Программная реализация поддержки передачи данных специальных типов IEC61131-3 в библиотеке мониторинга

А.И. Грюнталь[1], К.Г. Нархов[2], А.М. Щегольков[3]

ФГУ «ФНЦ Научно-исследовательский институт системных исследований РАН».
E-mail's: [1]grntl@niisi.ras.ru, [2]kostas@niisi.ras.ru, [3]ashch@niisi.ras.ru

Аннотация: В статье рассматривается возможность использования библиотеки мониторинга для контроля выполнения и отладки прикладных программ для программируемых логических контроллеров (ПЛК). Использование библиотеки мониторинга для ПЛК требует поддержки специальных типов языка программирования Structured Text (ST) стандарта IEC61131-3 на уровне средств приема-передачи команд, входящих в состав библиотеки мониторинга. В данной статье рассмотрены варианты расширения функциональных возможностей библиотеки мониторинга, а также предложены решения, реализующие средства отладки прикладных программ.

Ключевые слова: контролируемое выполнение, исключительная ситуация, исключение, библиотека мониторинга, многопоточная программа, поток управления, сигнал, операционная система реального времени, многопроцессорная система.

Введение

Библиотека мониторинга (БМ) [2, 5, 6] реализует функции, которыми должна обладать система, спроектированная в соответствии с принципами контролируемого выполнения [3, 4]. В соответствии с [3], программа с контролируемым выполнением – это программа со встроенными механизмами, обеспечивающими выполнение программы в критических условиях (например, при поступлении в программу некорректных данных, ошибок в среде исполнения или в самой прикладной программе). Средства контролируемого выполнения прикладной программы содержат механизмы, обеспечивающие контроль состояния выполняемой программы, сравнение параметров состояния прикладной программы с эталоном, а также генерацию управляющих воздействий в случае отклонения поведения программы от эталона.

Библиотека мониторинга обеспечивает выполнение контроля работоспособности, корректности и целостности прикладной программы на основании данных, получаемых от агентов мониторинга, аккумулирующих данные о выполнении прикладной программы (контрольные параметры состояния).

В статье рассматривается возможность использования библиотеки мониторинга для контроля выполнения и отладки прикладных программ, выполняющихся в среде операционной системы реального времени Багет 2.6, для программируемых логических контроллеров (ПЛК). ОС РВ Багет 2.6 является отечественной операционной системой, которая разработана в ФГУ ФНЦ НИИСИ РАН и предназначена для создания программного обеспечения программно-аппаратных комплексов, работающих в режиме реального времени [1].

1. Алгоритм функционирования библиотеки мониторинга

Библиотека мониторинга предназначена для реализации контролируемого выполнения многопоточных приложений распределенных многопроцессорных вычислительных систем [3, 4].

Библиотека мониторинга обеспечивает сбор данных о состоянии пользовательских потоков управления, генерацию и передачу в пользовательские потоки управляющих воздействий в том случае, когда требуется изменение режима выполнения приложения,

не предусмотренное алгоритмом функционирования приложения [2, 5, 6].

Библиотека мониторинга – это инфраструктурная программа, представляющая собой расширение приложения, контролирующее прикладную программу. Встраивание библиотеки мониторинга в готовое приложение требует минимальных изменений в исходном тексте приложения и в случае штатного исполнения не меняет алгоритм приложения.

Состав БМ: агенты, монитор, средства сбора данных, средства передачи команд. Агенты представляют собой встроенные в приложение функции, регистрирующие данные – параметры выполнения. Номенклатура параметров выполнения определяется разработчиком в зависимости от функций и назначения приложения. Средства передачи команд – это совокупность средств синхронизации, входящих в ОС РВ Багет 2.6 и протокола передачи данных верхнего уровня, реализованного в библиотеке мониторинга. Реализация протокола передачи данных содержит принципиальные ограничения, исключающие использование библиотеки мониторинга для отладки прикладных программ ПЛК, написанных в соответствии со стандартом IEC61131-3 [7]. В этой статье предложены варианты расширения функциональных возможностей библиотеки мониторинга, необходимые для снятия этих ограничений.

Параметры состояния прикладной программы передаются средствами библиотеки мониторинга в монитор для анализа параметров и, в случае необходимости, выработки управляющих воздействий – команд, влияющих на режим выполнения приложения. Наряду с командами, изменяющими режим (или алгоритм) приложения, в БМ реализованы команды, которые могут выполнять общесистемные действия, например – приостанавливать или повторно запускать потоки управления.

