ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р МЭК 61839— 2021

ПУНКТЫ УПРАВЛЕНИЯ АТОМНЫХ СТАНЦИЙ

Функциональный анализ и распределение функций при проектировании

(IEC 61839:2000, Nuclear power plants — Design of control rooms — Functional analysis and assignment, IDT)

Издание официальное

Москва
Стандартинформ
2021

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Акционерным обществом «Русатом Автоматизированные системы управления» (АО «РАСУ») на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 4

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 16 апреля 2021 г. № 222-ст

4 Настоящий стандарт идентичен международному стандарту МЭК 61839:2000 «Атомные электростанции. Проектирование пунктов управления. Функциональный анализ и распределение функций (IEC 61839:2000 «Nuclear power plants — Design of control rooms — Functional analysis and assignment», IDT).

Наименование настоящего стандарта изменено относительно наименования указанного международного стандарта для приведения в соответствие с ГОСТ Р 1.5—2012 (пункт 3.5).

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

Дополнительные сноски в тексте стандарта, выделенные курсивом, приведены для пояснения текста оригинала

5 ВВЕДЕН ВПЕРВЫЕ

*Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (*gost.e-ecolog.ru

© IEC, 2000 — Все права сохраняются
© Стандартинформ, оформление, 2021

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
2 Нормативные ссылки . . . 1
3 Термины и определения . . . 2
4 Процедура анализа и распределения функций . . . 2
4.1 Общее описание . . . 2
4.2 Основная техническая группа для выполнения ФА и распределения функций . . . 5
5 Функциональный анализ . . . 5
5.1 Общие положения . . . 5
5.2 Выявление функций . . . 5
5.3 Определение основных требований к информации и ее обработке . . . 6
6 Распределение функций . . . 7
6.1 Общие положения . . . 7
6.2 Анализ функций управления . . . 7
6.3 Разработка критериев распределения . . . 8
6.4 Процесс распределения . . . 11
Приложение А (справочное) Примеры декомпозиции целей и подцелей . . . 12
Приложение В (справочное) Начало функционального анализа ВВЭР (водо-водяного реактора под давлением) . . . 13
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов национальным стандартам . . . 14
Библиография . . . 15

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПУНКТЫ УПРАВЛЕНИЯ АТОМНЫХ СТАНЦИЙ

Функциональный анализ и распределение функций при проектировании

Control rooms of nuclear power plants.
Functional analysis and assignment when designing

Дата введения — 2021—12—01

1 Область применения

Настоящий стандарт устанавливает требования к функциональному анализу (ФА) и процедуре назначения функций (называемой также распределением функций) при проектировании системы пункта управления атомных станций и определяет правила разработки критериев для назначения функций*.

Настоящий стандарт дополняет МЭК 60964, применяемый при проектировании пунктов управления атомных станций.

Цель настоящего стандарта состоит в изложении специфических требований к проведению ФА и распределению функций, предусмотренных в 3.1 и 3.2 МЭК 60964, и, следовательно, данный стандарт заменяет руководство, приведенное в А.3.1 и А.3.2 МЭК 60964.

Настоящий стандарт допускается применять при проектировании новых или усовершенствовании (обновлении или модификации конструкции) существующих пунктов управления. В последнем случае следует уделять особое внимание определению областей, которые будут подвергнуты изменениям как непосредственно, так и косвенно.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты. Для датированных ссылок применяют указанное издание ссылочного стандарта. Однако при взаимном согласии заинтересованные стороны могут рассмотреть возможность применения последнего издания документа, указанного ниже. Для недатированных ссылок применяют последнее издание (включая все изменения).

IEC 60964:1989**, Design for control rooms of nuclear power plants (Проектирование пунктов управления атомных станций)

IEC 61771:1995, Nuclear power plants — Main control room — Verification and validation of design (Атомные станции. Блочный пункт управления. Верификация и валидация проекта)

---

* *Положения настоящего стандарта действуют в целом в отношении сооружаемых по российским проектам атомных станций за пределами Российской Федерации, а также в отношении сооружаемых на территории Российской Федерации атомных станций в части, не противоречащей требованиям Федеральных норм и правил в области использования атомной энергии.*

** *Заменен на IEC 60964:2018 «Nuclear power plants. Control rooms. Design».*

Издание официальное

3 Термины и определения

В настоящем стандарте применены термины по МЭК 60964, а также следующие термины с соответствующими определениями:

3.1 **аварийные условия** (accident conditions): Совокупность условий, установленных в отчетах по анализу безопасности или переходных процессов и/или в ходе действий по ликвидации аварий*.

3.2 **распределение функций** (functional assignment): Распределение функций между человеком и автоматизированными компонентами системы.

3.3 **человеко-машинный интерфейс;** ЧМИ (human machine interface, HMI): Взаимодействие между оперативным персоналом и системами контроля и управления, а также информационно-вычислительными системами, обеспечивающими управление системами атомной станции**. Интерфейс данного взаимодействия включает в себя средства отображения информации, органы управления и интерфейс системы поддержки оператора (см. человеко-машинный интерфейс в МЭК 60964).

3.4 **вероятностный анализ безопасности;** ВАБ (probabilistic risk assessment, PRA): Системный подход к определению последовательности аварийных ситуаций, которые могут быть инициированы широким кругом исходных событий, включающий в себя системный анализ и оценку частоты и последствий аварий***.

3.5 **функция управления** (control function): Управляющие действия, включая связанные с ними сбор и обработку информации, выполняемые людьми и ЭВМ для достижения функциональной цели*[4, 1)].

