Оригинальная статья
DOI: 10.21683/1729-2646-2018-18-1-46-52

Формирование системы с более высоким уровнем полноты безопасности из компонентов с низким уровнем полноты безопасности

Шебе Хендрик, *T V Rheinland InterTraffic, Кёльн, Германия*

Шебе Хендрик

Резюме. Цель. *Технические системы становятся все более сложными. Все большее число технических систем содержит электронное оборудование и программное обеспечение, и, таким образом, уровень их функциональной безопасности имеет большее значение. Уровень полноты безопасности задается дискретным номером, который характеризует набор мер против случайных и систематических отказов в зависимости от заданных требований по уменьшению риска. Концепция уровней полноты безопасности (УПБ) была разработана в рамках различных систем стандартов. При обсуждении архитектуры безопасности системы возникает основной вопрос: как при компонентах или подсистемах с низким УПБ формируются системы с более высоким УПБ? Ответ на этот вопрос позволит использовать уже существующие и сертифицированные компоненты для создания системы с заданным уровнем безопасности, возможно, также с более высоким УПБ, чем УПБ составных компонентов.* **Методы.** *Анализируются и сравниваются существующие правила комбинирования систем с уровнями безопасности, приведенные в различных стандартах функциональной безопасности, таких как EN 50126/8/9, ISO 26262, IEC 61508, DEF-STAN-00-56, SIRF и Желтая Книга (Yellow Book). Помимо допустимых интенсивностей отказов, требования к конструкции системы должны рассматриваться таким образом, что подсистемы с низкими УПБ комбинируются для построения системы с более высоким уровнем УПБ. Самый обширный набор методов определен для достижения УПБ 4. Однако этот набор методов не может быть переработан для всех возможных систем в форму простого правила для комбинации подсистем с более низким УПБ для формирования систем с более высоким УПБ. В общем случае комбинирование подсистем в серийную структуру приведет к системе, имеющей уровень полноты безопасности являющейся минимумом уровней подсистем. Ориентировочно можно исходить из того, что, комбинируя две подсистемы с тем же уровнем полноты безопасности, можно создать систему с уровнем полноты безопасности на одну степень выше уровня подсистем.* **Результаты.** *Показано, что общее правило для распределения УПБ, как установлено в стандарте DEF-STAN 00-56, в Желтой книге или в стандарте SIRF, не может рекомендоваться для всех стран и во всех ситуациях. Должны быть приняты во внимание интенсивности отказов и/или интервалы наблюдения. Обосновано, что общие правила могут быть даны только для подсистем, подключенных параллельно, и для некоторых комбинаций УПБ (см., например, Желтая книга, SIRF). В каждом случае общие отказы должны учитываться. Общее правило может быть следующим: для достижения УПБ системы на один уровень выше исходного уровня должны соединяться параллельно две составные подсистемы, имеющие УПБ на одну степень ниже. Другие архитектуры системы должны быть подробно изучены.*

Ключевые слова: *уровень полноты безопасности, комбинация подсистем, допустимая интенсивность опасных отказов.*

Формат цитирования: *Шебе Х. Формирование системы с более высоким уровнем полноты безопасности из компонентов с низким уровнем полноты безопасности // Надежность. 2018. Т. 18, № 1. С. 46-52. DOI: 10.21683/1729-2646-2018-18-1-46-52*

1. Введение

Технические системы становятся все более сложными. Все большее число технических систем содержит электронное оборудование и программное обеспечение, и, таким образом, уровень их функциональной безопасности имеет большее значение. Уровень полноты безопасности задается дискретным номером, который характеризует набор мер против случайных и систематических отказов в зависимости от заданных требований по уменьшению риска. Концепция уровней полноты безопасности (УПБ) была разработана в рамках различных систем стандартов. При обсуждении архитектуры безопасности системы возникает основной вопрос: как при компонентах или подсистемах с низким УПБ формируются системы с более высоким УПБ? Ответ на этот вопрос позволит использовать уже существующие и сертифицированные компоненты для создания системы с заданным уровнем безопасности, возможно, также с более высоким УПБ, чем УПБ составных компонентов.

Концепция уровней полноты безопасности определяется и используется в различных стандартах, таких как МЭК 61508 [6], DEF-STAN 0056 [1], EN 50126 [2], EN 50128 [3], EN 50129 [4] и многих других (см., например, [5, 7, 8]). Это обычная практика в указанных стандартах – определять различные четыре уровня полноты безопасности.

