УДК 004. 052

А.А. Орехова

Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков

ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ ОЦЕНИВАНИЯ БЕЗОПАСНОСТИ ЧЕЛОВЕКО-МАШИННЫХ ИНТЕРФЕЙСОВ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ

Предложена информационная технология оценки качества и функциональной безопасности ЧМИ ИУС, основанная на Safety Case методологии и предложенном автором методе комплексной оценки на всем жизненном цикле ЧМИ. Описана структура и основные этаны использования информационной технологии. Рассмотрены примеры инновационных технологий проектирования ЧМИ систем мониторинга и управления технологическим оборудованием. Разработаны инструментальные средства для поддержки предложенной информационной технологии, описаны их основные функции и возможности. Предложенная информационная технология и разработанные инструментальные средства могут быть использованы для оценки качества и функциональной безопасности ЧМИ ИУС критических систем.

Ключевые слова: *информационная технология, человеко-машинный интерфейс, качество в использовании, юзабилити, Safety Case, функциональная безопасность, информационно-управляющие системы.*

Введение

Человеко-машинные интерфейсы (ЧМИ) являются важной составляющей компьютерных информационно-управляющих систем (ИУС). Качество ЧМИ непосредственно влияет на характеристики ИУС. Для систем критического применения наиболее важными являются свойства надежности и безопасности. Проблемы обеспечения этих свойств в ЧМИ рассматриваются в новых отраслях знаний, таких как юзабилити-инженерия и инженерия безопасности. Следует отметить, что разработка удобной в использовании системы может привести к ухудшению ее безопасности. Чтобы спроектировать ЧМИ для критических приложений, (ракетно-космических систем, медицинских, бизнес-приложений и т.п.) должны быть обоснованы, сформулированы, оценены и выполнены требования к качеству, надежности и безопасности. Здесь ключевой является задача оценивания программных систем и их ЧМИ [1]. Значительную часть трудностей при разработке ИУС можно избежать, если с самого начала создавать программную систему в соответствии с определенной методологией [2]. Решение задачи оценивания может базироваться на CASE (Computer-Aided Software Engineering)-подходе, реализуемом с помощью набора компьютеризированных (методических и инструментальных) средств и методологии Safety Case, которая используется при оценке безопасности и качества в целом путем формирования набора “кейсов”, подтверждающих выполнение требований [3].

В настоящее время в мировой практике наметился определенный рост инновационных технологий в области ЧМИ. В качестве примеров инструментальных средств (ИС) проектирования ЧМИ ИУС можно привести «SIMATIC HMI» (фирма Siemens) [4], «HMI Visualisation Tools» (фирма Mitsubishi Electric) [5], «InstantHMI 6.0» (фирма Software Horizons inc.) - ИС проектирования ЧМИ для SCADA систем, работающих на платформах Windows PC, Windows CE и PDA [6] и др. Компания Usabilla (Нидерланды) разработала сервис, который помогает разработчикам провести комплексную оценку привлекательности своих интерфейсов [7]. Как показал анализ публикаций, средства оценки безопасности ЧМИ ИУС практически отсутствуют.

Цель работы – разработка информационной технологии оценки качества и безопасности ЧМИ ИУС на основе методологии Safety Case и предложенных автором моделях, методах и ИС. Усовершенствованная модель качества и безопасности в использовании, полученная на основе анализа современной нормативной базы различных отраслей, учитывающая человеческий фактор и особенности ЧМИ ИУС, рассмотрена в [8]. Метод оценки качества и безопасности ЧМИ, позволяющий повысить полноту, точность и достоверность оценки на всех этапах жизненного цикла за счет комплексирования количественных и качественных методик приведен в работах [9, 10].

Структура информационной технологии оценки безопасности ЧМИ

Под информационной технологией будем понимать совокупность методов, аппаратных и программных средств преобразования информации [11]. Функциональная модель информационной технологии оценки качества и безопасности ЧМИ ИУС представлена в виде IDEF0-диаграммы (рис. 1).

