ФУНКЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ СИСТЕМ В ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ

Щербина В.И.

Автономная некоммерческая организация «Всемирная Академия Наук Комплексной Безопасности» (АНО «ВАН КБ»), 119602, г. Москва, ул. Академика Анохина, 30, корп. 2, офис 128, e-mail: Scherbina.vladimir@gmail.com

В настоящее время в мировой практике утвердились следующие положения: 1 – для любой продукции, включая услуги, вторыми по важности характеристиками (после характеристик назначения) являются характеристики безопасности; 2 – главной характеристикой безопасности сложных технических систем (СТС) признана их функциональная безопасность; 3 – безопасность СТС достигают путем принятия мер по снижению риска на всех стадиях их жизненного цикла. Большинство аппаратных средств и программного обеспечения информационных технологий (ИТ) относятся к СТС, и они подпадают под действие базовых стандартов по функциональной безопасности. Рассмотрены требования функциональной безопасности применительно к системам и средствам ИТ.

Ключевые слова: функциональная безопасность систем, стандартизация функциональной безопасности систем, связанных с безопасностью, функциональная безопасность систем в области информационных технологий

FUNCTIONAL SAFETY OF SYSTEMS IN INFORMATION TECHNOLOGY

Shcherbina V.I.

Avtonomnaya non-profit organization "World Academy of Sciences for Complex Security" (ANO "WASCS"), 119602, Moscow, Academician Anokhin str., 30, Bldg. 2, office 128, e-mail: scherbina.vladimir@gmail.com

Currently the following positions in the world have adopted: 1 - the second most important features for any product, including services, (after the characteristics of appointment) are the safety characteristics; 2 - the main characteristic of the safety of complex technical systems (CTS) is their functional safety; 3 - functional safety of CTS is achieved by the adoption of risk reduction measures at all stages of their life cycle. Most of the hardware and software of information technology (IT) are the CTS. Therefore, they must to follow the requirements of basic standards for functional safety. The requirements for functional safety of IT systems is considered in the article.

Keywords: functional safety of systems, standardization of functional safety of safety-related systems, functional safety of systems in information technology

Введение

С начала текущего века в мировой практике произошли радикальные изменения в отношении подхода к обеспечению безопасности продукции (включая услуги), которые были закреплены в основополагающих международных руководствах и стандартах ИСО и МЭК по аспектам безопасности, функциональной безопасности систем, связанных с безопасностью, и системной деятельности [1 - 3]. В отношении сложных технических систем (СТС) подход может быть охарактеризован, как комплексный системный процессный риск-ориентированный подход. Важнейшими характеристиками продукции (после характеристик назначения) признаны характеристики безопасности; главной характеристикой безопасности систем признана их функциональная безопасность. Безопасность продукции достигают путем снижения риска причинения вреда на всех стадиях ее жизненного цикла. Эффективной мерой по снижению риска служит применение систем, связанных с безопасностью. В настоящее время действует около 200 международных стандартов по функциональной безопасности систем, связанных с безопасностью, в 40-а областях применения. В России принято свыше 30-и национальных стандартов в 8-и областях применения, однако в нашей стране в сфере информационных технологий эти стандарты до сих пор не нашли применения, что не способствует обеспечению приемлемого уровня безопасности широкого круга продукции и услуг в России.

Цель настоящей работы состоит в том, чтобы показать, почему требования функциональной безопасности должны быть распространены на объекты ИТ и как это повлияет на общий уровень безопасности в стране.

Предыстория

Впечатляющие научно-технические и технологические достижения прошлого века в атомной, ракетно-космической, машиностроительной отрасли, приборостроении в середине прошлого века были получены в условиях ограниченных вычислительных ресурсов. Основными инструментами для расчетов и проектирования сложных технических систем (СТС) служили арифмометры («железный Феликс»), логарифмические линейки и кульманы, и не было возможности в разумные сроки учесть и точно рассчитать множественные взаимосвязи составляющих СТС между собой и окружением, которые влияют на безопасность. Надежность и безопасность этих систем достигалась введением коэффициентов запаса в проектируемые системы и их составляющие. При этом молчаливо предполагалось, что свойства системы могут быть полностью определены суммой свойств ее составляющих как независимых единиц рассмотрения. Соответственно, это ошибочное допущение фигурировало в международных и национальных стандартах XX века, в том числе и в нашей стране.