Уровень полноты безопасности определяется следующими двумя основными аспектами:

а) Чтобы справиться со случайными отказами, не должна быть превышена максимально допустимая интенсивность опасных отказов всех выполняемых системой функций безопасности

б) Должен быть установлен набор мер, позволяющий защитить систему от систематических отказов.

Следует обратить внимание на то, что для программного обеспечения имеют значение только систематические отказы и не предусматривается определение значений интенсивности отказов. Это вызвано тем фактом, что нормальное программное обеспечение не должно иметь случайных ошибок.

2. Уровни полноты безопасности

В таблице 1 приводятся четыре уровня полноты безопасности и приемлемые для них уровни THR допустимой интенсивности опасных отказов, как определено в трех стандартах [1], [4] и [6].

Таблица 1 – Четыре значения для различных УПБ и стандартов

УПБ	МЭК 61508 / EN 50129	DEF-STAN-00-56
1	10^{-6} 1/ч ≤ THR < 10^{-5} 1/ч	Частая ≈ 10^{-2} 1/ч
2	10^{-7} 1/ч ≤ THR < 10^{-6} 1/ч	Вероятная ≈ 10^{-4} 1/ч
3	10^{-8} 1/ч ≤ THR < 10^{-7} 1/ч	Случайная ≈ 10^{-6} 1/ч
4	10^{-9} 1/ч ≤ THR < 10^{-8} 1/ч	Маловероятная ≈ 10^{-8} 1/ч

Допустимая интенсивность опасных отказов системы есть такой максимально допустимый уровень опасных отказов составного технического оборудования, который разрешен установленным для этого оборудования уровнем полноты безопасности. Здесь мы отмечаем, что значения УПБ идентичны для [4] и [6] и отличаются для [1]. Таким образом, их УПБ не сопоставимы. Даже несмотря на то, что значения THR для [4] и [6] совпадают, предусмотренные в них меры защиты от систематических отказов отличаются, так что их УПБ не идентичны.

Стандарты [2] и [3] не содержат целевых показателей интенсивности опасных отказов. Стандарт [2] требует только наличия уровней полноты безопасности, тогда как стандарт [3] посвящен программному обеспечению и дает описание УПБ без числовых значений для THR. Стандарт [1] содержит целевые показатели опасных отказов неявно, заявив только словесные эквиваленты.

3. Комбинирование уровней полноты безопасности

В этом разделе мы опишем правила комбинации уровней полноты безопасности так, как они используются в различных стандартах.

3.1. Стандарт DEF-STAN 0056

Правила стандарта [1] приводятся в приложении 7.4.4, таблица 8. Читателю не следует смешивать эти правила комбинирования УПБ ([1]) с УПБ для [4], так как они являются различными характеристиками.

Эти правила сводятся к следующему:

Сочетание двух устройств с УПБ 3, включенных параллельно, дает систему с УПБ 4;

Сочетание двух устройств с УПБ 2, включенных параллельно, дает систему с УПБ 3;

Сочетание двух устройств с УПБ 1, включенных параллельно, дает систему с УПБ 2;

Сочетание двух устройств с УПБ x и УПБ y, включенных параллельно, дает систему с $\max(x; y)$ УПБ.

Обратите внимание, что «сочетание устройств, включенных параллельно» означает, что два устройства или функции комбинируются таким образом, что только опасный отказ обоих компонентов (или их функций) может вызвать опасный отказ системы. Из этих правил мы видим, что сочетание двух устройств приведет в лучшем случае к УПБ, который только на один уровень выше, чем УПБ составных компонент. Кроме того, система с определенным УПБ не может строиться путем объединения устройств или функций без УПБ – по крайней мере, не используя эти общие правила сочетания УПБ.

3.2. Желтая книга

Еще один интересный источник – Желтая книга [10]. Желтая книга является инструментом национального регулирования Великобритании, который устарел с по-

явлением общих методов обеспечения безопасности. Тем не менее, она предоставляет интересную информацию. УПБ в [10] определяется так же, как и в [4], но эти правила весьма отличаются от тех, которые определены в стандарте [1].