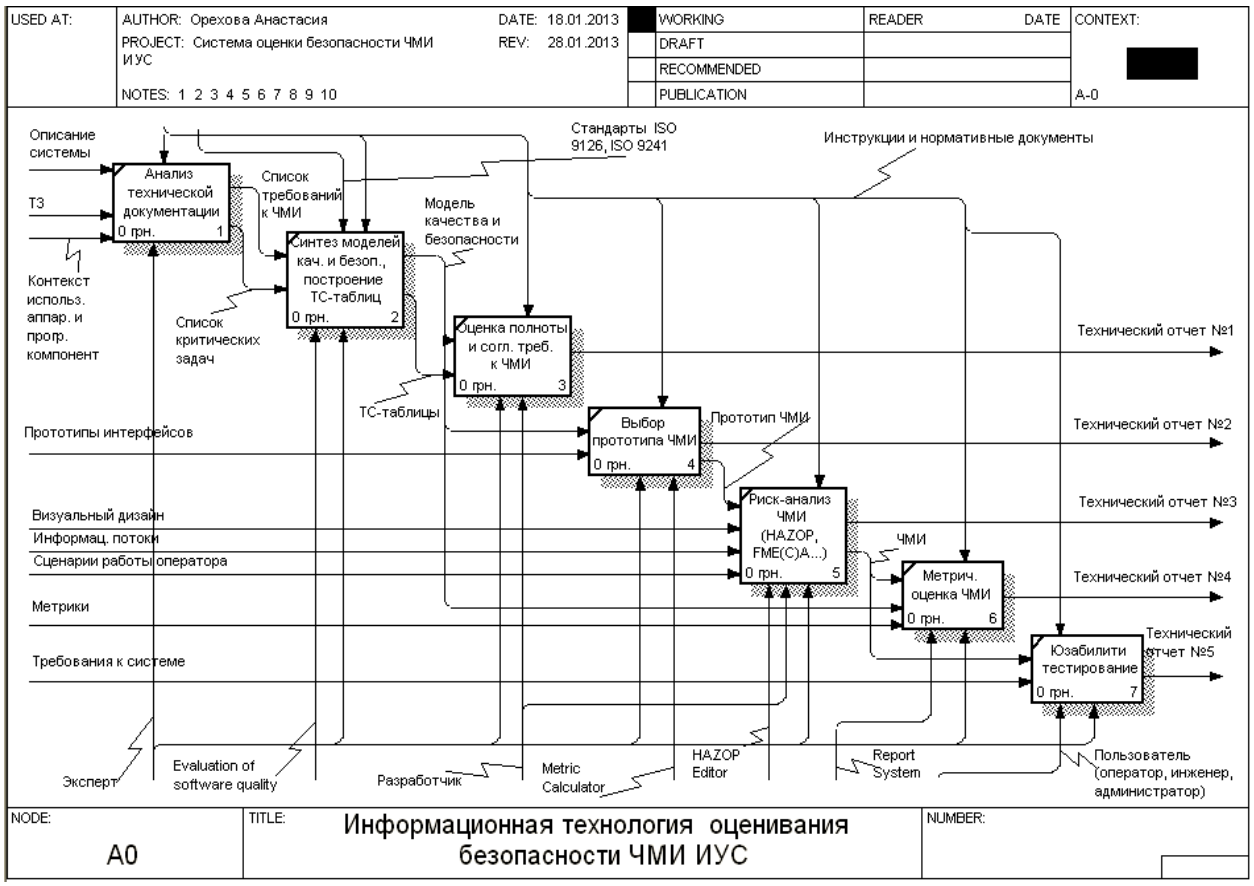

Рис. 1. Функциональная модель информационной технологии оценивания безопасности ЧМИ ИУС

Функциональная модель включает следующие этапы.

1. Проводится анализ технической документации ИУС и определяются требования к ЧМИ, а также идентифицируются критические задачи (функции) ИУС, для которых ошибки оператора могут привести к нежелательным последствиям.

Исходные данные: техническое задание на ИУС, контекст использования аппаратных и программных компонент ЧМИ.

Результат: список требований к ЧМИ, список критических задач.

2. В зависимости от класса системы и критичности решаемых задач эксперт обосновывает и строит модель качества и безопасности (МКБ), которая на этом этапе представляет собой профиль свойств (характеристик, критериев), которыми должен обладать интерфейс оператора. Чем выше степень критичности задачи, тем сложнее профиль и больше характеристик, учитывающих человеческий фактор. Формируются таблицы “Требования - Свойства” (ТС - таблицы) для различного класса задач.

