ЧЕЛОВЕКО-МАШИННЫЙ ИНТЕРФЕЙС В СИСТЕМАХ БЕЗОПАСНОСТИ

Лёвин Сергей Николаевич
главный конструктор ГК «СИГМА»

Вопросы взаимодействия человека и машины возникли задолго до компьютерной эры. Однако, именно развитие вычислительной техники и программного обеспечения дало мощный импульс направлению HMI (Human Machine Interface – человеко-машинный интерфейс). Сейчас также используется определение HCI (Human-Computer Interaction – человеко-компьютерное взаимодействие).

Если говорить о человеко-машинном интерфейсе в системах обеспечения физической безопасности объекта посредством технических средств охраны, то можно выделить два основных направления: это взаимодействие человека с оборудованием системы и программным обеспечением верхнего уровня. Конечно, в настоящее время общение с системой в большинстве случаев организуется через программный интерфейс, который предоставляет гораздо больше возможностей, чем приборные панели контроллеров. Тем не менее, рассмотрим все возможные варианты работы с системой. Также можно выделить три основные роли человека в этом процессе: это администратор, оператор и пользователь системы безопасности. Пользователем, в данном случае, можно назвать человека, чье взаимодействие с системой безопасности не является предметом его профессиональной деятельности. Обычно пользователи имеют возможность работы с системой контроля и управления доступом и охранной сигнализацией. В первом случае человек контактирует с системой при совершении проходов через точки доступа, во втором – при выполнении операций по постановке на охрану и снятии с охраны. Для выполнения этих действий человеком система должна предоставить определенный интерфейс: клавиатуру для ввода ПИН-кода и команд управления с дисплеем для отображения информации, считыватель для электронного идентификатора пользователя или терминал для считывания биометрических данных человека. В настоящее время практически у каждого при себе всегда имеется смартфон – универсальный терминал общения с системой. Современные системы безопасности в полной мере предлагают использовать эту возможность, с помощью смартфона можно получать тревожные и информационные извещения, просматривать изображения с камер системы видеонаблюдения, выполнять различные действия в системе и т. д.

Операторы и администраторы систем безопасности непосредственно с оборудованием сегодня работают все меньше, так как в большинстве случаев взаимодействие организуется через пользовательский интерфейс прикладного программного обеспечения системы безопасности. Тем не менее, для организации функций резервирования рабочего места оператора часто остаются требования по предоставлению информации и управлению системой непосредственно через оборудование: пульты управления, табло отображения состояния объекта охраны и т. п. Для администратора, в ряде случаев, также полезно иметь возможность доступа к настройкам оборудования напрямую, без использования компьютера и специального программного обеспечения.

Тем не менее, основная роль по организации человеко-машинного интерфейса возложена сегодня на программное обеспечение. Здесь существует целая группа терминов и определений по этой теме: UI (User Interface) – пользовательский интерфейс, GUI (Graphic User Interface) – графический пользовательский интерфейс, UX (User eXperience) – дизайн взаимодействия с пользователем, Usability – удобство пользовательского интерфейса.

Можно выделить две основные категории пользователей ПО: администраторы и операторы. Администраторы занимаются настройкой, программированием и обслуживанием системы, операторы выполняют прикладную задачу. В комплексной системе безопасности зачастую используется большая номенкла-

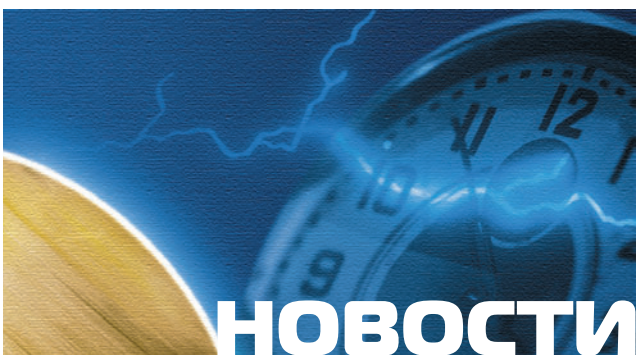
тура разнородного оборудования, и одна из основных задач, возлагаемая на ПО администрирования, – сконфигурировать все это «железо». Существует два основных подхода: отдельные конфигураторы для каждого типа оборудования и единый центр конфигурирования, реализуемый на базе интегрирующего ПО. Использование отдельных программных конфигураторов является самым простым и очевидным решением, так как подобное ПО для конфигурирования, как правило, поставляется производителем соответствующего оборудования. Тем не менее, разработчики интегрирующего ПО (в английском языке для этого класса ПО систем безопасности есть собственное название: PSIM – Physical Security Information Management) часто стремятся объединить в своем продукте не только функции дежурного режима, но и функциональность администрирования. С одной стороны, это задача чрезвычайно сложная и даже неблагодарная – редко кому удается сделать универсальный конфигуратор, который не уступает оригинальному ПО от производителя оборудования. С другой стороны, в случае единого центра администрирования, появляется уникальная возможность настраивать всю систему буквально в одном окне. Сложность разработки универсального конфигуратора обусловлена еще и тем, что при поддержке большого количества оборудования необходимо постоянно поддерживать актуальность конфигуратора по отношению к оборудованию. В случае добавления новых возможностей производителем оборудования в свою продукцию, разработчики интегрирующего ПО должны также дорабатывать свой конфигуратор, чтобы поддержать новые функции. Одна из главных проблем при создании универсального инструмента конфигурирования – это настройка прав пользователей в оборудовании системы контроля и управления доступом. Дело в том, что представление уровня доступа в контроллере СКУД практически никак не стандартизовано и каждый производитель предлагает свой вариант реализации записи о правах пользователя в своем оборудовании. Попытка создать единое представление уровня доступа в системе чаще всего приводит к каким-либо ограничениям при интерпретации общего уровня доступа в аппаратно-зависимые данные для каждого конкретного контроллера СКУД. Тем не менее, удобство администрирования часто перевешивает некоторые ограничения функционала оборудования.