Вычислительная система, на которой устанавливается библиотека мониторинга, представляет собой однопроцессорную или многопроцессорную вычислительную систему. Средства передачи монитору параметров состояния инвариантны относительно физического уровня, используемого для межпроцессорной передачи данных. Поэтому в качестве среды передачи данных могут использоваться интерфейсы RS232, RS422, RS485, Ethernet и RapidIO.

2. Описание протокола передачи данных

Агенты библиотеки мониторинга, регистрирующие и передающие контрольные параметры состояния, представляют собой функции, выполняемые в контексте прикладного потока управления. Параметры состояния содержат идентификационную информацию о прикладном потоке управления, в контексте которого исполняется агент, о группе функциональных потоков управления, в состав которой входит поток управления, и контрольный идентификатор состояния программы. Один поток управления может содержать несколько агентов, поэтому параметры состояния содержат также идентификационную информацию об агенте, сгенерировавшем эти параметры [2].

Агент мониторинга – это функция библиотеки мониторинга, вызов которой размещается в контрольной точке прикладной программы. Прототип функции агента библиотеки мониторинга:

```
int checkpoint_agent(
  struct gfp_thread_pool *tpool,
  int usercheckpoint_id,
  int userdata);
```

Этой функции передаются следующие аргументы:

– **`tpool`** – указатель на структуру с атрибутами потока управления, в контексте которого выполняется агент;

– **`usercheckpoint_id`** – идентификатор агента (номер контрольной точки);

– **`userdata`** – данные для передачи в монитор.

При вызове агента мониторинга параметры состояния прикладной программы (переданные в агент как аргументы функции) помещаются в очередь сообщений. Каждое сообщение в очереди сообщений имеет следующий формат [2]:

– битами **0-7** кодируется идентификатор процессора, на котором выполняется группа функциональных потоков управления;

– битами **8-15** кодируется идентификатор группы функциональных потоков управления, в которую входит поток управления;

– битами **16-23** кодируется числовой идентификатор (тег) потока управления;

– битами **24-31** кодируется идентификационная информация об агенте потока управления;

– битами **32-39** кодируются пользовательские данные – это может быть номер команды или значение переменной **errno**.

Распаковка сообщения выполняется монитором в структуру типа **agentmag_t** с помощью вызова входящей в состав программного модуля **monitor.c** библиотеки мониторинга функции

```
void doMessDecode(
 char * message,
 struct agentmsg_t * mess_block,
 unsigned int PRINT_DEBUG));
```

Структура **agentmag_t** содержит поля типа **char**, соответствующие заданным частям (байтам) сообщения.

На основании полученных данных от агента мониторинга монитор формирует управляющую реакцию.

3. Особенности протокола передачи данных

Ограничением рассмотренного выше протокола является размер пользовательских данных. Реализация протокола обеспечивает передачу в одном сообщении 1 байта данных (целое от 0 до 255). Данное ограничение обусловлено назначением и типовым использованием библиотеки мониторинга. Как было отмечено ранее, из агента мониторинга посредством пользовательских данных могут быть переданы номер команды и значение переменной **errno**. Эта переменная используется системными вызовами и некоторыми библиотечными функциями ОС РВ при ошибках для указания того, что именно произошло [1]. Реализация библиотеки мониторинга поддерживает 4 команды (завершение потока управления, останов потока управления, запуск остановленного потока управления, перезапуск потока управления), при этом переменная **errno** в ОС РВ Багет 2.6 принимает значения от нуля до 95.

Следует отметить, что в коротких сообщениях, передаваемых из потока управления средствами библиотеки мониторинга, используются данные размером не более 1 байта (биты **32-39** в сообщении).

4. Применение библиотеки мониторинга для программируемых логических контроллеров

В силу универсального характера заложенных в библиотеку мониторинга технических решений возможна модификация библиотеки мониторинга с целью её применение в задачах управления ПЛК.

ПЛК представляют собой автономно функционирующие ЭВМ, управляющие техническими объектами по заранее заданному (для конкретных условий эксплуатации) алгоритму. ПЛК осуществляет сбор данных с датчиков, устанавливаемых на техническом объекте, анализ данных и передачу управляющих воздействий.

В типовом случае несколько ПЛК взаимодействуют по сети с управляющей ЭВМ (УЭВМ). Цель управления – контроль за работой ПЛК, оперативное изменение режима работы ПЛК, сбор статистики о выполнением производственных процессов. Таким образом, ПЛК (один или несколько) представляет собой объект управления со стороны удалённой ЭВМ.

Возможны более сложные схемы взаимодействия ПЛК и УЭВМ. ПЛК, УЭВМ взаимодействующие по сети, специальное программное обеспечение ПЛК и УЭВМ образуют АСУ технологическим процессом (АСУ ТП).