В настоящее время в связи с интенсивным развитием ИТ технологий, совершенствованием общей теории систем, включая наиболее полную «Общую теорию систем Урманцева», так называемую ОТС(У) [4], широким внедрением системы менеджмента качества (серия ИСО 9000), основанной на опыте советского авиапрома, с ее процессным подходом, с учетом аспектов безопасности [1] с процессным риск-ориентированным комплексным подходом положение изменилось. Рядовым инструментом любого инженера и проектировщика стал персональный компьютер с огромными вычислительными возможностями и обширными наборами расчетных программ, математического моделирования и автоматизированного проектирования, и стало возможным проектировать СТС с учетом множественных взаимосвязей их составляющих между собой и окружением (рис. 1).

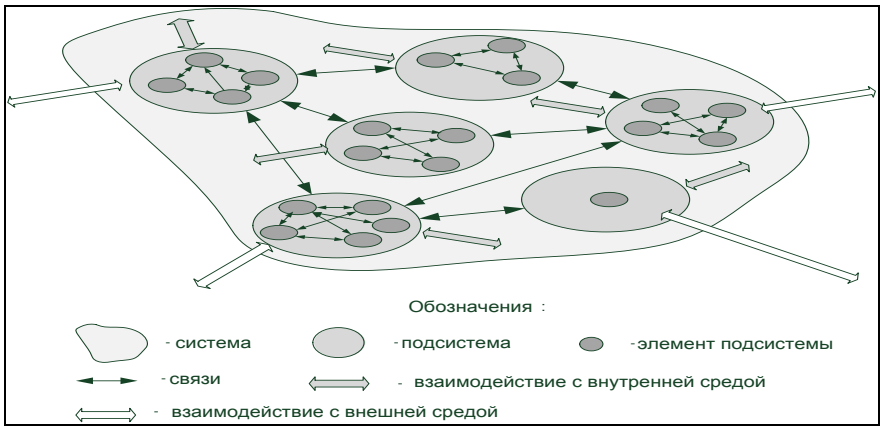


Рис. 1. Модель СТС.

Важнейшим шагом в области обеспечения безопасности послужило принятие основополагающих стандартов по функциональной безопасности электрических, электронных, программируемых электронных (Э/Э/ПЭ) систем, связанных с безопасностью [2] (российские аналоги – ГОСТ Р МЭК 61508-1 - ГОСТ Р МЭК 61508-7), и стремительное развитие этого направления стандартизации в самых различных областях применения. Стандарты данного направления охватили даже такую консервативную отрасль, как строительство. Первые в мировой практике стандарты по функциональной безопасности систем, связанных с безопасностью зданий и сооружений, были разработаны и приняты в России (серия ГОСТ Р 53195.1 - ГОСТ Р 53195.5). Они вызвали интерес за рубежом [5, 6], и на остове их положений в Германии разрабатываются аналогичные немецкие стандарты.

Ключевые положения стандартов в области функциональной безопасности систем, связанных с безопасностью

