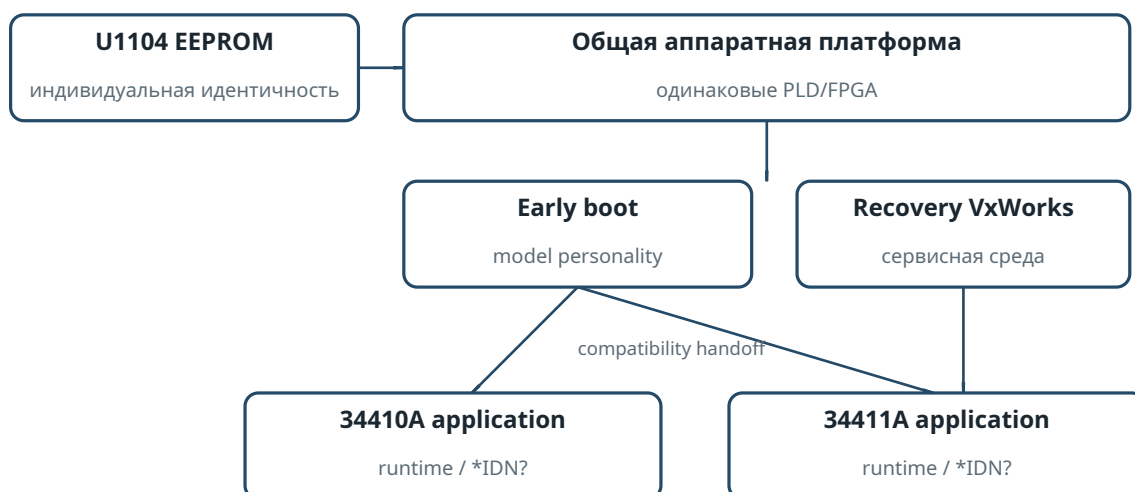


Исследование программной персонализации HP/Agilent 34410A и 34411A

Архитектура идентичности, проверки модели, recovery-среды и экспериментальное подтверждение



Публикационная версия: технические детали, позволяющие непосредственно изменить коммерческую модель прибора, намеренно исключены.

Аннотация

В ходе обратного анализа аппаратуры и встроенного программного обеспечения цифровых мультиметров HP/Agilent 34410A и 34411A исследовался механизм, определяющий модель прибора, взаимодействие раннего загрузочного кода, recovery-среды и основного application firmware, а также способ проверки совместимости firmware с аппаратной платформой.

Для исследованной аппаратной платформы установлено, что 34410A и 34411A используют одинаковую аппаратную основу; конфигурация PLD/FPGA также не отличается. Разделение продуктов реализуется на программном уровне. Статический анализ позволил выделить независимые уровни идентичности, а натурный эксперимент подтвердил реконструированный механизм: после согласования boot personality с оригинальным немодифицированным application firmware 34411A исходная платформа 34410A успешно загрузилась и штатно идентифицировалась как 34411A.

Исследование проводилось в целях изучения архитектуры, ремонта, долговременной поддержки приборов и разработки совместимых заменяемых узлов. Данные, превращающие материал в готовую инструкцию по изменению коммерческой модели, намеренно не публикуются.

1. Общая аппаратная платформа

Исследованные 34410A и 34411A построены на одной аппаратной основе. Сравнение плат показывает совпадение основных цифровых и аналоговых узлов. Наблюдавшиеся платы 34411A также несут маркировки семейства 34410, что хорошо согласуется с единой производственной платформой и поздней программной персонализацией.

Отдельно проверена программируемая логика: конфигурация PLD/FPGA у исследованных 34410A и 34411A одинакова. Следовательно, различие функциональности двух моделей не реализуется различными FPGA bitstream или отдельной аппаратной конфигурацией.

2. Независимые уровни идентичности

2.1 Индивидуальная идентичность экземпляра

Серийный номер, MAC-адрес и другая индивидуальная информация хранятся в отдельной I²C EEPROM U1104. Эти данные относятся к конкретному экземпляру и сохраняются независимо от установленного application firmware.

2.2 Application identity

Основное application firmware содержит собственную compile-time идентичность модели и формирует обычный ответ *IDN?. Таким образом, исполняемое application непосредственно определяет commercial model, сообщаемую внешнему интерфейсу.

2.3 Boot personality

Ранний загрузочный код формирует отдельную model personality и передаёт её основному приложению через небольшую boot-handoff область памяти. Application 34411A проверяет эту personality во время старта и отклоняет несовместимую конфигурацию. В application 34410A эквивалентная проверка фактически отсутствует, что объясняет асимметрию поведения двух firmware.

2.4 Recovery identity

Recovery environment представляет собой самостоятельный VxWorks image со своей compile-time идентичностью. В исследованном recovery image model name является фиксированной программной строкой и не служит основным механизмом проверки совместимости application firmware.

