DOI: 10.25728/mlsd.2022.1091

СИСТЕМА ОПЕРАТОР: СИСТЕМНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ LICS

Семенков К.В., Полетыкин А.Г., Промыслов В.Г.
Институт проблем управления им. В.А. Трапезникова РАН,
Россия, г. Москва ул. Профсоюзная д.65,
poletik@inbox.ru

Аннотация: приводятся сведения об одной из технологий, реализованных в системе Оператор специализированной операционной системе на базе Linux — системном программном обеспечении LICS. Изложены причины создания специализированного дистрибутива Linux, показано, как общие требования к АСУ ТП транслируются в требования с операционной системе. Дано описание истории создания LICS и основные характеристики текущей версии ОС.

Ключевые слова: операционные системы, Linux, программно-технические комплексы, АСУ ТП, АЭС.

Введение

Система Оператор (далее "Оператор" система") — это интеграционная платформа для АСУ ТП, внесенная в «Единый реестр российских программ для электронных вычислительных машин и баз данных» Минкомсвязи России (Reg. №. 3290). О ее назначении, функциях и особенностях реализации, внедрениях для АСУ ТП АЭС см. [1-4].

Раздел посвящен более подробному изложению одной из технологий, реализованных в Оператор. Она выполняет роль операционной системы. Название: системное программное обеспечение (СПО) LICS. Свидетельство о государственной регистрации программы для ЭВМ №2019618036 РФ; Зарег. 26.06.2019.

Выбирая операционную систему (ОС), под управлением которой будет функционировать программное обеспечение (ПО) вновь разрабатываемой АСУ ТП, необходимо иметь в виду некоторые отличительные особенности АСУ ТП: долгий жизненный цикл системы, длительный период разработки и наладки системы, ограниченный и специфический набор компонентов, из которых собрана система (включая компьютеры), сложность внесения изменений в работающую систему, ограничения на время простоя.

Современные операционные системы «общего» назначения поддерживают широкий набор оборудования, включают в себя, как правило, новейшие на момент создания ОС компоненты, регулярно обновляются. Но при использовании этих ОС в АСУ ТП возникают сложности.

Во-первых, производитель поддерживает ОС в течение 3-5 лет, затем поддержка прекращается, то есть по истечении этого срока все проблемы, связанные с ОС, разработчик АСУ ТП или эксплуатирующая организация должны решать самостоятельно.

Во-вторых, для работы АСУ ТП нужен определенный набор программных компонентов (пакетов) и зачастую определенные версии этих пакетов, что ОС общего назначения не всегда может обеспечить. К тому же, набор пакетов «по умолчанию» имеющийся в ОС общего назначения, как правило, избыточен для АСУ ТП.

В-третьих, промышленные компьютеры, на которых работает АСУ ТП, могут состоять из довольно специфических компонент, требующих доработанных, исправленных драйверов или особых режимов работы ОС.

В-четвертых, требования к надёжности для промышленной системы кардинально отличаются от того, что является приемлемым в плане надёжности для обычного пользователя. Например, если «обычный» пользователь будет вынужден перезагружать программу раз в день, то это может считаться нормально, т.к. сценарии в большинстве случаев не предусматривают круглосуточную работу, но такая «надёжность» абсолютно не приемлема для промышленной системы с режимом работы 24x7x365.

Иными словами, в АСУ ТП оборудование, операционная система и прикладное ПО должны быть очень хорошо совмещены и протестированы, чтобы обеспечить бесперебойное функционирование системы управления в течение всего срока ее эксплуатации.

1 Цели и история создания СПО LICS

Вопрос санкций и независимости разработчика АСУ ТП от поставщика ПО и, в частности, ОС не является проблемой сегодняшнего дня, он был актуален всегда. В конце прошлого века АСУ ТП функционировали либо на специализированных операционных системах реального времени (VxWorks, QNX), либо на проприетарных ОС семейства UNIX (HP-UX, SunOS, Solaris и т.п.). Часть из этих систем работает на весьма ограниченном наборе оборудования, который намного уже набора оборудования,

используемого в АСУ ТП, но основная проблема, что все эти системы принадлежат американским и канадским компаниям, что делает невозможным использовать их в странах, попавших под экспортные ограничения США и Канады. В настоящее время один из возможных вариантов способов избавиться от технологической зависимости — создать специализированный дистрибутив ОС для работы АСУ ТП, лишённый указанных недостатков [0, 0] и написанного либо с «чистого листа» [0] либо на основе свободно распространяемого ПО.