4.1. Специальные типы данных IEC61131-3

Библиотека мониторинга может быть использована для контроля выполнения программ для ПЛК. Исходный код прикладной программы для ПЛК разрабатывается на языке программирования Structured Text (ST) стандарта IEC61131-3. Особенностью этого языка программирования является наличие специальных типов данных **BYTE**, **WORD**, **DWORD** и **LWORD**, соответствующих по длине следующим типам языка Си: **char**, **short**, **int** и **long**. Поддержка специальных типов ST на уровне протокола передачи данных библиотеки мониторинга позволяет обеспечивать контроль состояния прикладной программы и, в случае необходимости, генерацию управляющих воздействий.

В соответствии с реализацией текущего протокола передачи данных и вытекающими из нее ограничениями, которые кратко описаны выше, библиотека мониторинга поддерживает только специальный тип **`BYTE`** языка ST.

Библиотека мониторинга может использоваться для удаленной отладки прикладной программы. В текущей реализации отладка предполагает просмотр и протоколирование значений переменных: в контрольных точках прикладной программы устанавливаются агенты мониторинга, в которые передаются значение отлаживаемых переменных. Трасса вызовов агентов мониторинга протоколируется монитором и впоследствии исследуется прикладным программистом. Текущая реализация библиотеки мониторинга не предполагает отладку в реальном времени.

В текущей реализации библиотека мониторинга используется только для отладки **`char`** (или **`BYTE`** в терминах ST) переменных.

Расширение функциональных возможностей библиотеки мониторинга, которые следует реализовать для устранения рассмотренных выше ограничений:

– поддержка специальных типов данных **`WORD`**, **`DWORD`** и **`LWORD`** языка программирования ST стандарта IEC61131-3;

– возможность удаленной модификации значения переменной в заданной контрольной точке;

– возможность удаленной отладки (просмотр и модификация значений переменных) прикладной программы в реальном времени.

4.2. Поддержка передачи данных специальных типов IEC61131-3

Структура прикладной программы, работающей совместно с библиотекой мониторинга на многопроцессорной системе, представлена на рисунке 1. При работе библиотеки мониторинга на многопроцессорной системе используются удалённый (главный) и локальный (подчиненный) мониторы. Главный монитор назначается при конфигурировании библиотеки мониторинга, при этом прочие мониторы считаются подчиненными [5]. На рисунке 1 представлены компоненты библиотеки мониторинга, которые функционально связаны с передачей данных и требуют изменения:

– агент мониторинга: в исходном тексте прикладной программы размещены вызовы функций агентов мониторинга, посредством которых выполняется связь с локальным монитором;

– локальный монитор: в однопроцессорной системе выполняет функции удаленного монитора, в многопроцессорной системе выполняет прием-передачу данных из удаленного монитора (в удаленный монитор) через подпрограмму связи с удаленным монитором;

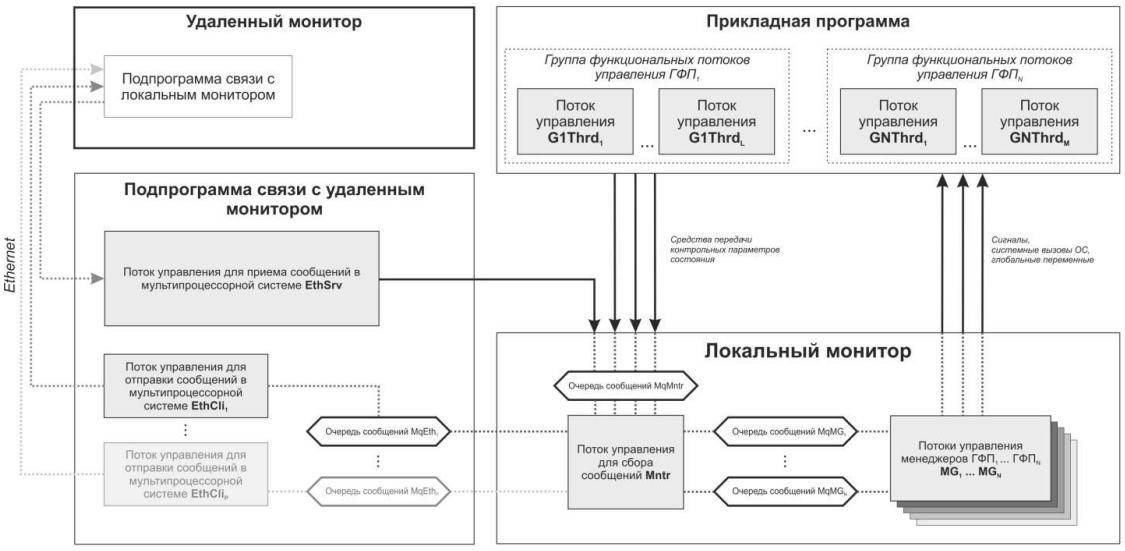

Рисунок 1 – Библиотека мониторинга в многопроцессорной системе

– подпрограмма связи с удаленным монитором: обеспечивает передачу данных между локальным и удаленным монитором по протоколу TCP/IP;

– удаленный монитор: принимает данные из локального монитора и генерирует управляющие воздействия, которые передаются обратно в локальный монитор.