Не смотря на всю востребованность и сложность разработки инструментов администрирования системы безопасности, все-таки самым важным программным элементом является ПО дежурного режима. От продуманности и качества реализации пользовательского интерфейса оператора зависит, насколько эффективно будет осуществляться охрана защищаемого объекта. Подходы к реализации интерфейса оператора зависят от масштаба системы, от функционального разделения рабочих мест операторов, от требований к системе по информационной поддержке действий оператора и т. д. В любом случае, для интерфейса оператора должны выполняться некоторые обязательные требования. Оператор в любой момент времени должен видеть общую картину состояния объекта охраны. Это может быть реализовано в виде краткой сводки, обобщенного табло состояния объекта или каким-либо иным способом. Оператор не должен пропустить тревожное извещение от системы безопасности. Для этого тревоги должны обязательно сопровождаться звуковой сигнализацией, человек ведь не может безотрывно смотреть на монитор, поэтому звуковое сопровождение необходимо. Тревожные извещения не должны замещаться менее приоритетными событиями в системе. Другими словами, тревоги должны постоянно находиться в фокусе внимания оператора. Если имеется факт наличия множественных тревог, оператор должен иметь возможность постоянно видеть их общее количество, оперативно получать доступ к каждому тревожному объекту в системе.

Если система безопасности небольшая и достаточно одного рабочего места оператора, программное обеспечение

должно иметь возможность организовать на одном компьютере пользовательский интерфейс ко всем подсистемам: охранно-пожарная сигнализация, СКУД, видеонаблюдение. Для отображения большого количества информации от разных подсистем может потребоваться использование нескольких мониторов в рамках одного рабочего места. Это позволяет эффективно организовать информационное пространство для оператора. На одном мониторе может быть показан графический план объекта охраны, на других мониторах выведены изображения от камер видеонаблюдения. Что касается графического представления объекта охраны, то классическим является набор двухмерных планов объекта, на которых отображаются значки технических средств охраны. Сегодня все чаще предпринимаются попытки трехмерного отображения охраняемого объекта. Выглядит это безусловно эффектно, однако на практике, для быстрой оценки обстановки и принятия решения о необходимых действиях в сложившейся ситуации, оператору достаточно указания места тревоги на обычном плане – информация с плоской карты человеком считывается гораздо быстрее. Для крупных объектов, где организуется несколько рабочих мест или несколько постов охраны, логичным выглядит разделение задач операторов по функциональным подсистемам или по отдельным частям объекта. Часто сочетаются оба варианта. Например, может быть создано отдельное рабочее место оператора системы видеонаблюдения, куда сводится большое количество видеоканалов. А на отдельных постах охраны могут быть организованы универсальные рабочие места, куда выводится информация от всех подсистем, но ограниченная только той частью объекта охраны, которая находится в зоне ответственности данного поста охраны. Для больших систем актуальным является разграничение прав и области видимости операторов. Это нужно, чтобы оператор получал информацию прежде всего для своего участка охраны и не был перегружен данными от других участков. Кроме того, ограничение прав не позволит оператору видеть и иметь доступ к «чужим» техническим средствам охраны. Для надежной защиты важных объектов может использоваться дублирование рабочих мест операторов с возможностью передачи или перехвата управления в зависимости от складывающейся ситуации. Важной задачей пользовательского интерфейса является автоматическое предоставление оператору нужных данных от разных подсистем по определенным событиям, прежде всего тревожным. Например, при срабатывании охранной сигнализации автоматически вывести на монитор изображение от видеокамеры, на котором видно место срабатывания. Или при просмотре протокола событий, указав на интересующее событие, сразу получить доступ к записи из видеоархива по связанной с данным событием видеокамерой с учетом времени наступления события. Таких примеров можно привести много, поэтому лучше всего, если подобные связи между объектами и подсистемами можно настраивать на объекте непосредственно под конкретную задачу.