Таблица 2 – Сочетание правил для УПБ в Желтой книге (Таблица 17-2)

Верхний уровень УПБ	УПБ функции нижнего уровня		Комбинатор (если присутствует)
	Главная	Другие	
УПБ 4	УПБ 4	нет	нет
	УПБ 4	УПБ 2	УПБ 4
	УПБ 3	УПБ 3	УПБ 4
УПБ 3	УПБ 3	нет	нет
	УПБ 3	УПБ 1	УПБ 3
	УПБ 2	УПБ 2	УПБ 3
УПБ 2	УПБ 2	нет	нет
	УПБ 1	УПБ 1	УПБ 2
УПБ 1	УПБ 1	нет	нет

3.3. ГОСТ Р/МЭК 61508

В стандарте [6] нет такого хорошего правила сочетания УПБ, как в ранее рассмотренных стандартах. Тем не менее, этот стандарт обеспечивает возможность достижения уровня повышенной полноты безопасности через комбинацию более низких УПБ составных подсистем. Общее правило заключается в следующем (см. МЭК 61508-2, приложение 7.4.4.2.4): «Выбор канала с высоким уровнем полноты безопасности, который был достигнут для функции безопасности, и затем добавление N уровней полноты безопасности для достижения максимального уровня полноты безопасности путем общей комбинации подсистемы». Здесь N – это количество допускаемых в системе опасных ошибок параллельно скомбинированных элементов, т.е. количество опасных ошибок, которые допускаются в системе. Следует обратить внимание на то, что для достижения определенного уровня полноты безопасности системы комбинацией составных элементов, требования для количества допускаемых в системе опасных ошибок и доли безопасных отказов элементов должны быть выполнены согласно таблице МЭК 61508-2. Здесь надо различать элементы/системы типа А/В систем (МЭК 61508-2, глава 7.4.4.1.2).

Элемент может рассматриваться как элемент типа А, если для компонентов, необходимых для достижения функции безопасности, выполняются следующие условия:

а) виды отказов всех составных компонентов четко определены;

б) характер поведения элемента при неисправности может быть полностью определен;

в) существует достаточно надежный массив данных, чтобы подтверждать, что заявленные интенсивности отказов для обнаруживаемых и не обнаруживаемых опасных отказов выполняются.

Другие элементы / системы относятся к типу В. Правила для достижения требуемых УПБ систем типа А и типа В согласно МЭК 61508-2-2 приведены в таблицах 3 и 4 соответственно

Таблица 3 – Правила для достижения требуемых УПБ систем типа А

Доля безопасных отказов элемента	Количество допускаемых в системе опасных ошибок		
	0	1	2
< 60%	УПБ 1	УПБ 2	УПБ 3
60%-< 90%	УПБ 2	УПБ 3	УПБ 4
90%-< 99%	УПБ 3	УПБ 4	УПБ 4
> 99%	УПБ 3	УПБ 4	УПБ 4

Таблица 4 – Правила для достижения требуемых УПБ систем типа В

Доля безопасных отказов элемента	Количество допускаемых в системе опасных ошибок		
	0	1	2
< 60%	Не допускается	УПБ 1	УПБ 2
60%-< 90%	УПБ 1	УПБ 2	УПБ 3
90%-< 99%	УПБ 2	УПБ 3	УПБ 4
> 99%	УПБ 3	УПБ 4	УПБ 4

Эти обе таблицы 3 и 4 наглядно показывают, что стандарт [6] не дает простого правила для комбинирования УПБ. Не только варианты объединения подсистем и количество допускаемых в системе опасных ошибок решают вопрос о полноте уровня безопасности системы, но и доля безопасных отказов элемента. Однако можно наблюдать, что с увеличением количества допускаемых в системе опасных ошибок и сохранения доли безопасных отказов элемента при использовании подсистем того же типа (А или В), УПБ увеличивается на единицу. Это означает, что если есть две подсистемы с одинаковым УПБ с одной и той же долей безопасных отказов элемента, то их сочетание будет увеличить УПБ системы на одну степень. Комбинация подсистем различных типов и / или с различными долями безопасных отказов элемента может привести к другим результатам и в этом случае следует провести дополнительный анализ.

3.4. SIRF 400

Стандарт SIRF [9] – это немецкий стандарт способов обеспечения безопасности подвижного состава железных дорог, подготовленный совместно немецкой железнодорожной отраслью, немецкими железными дорогами, обществом немецких железнодорожных операторов и немецким федеральным железнодорожным органом. В Германии можно сделать ссылку на этот

документ, однако за пределами Германии, признание этого стандарта не гарантируется.

