Способы повышения надежности СКУД

Надежность — это свойство систем выполнять возложенные на них функции в течение заданного промежутка времени и при определенных условиях эксплуатации. Данное определение в полной мере относится и к системам контроля и управления доступом. Так как общая надежность всей системы зависит от надежности ее отдельных элементов, то вполне очевидно, насколько важными являются задачи выявления в системе слабых звеньев и принятие мер для их устранения

В ГОСТ Р51241-98 определены составные части Системы Контроля и Управления Доступом (СКУД), а именно: устройства управляющие, устройства ввода идентификационных признаков и устройства преграждающие управляемые. Рассмотрим основные пути повышения надежности каждой из этих частей.

Устройства управляющие

Самыми сложными элементами в СКУД являются устройства управляющие (УУ), которые соответственно представляют собой и наименее надежные узлы данной системы.

Начнем рассмотрение с аппаратных УУ. Это различные контроллеры и интерфейсные модули На самом деле сюда можно отнести и компьютерное оборудование, на котором установлены программные УУ. При выходе аппаратных УУ из строя - а для больших (распределенных) систем при потере связи между ними - СКУД практически полностью перестает функционировать. Данный факт указывает на то, что во многом работоспособность определяется архитектурой системы.

Архитектура системы

В настоящее время считается наиболее надежным построение по принципу смешанной архитектуры. Она представляет собой слияние более ранних вариантов систем с централизованной и распределенной архитектурой. Напомним, что в централизованной архитектуре имеется один основной контроллер управления, а все периферийное оборудование подключается через неинтеллектуальные интерфейсные модули. В распределенной архитектуре - много мелких интеллектуальных контроллеров, к которым непосредственно подключается периферийное оборудование, при этом координация работы системы в целом (например, глобальный контроль повторного прохода, организация различных реакций на события) возложена на программное обеспечение. Переход на "смешанную" архитектуру осуществлен производителями путем замены "тупых" интерфейсных модулей на аналог мелких интеллектуальных контроллеров или за счет добавления в систему центральных "сетевых".

Замысел понятен. Нововведения вроде бы должны повысить надежность, однако попробуем разобраться, насколько удачным оказалось такое решение. При выходе из строя центрального контроллера либо при нарушении связи с ним система переходит в режим функционирования, отличающегося очень ограниченными возможностями. С одной стороны, обе архитектуры повысили свою надежность, но, с другой стороны, у них при этом остались прежние недостатки.

Резервирование

Общими для разных систем мерами обеспечения требуемой надежности является резервирование недостаточно надежных элементов, то есть их дублирование и функциональная избыточность.

В СКУД, конечно, можно организовать "горячее" резервирование центральных контроллеров и линий связи. Однако данное решение, во-первых, ведет к удорожанию системы, во-вторых, существенно повышает ее сложность, что в свою очередь опять-таки отрицательно влияет на надежность.
Получается своеобразный замкнутый круг. (Следует заметить: грамотное решение по резервированию линий связи - с учетом того, что применяемые в системе интерфейсы могут быть самыми разнообразными, - это тема для отдельной статьи по СКС.)

«Распределенный интеллект»

Идеальным решением было бы появление систем с действительно распределенным интеллектом. Подразумевается, что в такой системе контроллеры способны общаться между собой без помощи центрального контроллера или программного обеспечения. В этой системе можно резервировать отдельные ее узлы и определенные заранее линии связи. Выход из строя отдельного (любого) элемента не приведет к глобальным последствиям, вызванным тем, что система потеряет возможность выполнять свои функции. К сожалению, несмотря на заявления некоторых производителей, реально работающие СКУД такого типа на нашем рынке не представлены.

Надежность программного обеспечения

Стоит отдельно упомянуть о надежности программных устройств управления СКУД, то есть программного обеспечения (ПО), установленного на компьютерах управления, серверах баз данных, дополнительных рабочих местах и т.д. Чаще всего сам компьютер (если говорить начистоту, то и ПО, установленное на нем) является самым ненадежным элементом. При выходе компьютера из строя (даже если система в полном объеме сохраняет работоспособность) теряются такие важные функции, как отображение информации, поступающей к операторам, и возможность управления техническими средствами вручную. Для устранения влияния данного фактора можно, как и в случае с центральными контроллерами, применять "горячий" резерв. Однако если в системе очень много компьютеров, на которых хранятся базы данных, или управляющих компьютеров, то "горячее" резервирование каждого из них обойдется слишком дорого. В таких случаях допустимо создание "холодного" резерва. С этой целью один из компьютеров собирает сведения об изменениях конфигурации (составе баз данных и т.д.) со всей системы. При выходе из строя какого-либо элемента сети производится замена из ЗИПа, а далее вся необходимая конфигурация "заливается" из компьютера "холодного" резерва.

Надежность программных устройств управления следует рассматривать и с точки зрения обеспечения необходимого уровня защиты от несанкционированного доступа к информации, а также возможности разграничения полномочий доступа и прав операторов. Для этого могут использоваться не только опции, встроенные в операционные системы, но и специализированные инструменты, которые реализованы либо программными, либо программно-аппаратными средствами. Необходимо обратить внимание на лицензии и сертификаты таких средств и выбирать те, которые соответствуют требованиям оснащаемого объекта.

Защита аппаратных средств, линий связи и управления

Безусловно, а также крайне важно предусматривать защиту от несанкционированного доступа к аппаратным средствам, линиям связи и управления. Достигается это за счет размещения контроллеров в защищенных зонах и обязательного оснащения их датчиками вскрытия корпуса. Также по возможности необходимо оснащать датчиками вскрытия устройства ввода идентификационных признаков, так как интерфейс обмена между ними и контроллерами чаще всего не позволяет идентифицировать попытки несанкционированного воздействия.

Кабельные трассы следует прокладывать в защищенных зонах, исключая вероятность доступа к ним злоумышленников. Если это не представляется возможным, то нужно установить сигнализацию, сообщающую о проникновении к ним (правда, чаще всего данное решение обходится очень дорого или вообще не может быть реализовано), или использовать кольцевые архитектуры и кодированные сигналы.

Устройства ввода идентификационных признаков

Выбор правильных устройств ввода идентификационных признаков значительно влияет на надежность СКУД. Здесь важно учитывать возможность подделки самого идентификатора.

Карточку, брелок и другие подобные идентификаторы технически просто изготовить, а кроме того, если известен номер, их можно заказать, купить. Далее по надежности идут Smart-карты. Smart-карты, благодаря технологии шифрования передаваемых на считыватель данных, гораздо более надежны сточки зрения копирования/изготовления. Подделка биометрического признака потребует специальных знаний и действий. Наиболее распространенные в настоящее время в системах управления доступом Proximity-карты подделать проще всего. Зная номер карты, достаточно заказать карточку с таким же номером или незапрограммированную карту и программатор. В этом смысле особенно прост формат EM-Marine, который производят практически все кому не лень. Однако и с картами "брендовых" производителей сейчас особых

сложностей не возникает.

Как один из способов защиты от этой угрозы можно предложить использование считывателей, совмещенных с кодонаборными устройствами. Теоретическая возможность заказать применяемые в ситеме контроля и управления доступом Smart-карты с определенным номером, используемым в системе, осложняется тем, что расшифровать его в момент передачи практически невозможно. Однако надо исходить из здравого смысла, ведь вряд ли кто-то будет определять номер карты на этапе поднесения ее к считывателю. Как и в случае с хакерскими взломами ПО, здесь также проще и легче использовать другие пути. Так, к примеру, часто номер карты бывает напечатан на ней самой (что сразу же понижает надежность системы). Кроме того, нетрудно получить доступ к человеку, который сам имеет возможность узнать необходимую информацию, хранящуюся в базе данных бюро пропусков или раздобыть нужные сведения у поставщиков.

Биометрические считыватели - это пока все-таки достаточно дорогое удовольствие. Да и часто по скорости идентификации они не могут соперничать с Proximity (хотя бы потому, что сотрудников трудно научить правильно их применять). Имеет смысл использовать биометрические считыватели лишь на точках доступа в особо важные зоны.

Устройства преграждающие управляемые

Устройства преграждающие управляемые (УПУ) могут кардинально повлиять на общую надежность системы управления доступом.

Какую бы сложную и надежную систему контроля и управления доступом вы не организовали, но если в точке доступа стоит хлипкая дверь с гнилым косяком, которую можно открыть, толкнув ее плечом, и в придачу к этому датчик положения двери открыт для внешних воздействий, - все ваши усилия по повышению надежности работы системы пропадут даром.

Необходимо четко определить, для каких целей применяется УПУ на точке доступа (для контроля учета рабочего времени, контроля количества проезжающих автомобилей или проходящих сотрудников/посетителей, защиты от проникновения в защищаемую зону и т.д.), и, исходя из этого, выбирать типы устройств (турникеты, шлагбаумы, замки, противотаранные устройства и т.д.), которые оптимально позволят решать поставленные задачи.

В заключение хочется подчеркнуть, что надежность построенной системы закладывается на этапе проектирования. Именно тогда необходимо не только определиться с концепцией общего построения системы и с алгоритмами ее работы, но и правильно выбрать производителей составных частей системы, которые оптимальным образом решат поставленные задачи.

Следует предусмотреть все возможные варианты возникновения внештатных ситуаций, которые могут привести к неработоспособности системы. Надо не забыть и про комплектность ЗИП, без которого любой мелкий отказ может превратиться в серьезную проблему. Безусловно, необходимо обратить внимание и на подготовку специалистов, которые будут обслуживать такую современную систему. Она в настоящее время является практически самой сложной из систем безопасности. Без обученного персонала (операторов, администраторов) даже самая хорошая система не сможет функционировать достаточно надежно.