К началу двухтысячных годов операционная система Linux вышла на уровень, где ее можно было рассматривать как кандидата на роль операционной системы для АСУ ТП АЭС. Поэтому в ИПУ РАН при создании системы верхнего блочного уровня АЭС «Бушер-1» был разработан дистрибутив Linux, получивший название LICS — Linux of Institute of Control Sciences. LICS успешно прошел приемочные межведомственные испытания в 2001 г. и рекомендовано в 2003 г. Госатомнадзором России и ВО “Безопасность” для использования в системах, важных для безопасности в атомной энергетике.

2 При разработке первой версии СПО LICS были решены следующие ключевые задачи:

- обеспечена высокая надежность и бесперебойная работа в течение длительного времени на промышленных системах;
- получена сбалансированная система без лишних и непроверенных компонентов;
- внедрена уникальная система контроля целостности программного обеспечения;
- обеспечена лицензионная чистота для применения ПО в Российской Федерации и в странах, где эксплуатируются объекты, построенные Российской Федерацией.

Программный продукт был верифицирован по российским и международным нормам, принятым в атомной промышленности [0, 0]. Тестирование LICS производилось в течении двух лет независимыми организациями на полигоне АСУ ТП АЭС в Электорогорском научно-исследовательском центре по безопасности АЭС, г. Электрогорск, и в составе поставочного комплекта системы верхнего блочного уровня АСУ ТП АЭС "Бушер" (Иран), который был собран в полном объеме в Научно-исследовательском институте измерительных систем им. Ю.Е. Седакова, Нижний Новгород [0, 0].

Первая версия СПО LICS уже почти 20 лет успешно эксплуатируется на энергоблоке АЭС «Бушер» в составе АСУ ТП.

3 Современное состояние разработки

При существенном обновлении ПО АСУ ТП обновляется и операционная система LICS. Текущая версия, LICS 1000 v.5, прошла приемочные испытания в 2018 г. При создании СПО LICS уделялось внимание тому, чтобы обеспечить транслируемость свойств создаваемой АСУ ТП в требования для ОС. Обзор соответствия свойств АС ТП и требований к ОС приведен в таблице 1.

Таблица 2. Транслируемость свойств АСУ ТП в требования к ОС

Свойство АСУ ТП	**Требование к ОС LICS**
АСУ ТП работает на определенных технических средствах в течение долгого срока.	Технические средства должны поддерживаться операционной системой. Должны проводиться тесты в различных режимах работы.
Отсутствие лицензионных ограничений.	В состав ОС должны входить только те компоненты, исходный код которых доступен и на которые не наложены лицензионные ограничения.
Основная задача операционной системы — обеспечение функционирования прикладного ПО	Состав ОС должен быть достаточным для обеспечения основной задачи. ОС не должна содержать избыточного ПО.
В рабочую среду АСУ ТП не должны входить средства разработки, однако должна быть возможность вести разработку на отдельных компьютерах.	Должно быть, как минимум, два варианта установки ОС, отличающихся набором компонент: среда работы АСУ ТП и среда разработки. Процедура установки должна быть простой.
Все приборные стойки защищены источниками бесперебойного питания.	ОС должна взаимодействовать с ИБП.
В структуре сети Ethernet АСУ ТП могут выделяться VLAN.	В ОС должна быть возможность поддержки VLAN.
АСУ ТП работает по сетевым протоколам TCP/IP, UDP/IP.	ОС должна поддерживать сетевые протоколы TCP/IP, UDP/IP.
В АСУ ТП осуществляется диагностика технических и программных средств.	ОС должна поддерживать работу по протоколу SNMP.

Свойство АСУ ТП	Требование к ОС LICS
АСУ ТП работает на определенных файловых системах, включая распределенные.	ОС должна поддерживать необходимые файловые системы.
Часы в пределах АСУ ТП должны быть синхронизированы.	ОС должна поддерживать необходимые протоколы синхронизации времени.
Графическая подсистема рабочих станций АСУ ТП должна обеспечивать функционирование прикладного ПО, не перегружая систему сторонними задачами.	ОС должна поддерживать облегченный графический интерфейс.
Ряд задач АСУ ТП решается при помощи Web-технологий.	ОС должна содержать веб-сервер и браузер.
Прикладное ПО АСУ ТП состоит как из двоичных исполняемых файлов, так и из скриптов.	В состав ОС должны входить необходимые системные библиотеки, а также интерпретаторы языков, используемых в АСУ ТП, с соответствующим набором пакетов.
Среда разработки должна поддерживать языки программирования, используемые в АСУ ТП.	ОС в варианте разработчика должна поддерживать необходимые языки программирования.
В штатном режиме работы оператор АСУ ТП должен иметь доступ только к ПО, непосредственно участвующему в процессе управления.	В ОС должен быть режим работы с ограниченным пользовательским интерфейсом, где пользователю доступен минимально необходимый функционал.
Должна обеспечиваться и контролироваться целостность ПО АСУ ТП.	ОС должна давать возможность организовать защиту и контроль целостности системного и прикладного ПО.

