Обеспечение доверия к ЭКБ

АО (ФГУП) «НТЦ «АТЛАС»

«Доверенность» это новая категория?

- «Trusted» - USA Trusted foundry program
- «Assured» ISO 15408 Common Creteria
- «Assured»/«Trusted» FIPS 140-2
- «Assured» DO-254
- «Assured» ISO 26262

- документация на элемент полна
- элемент ведет себя так и только так, как описано в документации

Что необходимо для получения ЭКБ, обладающей «новым» качеством?

Требования

Порядок подтверждения соответствия

Механизмы, технологии и квалифицированные исполнители работ по оценке соответствия

Требования — ИСО/МЭК 15408

ADV: Development

- **сквозное обеспечение Non-bypassability, Self-protection, Domain separation**
- **документирование и обоснование архитектуры**
- **документирование и обоснование реализации средств защиты**
- **документирование всех аспектов объекта оценки, включая:**
  - **Program interfaces,**
  - **Communication interface,**
  - **IC surface**

Требования — ИСО/МЭК 15408

ALC: Target of evaluation life cycle

- **контроль средств разработки**
- **контроль доступа к исходным данным и промежуточным результатам процесса разработки**

ATE: Testing requirements

- **соответствие тестового покрытия документации на объект оценки**
- **достаточность глубины/детальности тестирования**

Требования — ИСО/МЭК 15408

Набор готовых прошедших апробацию профилей защиты

- **профили для различных видов смарткарт**
- **профили для встроенных и отдельностоящих подсистем безопасности (secure element) для IoT, V2x**
- **профили для интегральных микросхем в составе идентификационных документов**
- **профили для HSM-ов**

Требования — DO-254

- концепция разработки основанной на требованиях (requirements-based design and verification)
- обоснование целостности, непротиворечивости и адекватности требований
- обоснование достаточности и адекватности реализации требований в элементе
- расширенные методы верификации (Avdanced verification methods)
- архитектурые решения по предотвращению опасных событий (Architectural mitigation)

Требования — ИСО/МЭК 26262

- концепция общеиспользуемого элемента (Safety Element out of Context - SEooC)

Порядок подтверждения соответствия

Тут ничего нового:

- **система аккредитации для лабораторий**
- **система экспертизы и сертификации результатов исследований, проведенных лабораториями**
- **управление жизненным циклом сертификатов**

Механизмы, технологии и квалифицированные исполнители работ по оценке соответствия

ИСО/МЭК 15408

- **апробированный и проработанный набор технических и административных документов, содержащих трактовки и рекомендации по применению СС для сертификации интегральных микросхем**

DO-254

- **наработанные практики по применению коммерческих САПР-ов для проведения исследований интегральных микросхем на соответствие DO-254**

Нужно ли менять порядок разработки?

ИСО/МЭК 15408

- уровни выше (ОУД4)EAL4 практические не достижимы без изменения процесса разработки

DO-254

- применение сложной ЭКБ, разработанной вне рамок предписываемых процессов является неординарной ситуацией, требуемые меры соответствующие

ИСО/МЭК 26262

- подтверждение для COTS элементов, например, на основе большой базы данных результатов практического применения

Нужны ли специализированные лаборатории?

Набор действий при оценке соответствия ИСО/МЭК 15408

- анализ процессов и процедур жизненного цикла объекта;
- проверку выполнения декларируемых процессов и процедур;
- анализ соответствия между различными уровнями представления (TLM, RTL, netlist …);
- анализ соответствия каждого уровня представления проекта ОО требованиям;
- верификацию представленных доказательств;
- анализ эксплуатационной документации;
- анализ разработанных функциональных тестов и предоставленных их результатов;
- независимое функциональное тестирование;
- анализ уязвимостей, включающий предположения о недостатках;
- тестирование проникновения (проведение атак).

Нужны ли специализированные лаборатории?

Требуемые знания и навыки при оценке соответствия ИСО/МЭК 15408

- понимание принципов проектирования и функционирования электронных микросхем,
- практический опыт реализации различных этапов в рамках маршрута проектирования интегральных микросхем,
- понимание технологии изготовления кристаллов и корпусирования микросхем,
- актуальные и достаточно полные знания в части атак на интегральные микросхемы и уязвимостей, которые они используют,
- опыт практической реализации атак.

Нужны ли специализированные лаборатории?

Инструментальные средства применяемые при оценке соответствия ИСО/МЭК 15408

- Системы автоматического проектирования и верификации интегральных микросхем (САПР),
- установки для реализации химической и механической декапсуляции,
- системы фокусированного ионного пучка (FIB),
- оптические и электронные микроскопы,
- установки для генерирования помех в интегральных микросхемах (laser, EM…).

Предлагаемые первоочередные шаги

- формирование нормативной базы на основе ИСО/МЭК 15408
- определение отдельного класса специализированных лабораторий и определение правил регулирования их деятельности
- инвестиции в развитие специализированных лабораторий
- формирование/адаптация типовых профилей защиты ЭКБ для объектов КИИ.

СПАСИБО ЗА ВНИМАНИЕ !