Исходные данные: список требований к ЧМИ, множество инструкций и нормативных документов.

Результат: множество профилей свойств и ТС-таблиц.

3. Оценивается полнота требований к ЧМИ и их согласованность с МКБ. При этом, если требования не покрывают всех свойств, то разработчик должен дополнить ТЗ новыми требованиями. Если для каких-то требований нет соответствующих свойств, то требования являются избыточными либо имеют не ясную формулировку. Такие требования разработчик должен пересмотреть или исключить.

Исходные данные: заполненные ТС - таблицы.

Результат: технический отчет по безопасности, включающий список требований, которые необходимо пересмотреть и список свойств, которым не отвечает проект ЧМИ.

4. Решается задача выбора прототипа ЧМИ оптимального с точки зрения соответствия МКБ. Выполняется доработка (реинжиниринг) выбранного прототипа или корректируется проект разрабатываемого ЧМИ ИУС.

Исходные данные: прототипы ЧМИ.

Результат: отчет по безопасности, содержащий МКБ и выполненные расчеты, подтверждающие обоснование выбора наиболее безопасного прототипа.

5. После этапа детального проекта для компонент ЧМИ, важных для безопасности при необходимости выполняется HAZOP или FME(C)A анализ. Элементами такого анализа могут быть:

– диалоги между оператором и системой, заданные в форме сценариев решаемых оператором задач;

– потоки передаваемой информации;

– элементы визуального дизайна.

Исходные данные: сценарии использования, информационные потоки и способы кодирования, компоновка элементов интерфейса, HAZOP или FMECA-таблицы.

Результат: отчет по безопасности, содержащий обоснование того, что детальный дизайн ЧМИ обеспечивает безопасную работу оператора.

6. Для количественной оценки готового проекта ЧМИ ранее построенная экспертом МКБ преобразуется в иерархическую метрическую модель качества и безопасности (ММКБ). Эксперт выбирает метрики, проводит их анализ с точки зрения сложности и возможности практического применения.

Исходные данные: база данных характеристик и метрии, исходные МКБ.

Результат: отчет по безопасности, содержащий иерархические метрические модели качества и безопасности, а также результаты количественных измерений отдельных характеристик, влияющих на безопасность в использовании ЧМИ.

7. На этапе приемо-сдаточных испытаний выполняется юзабилити тестирование ЧМИ операторами ИУС, которое подтверждает правильность и адекватность выполненных ранее оценок.

Исходные данные: требования к системе, результаты проведенных ранее исследований опасности и работоспособности отдельных компонент ЧМИ.

Результат: итоговый технический отчет по безопасности, включающий модель качества и безопасности, результаты анализа требований к ЧМИ на полноту и согласованность, обоснование выбранного прототипа, результаты риск анализа компонент интерфейса для задач, важных для безопасности, результаты метрической оценки и юзабилити тестирования.

Архитектура системы и инструментальные средства оценивания безопасности ЧМИ

С целью инструментальной поддержки методов анализа, повышения достоверности, точности и полноты оценки ЧМИ ИУС разработано CASE-средство «Оценка безопасности ЧМИ». Оно позволяет автоматизировать процесс синтеза моделей качества и безопасности, их хранение и повторное использование, поддерживает процесс оценки, принятия экспертных решений, отображение получаемых результатов и создание отчетов по безопасности на всех этапах жизненного цикла ЧМИ.

CASE-средство базируется на предложенных автором моделях качества и безопасности в использовании, а также методе комплексной оценки ЧМИ [9]. Системная архитектура CASE-средства показана на рис. 2.