Полученная в результате разработки ОС LICS обладает следующими свойствами.

ОС LICS обеспечивает программную среду для функционирования и разработки прикладного и тестового ПО, а также рабочих баз данных в составе систем верхнего уровня АЭС, отнесенных по классу безопасности к классу 3Н и ниже по НП-001-97 [0].

Само программное изделие имеет эталонный и рабочий образы. Эталонный образ размещен на USB-флеш диске, контрольная сумма эталонного образа занесена в формуляр на систему, предусмотрена периодическая сверка контрольной суммы образа на диске с формуляром.

Рабочий образ — это развернутая на конкретном техническом средстве операционная система с конкретными настройками. Рабочий образ ОС отдельно не создается, а входит в состав рабочего образа всего ПО, установленного на компьютере.

ОС LICS предусматривает два варианта установки — исполняемая среда и система разработчика, отличающиеся набором компонент. В систему разработки входят компиляторы, средства отладки, файлы заголовков и прочие компоненты, необходимые для разработки ПО.

ОС LICS обладает следующими функциональными характеристиками.

1. Это 64-битная операционная система, работающая на архитектуре x86_64; при этом она обеспечивает возможность запуска и исполнения 32-битных приложений.
2. Система гарантированно обеспечивает работоспособность компонент из состава технических средств АСУ ТП и ПО системы Оператор.
3. Поддерживается виртуализация на уровне ядра KVM/QEMU.
4. Поддерживаются стандартные сетевые протоколы TCP/IP.
5. В состав системы входит виртуальный коммутатор OpenVSwitch.
6. Поддерживаются сетевые файловые системы NFS версий 3 - 4.2 и CIFS.
7. Поддерживаются файловые системы ext2-ext4, FAT16, FAT32, NTFS, ISO 9660, UDF.
8. В системе присутствуют стандартные базовые утилиты Unix/Linux: оболочки (bash, tcsh), архиваторы (tar, gzip, bzip2, xz), обработчики текстов (awk, sed, groff и т.д.).
9. Графическая подсистема включает в себя:
   a) графический сервер протокола X11;
   b) графическую оболочку LXDE;
   c) графические библиотеки OpenMotif;
   d) графические библиотеки Qt.
10. Поддерживается синхронизация времени по протоколам NTP v3 и v4.
11. Поддерживаются протоколы SNMP v1-3.
12. В состав системы также входят:

e) интерпретаторы языков Python и Perl с расширенным набором пакетов;
f) веб-сервер;
g) браузер;
h) сервер баз данных PostgreSQL и система управления базами данных класса NoSQL.

13. В состав системы разработки входят компиляторы и средства разработки для языков программирования:

i) C с поддержкой стандартов C89 (C90) [0, 0], C99 [0], C11 [0];
j)C++ с поддержкой стандартов C++98 [0], C++11 [0], C++14 [0];
k) Fortran с поддержкой стандарта Fortran 95 [0].

4 Технические меры кибербезопасности

Помимо стандартной для систем UNIX дискреционной модели доступа с правами на чтение, запись и исполнение, ОС LICS поддерживает ряд дополнительных мер киберзащиты.

Ядро ОС LICS поддерживает загрузку только авторизованных, подписанных модулей. Подписывание проводится на этапе компиляции, и закрытый ключ не хранится в рабочей системе.

В ОС LICS поддерживается система привилегий на уровне ядра (Linux capabilities). Привилегии на уровне ядра — это атрибуты ядра, которые дают некоторые привилегии администратора (root) процессам или исполняемым файлам. Например, право изменить UID процесса на 0 (UID пользователя root) или право монтировать/размонтировать файловые системы.

В OS LICS включена поддержка системы защиты целостности IMA/EVM (Integrity Measurement Architecture/Extended Verification Module) на уровне ядра [0]. При использовании этой подсистемы можно запретить исполнение неавторизованных (неподписанных или измененных нештатным способом) файлов, контролировать целостность файлов и их атрибутов.