4.3. Новый формат сообщения

Поддержка специальных типов данных **WORD**, **DWORD** и **LWORD** языка программирования ST стандарта IEC61131-3 требует изменение формата сообщения библиотеки мониторинга:

– битами **0-7** кодируется идентификатор процессора, на котором выполняется группа функциональных потоков управления;

– битами **8-15** кодируется идентификатор группы функциональных потоков управления, в которую входит поток управления;

– битами **16-23** кодируется числовой идентификатор (тег) потока управления;

– битами **24-31** кодируется идентификационная информация об агенте потока управления приложения;

– битами **32-39** кодируется информация о пользовательских данных: специальный тип данных (**BYTE**, **WORD**, **DWORD** и **LWORD**), тип сообщения (отладочное сообщение, команда, цепочка команд или данные), количество команд в цепочке, флаг ожидания (агент, передавший сообщение, приостанавливает поток управления, в контексте которого он выполнен);

– битами **40-127** кодируются пользовательские данные.

Таким образом, сообщение состоит из заголовка (0-39 бит) и данных (40-127) бит и имеет длину 16 байт.

4.4. Использование цепочек команд и команд с параметром при мониторинге прикладной программы

Сообщения нового формата позволяют библиотеке мониторинга не только пересылать пользовательские данные специальных типов **WORD**, **DWORD** и **LWORD** языка программирования ST стандарта IEC61131-3, но и использовать в сообщении несколько команд. Командами в библиотеке мониторинга называются управляющие воздействия, передаваемые из монитора в заданный поток управления прикладной программы. Размер команды составляет 1 байт, поэтому в сообщении нового формата можно уместить до 11 команд (биты **40-127** в сообщении).

Следует отметить, что новый формат сообщения позволяет доставлять в поток управления команду с параметром. В качестве параметра могут использоваться следующие значения:

– один аргумент специального типа **LWORD**;

– два аргумента специального типа **DWORD**;

– четыре аргумента специального типа **WORD**;

– восемь аргументов специального типа **BYTE**.

Команда с параметром необходима для реализации возможности удаленной модификации значения переменной в заданной контрольной точке, а также для удаленной отладки.

5. Оценка производительности передачи данных специальных типов IEC61131-3

Для оценки производительности передачи данных специальных типов IEC61131-3 библиотекой мониторинга была использована контрольная задача, состоящая из шести групп функциональных потоков управления. В каждой группе работало по три потока управления, и в каждом потоке управления было установлено не более пяти контрольных точек (агентов мониторинга). Группы функциональных потоков управления были развернуты на двух процессорах по схеме 50/50: три группы на один процессор, три – на другой.

Каждый из потоков управления выполнил 100 тысяч итераций. При выполнении потоков управления монитор реагировал на искусственно порождаемые в потоках управления сбои и направлял в эти потоки управления необходимые команды, соответствующие сбоям.

По результатам выполнения контрольной задачи отмечено, что экспериментальная версия библиотеки мониторинга со встроенной поддержкой специальных типов IEC61131-3 функционально совместима с версией библиотеки без поддержки специальных

типов. Однако является менее производительной. Отмечено замедление выполнения контрольной задачи на 15% по сравнению с версией библиотеки без поддержки специальных типов [2, 6, 7].

Исследование причин, лежащих в основе замедления работы библиотеки, предлагаются определило следующие способы ускорения работы библиотеки мониторинга со встроенной поддержкой специальных типов IEC61131-3:

– оптимизация алгоритма упаковки/ распаковки сообщения;

– реализация кэширования сообщений, например, если агент мониторинга фиксирует на итерации n состояние идентичное ранее переданному на итерации n-1 состоянию, то данные в монитор не передаются и агент мониторинга использует последнюю полученную от монитора команду (без ожидания приема-передачи этой команды от монитора);

– децентрализация многопроцессорной системы: часть функций удаленного монитора делегировать локальному монитору, например, использовать локальный монитор для протоколирования работы группы функциональных потоков управления (сохранение протокола работы по протоколу сетевого доступа к файловым системам **`nfs`**).