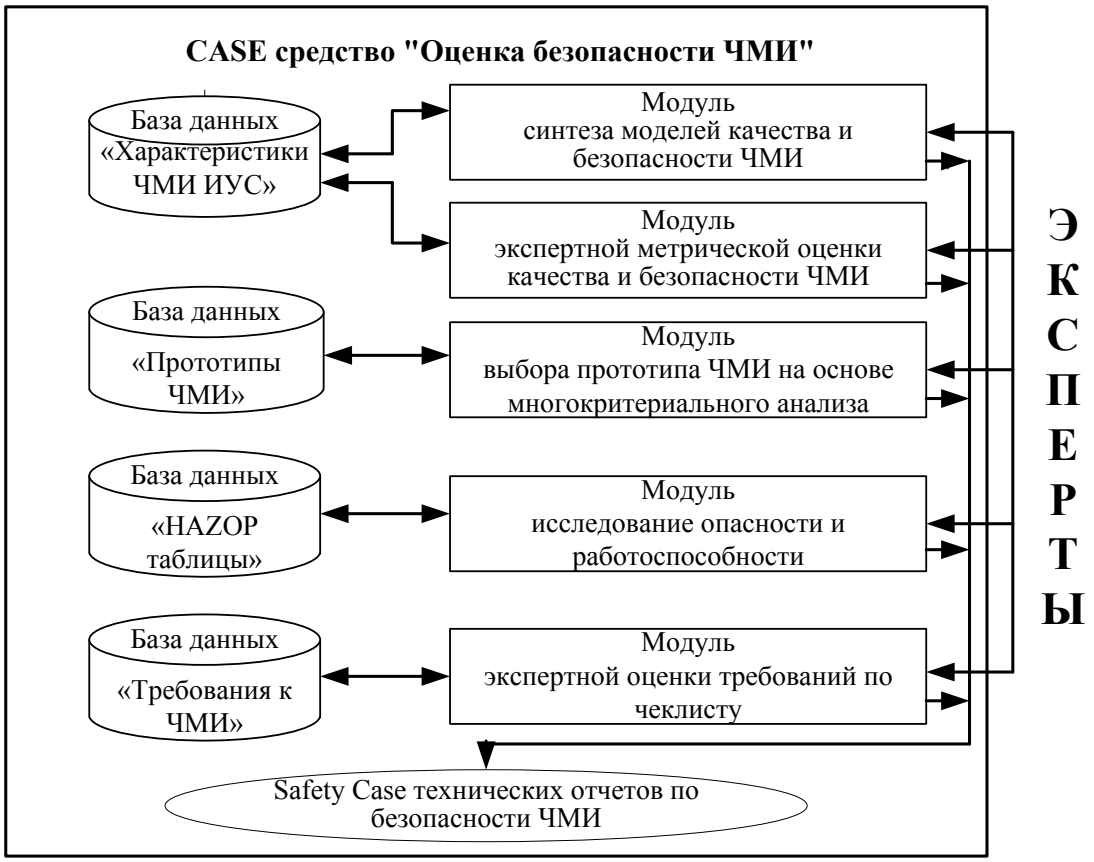

Рис. 2. Архитектура системы оценки качества и безопасности ЧМИ ИУС

CASE-средство имеет три режима работы:

1) режим синтеза моделей качества и безопасности в использовании;

2) режим оценивания;

3) режим генерации отчетов по безопасности.

Основными режимами работы являются режим синтеза моделей и режим оценивания, в которых выполняется автоматизированный выбор характеристик и установление связей между ними, а также выбор методов в зависимости от критичности решаемых оператором задач и этапа жизненного цикла ЧМИ.

Функциями CASE-средства в режиме синтеза моделей качества и безопасности в использовании являются (рис. 3):

– выбор профиля свойств проекта ЧМИ из базы данных в виде перечня характеристик верхнего уровня иерархии модели качества и безопасности в использовании;

– выбор и автоматическое установление связей с характеристиками нижних уровней;

– выбор метрик (метода и шкалы);

– ввод весовых коэффициентов;

– ввод новых характеристик и их описания;

– сохранение профиля в базе данных для его повторного использования.