В документе описаны следующие принципы. Подключая две подсистемы в серии (например, с помощью условия «ИЛИ» в дереве отказов), наименьшее УПБ будет также результирующим УПБ такой системы.

Для комбинации параллельных подсистем предоставляются следующие правила:

а) системы с УПБ > 0 не должны быть построены из элементов с УПБ 0;

б) УПБ может быть понижен только на один уровень для условия «И» в дереве отказов;

в) исключение из (б): одна ветвь полностью берет на себя функции безопасности;

г) исключение из (б): проводится анализ общих отказов;

д) в случае пункта (г) подходящий метод (FMEA, HAZOP и т.д.) должен быть использован до самого нижнего уровня дерева отказов, чтобы показать, что возможность общих отказов исключаются.

Рисунок 1 – Допустимые комбинации для УПБ 1 (взято из стандарта [9])

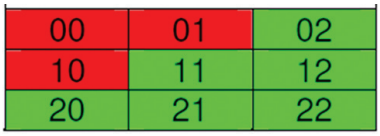

Рисунок 2 – Допустимые комбинации для УПБ 2 (взято из [9])

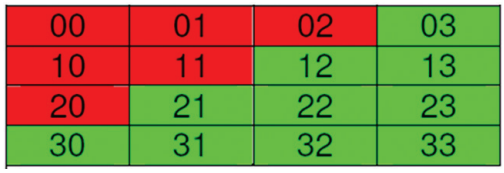

Рисунок 3 – Допустимые комбинации для УПБ 3 (взято из [9])

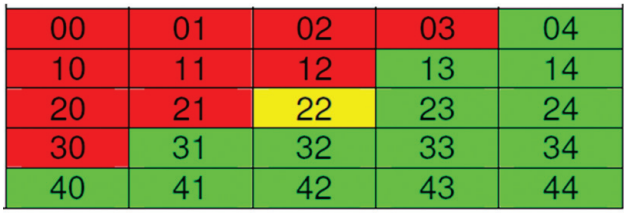

Рисунок 4 – Допустимые комбинации для УПБ 4 (взято из [9])

Обратите внимание, что стандарт SIRF использует термин «SAS», который главным образом эквивалентен УПБ, но не совсем аналогичен этому понятию. На следующих рисунках 1-4 изображены разрешенные и запрещенные комбинации. Здесь зеленый цвет означает допустимые комбинации, красный показывает запрещенные комбинации и желтый означает, что только на основе глубокого анализа должны быть установлены независимости подсистем. Следующие изображения (рисунки 1-4) показывают комбинации УПБ, которые разрешены согласно [9].

Пренебрегая сочетанием двух независимых подсистем с УПБ 2 для достижения УПБ 4 системы, мы видим, что, главным образом, сочетание двух подсистем с тем же УПБ даст систему, которая имеет УПБ на один уровень выше.

3.5. Численный подход

В этом подразделе мы проведем расчет только на основе интенсивностей опасных ошибок, т.е. допустимых интенсивностей опасности, которые должны быть достигнуты путем сочетания однотипных подсистем. При этом не учитываются возможные меры защиты от систематических отказов.

Для анализа используются следующие предположения:

1) компаратор не требуется;

2) T-интервал проверки. В инспекции все неудачи и недостатки обнаружены и удалены так, что подсистема будет как новая;

3) система состоит из двух подсистем, которые соединены параллельно и имеют одинаковые УПБ;

4) нужно создать систему с УПБ, который на один уровень выше, чем УПБ у составных подсистем.

Ориентировочно интенсивность опасного отказа комбинированной системы определяется как

$$\lambda=\lambda_1\cdot\lambda_2\cdot T,$$

где: λ_1 – интенсивность отказа первой системы, 1/ч;

λ_2 – интенсивность отказа второй системы, 1/ч;

T – интервал наблюдения, ч.

Следующая таблица 5 содержит результаты для временного интервала T = 10000 ч, т.е. приблизительно один год.