3.6 **задачи** (tasks): Управляющие действия, осуществляемые людьми для достижения функциональной цели[1)].

4 Процедура анализа и распределения функций

4.1 Общее описание

В соответствии с требованием раздела 3 МЭК 60964 анализ и распределение функций необходимы в качестве первого шага при проектировании пункта управления (см. рисунок 1). Цель этой процедуры состоит, прежде всего, в выявлении всех функций, необходимых для работы атомной станции, и последующем назначении этих функций людям или машинам.

Должны быть выполнены два основных шага:

a) функциональный анализ;

b) распределение функций.

Эти процедуры описаны соответственно в разделах 5 и 6.

---

* *В НП-001-15 под термином «авария на АС (авария)» понимают нарушение нормальной эксплуатации АС (атомной станции), при котором произошел выход радиоактивных веществ и/или ионизирующего излучения за границы, предусмотренные проектной документацией АС для нормальной эксплуатации, в количествах, превышающих установленные пределы безопасной эксплуатации. Авария характеризуется исходным событием, путями протекания и последствиями.*

** *В НП-026-16 под термином «интерфейс «человек-машина» понимают совокупность предусмотренных в проекте АС технических мер по обеспечению оператора АС необходимой информацией и возможностями для контроля и управления системами и элементами АС.*

*** *В НП-001-15 под термином «вероятностный анализ безопасности» понимают качественный и количественный анализ безопасности АС, выполняемый для определения вероятности реализации путей протекания и конечных состояний аварий, в том числе вероятности тяжелых аварий и большого аварийного выброса.*

[4] В НП-026-16 под термином «управляющая функция» понимают совокупность действий управляющих систем, важных для безопасности (функциональной группы), направленную на достижение определенной цели, указанной в проектной документации АС, реализующую управление объектом (системой или элементом АС) по заданным целям, критериям и ограничениям.

[1)] Настоящее определение отличается от определения, данного в МЭК 60964, однако отражает современное использование данного понятия.

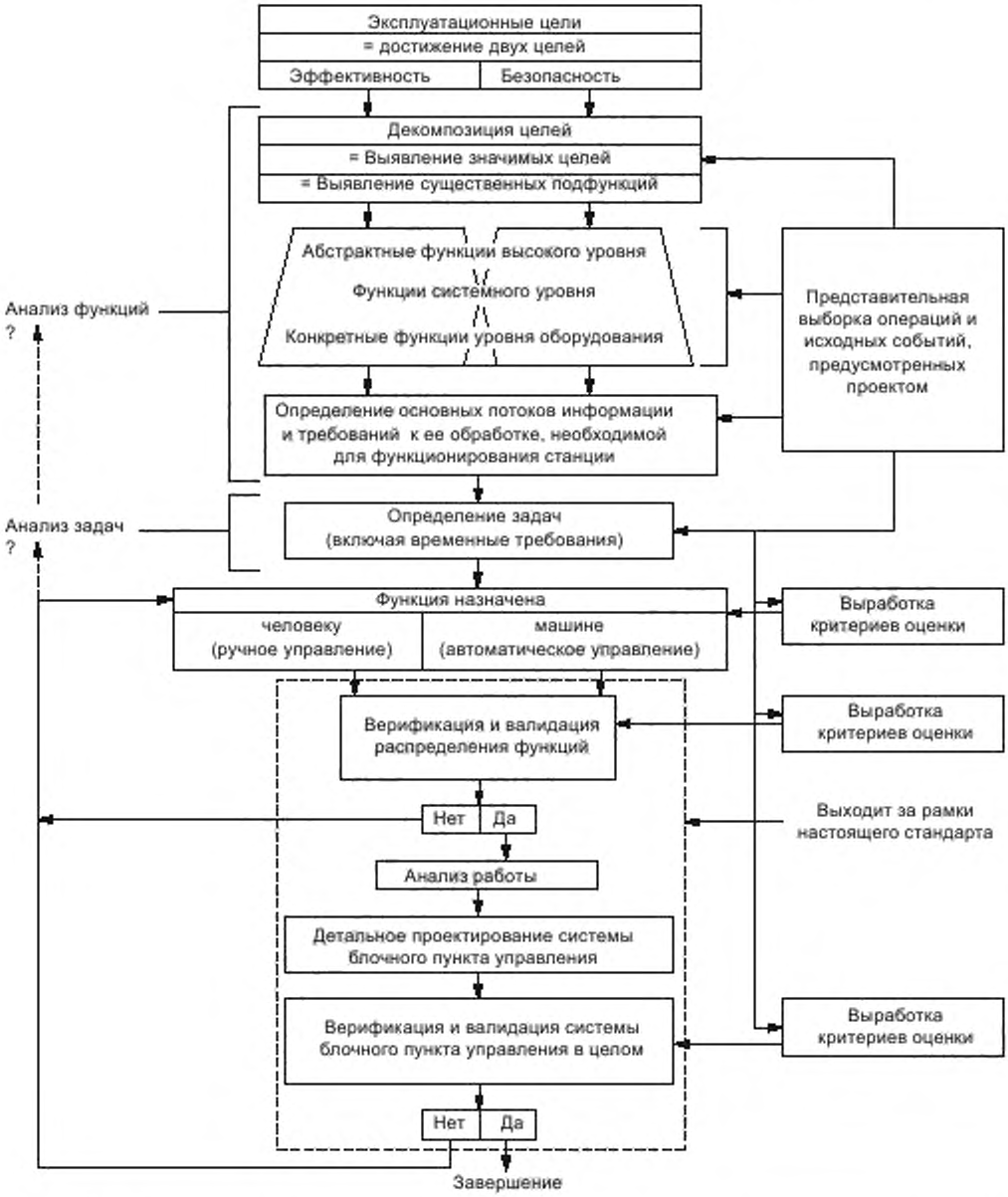


Рисунок 1 — Иллюстрация последовательности ФА и распределения функций, приведенных в МЭК 60964