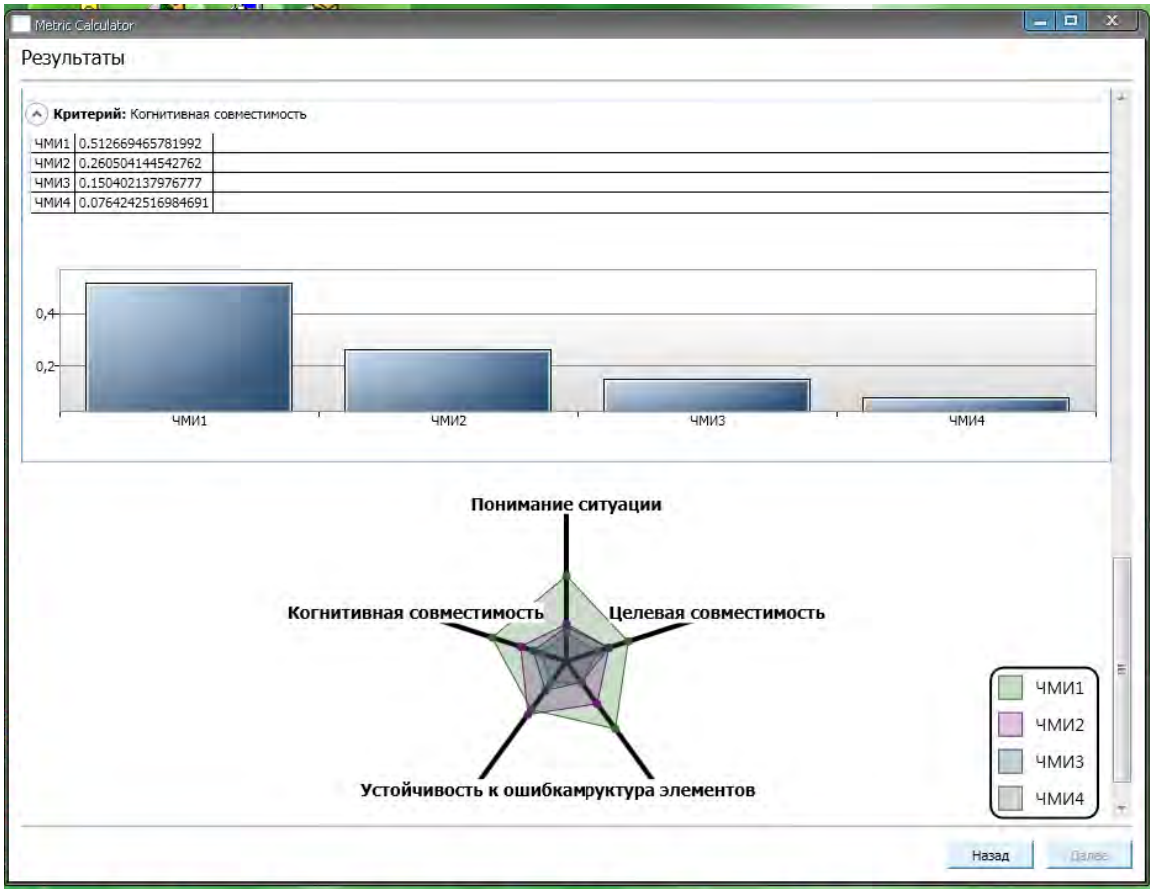

Рис. 3. Окно системы в режиме оценивания и выбора прототипа ЧМИ

В режиме оценивания CASE-средство поддерживает:

– анализ полноты и согласованности требований ЧМИ с профилем качества и безопасности в использовании;

– экспертную оценку соответствия проекта ЧМИ требованиям ТЗ по чеклисту;

– выбор прототипа ЧМИ, наилучшим образом удовлетворяющего профилю качества и безопасности в использовании;

– HAZOP и FMEA анализ (или их комплексирование) для оценки рисков и отклонений детального проекта ЧМИ, которые могут привести к ошибке оператора;

– количественную оценку интегральных и промежуточных характеристик ЧМИ на основе иерархической модели качества и безопасности в использовании, соответствующей требованиям технического задания.

В режиме генерации отчетов по безопасности CASE-средство поддерживает:

– создание и хранение отчетов, содержащих данные о проекте, эксперте, дате и времени проведения экспертизы, применяемых моделях и результатах оценки в различном виде;

– генерацию отчетов по безопасности в различных форматах.

Заключение

В данной статье была предложена информационная технология оценки функциональной безопасности ЧМИ ИУС, включающая в себя модули синтеза моделей качества и безопасности ЧМИ, выбора прототипа ЧМИ на основе многокритериального анализа, экспертной метрической оценки, оценки требований по чеклисту, исследования опасности и работоспособности и составления обоснования безопасности.

Для поддержки данной информационной технологии было разработано CASE-средство.

Дальнейшие исследования могут быть направлены на совершенствование данного инструментального средства и системы в целом в части выбора методов обеспечения безопасности.

Список литературы

1. CASE-оценка критических программных систем. В 3-х т. Том 1. Качество / В.О. Мищенко, О.В. Поморова, Т.А. Говорущенко; под. ред. В.С. Харченко. – Х: Нац. аэрокосмический ун-т "Харьковский авиац. ин-т", 2012. – 201 с.