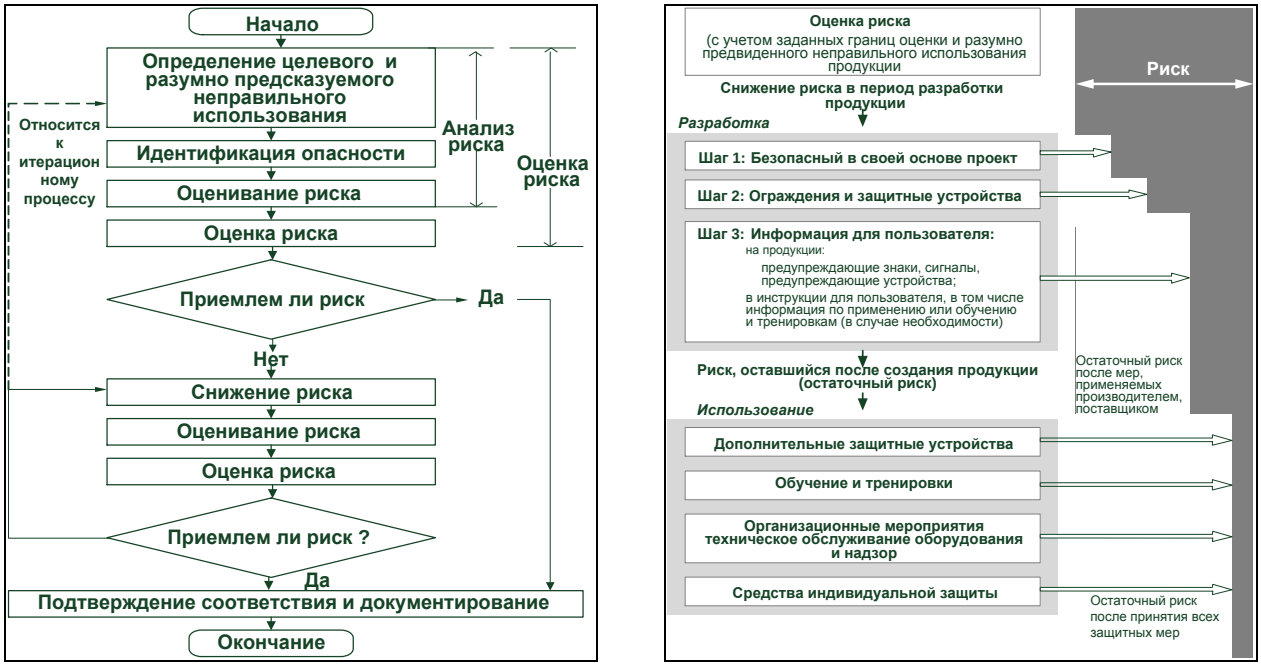
Системы, связанные с безопасностью, (СБ системы) – это системы, которые воздействуя на управляемое оборудование или системы управления управляемым оборудованием, выполняют функцию иди функции безопасности, обеспечивая снижение риска причинения вреда жизни и здоровью людей, имуществу, окружающей среде. Примерами СБ систем служат системы противоаварийной защиты, противопожарной защиты, противокриминальной и антитеррористической защиты, системы защиты машин и оборудования перерабатывающей промышленности и энергетики, транспортных средств (таких, как автоблокировочная система автомобилей или автоматического пожаротушения и т.п.), современного ручного инструмента и многие другие. К наиболее распространенным СБ системам относятся программируемые электронные системы.

Системы, связанные с безопасностью зданий и сооружений (СБЗС системы), – это системы, которые установлены в зданиях или сооружениях и входят в состав этих объектов неотъемлемой частью. Они взаимодействуют с системой строительных конструкций, друг с другом, с другими инженерными системами и средой. СБЗС системы могут выполнять свои функции безопасности и могут быть оценены на соответствие только в том месте, где здания или сооружения построены и системы установлены.

Функция безопасности имеет две составляющие – назначение (что выполняет функция) и полноту безопасности (вероятность успешного выполнения функции безопасности). В стандартах фигурирует 4 уровня полноты безопасности (УПБ 1 – УПБ 4), где УПБ 1 – наинизший, а УПБ 4 – наивысший уровень полноты безопасности.

Опасность в стандартах МЭК 61508, как и в [1], выражается в численных значениях риска. Необходимый уровень безопасности определяется как уровень снижения риска до приемлемого значения с помощью СБ системы (систем).

Требуемый уровень полноты безопасности достигают путем применения итерационного процесса анализа опасностей и риска, общей оценки риска, сравнения с необходимым значением риска и принятия мер по снижению риска до тех пор, пока не будет достигнут приемлемый риск (рис. 2а). Подобный итерационный процесс осуществляют на всех стадиях жизненного цикла систем (рис. 2б). К СБ системам предъявлены требования функциональной безопасности систем, их аппаратных средств (АС) и программного обеспечения (ПО).



а) б)

Рис. 2. Снижение риска на ЖЦ продукции.

с учетом взаимосвязи систем и их составляющих между собой, с другими системами и средой. Стандартами предусмотрена верификация и оценка соответствия СБ систем и их составляющих на стадиях их проектирования и создания и эксплуатации. На рис. 3 показана V-образная модель создания, верификации и подтверждения соответствия комплексной системы обеспечения безопасности (КСБ) зданий и сооружений с ее Э/Э/ПЭ СБЗС системами, их составляющими, АС и ПО.

Выполнение требований стандартов серий ГОСТ Р МЭК 61508 и ГОСТ Р 53195 позволяет гарантировать достижение и поддержание необходимой полноты безопасности СБ и СБЗС систем, в отличие от выполнения требований прежних стандартов, когда СБ и СБЗС системы установлены в (на) защищаемых объектах (машинах и оборудовании, зданиях и сооружениях), а гарантии выполнения ими функций безопасности с необходимой степенью вероятности отсутствуют.

Функциональная безопасность ИТ систем

В состав практически всех современных СБ и СБЗС систем входят системы и подсистемы ИТ с их с их АС и ПО, на которые распространяются требования функциональной безопасности, установленные стандартами серий ГОСТ Р МЭК 61508 и ГОСТ Р 53195.