4.1.1 Функциональный анализ

Выявление функций (см. 5.2) следует начинать с определения основной или наиболее существенных целей эксплуатации атомной станции, которые состоят в безопасном и эффективном производстве электроэнергии и защите населения от радиационной опасности. После этого выявляют функции верхнего уровня, обеспечивающие достижение этих целей, и выстраивают их иерархию, в соответствии с которой в нижней части находятся функции контроля, назначаемые людям или машинам. Общий функциональный анализ атомной электростанции является средством определения всех функций, реализуемых из блочного пункта управления.

В базу данных о функциях различных уровней, выявленных на предыдущем шаге, заносят также данные потока основной оперативной информации и требования, предъявляемые к их обработке, необходимой в ходе эксплуатации атомной станции (см. 5.3.1).

Следующий шаг функционального анализа состоит во введении временных требований, которое выполняют с учетом достаточного числа основных проектных событий и режимов работы станции (нормальные, нарушенные и аварийные условия) (см. 5.3.2). Таким образом идентифицируют все элементы, необходимые для описания функций, связанных с пунктом управления.

4.1.2 Распределение функций

Настоящий процесс представляет собой распределение функций между человеком и автоматическими компонентами системы.

В качестве первого шага необходимо определить характеристики выявленных функций с целью:

a) их объединения в группы, если это необходимо (см. 6.2.1);

b) выявления и подробного описания всех действий, необходимых для выполнения функций (см. 6.2.2);

c) определения типичных значений измеряемых характеристик функций (см. 6.2.3).

Затем на основании предварительно разработанного набора критериев (см. 6.3) выполняют распределение функций.

Назначение функций человеку означает выполнение этих функций с помощью ручного управления, контроля со стороны человека, активного мыслительного процесса или их комбинации. Назначение функций машинам означает их автоматическое осуществление. Следовательно, на функциональном уровне в качестве машины выступает автоматика, а в качестве человека — персонал пункта управления (см. таблицу 1).

Термин «машина» охватывает ряд аппаратных средств, включающий в себя систему контроля и управления (СКУ) и систему поддержки оператора.

Следует отметить, что системы ручного управления, органы управления и средства отображения информации, являющиеся частью СКУ, должны обеспечивать возможность персоналу пункта управления исполнять назначенные ему функции.

Верификация и валидация распределения функций выходят за рамки настоящего стандарта (см. МЭК 61771).

Примечание — Проект атомной станции и последующий анализ функций и задач ограничены прогнозируемыми исходными событиями, сценариями и прогнозируемыми комбинациями событий и отказов. Возможно появление потребности учета функций диагностики и ручного управления в непредвиденных эксплуатационных ситуациях, когда функции, очевидно, должны выполняться вручную оперативным персоналом, однако их рассмотрение выходит за рамки настоящего стандарта.

Таблица 1 — Человек и машина на функциональном и физическом уровне

<table>
<tr><th colspan="2">Функциональный уровень</th><th colspan="2">Физический уровень</th></tr>
<tr><th>Функции назначены</th><th>Функции исполняются с помощью</th><th colspan="2">Машина (оборудование)</th><th>Человек</th></tr>
<tr><td>человеку</td><td>абстрактного мышления
контроля (связанного как с ручным, так и с автоматическим управлением)
ручного управления (включая дублирование автоматики)</td><td colspan="2">Система поддержки оператора
Средства отображения информации
Органы управления
Система ручного управления
Человеко-машинный интерфейс
Интерфейс СКУ</td><td>Оперативная смена</td></tr>
<tr><td>машине</td><td>автоматического управления</td><td colspan="2">Система автоматического управления</td><td></td></tr>
</table>

4.2 Основная техническая группа для выполнения ФА и распределения функций

Как правило, основная техническая группа, выполняющая анализ и распределение функций, должна включать в себя специалистов в следующих областях:

- проектирование атомных электростанций и энергетических систем, не использующих ядерную энергию;
- системный анализ;
- проектирование СКУ,
- проектирование информационно-вычислительных систем;
- инженерная психология и эргономика;
- эксплуатация атомных станций;
- разработка процедур нормальной эксплуатации и аварийных процедур.

Далее эту техническую группу называют «разработчик».

5 Функциональный анализ

5.1 Общие положения

Процедура функционального анализа должна состоять из двух этапов:

- выявление функций;
- выявление потока информации и требований к обработке информации.

5.2 Выявление функций

Цель выявления функций управления состоит в том, чтобы убедиться, что предназначенный для них ЧМИ будет поддерживать их выполнение правильно и в достаточной мере. Например, конструкция ЧМИ пункта управления должна предусматривать наличие и ясное представление оператору всех сигналов и органов управления, связанных с функциями безопасности.

Выявление необходимых функций управления должно быть основано на общей декомпозиции функций атомной станции. Для этого использован строго иерархический подход. Данная декомпозиция должна быть получена путем представления общего проекта атомной станции в иерархическом порядке с указанием целей эксплуатации станции, а именно:

a) цели обеспечения безопасности (предотвращения выхода радиоактивности в окружающую среду),

b) цели обеспечения эффективности (управляемого производства электроэнергии).