Также в ОС LICS включена поддержка мандатной модели контроля доступа на уровне ядра SMACK (Simple mandatory access control kernel). Активизировав модель безопасности SMACK, можно задавать расширенные правила доступа процессов к файлам и сетевым сокетам. Например, можно задать правила, в соответствии с которыми даже администратор системы (root) не сможет изменить или удалить определенные файлы в системе.

Решая задачу обеспечения защищенного режима работы оператора .т.е. ограниченного по доступу к файлам и программам пользовательского интерфейса, мы пришли к выводу, что имеющимися средствами Linux этот функционал реализовать невозможно. Поэтому после модификации исходного кода были созданы специальные версии пакетов графического интерфейса, включая файловый менеджер, которые и используются в сеансе работы оператора.

5 Вопрос о взаимоотношениях с дистрибутивами Linux широкого профиля

При общении со специалистами задаются типовые вопросы: «Почему в Оператор используется собственная ОС? Почему не применяется один из имеющихся дистрибутивов Linux?»

Ответ, как показано выше, состоит в том, что в любом случае для стабильной работы АСУ ТП необходима операционная система, подобная LICS —узкоспециализированной компоненте, созданной на основе существующих дистрибутивов и депозитариев компонент Linux и адаптированной для работы прикладного ПО на выбранном круге технических средств. Отличиями LICS как специфического вида программных продуктов от ОС «общего назначения» является подтверждение требований, перечисленных выше: отсутствие «лишнего», доведенная до предела простота эксплуатации и гарантия поддержки в течение всего срока использования ограниченного набора технических средств.

Заключение

СПО LICS является успешным примером создания операционных систем целевого применения на основе свободно-распространяемы компонент Linux. Оно будет жить и развиваться как неотъемлемая компонента системы Оператор.

Литература

1. *Бывайков М.Е., Жарко Е.Ф., Зуенкова И.Н., Менгазетдинов Н.Э., Полетыкин А.Г., Промыслов В.Г.* Программное обеспечения для атомной энергетики // Автоматизация в промышленности. 2006. № 8. С. 52-56.
2. *Масолкин С.И., Промыслов В.Г., Пульман М.И.* Вопросы обеспечения портирования прикладного ПО (ППО) на различные системы семейства Linux // Материалы 6-й международной конференции «Управление

развитием крупномасштабных систем, MLSD-2012», Москва, 01-03 октября 2012 г., С. 260-262.
3. *Бывайков М.Е., Жарко Е.Ф., Зуенкова И.Н., Менгазетдинов Н.Э., Полетыкин А.Г., Прангишвили И.В., Промыслов В.Г.* Опыт проектирования и внедрения системы верхнего блочного уровня АСУ ТП АЭС // Автоматика и телемеханика. 2006. Т. 5. С. 65-79.
4. *Прокофьев В.Н., Коган И.Р., Коршунов А.С., Фельдман М.Е., Кольцов В.А.* Комплекс работ по созданию первой управляющей системы верхнего блочного уровня АСУ ТП для АЭС «Бушер» на основе отечественных информационных технологий. М.: ИПУ РАН, 2013. – 95с. https://www.ipu.ru/sites/default/files/page_file/busher.pdf
5. https://web.archive.org/web/20090403073202/http://www.phystechsoft.ru/ptsdos/products/ptsdos32/. Доступ 2.06.2022.
6. НП-001-97 (ПНАЭ Г-01-011-97) Общие положения обеспечения безопасности атомных станций ОПБ-88/97 / Правила и нормы атомной энергетики от 14 ноября 1997 г.
7. ГОСТ Р МЭК 60880-2010 Атомные электростанции. Системы контроля и управления, важные для безопасности. Программное обеспечение компьютерных систем, выполняющих функции категории А.
8. ANSI X3.159-1989. Programming Languages – C.
9. ISO/IEC 9899:1990. Programming Languages – C.
10. ISO/IEC 9899:1999. Programming languages – C.
11. ISO/IEC 9899:2011. Information technology – Programming languages – C.
12. ISO/IEC 14882:1998. Programming languages – C++.
13. ISO/IEC 14882:2011. Programming languages – C++.
14. ISO/IEC 14882:2014. Programming languages – C++.
15. ISO/IEC 1539-1:1997. Information technology – Programming languages – Fortran - Part 1: Base language.
16. https://sourceforge.net/p/linux-ima/wiki/Home/ Доступ 2.06.2022.