Можно увидеть, что для всех трех случаев (УПБ 2...4 для системы) подсистемы будут выполнять требования (требуемый уровень), если подсистемы имеют уровни УПБ, которые на одну степень ниже требуемого УПБ

Таблица 5 – УПБ и допустимые интенсивности опасных отказов подсистем и системы в целом для интервала наблюдения 10000 часов,

Система		Подсистемы		
УПБ	**Значение интенсивности**	**Требуемый уровень интенсивности**	**УПБ**	**Значение интенсивности**
4	10^{-8} 1/ч	10^{-10} 1/ч	3	10^{-7} 1/ч
3	10^{-7} 1/ч	10^{-8} 1/ч	2	10^{-6} 1/ч
2	10^{-6} 1/ч	10^{-6} 1/ч	1	10^{-5} 1/ч

для системы. Однако это вычисление еще необходимо дополнить анализом общих отказов. Для этого мы используем [6]. Хотя, [4] дает другой подход в 3.2, мы используем [6] по той простой причине, что он дает численное значение. В худшем случае бета – коэффициент учета общих отказов – будет составлять 10%. Это та доля интенсивности отказов, которая должна быть использована для описания общих отказов. Затем, при определении интенсивности опасных отказов комбинированной системы, общие отказы будет доминировать. Если теперь каждая подсистема имеет УПБ n, то интенсивность опасных ошибок комбинированной системы будет составлять 10% от $10^{-(n+4)}$1/ч, то есть, будет равна $10^{-(n+5)}$1/ч.

Таким образом, комбинированная система в лучшем случае сможет иметь УПБ (n+1). Следует заключить, что без особых предположений об общих отказах безопасность системы может быть повышена на один уровень при комбинировании двух подсистем с тем же УПБ.

3.6. Краткое резюме методов комбинаций УПБ

Помимо допустимых интенсивностей отказов, требования к конструкции системы должны рассматриваться таким образом, что подсистемы с низкими УПБ комбинируются для построения системы с более высоким уровнем УПБ. Стандарт [1] требует в приложении 7.3.3: «Проектирование, правила и методы, соответствующие каждому уровню полноты безопасности… должны быть определены до начала осуществления...». Никаких конкретных правил нет.

Стандарты [6] (часть 2, приложение А3, приложение В) и [4] (Приложение Е) содержат различные методы для различных УПБ. Самый обширный набор методов определен для достижения УПБ 4. Однако этот набор методов не может быть переработан для всех возможных систем в форму простого правила для комбинации подсистем с более низким УПБ для формирования систем с более высоким УПБ. Однако общее правило, кажется, состоит в том, что улучшить УПБ системы на один уровень возможно путем объединения двух подсистем с некоторыми более низкими УПБ.

4. Примеры

Пример 1

Система состоит из двух подсистем и не содержит программного обеспечения. Компаратор не нужен. Каждая подсистема проверяет различие между собой и другой подсистемой и выключает другую подсистему в случае существования различия. Это означает, что отключение всей системы является безопасной ситуацией. На рисунке 5 показана блок-схема системы примера 1.

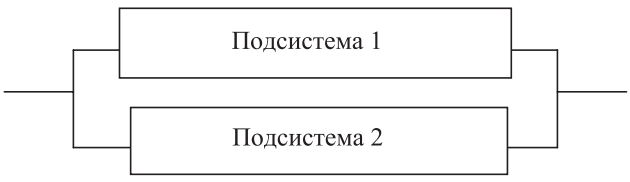

Рисунок 5 – Блок-схема системы примера 1

Если уровень полноты безопасности обеих подсистем есть УПБ 3 и они независимы, то они могут быть комбинированы в систему с УПБ 4. Правила проектирования имеют незначительные отличия между построением систем с УПБ 3 и УПБ 4. Если система должна иметь УПБ 2, то достаточно объединить две подсистемы с УПБ 1. Если обе подсистемы имеют УПБ 2 и система должна иметь УПБ 3, требуется более глубокое исследование относительно системы. Правила проектирования, необходимые для системы с УПБ 3, отличаются от тех правил, которые предъявляются при проектировании системы с уровнем УПБ 2.

Пример 2

Система в основном аналогична примеру 1, однако обе подсистемы находятся в ведении общего программного обеспечения (см. рисунок 6).