6. Использование библиотеки мониторинга для отладки прикладных программ для ПЛК

Под отладкой прикладных программ для ПЛК понимается работа по просмотру и модификации значений переменных прикладной программы, выполняемой на целевой ЭВМ (ПЛК). Эта работа выполняется с помощью интегрированной среды разработки, установленной на инструментальной ЭВМ.

Для реализации функциональных возможностей отладки следует расширить функциональные возможности библиотеки мониторинга следующим образом:

– портировать функционал удаленного монитора в интегрированную среду разработки на инструментальной ЭВМ (инструментальный монитор);

– доработать библиотеку мониторинга в части конфигурирования: на этапе конфигурирования библиотеки требуется задать значения для доступа к ИЭВМ (IP-адрес, порт и т. д.);

– реализовать маршрутизацию сообщений в инструментальный монитор из удаленного монитора;

– реализовать графический интерфейс для отображения отладочной информации и ввода значений для отлаживаемых переменных.

7. Заключение

В результате изменения формата и расширения размера сообщения в протоколе передачи данных, используемом в библиотеке мониторинга, удалось реализовать поддержку специальных типов данных стандарта IEC61131-3 **`WORD`**, **`DWORD`** и **`LWORD`** языка программирования ST стандарта IEC61131-3.

Поддержка специальных типов данных стандарта IEC61131-3 позволяет использовать библиотеку мониторинга для контроля выполнения прикладных программ на программируемых логических контроллерах.

В библиотеку мониторинга встроена функциональная возможность выполнения приема-передачи в одном сообщении групп команд (цепочек команд), а также команд, сопровождаемых пользовательскими данными.

Выполнена оценка производительности библиотеки мониторинга с новыми функциональными возможностями и предложены способы её ускорения.

Планируется расширить библиотеку мониторинга средствами удаленной отладки прикладных программ для программируемых логических контроллеров.

Публикация выполнена в рамках государственного задания по проведению фундаментальных научных исследований по теме (проекту) «39. Архитектура, системные решения, программное обеспечение, стандартизация и информационная безопасность информационно-вычислительных комплексов и сетей новых поколений. Разработка методов и средств контролируемого выполнения приложений, функционирующих в реальном масштабе времени (№ 0065–2018–0011), АААА–А18–118041190171–0».

Handling Exceptions Using the Monitor Library

A. Gryuntal, K. Narkhov, A. Shchegolkov

Abstract: The article discusses the methods of using the monitoring library for controlling and debugging programmable logic controllers (PLCs). The monitoring library requires the support of special types, provided by the programming language Structured Text (ST) of IEC 61131-3 standard, at the level of tools for receiving and transmitting commands included in the monitoring library. This article discusses options for expanding the monitoring library functionality, and proposes solutions that implement the tools for debugging applications.

Keywords: controlled execution, exception, monitor library, multithread program, thread, signal, real-time operating system, multiprocessing system.

Литература

1. Годунов А.Н., Солдатов В.А. Операционные системы семейства Багет (сходства, отличия и перспективы) – «Программирование», Москва, 2014, №5, с. 68-76.
2. А.И. Грюнталь, К.Г. Нархов, А.М. Щегольков, Реализация принципа контролируемого выполнения для прикладных программ реального времени. // Труды НИИСИ РАН. – Том 5 № 2. Построение программ реального времени. ISSN 2225-7349, Москва, 2015, с. 113-121.
3. В.А. Галатенко, Контролируемое выполнение / В.А. Галатенко, К.А. Костюхин, К.А., Н.В. Шмырев – М: НИИСИ РАН, 2012. – 157 с.
4. В.Б. Бетелин, Контролируемое выполнение с явной моделью / В.Б. Бетелин, В.А. Галатенко, К.А. Костюхин – ПРОГРАММИРОВАНИЕ, 2014, N- 6, с. 45-55.
5. А.И. Грюнталь, К.Г. Нархов, А.М. Щегольков, Библиотека мониторинга для многопоточных программ. // Труды НИИСИ РАН. – Том 7 № 1. Построение программ реального времени. ISSN 2225-7349, Москва, 2017, с. 70-74.
6. А.И. Грюнталь, К.Г. Нархов, А.М. Щегольков, Обработка исключительных ситуаций с использованием библиотеки мониторинга. // Труды НИИСИ РАН. – Том 7 № 4. Построение программ реального времени. ISSN 2225-7349, Москва, 2017, с. 96-101.
7. International Standard IEC 61131-3, Programmable controllers –Part 3: Programming languages, Second edition, 2003, IEC Central Office, Geneva, ISBN 2-8318-6653-7.