Затем эти цели должны быть разбиты на подцели, в результате чего образуется иерархическая структура целей, т. е. функционально цели и подцели выстраивают в иерархическом порядке.

Для упомянутой выше иерархической структуры целей должны быть выявлены все функции атомной станции, необходимые для достижения этих целей и подцелей. Выявление функций должно вытекать непосредственно из выявления целей. В принципе понятия «цель» и «функция» являются взаимозаменяемыми. Однако на верхних уровнях иерархии проект атомной станции лучше рассматривать и выражать через цели, в то время как на нижних уровнях более уместно использовать понятие функции как действия или роли, исполняемой человеком или автоматизированными системами (определение по МЭК 60964).

Разработчик должен последовательно провести подразделение этих функций и выработать набор правил, определяющих тот момент, когда иерархический анализ достигает достаточного уровня детализации. Декомпозицию функции обычно прекращают, когда:

a) функция больше не содержит функций управления, например является чисто механической;

b) достигнут уровень управления отдельными функциями, параметрами или исполнительными механизмами.

Установленные правила должны гарантировать, что на нижнем уровне иерархии присутствует полный набор функций, классифицированных и описанных в соответствующих понятиях, или что процесс декомпозиции будет остановлен после того, как будут достигнуты элементарные функции и выявлены наиболее важные элементы структуры.

В любом случае окончательный уровень декомпозиции должен обеспечивать информацию, требуемую для следующего шага проектирования (см. последующие разделы). Чтобы достичь этого окончательного уровня, может понадобиться повторение процедуры.

Получившаяся в результате иерархия будет состоять из функциональных целей на верхнем уровне, функций системного уровня в середине и элементарных функций управления на нижнем уровне, назначенных людям или машинам.

Необходимо отметить, что, даже если безопасность и эффективность образуют отдельные точки входа в иерархии функций, они часто сводятся к одним и тем же общим функциям (за исключением таких специфических функций, как обеспечение целостности защитной оболочки). В результате для таких частных случаев цели достижения эффективности и безопасности с точки зрения функционального анализа могут быть рассмотрены вместе.

При проектировании новой станции процесс декомпозиции сверху вниз обычно используют для всех систем станции (для технологических систем, электрических систем и др.). Такая декомпозиция общих целей на функции, назначаемые затем людям или машинам, должна быть частью общего процесса проектирования атомной станции, а не относиться исключительно к проектированию пункта управления. Это позволяет приступать к проектированию пункта управления уже на ранней стадии проектирования всей станции и, как следствие, избегать итераций.

Принципы и критерии, используемые для анализа функций, должны быть задокументированы.

Следует отметить, что строгая иерархическая декомпозиция функций не является единственным способом структурирования и представления атомной станции. В зависимости от задач проектирования, могут оказаться более подходящими и другие способы представления функций. Примеры декомпозиции функций приведены в приложениях А и В.

5.3 Определение основных требований к информации и ее обработке

Следующий шаг функционального анализа состоит в определении основных требований к информации и ее обработке, необходимых для выполнения каждой из функций управления, определенных на предыдущей стадии.

Сначала каждую функцию анализируют отдельно, после чего функции рассматривают совместно с точки зрения реагирования на определенные события в работе атомной станции, что позволяет оценить временные требования и ограничения.

5.3.1 Анализ отдельных функций

Для каждой функции управления разработчик должен определить следующее:

- наблюдаемые параметры, которые отражают состояние систем атомной станции и/или могут быть использованы в качестве входной информации для функции;
- действия, выполняемые функцией, и используемое при этом оборудование;
- эксплуатационные показатели, позволяющие оценить, выполняется ли данная функция;
- влияние на безопасность (т. е. категорию безопасности).

Разработчик должен также определить:

- как оценить правильность работы данной функции;
- какие альтернативы имеются в случае деградации функции и как эти альтернативы можно выбрать. Речь идет об альтернативах, касающихся функций, которые способны вместо анализируемой функции обеспечить достижение функции более высокого уровня. Например, в зависимости от состояния атомной станции могут быть выбраны различные резервные способы отвода тепла;
- эксплуатационные режимы станции, в которых требуется выполнение функции (например, останов при работе на номинальном уровне мощности);
- состояния станции, требующие исполнения функции (например, нормальная эксплуатация, нарушение нормальной эксплуатации, аварии);
- обеспечивающие функции (например, вентиляция или электроснабжение).

На данной стадии подход должен быть обобщенным и не должен касаться конкретной реализации или степени участия персонала. Если по технологическим или другим причинам этот выбор уже сделан, то он должен быть четко указан и подробно описан.

При идентификации эксплуатационных показателей, свидетельствующих о выполнении функции, иногда целесообразно использовать информацию об основных проектных авариях. Наилучшим вариантом была бы разработка эксплуатационных показателей на основе чисто физического подхода. Например, один из показателей, отражающий отвод тепла от активной зоны, может быть определен на основе знаний о свойствах материалов, использованных в оболочке тепловыделяющих элементов, таких как температура плавления. Однако не все показатели можно определить таким образом. Иногда приходится опираться на информацию, полученную в результате анализа аварий.

5.3.2 Выявление временных требований и репрезентативных событий

Чтобы должным образом описать функции, представленные в иерархической структуре, и определить характеристики, зависящие от времени, разработчик должен включить в анализ все репрезентативные события. Данный анализ позволяет определить скорость, с которой влияние исходного события будет распространяться по иерархии и затронет функции верхнего уровня. Соответственно, должны быть определены требования ко времени, в течение которого необходимо выполнить определенные функции.

