СВР, с допущением о том, что верификация и валидация в отношении аспектов программного обеспечения СВР уже выполнены согласно надлежащим требованиям к безопасности и качеству.

Необходимо, чтобы организация обеспечения качества гарантировала, что любой обнаруженный отказ исправляют надлежащим образом, а сопутствующую документацию соответственно обновляют.

9.6.2 Техническая верификация СВР

Цель верификации СВР — обнаружение ошибочного применения функций 8.2, а именно:

- использование неопределенных символов, слов, графиков и т. д.;
- несоответствия между именами переменных и отображаемой информацией;
- несоответствия между текстом шага и руководством;
- несоответствия между текстом шага и соответствующей командой.

Цель верификации — обнаружение ошибочного проектирования или программирования процедур, препятствующего достижению целей безопасности или эксплуатации, например:

- замкнутые циклы в процедурах;
- взаимоблокировки, процедура А ожидает информацию от процедуры В, тогда как процедура В ожидает информацию от процедуры А;
- открытые или неверные ссылки на страницы или шаги.

Предусматривают условия, чтобы техническая верификация СВР:

- была как можно более всесторонней исходя из технической возможности и целесообразности;
- опиралась на методы и инструментарий, сводящие к минимуму неоднозначности толкования человеком;
- выдавала проверяемые результаты;
- и легко поддавалась анализу;
- облегчала регрессионное тестирование.

С целью обнаружения возможных ошибок, как в программировании, так и в эксплуатации, рекомендуется автоматически обрабатывать все или избранные процедуры, чтобы отработать предопределенные сценарии, рассчитанные имитатором технологического процесса. Сценарии, включая нештатные ситуации на станции, определяют, чтобы активировать как можно больше функциональных возможностей СВР.

9.6.3 Функциональная и эргономическая валидация

Валидацию выполняют таким же образом, как для процедур на бумажном носителе, с участием полной эксплуатационной группы и полномасштабного технологического имитатора, способного моделировать как можно точнее нормальные и аномальные переходные процессы, для которых предназначена СВР.

Функциональная и эргономическая валидация нацелена на гарантию того, что:

- оператор может понять и применить СВР правильным образом;
- СВР помогает оператору достигнуть ожидаемых функций;
- не остается необнаруженных ошибок в стратегии эксплуатации;

- СВР повышает надежность действий оператора и снижает риск того, что оператор не соблюдает регламент;
- операторам в любое время предоставляется надлежащее представление технологического процесса и их продвижения по ходу процедур;
- координация в группе правильна;
- операторы способны контролировать и обнаруживать любой отказ в системе СВР;
- операторы способны переключаться с СВР и системы СВР на набор резервных процедур и обратно;
- наглядность и восприятие СВР совместимы с наглядностью и восприятием, реализованными в системе HMI.

При валидации необходимо оценить специфические вопросы компьютеризации следующим образом:

- навигация между страниц

оператору может быть трудно понять, какую часть стратегии он применяет, и спланировать свои следующие действия, «перелистывая» компьютеризированные страницы;

- туннельный эффект

оператор может потерять способность думать самостоятельно, каковы бы ни были этому причины. Например, оператор может потерять осознание стратегии и применять СВР механически, или для правильного использования СВР необходимо слишком сосредоточиться, так что оператор уже не понимает их содержания;

- абстрактное мышление операторов

оператор должен быть способен в полной мере и с легкостью понимать состояние станции и возможные последствия действий, предлагаемых СВР;

- информационная связь между членами эксплуатационного персонала и, возможно, с лицами, не входящими в эксплуатационный персонал.

9.7 Внедрение компьютеризированных процедур

СВР обычно реализуют как программное приложение, выполняемое в системном программном обеспечении (далее — ПО), независимом от приложений. Нижеследующие формулировки относятся к внедрению данного программного приложения. Модификация системного ПО системы СВР, как правило, подразумевает дополнительные ограничения, не представленные здесь.

СВР необходимо внедрять слаженными и четко определенными наборами. Набор может охватывать несколько типов процедур, которые взаимозависимы.

Каждый набор необходимо внедрять в режиме «онлайн» единым пакетом, не оказывая влияния на операции станции. Обработку следует существенно автоматизировать.

Для внедрения новой версии СВР необходимо выполнение следующих условий:

- учтены результаты этапа верификации и валидации;
- операторы адекватно обучены и информированы;
- при необходимости возможна переустановка старой версии СВР.

С целью упрощения местного управления СВР, на этапах проектирования и разработки СВР следует выдать некоторые специфические требования к:

- интерактивным средствам управления;
- версии СВР, которая:
  - легко внедряется, т. е. это существенно автоматизированный процесс,
  - не требует изменения состояния станции,
  - не влияет на эксплуатацию станции,
  - не влияет на систему HMI, при наличии таковой,
  - не влияет на операционную систему системы СВР;
- архивированию старой версии СВР.

Для каждого внедрения необходимо обеспечить адекватное качество, т. е. подробную обработку и контролепригодность. Следует избегать слишком частого внедрения вновь разработанных или пересмотренных СВР.