2. Боэм Б. Характеристики качества программного обеспечения / Б. Боэм, Дж. Браун, Х. Каспар и др. – М.: Мир, 1981. – 208 с.

3. Safety Case-Oriented Assessment of Critical Software: Several Principles and Elements of Techniques / A. Andrashov, V. Kharchenko, K. Netkachova, et.al. Monographs of System Dependability. Dependability of Networks, Wroclaw, OWPW, 2010. – P. 11-25.

4. SIMATIC HMI. [Электронный ресурс]. – Режим доступа к ресурсу: www.intechcom.ru/HMI_cat.pdf.

5. HMI - Visualisation Tools. [Электронный ресурс]. – Режим доступа к ресурсу: http://www.siriustrading.ro/Download/HMIComercial&Technical Catalogue 2007.pdf.

6. InstantHMI Manual. [Электронный ресурс]. – Режим доступа к ресурсу: www.instanthmi.com/ manuals/IHMI6-Manual.pdf.

7. A new standard in user feedback. [Электронный ресурс]. – Режим доступа к ресурсу: usabilla.com.

8. Орехова А.А. Нормативная база и оценка качества человеко-машинных интерфейсов ИУС АЭС на основе Safety case методологии / А.А. Орехова, В.С. Харченко // Інженерія програмного забезпечення. – К.: Національний авіаційний університет. – 2011. – № 4(8). – С. 22–34.

9. Орехова А.А. Методика комплексной оценки безопасности человеко-машинного интерфейса ИУС критического применения / А.А. Орехова, В.Р. Тилинский, В.С. Харченко // Радіоелектронні і комп'ютерні системи. – Х.: НАКУ «ХАІ». – 2012. – № 5(57). – С. 230-235.

10. Orekhova A. Safety case-oriented assessment of human-machine interface for NPP I&C system / A. Orekhova, V. Kharchenko, V. Tilinskiy // RT&A # 03 (26) (Vol.7), 2012. – P. 27-38.

11.Советов Б.Я. Информационные технологии / Б.Я. Советов, В.В. Цехановский. – М.: Высш. шк., 2006. – 263 с.

Поступила в редколлегию 28.12.2012

Рецензент: д-р техн. наук, проф. Б.М. Конорев, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков.

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ОЦІНЮВАННЯ БЕЗПЕКИ ЛЮДИНО-МАШИННОГО ІНТЕРФЕЙСУ ІНФОРМАЦІЙНО-КЕРУЮЧИХ СИСТЕМ

А.О. Орєхова

Запропонована інформаційна технологія оцінки якості та функціональної безпеки ЛМІ ІКС, заснована на Safety Case методології та запропонованому автором методі комплексної оцінки на всьому життєвому циклі ЛМІ. Описано структуру та основні етапи використання інформаційної технології. Розглянуто приклади інноваційних технологій проектування ЛМІ систем моніторингу та управління технологічним обладнанням. Розроблені інструментальні засоби для підтримки запропонованої інформаційної технології, описані їх основні функції та можливості. Запропонована інформаційна технологія та розроблені інструментальні засоби можуть бути використані для оцінки якості та функціональної безпеки ЛМІ ІКС критичних систем.

Ключові слова: *інформаційна технологія, людино-машинний інтерфейс, якість у використанні, юзабіліті, Safety Case, функціональна безпека, інформаційно-керуючи системи.*

INFORMATION TECHNOLOGY FOR EVALUATION THE SAFETY INFORMATION AND CONTROL SYSTEMS HUMAN-MACHINE INTERFACE

A.A. Orekhova

Proposed information technology quality assessment and functional safety I&C systems HMI is based on Safety Case methodology and method of a comprehensive assessment of the whole life cycle of HMI proposed by the author. The structure and main steps of utilizing the technology are described. Examples of innovative design technology HMI monitoring and control of technological equipment were considered. Software tools supporting the proposed information technology are developed, the basic functions and features of the tools are outlined. The proposed information technology and software tools can be used to assess quality and functional safety of the entire I&C systems HMI.

Keywords: *information technology, human-machine interface, quality-in-use, usability, Safety Case, functional safety, information and control system.*