Для этого должны быть проанализированы следующие сценарии:

a) последовательность всех эксплуатационных операций, таких как пуск и работа на нормальной мощности;

b) все предусмотренные проектом исходные события, перечисленные в отчете по обоснованию безопасности (например, авария с потерей теплоносителя, потеря мощности в сети переменного тока и др.);

c) по мере необходимости, запроектные (тяжелые) аварии, такие как расплавление активной зоны, паровые взрывы и др.

В ходе этого анализа должны быть выявлены те исходные события, которые накладывают самые жесткие требования на временные характеристики и надежность. Следует рассмотреть следующие исходные события:

- проектные события, сопровождаемые аварийным остановом реактора или угрозой безопасности;
- события, требующие выполнения операций, субъективно оцениваемых как трудные с точки зрения сложности интерпретации данных или скорости управления и т. п.;
- события, требующие высочайшей уверенности в правильности реакции, например некоторые аварии;
- события, важные с точки зрения вероятностной оценки риска;
- события, при которых существует высокая вероятность аварийного останова блока атомной станции, если вовремя не предприняты корректирующие действия;
- события, частота появления которых высока;
- события, связанные с потерей определенной функции.

6 Распределение функций

6.1 Общие положения

Распределению подлежат функции управления, полученные в результате декомпозиции различных функций. Процедура распределения включает в себя три этапа:

- анализ функций управления;
- разработка критериев распределения;
- процесс распределения.

6.2 Анализ функций управления

Используя базу данных, созданную в ходе функционального анализа (т. е. требования к потоку информации и к ее обработке), разработчик должен выполнить анализ с целью выявления фрагментов (функциональных единиц) и характеристик функций.

Этот анализ проводят в три этапа.

6.2.1 Идентификация функциональных единиц

Первый этап связан с возможной перегруппировкой функций, выявленных в соответствии с 5.2, чтобы сформировать группы в соответствии с обстоятельствами их предполагаемого использования и затем иметь возможность определить их общие характеристики. При этом может оказаться, что некоторые функции уже связаны таким образом, что могут рассматриваться как единое целое, т. е. как одна функция.

Разработчик должен выявить функции, требующие одновременного совместного выполнения для обеспечения таких эксплуатационных задач, как пуск станции, изменение мощности, смягчение негативного воздействия проектных аварий. Это позволит определить такие факторы, как рабочая нагрузка и временные ограничения, которые не входят в состав характеристик отдельных функций. Взятые вместе, они могут быть рассмотрены как функциональная единица.

6.2.2 Описание функций управления

Для каждой функции управления, рассматриваемой в контексте функциональных единиц, разработчик должен определить следующее:

- логические предпосылки для ее реализации (почему требуется исполнение функции);
- управляющие действия, необходимые для ее исполнения (как она может быть осуществлена);
- параметры, необходимые для совершения управляющих действий;
- критерии оценки результата управляющих действий;
- параметры, необходимые для этой оценки;
- критерии выбора альтернатив.

Параметры, определенные в результате описанного выше анализа, создают основу для выбора оборудования СКУ и/или интерфейсных устройств взаимодействия с оператором, таких как органы управления и средства отображения информации. Кроме того, это обеспечивает основу для группирования средств отображения информации и органов управления.

Ниже приведен пример функции управления.

Для выполнения заданной функции на основе определенных технологических параметров (например, низкий/высокий уровень в баке) должен быть запущен/остановлен насос.

В данном случае управляющее действие может быть выполнено вручную (оператор включает/отключает насос, основываясь на показаниях уровня и инструкциях) или автоматически (фактический уровень сравнивается с уставками по уровню, в результате чего вырабатывается необходимый управляющий сигнал на включение/отключение). Инициирующим параметром является уровень в баке. Критерием оценки результата управляющего действия служит нахождение уровня в разрешенном диапазоне, при этом параметром для оценки является уровень в баке. В качестве альтернативных параметров могут выступать потребление тока двигателем насоса, расход нагнетания насоса, сигнализация об уровне ниже нижнего или выше высшего предела и др.

6.2.3 Оценка характеристик функций управления

Разработчик должен оценить значения характеристик функции управления и установить класс каждой характеристики (в соответствии с их уровнем значимости). В ходе оценки характеристик для каждой функции управления должны быть определены требования к ее исполнению. Разработчик должен учесть как надежность, так и обоснованность оценки и определить уровень важности каждой из них. Для принятия решения руководствуются как объективными (например, время, скорость), так и субъективными параметрами. При выборе субъективных параметров необходимо применять количественно масштабированные решения.

Разработчик должен рассмотреть, как минимум, следующие характеристики, принимая также во внимание нагрузку, обусловленную другими функциями управления, выполняющимися совместно с анализируемой функцией:

- потенциальная рабочая нагрузка на человека во всех эксплуатационных режимах;
- временные факторы (например, скорость, запас/ограничение времени);
- точность и повторяемость;
- сложность логических рассуждений;
- типы и сложности принятия решений (например, оценка нелинейных связей, недостаточно исчерпывающе проанализированные сценарии);
- влияние типа события, на фоне которого выполняется задача, на показатели эффективности функции управления;
- последствия потери функции и связанные с этим временные факторы.

При оценке соответствующих характеристик разработчику целесообразно проконсультироваться со специалистами в области эргономики или прикладной психологии, имеющими опыт использования методов анализа задач и их применения при проектировании систем, а также с разработчиками самой системы. По окончании анализа разработчик должен классифицировать каждую функцию управления в соответствии со значениями ее характеристик.

Принципы и критерии, используемые в ходе данного анализа, должны быть документально оформлены.