В ГОСТ Р МЭК 61508 и ГОСТ Р 53195 установлено, что системы, которые используются для измерений, испытаний, расчетов, проектирования и производства СБ и СБЗС систем, также подлежат оценке и подтверждению соответствия на их функциональную безопасность.

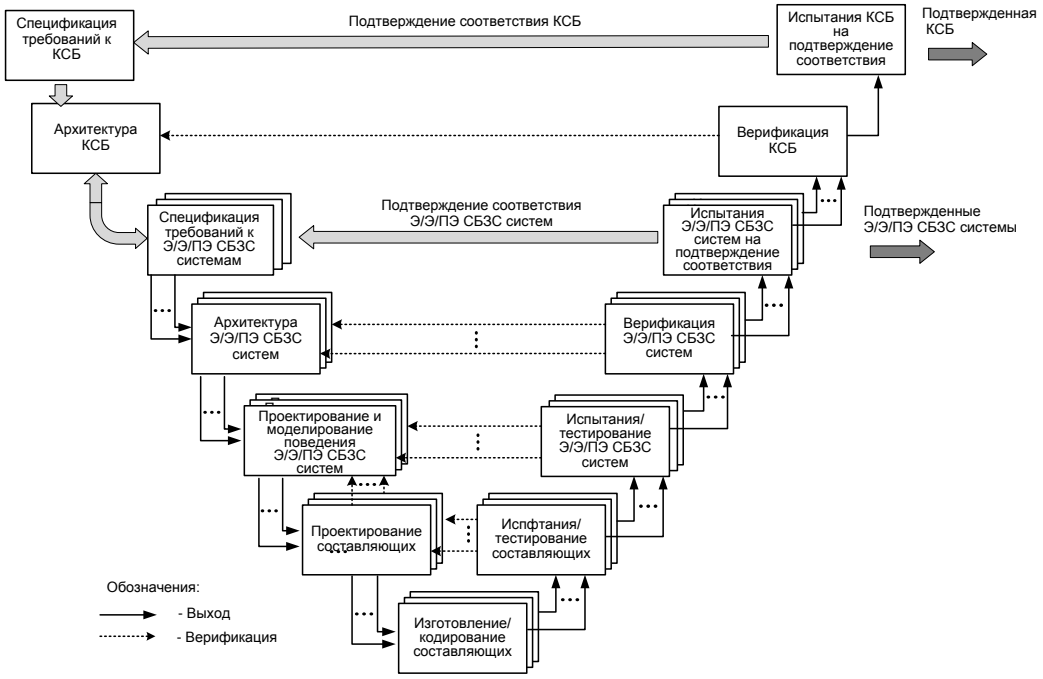


Рис. 3. V-образная модель создания, верификации и подтверждения соответствия КСБ здания (сооружения).

Таким образом, под действие ГОСТ Р МЭК 61508 подпадают персональные компьютеры с их АС и системным ПО, прикладные программы, используемые для расчетов, математического моделирования и автоматизированного проектирования СБ систем и средств; измерительные приборы и испытательное оборудование с входящими в их состав программируемыми контроллерами и производственными компьютерами, применяемые при производстве и испытаниях (заводских и сертификационных) СБ систем, а также измерительные и испытательные средства, применяемые для периодического контроля СБ систем в период эксплуатации.

В области строительства в соответствии с требованиями ГОСТ Р 53195 оценке и подтверждению соответствия требованиям функциональной безопасности подлежат сами СБЗС системы; системы автоматизированного проектирования систем и строительных объектов; системы испытаний и контроля СБЗС систем в период строительства, ввода в эксплуатацию, а также в период эксплуатации.

Если для перечисленных ИТ систем не выполнены требования к их функциональной безопасности, то выполнение СБ и СБЗС системами функций безопасности не может быть гарантировано, т. е. системы могут быть разработаны, изготовлены, установлены, пущены в действие, а их функции безопасности могут оказаться не выполненными, что, к сожалению, регулярно наблюдается на практике.

Применение стандартов по функциональной безопасности систем в информационных технологиях будет способствовать гарантированному выполнению функций безопасности СБ и СБЗС системами (выполненными по этим стандартам) и повышению общего уровня безопасности в стране.

Выводы

1. Современные требования к системам, связанным с безопасностью, основаны на комплексном системном процессном риск-ориентированном подходе.

2. В мире и в России действует большое число стандартов по функциональной безопасности систем, которая признана главной характеристикой безопасности сложных технических систем.