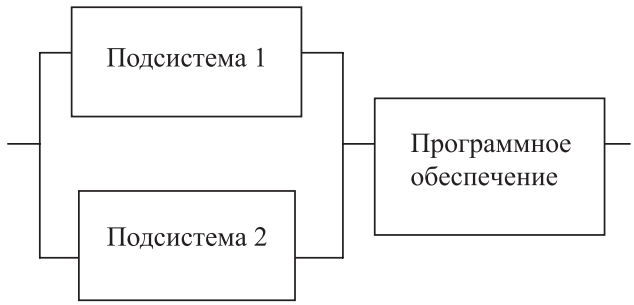

Рисунок 6 – Блок-схема системы примера 2

Если система должна иметь УПБ 4, то программное обеспечение должно также иметь уровень УПБ 4. (УПБ программного обеспечения должно быть, по крайней мере, таким же высоким, как и у самой системы). Системы с УПБ 2 могут быть построены из двух параллельных систем УПБ 1 с программным обеспечением УПБ 2. Если система должна иметь УПБ 3, то программное обеспечение также должно иметь УПБ 3. Если аппаратное обеспечение имеет УПБ 2, то для достижения в системе уровня УПБ 3 должны быть учтены дополнительные соображения такие же, как и в примере 1.

Пример 3

Эта система также похожа на систему примера 1, однако она содержит разнообразное программное обеспечение. На рисунке 7 показана блок-схема системы примера 3.

Есть разнообразные программы, используемые в обеих подсистемах. Те же соображения, как и в примере 1, применяются относительно распределения УПБ. Уровень УПБ 4 системы может быть обеспечен с помощью двух подсистем УПБ 3, где каждая с программным обеспечением УПБ 3. Системы с УПБ 2 могут быть

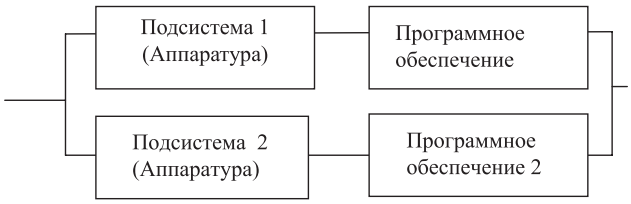

Рисунок 7 – Блок-схема системы примера 3

построены из двух подсистем УПБ 1. Для построения системы с УПБ 3 из двух подсистем с УПБ 2 каждая, необходимо учитывать дополнительные соображения.

Пример 4

Система состоит из одного канала аппаратного оборудования, но программное обеспечение является избыточным (рисунок 8). «Избыточность» программного обеспечения может быть создана с помощью двух различных пакетов программ или избыточных методов программирования (разнообразное программное обеспечение). В любом случае должно быть обеспечено разнообразие программного обеспечения.

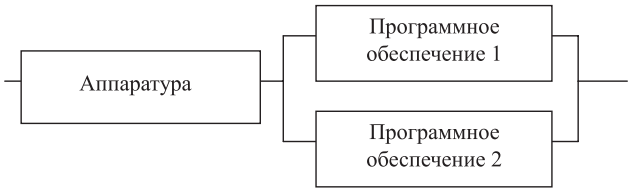

Рисунок 8 – Блок-схема системы примера 4

Пусть система должна иметь УПБ 4. В этом случае и аппаратное оборудование должно иметь УПБ 4, а обе версии программного обеспечения должны быть созданы, по крайней мере, согласно УПБ 3. Кроме того, должно быть доказано, что каждый отказ оборудования обнаруживается программным обеспечением, т.е. созданы хотя бы две версии программного обеспечения, и что существуют средства для приведения системы в безопасное состояние. Если система должна иметь УПБ 2, то оборудование должно иметь УПБ 2 и две версии программного обеспечения, разработанные хотя бы с УПБ 1 каждая. Достижение УПБ 3 системы возможно, если аппаратное обеспечение имеет уровень УПБ 3 и каждая из версий программного обеспечения соответствует уровню УПБ 2. Однако при этом необходимо детальное изучение такой возможности. Вопрос о независимости двух версий программного обеспечения, работающих в том же самом оборудовании, не является тривиальным. В любом случае программное обеспечение должно быть разнообразным.

Пример 5

В этом примере, мы рассматриваем электронную подсистему, состоящую из аппаратного и программного обеспечения и другого оборудования системы, действующего параллельно (аппаратный обход) (рисунок 9).