Какой бы ни был удобный интерфейс программы, для того, чтобы оператор системы безопасности мог эффективно выполнять свою работу, особенно в чрезвычайной ситуации, необходимо в совершенстве знать и уметь применять все возможности ПО. Чтобы оператор «подружился» с пользовательским интерфейсом, лучше всего иметь возможность проводить специальные тренинги, где на программном уровне имитируются различные ситуации на охраняемом объекте. В результате такого обучения вырабатываются необходимые навыки, разрабатываются возможные сценарии поведения персонала в той или иной ситуации. В процессе моделирования поведения системы и сам заказчик может объективно оценить эффективность выбранной системы безопасности, определить необходимую численность персонала службы безопасности, постоянно контролировать уровень подготовки сотрудников. Ведь в конце концов, только при слаженном взаимодействии машин и людей можно получить действительно работающую систему, а для этого между ними должен быть качественный и надежный интерфейс.



НОВОСТИ

■ Новые AHD-камеры от PRIME. PR-MD720F-IR с матрицей 1/4" Megapixel CMOS Aptina, чувствительностью записи 0.001 Лк на базе процессора NextChip, с разрешением 720p. Объектив 2.8 мм. 2 Мп купольная PR-MD1080F-IR во многом повторяет характеристики. Отличия: сенсор 1/3" Megapixel SONY IMX322 с чувствительностью 0.001 Лк, объектив 2.8/3.6 мм. Функции корректировки видеозаписи, встроенная ИК подсветка до 15 м, степень защиты IP66, рабочие температуры от –20 до +40° С. Питание от 12 В.

■ Компания «Коммуникации» выступила первооткрывателем в области защиты ПО систем оперативно-технологической связи и оповещения. Выпущен модуль SWMS. Схема его функционирования схожа с компьютерной технологией «антивируса». Принцип работы заключается в создании дополнительного защитного барьера при подключении к оборудованию, установленному на предприятии. Модуль SWMS является универсальным продуктом и может быть адаптирован к установке в уже функционирующие системы оперативно-технологической связи и оповещения различных производителей.

■ IP-камеры с вариофокальным объективом IDp1.0 (2.8-12) и IDp2.1 (2.8-12) для помещений пополнили ассортимент оборудования EL. Это 1 Мп камера с максимальным углом обзора 70° и 2,1 Мп камера с максимальным углом обзора 95°. Купольные корпуса, температуры эксплуатации от –10 до +50° С. ИК подсветка до 20 м.

■ Вышла новая версия ПО для видеонаблюдения «Линия». Система расширила свой функционал диалога редактирования списка серверов. Реализован режим циклического монитора. Добавлена возможность экспорта мультивида. Также добавлены новые возможности и внесены важные изменения. Интегрированы новые бренды IP-камер, расширены линейки производителей. Всего программа официально поддерживает 3585 моделей цифровых камер.

■ Состав уличных IP-камер Pelco by Schneider Electric пополнили 3 модели Sarix Enhanced II IBE – 3 Мп IBE329-1R, 2 Мп IBE229-1R и 1 Мп IBE129-1R. Ударопрочный цилиндрический термокожух с IK10/IP66, P-Iris объектив, ИК прожектор, питание от источников 12/24 В или по PoE. Чувствительные сенсоры, технология SureVision 3.0. Пакет из 8 модулей видеоаналитики, запись на карту памяти SD/SDHC/SDXC. Трансляция со скоростью 60 к/с с максимально возможным разрешением. В наличие аудиоканалы. Удаленный доступ и настройка через веб-браузер, а также приложение Pelco Mobile.

■ Новинка для серьезного бизнеса – 2.4 Мп IP-камера AltCam ISDV24IR. Камера обладает 22-кратным зумом, скоростью поворота до 60 °/сек, наклона – 45 °/сек. Дальность ИК подсветки составляет 120 метров. Бесперебойную работу обеспечивает пыленепроницаемый корпус с защитой от сильных водяных струй и от перенапряжений, грозовых разрядов, импульсных помех. Камера работает при температуре от –40 до +60° С.

■ Ассортимент MorphoAccess® SIGMA компании Safran пополнили считыватели отпечатков пальцев Sigma Lite и Sigma Lite Plus, с вандалозащищенным корпусом, оптическим сенсором с разрешением 500 dpi и мощным процессором. Sigma Lite Plus оснащен 2,8» сенсорным экраном с пользовательским интерфейсом, а модель Sigma Lite имеет более простую конструкцию со светодиодным индикатором. Обе модели способны обслуживать до 250000 пользователей в режиме верификации и до 10000 в режиме биометрической идентификации, а также снабжены интерфейсами RS-422/485, Wiegand и веб-сервером. Рабочая температура от –20 до +50° С, класс климатической защиты IP65 и ударопрочности IK08.