4. Оценке и подтверждению соответствия подлежат СБ и СБЗС системы.

5. Аппаратные и программные средства ИТ, такие, как компьютеры, процессоры, контроллеры, средства оперативной и долговременной памяти и др. системное и прикладное ПО, включая ПО для измерительных приборов, испытательного, производственного оборудования с числовым программным управлением, систем автоматизированного проектирования и т. п., применяемые для проектирования, производства испытаний и

контроля СБ и СБЗС систем, подлежат оценке и подтверждению их соответствия требованиям функциональной безопасности.

6. Невыполнение требований функциональной безопасности СБ и СБЗС системами, а также ИТ системами, входящими в состав средств математического моделирования, проектирования, производства, измерений, испытаний и контроля этих систем, не позволяет гарантировать выполнение СБ и СБЗС системами их функций безопасности в период эксплуатации, что снижает общий уровень безопасности в стране.

7. С учетом п. 6 особенно актуально повсеместное применение стандартов серий ГОСТ Р МЭК 61508 и ГОСТ Р 53195 теми лицами, действия (бездействие) которых влияют на безопасность СТС.

Предложения и рекомендации

1. Разработчикам поставщикам АС и ПО, предназначенного для математического моделирования, проектирования, производства, измерений, испытаний и контроля СБ и СБЗС систем предлагается применять в своей работе стандарты серий ГОСТ Р МЭК 61508 и ГОСТ Р 53195 и подтверждать соответствие разрабатываемых АС и ПО требованиям функциональной безопасности.

2. Разработчикам, осуществляющим разработку СБ систем и проектировщикам Э/Э/ПЭ систем, рекомендуется применять в своей работе системы автоматизированного проектирования, их АС и ПО, сертифицированные на соответствие требованиям функциональной безопасности.

3. Производителям СБ систем, строителям, выполняющим монтаж и пуско-наладку СЬЗС систем, а также лицам, осуществляющим контроль этих систем в период эксплуатации, рекомендуется применять в своей работе производственное, измерительное, испытательное оборудование и приборы, содержащие средства ИТ, сертифицированные на функциональную безопасность.

Список литературы

1. ISO/IEC Guide 51:2014 Safety aspects – Guidelines for their inclusion in standards. www.iso.org (accessed 17 November 2016).
2. IEC 61508:2010 (all parts) Functional safety of electrical/electronic/programmable electronic safety-related systems. www.iec.ch (accessed 17 November 2016).
3. Vreeswijk, F.W.P. Systems activities in IEC. IEC Administrative Circular AC/33/2013:2013-09-20. To all Committees to all technical committee and subcommittee officers.
4. Урманцев Ю.А. Общая теория систем в доступном изложении. R&C Dynamics, Москва Ижевск, 2014. 408 с. ISBN: 978-5-93972-974-1.
5. Shcherbina, V.I., Puzurevskaya, T.I., Lubimov, M.M, Matveev,V.P. Functional safety-related systems in construction. VDI-Berichte Nr. 2126, 2011. Pp. 255-264.
6. Нахтигаль Е. Функциональная безопасность в строительстве на примере на примере ГОСТ Р 53195 «Безопасность функциональная связанных с безопасностью зданий и сооружений систем». «Стандарты и качество». № 2. 2013. С. 34-37.

References

1. ISO/IEC Guide 51:2014 Safety aspects – Guidelines for their inclusion in standards www.iso.org (accessed 17 November 2016).
2. IEC 61508:2010 (all parts) Functional safety of electrical/electronic/programmable electronic safety-related systems www.iec.ch (accessed 17 November 2016).
3. Vreeswijk, F.W.P. Systems activities in IEC. IEC Administrative Circular AC/33/2013:2013-09-20. To all Committees to all technical committee and subcommittee officers.
4. Urmantsev, U.A. Obshchaya teoriya system v dostupnom izlohgenii. R&C Dynamics, Moskva - Ihgevsk. 2014. 408 p.
5. Shcherbina, V.I., Puzyrevskaya, T.I., Lubimov, M.M, Matveev, V.P. Functional safety-related systems in construction. VDI-Berichte Nr. 2126, 2011, pp. 255-264.
6. Nahtigal, E. Funkcionalnaya bezopastnost v stroitelstve na primere GOST R 53195 “Bezopastnost funkcionalnaya svyazannyh s bezopasnostyu zdaniy i sooruhgeniy sistem”. Standarty i kachestvo, no. 2, 2013. pp. 34-37.