U1104	-> индивидуальная идентичность
application firmware	-> commercial/runtime identity
early boot	-> model personality
recovery VxWorks	-> сервисная identity

3. Архитектура загрузки

После аппаратного reset процессор входит в ранний boot code, расположенный в верхней части NOR. Этот этап проверяет boot/recovery image и application image, инициализирует boot-handoff memory, записывает status application и model personality, после чего запускает recovery VxWorks.

Recovery environment анализирует application status. При нормальном состоянии управление передаётся основному application. Если application невалиден либо был запрошен специальный recovery boot, recovery остаётся активным. Важный вывод: recovery выполняется независимо от main application и может обслуживать его обновление.

```
RESET
-> early boot
-> validate recovery + application
-> prepare handoff state
-> start recovery VxWorks
-> normal state: application
    recovery request/error: stay in recovery
```

4. Recovery environment

Recovery subsystem оказался существенно функциональнее минимального bootloader. Это самостоятельная VxWorks-среда, содержащая поддержку flash programming, InstrumentNv/I²C, SCPI, network stack, firmware download engine, service shell, front-panel communication и recovery UI.

Такое устройство позволяет перепрограммировать application flash, продолжая выполнение кода из отдельной recovery-области.

5. Принудительный переход в recovery

Официальная Firmware Update Utility способна перевести полностью исправный прибор в recovery environment без намеренного повреждения application.

Для этого используется специальный soft reboot mode. Ранний boot code распознаёт этот режим и записывает в handoff area состояние forced recovery. Recovery затем не передаёт управление обратно в application. Само application при этом не требуется стирать или делать невалидным.

```
работающее application
-> update reboot
-> early boot
-> forced-recovery handoff
-> recovery VxWorks
-> programming / service
```

6. Commercial model и loader state

Разбор PC-side Firmware Update Utility показывает, что commercial model и текущее execution state - разные понятия. При первоначальном подключении updater получает *IDN? и проверяет совместимость package с commercial model.

Для обновления application прибор затем переводится в recovery. После reconnect updater в первую очередь проверяет, что target действительно находится в loader state, а не повторяет прежнюю commercial-model проверку в том же виде. Такая архитектура допускает общую recovery-среду для нескольких близких моделей.

7. Механизм model compatibility

Application 34411A при запуске проверяет model personality, подготовленную ранним boot code. Совместимая personality разрешает нормальный startup; personality другой модели приводит к отказу запуска; некорректное значение обрабатывается отдельной диагностической веткой семейства 3441x.

Наличие обозначения 3441x интересно само по себе: оно показывает, что разработчики рассматривали приборы как семейство. В то же время PC updater не использует 3441x как wildcard для commercial-model matching.

8. Экспериментальная проверка

После завершения статического анализа механизм был проверен на реальном приборе. Была согласована только необходимая boot personality information с сохранением корректной целостности boot image. Затем установлено оригинальное, немодифицированное application firmware 34411A revision 2.43.

Прибор успешно завершил startup и штатно идентифицировался как 34411A. Индивидуальные данные экземпляра, включая серийный номер, сохранились; boot/recovery revision также осталась неизменной.

*IDN?

Agilent Technologies,34411A,<serial omitted>,2.43-2.35-0.09-46-09

9. Что эксперимент не доказывает

Эксперимент доказывает достаточность программной персонализации для работы оригинального 34411A application на исследованной аппаратной платформе 34410A. Однако он не доказывает, что заводские upper-NOR images обеих моделей отличаются только минимальным personality-related изменением.

Для окончательного ответа требуется оригинальный 34411A и полный dump его NOR. Особенно полезно будет отдельно сравнить early boot code, compressed recovery stream, decompressed recovery VxWorks, reset stub/vector, boot header и application image.

10. Заключение

Для исследованной аппаратной платформы 34410A и 34411A разумно рассматривать как две программные конфигурации одного физического прибора. Аппаратная часть и конфигурация PLD/FPGA совпадают. Индивидуальная идентичность хранится отдельно от model personality; commercial model определяется сочетанием early-boot personality и application firmware, а recovery environment образует независимый сервисный уровень.

Натурный эксперимент подтвердил реконструированную архитектуру: после согласования boot personality оригинальное firmware 34411A штатно работает на исходной аппаратной платформе 34410A.

```
hardware platform
per-unit identity
boot personality
recovery environment
application identity
```

Этика публикации

В отчёте намеренно отсутствуют точные значения model personality, адреса и байты патча, пересчитанные integrity values, скрытые service switches, готовые update images и пошаговая процедура изменения SKU.

Цель публикации - документирование архитектуры и результатов reverse engineering, а не создание инструкции по обходу коммерческого product segmentation. Модифицированный прибор также не следует маркировать или представлять третьим лицам как заводской 34411A: его производственное происхождение остаётся исходным.