6.3 Разработка критериев распределения

Параллельно с анализом функций управления разработчик должен выработать критерии для принятия принципиального решения по распределению функций:

- людям или машинам;

- для дистанционного ручного управления или для ручного управления по месту.

Критерии должны быть основаны:

- на значениях характеристик и возможностях человека и машины;
- национальном законодательстве, национальных и международных правовых нормах и руководствах;
- правилах и политике эксплуатирующей организации и поставщиков (опыт эксплуатации и обслуживания, социальные аспекты и т. д.);
- стоимости.

6.3.1 Значения характеристик и возможности человека и машины

6.3.1.1 Основные критерии

a) Критерии назначения функций человеку или машине

Критерии для назначения функций человеку или машине должны в первую очередь учитывать следующие факторы:

- потенциальная рабочая нагрузка на человека во всех эксплуатационных режимах;
- точность и повторяемость;
- временные факторы;
- типы и сложность принятия решения и необходимых логических рассуждений.

Основные критерии приведены в таблице 2.

Быстрое развитие возможностей и ресурсов СКУ приводит к исчезновению четкой границы между функциями, которые лучше всего назначать оператору, и функциями, предназначенными для машины. Для каждого нового проекта может потребоваться пересмотр списка критериев назначения. Следует также иметь в виду, что люди и машины должны рассматриваться как взаимно дополняющие друг друга компоненты пункта управления.

Таблица 2 — Основные критерии назначения функций человеку и машине

Характеристика	Назначение	
	человеку	машине
Нагрузка	Средняя	Высокая, очень низкая
Запас времени	Большой	Малый, очень большой
Скорость	Средняя	Высокая, очень низкая
Сложность логических рассуждений	Простая	Сложная
Типы и сложность процесса принятия решений	Плохо структурированный	Хорошо структурированный

b) Критерии выбора дистанционного или местного ручного управления функцией

Критерии для выбора дистанционного или местного ручного управления функцией должны быть, прежде всего, основаны на значениях следующих характеристик:

- временные факторы;
- легкость доступа и необходимое для этого время;
- наличие операторов по месту;
- последствия потери функции и связанные с этим временные факторы;
- легкость связи;
- мощность облучения;
- факторы окружающей среды (температура, шум);
- средства управления, которые могут потребоваться по месту в случае эвакуации из пункта управления.

Функции, которые требуют немедленного или относительно быстрого реагирования, не должны управляться из зоны, в которой отсутствует постоянно дежурящий персонал (т. е. по месту). Если нет четкого обоснования применения ручного управления, то функция должна исполняться автоматикой.

Следует также учитывать критерии, вытекающие из общей концепции автоматизации атомной станции (см. 6.3.3).

6.3.1.2 Возможности оператора

В зависимости от характера действий, назначаемые оператору функции подразделяют следующим образом:

- оператор выполняет собственно саму задачу управления;
- оператор контролирует работу автоматической системы, выполняющей функцию управления;
- оператор решает задачи, связанные с абстрактным мышлением, такие как диагностика.

Настоящий анализ должен дать информацию, необходимую для разработки концептуальной структуры информационной системы и функциональной организации ресурсов для выполнения каждой задачи по принятию решения и управлению.

Для каждой потенциальной функции оператора необходимо иметь оценки базовых возможностей человека, связанных с обработкой информации и физической реакцией. Базовые возможности человека включают в себя характеристики восприятия при обнаружении сигналов (например, визуальное восприятие), объем памяти и скорость реакции. Для выполнения предварительного распределения эти базовые возможности человека следует сопоставить со способностями, необходимыми для исполнения каждой функции. Также важно, чтобы разработчик ознакомился с опытом эксплуатации соответствующих предыдущих проектов с целью выявления любых проблем, связанных с работой человека. Оценки способностей человека, требуемых для исполнения каждой функции, должны быть уточнены на основе верификации результатов и использованы для пересмотра распределения функций, а также для более детального описания способностей, которыми должен обладать оператор.

Если время реакции оператора не отвечает заданным требованиям, необходимо рассмотреть возможность полной автоматизации данной функции управления.

В качестве источника критериев для принятия решения о распределении задач, связанных с безопасностью в аварийных ситуациях, могут выступать руководства по аварийным процедурам предшествующих проектов для станций с аналогичными характеристиками, которые послужили технической основой для описания процедур по управлению авариями.

Различные типы данных, предоставляемых оператору, должны быть сгруппированы по решаемым задачам, а не по источникам этих данных. Конечной целью является такая организация информации, поступающей из различных источников, которая ориентирована на каждую задачу, требующую принятия решения. Это позволяет обеспечить оператора исчерпывающей информацией и избежать при этом его чрезмерной нагрузки.

6.3.1.3 Возможности СКУ по обработке информации

Анализ возможностей системы контроля и управления по обработке данных следует начинать с определения ограничений и функциональных требований к системе и/или оборудованию, за которым следует более подробное описание последовательности эксплуатационных событий и требований к человеко-машинному интерфейсу для каждой задачи. Цель этого процесса состоит в упорядочении машинной информации и возможностей машины по отношению к задачам, предусматривающим взаимодействие с оператором.

Такое упорядочение облегчает оценку возможностей как автоматического управления, так и управления, реализуемого человеком, по отношению к каждой задаче, требующей принятия решений и управления. Оценка возможностей СКУ по обработке информации, в конечном счете, позволяет установить требования к объему данных, времени отклика и точности, которым должны удовлетворять система и/или оборудование, а также стандарты эргономического подхода, определяющие человеко-машинный интерфейс для каждого типа оборудования.