Перед внедрением новой версии необходимо обучить ее использованию все эксплуатационные смены.

Инциденты в системе СВР и ошибки СВР регистрируют и оперативно передают в организацию обслуживания.

9.8 Выходная документация

Следует использовать МЭК 61513, МЭК 60880 и МЭК 62138 для выпуска адекватной документации в отношении:

- организации проектирования, разработки и валидации СВР, а также организации обслуживания СВР после вода в действие, на основе требований 9.3 и 9.4;
- документов по программированию и документов, указанных в 9.5;
- верификации и валидации, см. 9.6;
- следует автоматизировать для упрощения нерегрессионного тестирования в случае обновления СВР;
- внедрения СВР, см. 9.7.

Необходимо вести обзор полной документации, приведенной в разделах 5—9 для гарантии ее полноты и согласованности.

9.9 Обслуживание компьютеризированных процедур и системы компьютеризированных процедур

Обновление СВР необходимо подготовить в автономном режиме и планировать таким же образом, как для процедур на бумажном носителе.

Для каждой реализации значительных изменений следует предусмотреть меры обеспечения качества для как можно более раннего обнаружения ошибок. К верификации процедур можно привлекать операторов.

В системе СВР следует обеспечить структуру системного ПО, которая позволяет загружать версии СВР без лишних изменений в эксплуатации, обеспечиваемой самой системой СВР.

Необходимо вести хронологическую документацию эксплуатации, ремонта и обслуживания системы СВР, если она автономна. Необходимо проводить оценку эксплуатационных записей и отчетов с определенной периодичностью для идентификации и инициирования любых мероприятий по обслуживанию или модификации, которые могут понадобиться. В случае если СВР обрабатываются как часть цифровой системы HMI, при обслуживании последней необходимо учитывать готовность и надежность СВР.

Примечание — Точные требования к документации зависят от конкретной эксплуатирующей организации.

9.10 Обучение оперативного персонала

Необходимо, чтобы фундаментальные цели и организация обучения были аналогичны целям и организации для процедур на бумажном носителе. Операторы, участвовавшие в этапах валидации СВР, помогают разрабатывать программу обучения.

Необходимо, чтобы обучение дополнительно приучило оператора:

- вести эксплуатацию станции с помощью СВР во всех применимых случаях ее реализации;
- периодически принимать необходимые меры для правильного функционирования системы СВР и обнаруживать потенциальные отказы;
- вести данные в систему резервирования процедур и дублировать процедуры, а также эксплуатировать станцию с их помощью.

В случае если в качестве резервной копии используются процедуры на бумажном носителе, в ходе обучения необходимо компенсировать недостаток опыта их применения.

Следует предусмотреть обратную связь в передаче опыта и его использование в будущем, например, модернизировать СВР и усовершенствовать обучение операторов. Сбор данных обратной связи от эксплуатационного опыта ведут с начала проекта.

Особое внимание следует уделить первым месяцам эксплуатации с помощью СВР.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
IEC 60671	—	*
IEC 60880	IDT	ГОСТ Р МЭК 60880—2010 «Атомные электростанции. Системы контроля и управления, важные для безопасности. Аспекты программного обеспечения компьютерных систем, выполняющих функции категории А»
IEC 60964:2009	—	ГОСТ Р МЭК 60964:2009—2012 «Атомные станции. Пункты управления. Проектирование»
IEC 60965:2009	—	*
IEC 61513	—	ГОСТ Р МЭК 61513—2011 «Атомные станции. Системы контроля и управления, важные для безопасности. Общие требования»
IEC 61772	—	*
IEC 62138	—	ГОСТ Р МЭК 62138—2010 «Атомные электростанции. Системы контроля и управления, важные для безопасности. Программное обеспечение компьютерных систем, выполняющих функции категорий В и С»
IEC 62241:2004	—	*
ISO 11064 (все части)	—	*

*Соответствующий национальный стандарт отсутствует. До его утверждения рекомендуется использовать перевод на русский язык данного международного стандарта. Перевод данного международного стандарта находится в Федеральном информационном фонде технических регламентов и стандартов.

Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандарта:

- IDT — идентичный стандарт.

Библиография

IEC 61226, Nuclear power plants — Instrumentation and control systems important to safety — Classification of instrumentation and control functions

IEC 62645[1)], Nuclear power plants — Instrumentation and control systems — Requirements for security programmes for computer-based

[1)] Находится на рассмотрении.

УДК 621.311.049.75:006.354 ОКС 27.120.20 IDT

Ключевые слова: атомные станции; пункты управления, компьютеризированные процедуры, валидация компьютеризированных процедур, верификация компьютеризированных процедур

Редактор *В.А. Сивалапов*
Технический редактор *В.Н. Прусакова*
Корректор *О.В. Лазарева*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 22.06.2016. Подписано в печать 05.07.2016. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 3,72. Уч.-изд. л. 3,36. Тираж 25 экз. Зак. 1588.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.

gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru