14. Надежность открытых систем

Автор: Александр
21.06.2009 22:14

Большинство ведущих производителей распределенных систем управления и программируемых контроллеров стали расхваливать открытость как главный атрибут своей продукции. И хотя то, что при этом предлагалось, было далеко от идеала, поставщики управляющих устройств действительно стали выполнять часть своих обещаний. При помощи технологии Ethernet и ставшего стандартом де-факто протокола TCP/IP операторские станции действительно можно было подключать к некоторым распределенным системам управления и ПЛК. Однако странные, необъяснимые и невоспроизводимые отказы систем всё же возникали; нередко по прошествии длительного времени стабильной работы.

Надежность часто определяется как "возможность успешного выполнения предписанных функций в течение определенного периода времени"; при этом учитываются все источники аппаратных и программных отказов системы.

Анализируя возможные причины неисправностей в открытой системе, не приходится удивляться необъяснимым и случайным отказам. В плане надежности и безопасности открытые системы не имеют ничего общего с фирменными распределенными системами управления и ПЛК (DCS/PLC). Характеристики открытых систем более гибкие, более сложные и сравнительно неуправляемые (по крайней мере, с точки зрения обеспечения согласованной работы всех компонентов и частей системы, что является целью сертификации).

Коммуникационные протоколы фирменной системы, поставщиком продуктов для которой являлся единственный производитель, обычно создавались одним и тем же коллективом разработчиков, иногда даже одним человеком. Все сообщения, которыми могли обмениваться операторская станция и контроллер, были, как правило, четко определены. Если в системе каким-то чудом появлялось неверное сообщение, подпрограммы контроля ошибок просто отбрасывали все, что не относилось к разряду допустимых пересылок. Все программное обеспечение, от драйверов до обработчиков сообщений, писалось одной и той же командой программистов, работавших по единой спецификации. Создание устойчивого программного обеспечения является в такой ситуации сравнительно простой задачей.

Сбои были нередки даже в таких условиях, однако когда они случались, было совершенно ясно, кто несет за это ответственность. Вся ответственность за надежность и безопасность работы фирменных DCS-систем и систем на базе контроллеров лежала на единственном коллективе разработчиков, что принципиально невозможно в случае открытых систем.

В открытых системах вероятность передачи непредвиденных данных выше. Коммуникационные протоколы общего назначения стали гораздо сложнее, что затруднило задачу фильтрации некорректных сообщений. Единого коллектива разработчиков, отвечающего за весь проект целиком, нет, и кто должен нести ответственность за возникновение сбоя, совершенно непонятно. В результате систему приходится часто перезагружать, информация об отказах не регистрируется, и автоматизированные системы управления становятся менее надежными.

Несмотря на все усилия, прилагаемые разработчиками для повышения качества создаваемого ими программного обеспечения, независимые проверки показали, что во многих организациях ситуация с разработкой ПО может быть охарактеризована словом

"хаос". Выяснилось также, что программисты не всегда разбираются в методах обеспечения безопасности и надежности ПО, и, хотя многих из них никак нельзя упрекнуть в отсутствии профессионализма, разброс в характеристиках программных продуктов слишком велик. Одного этого более чем достаточно, чтобы значительно повысить вероятность отказа системы управления.