Для снижения вероятности ошибок оператора системы управления должны быть разработаны таким образом, чтобы удерживать станцию в безопасных пределах без какого-либо вмешательства оператора в течение заданного периода времени после возникновения определенных аварийных ситуаций. Этот период времени должен быть отражен в функциональных требованиях и требованиях к надежности систем автоматической защиты и управления.

Примеры проектных требований относительно рекомендуемого периода задержки вмешательства оператора приведены в ANSI/ANS 58.8 или в различных национальных регламентах (правила 10 минут, 30 минут).

6.3.2 Национальное законодательство, национальные и международные правовые нормы и руководства

Национальное законодательство может устанавливать некоторые требования к проекту, фиксируемые на этапе предварительного утверждения проекта. Такие требования могут быть специфическими

для определенной страны или основываться на международных правилах, например на руководствах по безопасности или нормах и правилах МАГАТЭ.

6.3.3 Правила и политика эксплуатирующей организации и поставщиков

Критерии, используемые при разработке генерального проекта атомной станции, концепция автоматизации и роль персонала станции составляют главные вопросы, решаемые, как правило, заранее, на этапе технико-экономического обоснования проекта. Эти данные могут быть использованы в качестве исходных для процесса распределения функций.

Комплектование персонала пункта управления хорошо обученными и тренированными операторами — важный фактор эффективной работы и, следовательно, экономичности станции. Вопросы и принципы промышленной эксплуатации атомных станций описаны в 2.6 МЭК 60964.

6.4 Процесс распределения

Процесс распределения начинают с выявления тех функций управления, для которых автоматизация является обязательной, а также тех функций, для которых обязательным является управление человеком. Обычно это делают на основе анализа регламентов, политики и прямых оценок ограничений, присущих работе человека или машины. Например, функцию обязательно назначают машине, если агрессивные условия окружающей среды делают невозможным присутствие человека или когда требуемое время реакции превышает человеческие возможности.

Результаты процесса распределения служат в качестве исходных данных для последующего детального проекта автоматизации станции и для выпуска инструкций по производственным процедурам (инструкций по эксплуатации, инструкций по ликвидации аварийных ситуаций).

Процесс распределения является более трудным для тех функций, для которых невозможно однозначно определить их обязательное назначение. В этом случае цели, определенные в ходе функционального анализа, должны быть сопоставлены с возможностями людей и машин на основе критериев, разработанных в соответствии с 6.3.1.

Разработчик должен выполнять распределение функций, сравнивая значения классификационных характеристик функций управления с критериями распределения. Распределение функций продолжают до тех пор, пока не будут выявлены все недостатки проекта на стадии верификации и валидации в соответствии с МЭК 61771.

Дальнейшие рекомендации приведены в IAEA TECDOC 668. Предлагаемый способ состоит в разделении функций на следующие четыре категории:

- функции, которые должны быть автоматизированы;
- функции, которые лучше автоматизировать;
- функции, которые должны быть отданы людям;
- функции, которые должны выполняться совместно.

В конечном итоге могут быть выявлены функции, для выполнения которых необходимо совместное участие людей и машин. В большинстве случаев, даже если функция управления автоматизирована, некоторое вмешательство человека все равно необходимо (например, проверка правильности работы автоматики, дублирование, ручное управление при отказе автоматики).

Поскольку процесс распределения является повторяющимся, все назначения, включая те, которые определены как обязательные, следует проверять с учетом влияния экономических и технологических факторов и согласованности между установленной ролью оператора (см. 6.3) и ролью, вытекающей из процесса распределения. В результате могут понадобиться дополнительные циклы распределения.

Принципы и критерии, используемые в анализе, должны быть задокументированы и должны включать в себя факторы, связанные с возможностями и ограничениями для персонала пункта управления и для автоматической системы управления.