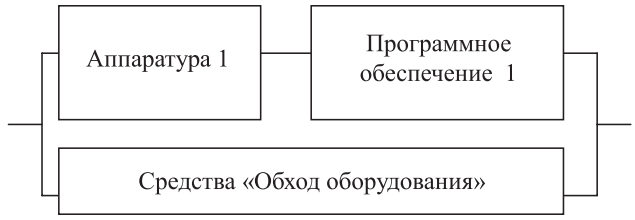

Рисунок 9 – Блок-схема системы примера 5

Если средства «обход оборудования» имеют необходимый для системы УПБ, то к аппаратному обеспечению 1 и программному обеспечению 1 не нужно предъявлять каких либо требований по УПБ. Кроме того, может применяться та же логика, как и в примере 1: УПБ 4 системы могут быть достигнуты из УПБ 3 подсистем (аппаратного 1 и программного обеспечения 1 на одной стороне и УПБ 3 средств «обхода оборудования» на другой стороне). Программное обеспечение 1 должно иметь УПБ не ниже, чем УПБ аппаратуры 1.

5. Заключение

Общее правило для распределения УПБ как установлено в стандарте DEF-STAN-00-56, в Желтой книге или в стандарте SIRF не может рекомендоваться для всех стран и во всех ситуациях. Должны быть приняты во внимание интенсивности отказов и/или интервалы наблюдения. Общие правила могут быть даны только для подсистем, подключенных параллельно, и для некоторых комбинаций УПБ (см., например, Желтая книга, SIRF). В каждом случае общие отказы должны учитываться. Общее правило может быть следующим: для достижения УПБ системы на один уровень выше исходного уровня должны соединяться параллельно две составные подсистемы, имеющие УПБ на одну степень ниже. Другие архитектуры системы должны быть подробно изучены. Хорошим показателем соответствия выбранной архитектуры системы заданному УПБ является выполнение условия, когда требуемая интенсивность отказа системы согласно УПБ не превышает значения интенсивности отказов системы, рассчитанного по интенсивности отказов составных подсистем. Как правило, путем сочетания подсистем в серии создается система, которая имеет уровень полноты безопасности, соответствующий минимальному УПБ составных подсистем.

6. Библиографический список

1. DEF-STAN 0056 (1996) Требования для систем обороны по управлению безопасностью. Часть 1: требования. Часть 2: руководство. Выпуск 2, 13.2.1996.

2. EN 50126 – ГОСТ Р МЭК 62278 Определение и подтверждение надежности, эксплуатационной готовности, ремонтопригодности и безопасности (RAMS) на железных дорогах, 2008.

3. EN 50128 – СТБ IEC 62279 Системы связи, сигнализации и обработки данных. Программное обеспечение

для систем управления и защиты на железных дорогах, 2011.

4. EN 50129 – СТБ IEC 62425 Системы связи, сигнализации и обработки данных. Электронные системы сигнализации, связанные с безопасностью, 2011.

5. Gräfling, S., Schäbe, H. (2012), Сельскохозяйственный уровень полноты производительности – или, как вы называете это?, ESREL 2012 / PSAM 11, статья 26 Fr2_1, 10 p.

6. IEC 61508 (2010), Функциональная безопасность электрических / электронных / программируемых электронных связанных с безопасностью систем – части 1-7, 1.4.2010.

7. Schäbe, H. (2014), Определение уровней полноты безопасности и влияния предположений, методов и принципов, труды PSAM 7 / ESREL 2004: Вероятностный анализ безопасности и управления (Редакторы C. Spitzer, U. Schmocker, V.N. Dang), Vol 4, pp. 1020-1025.

8. Schäbe, H., Jansen, H. (2010), Компьютерные архитектуры и распределения уровней полноты безопасности. Функциональная и информационная безопасность железнодорожного оборудования (Редактор G. Sciutto) WIT Press, 2010, стр. 19-28.

9. SIRF (2011), Правила политики безопасности транспортных средств, версия 1,1.6.2011.

10. Жёлтая книга (2007), Техника управления безопасностью (Желтая книга), тома 1 и 2. Основные принципы и руководящие указания, выпуск 4.

Примечание: Желтая книга заменена руководством по применению CSMREA.

Сведения об авторах:

Шебе Хендрик, доктор физико-математических наук, заведующий отделом анализа рисков и опасностей, TÜV Rheinland InterTraffic, Cologne, Germany**,** e-mail: schaebe@de.tuv.com

Поступила 28.11.2017