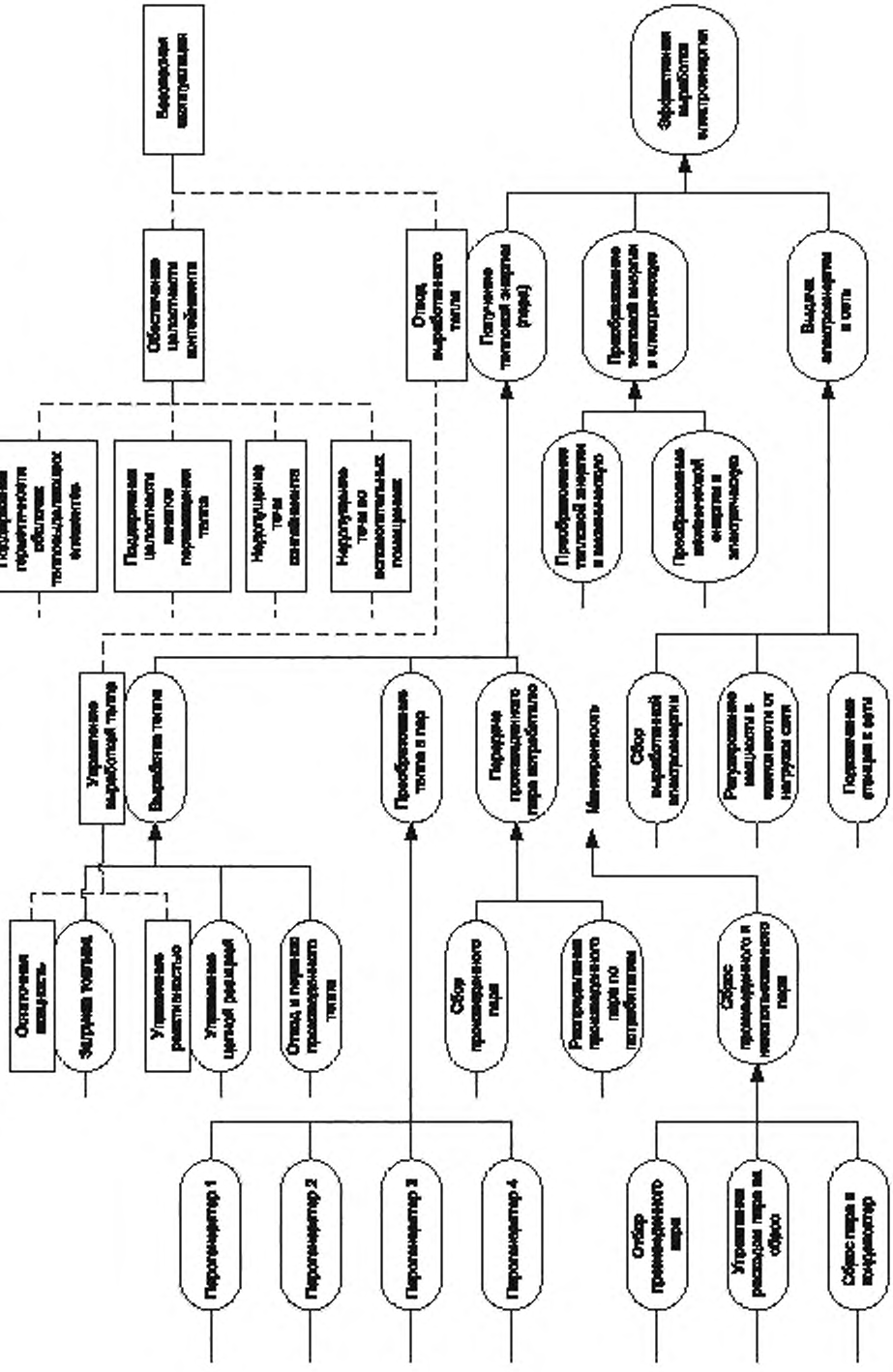
Приложение А
(справочное)

Примеры декомпозиции целей и подцелей



Приложение В
(справочное)

Начало функционального анализа ВВЭР (водо-водяного реактора под давлением)



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 60964:1989	—	*, 1)
IEC 61771:1995	—	*
* Соответствующий национальный стандарт отсутствует. Текст стандарта на русском языке доступен на сайте http://www.iaea.org/.		

1) Действует ГОСТ Р МЭК 60964—2012 «Атомные станции. Пункты управления. Проектирование», идентичный МЭК 60964:2009.

Библиография

IEC 60960:1988, Functional design criteria for a safety parameter display system for nuclear power stations

IEC 60965:1989, Supplementary control points for reactor shutdown without access to the main control-room

IEC 61225:1993, Nuclear power plants — Instrumentation and control systems important for safety — Requirements for electrical supplies

IEC 61226:1993, Nuclear power plants — Instrumentation and control systems important for safety — Classification

IEC 61227:1993, Nuclear power plants — Control-rooms — Operator controls

IEC 61772:1995, Nuclear power plants — Main control-room — Application of visual display units (VDU)

IAEA Safety Series 110:1993, The safety of nuclear installations

IAEA 50-P-4:1992, A Safety Practice — Procedures for conducting probabilistic safety assessments of nuclear power plants (Level 1)

IAEA 50-C-0 (rev. 1):1988, Code of Practice. Code on the safety of nuclear power plants: Operation. STI/PUB/799

IAEA 50-C-D (rev. 1):1989, Code on the safety of nuclear power plants: Design

IAEA Safety Guide 50-SG-D3:1980, Protection system and related features in nuclear power plants

IAEA Safety Guide 50-SG-D8:1984, Safety related instrumentation and control systems for nuclear power plants

IAEA Safety Guide 50-SG-D11:1986, General design safety principles for nuclear power plants

IAEA Proceedings, Munich, STI/PUB/843:1991, Balancing automation and human action in nuclear power plants. IAEA/OECD/NEA Meeting

IAEA TECDOC 538:1990, Human error classification and data collection

IAEA TECDOC 565:1990, Control-rooms and man/machine interface in nuclear power plants

IAEA TECDOC 618:1991, Human reliability data collection and modeling

IAEA TECDOC 668:1992, The role of automation and human in nuclear power plants

IAEA TECDOC 812:1995, Control-room systems design for nuclear power plants

IAEA 75-INSAG-3:1988, Basic safety principles for nuclear power plants

EPRI NP-6560-L:1990, Human Reliability Analysis Approach Using Measurements for Individual Plant Examination (IPE)

ANSI/ANS 58.8:1994, Time Response Design Criteria for Nuclear Operator Actions

УДК 621.311.3.049.75:006.354 ОКС 27.120.20

Ключевые слова: атомные станции, функциональный анализ, пункт управления, человеко-машинный интерфейс, вероятностный анализ отказа

Редактор *Н.В. Таланова*
Технический редактор *В.Н. Прусакова*
Корректор *Е.Д. Дульнева*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 19.04.2021. Подписано в печать 23.04.2021. Формат 60×84¼. Гарнитура Ариал.
Усл. печ. л. 2,32. Уч.-изд. л. 2,15.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении во ФГУП «СТАНДАРТИНФОРМ»
для комплектования Федерального информационного фонда стандартов
117418 Москва, Нахимовский пр-т, д. 31, к. 2.
gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru