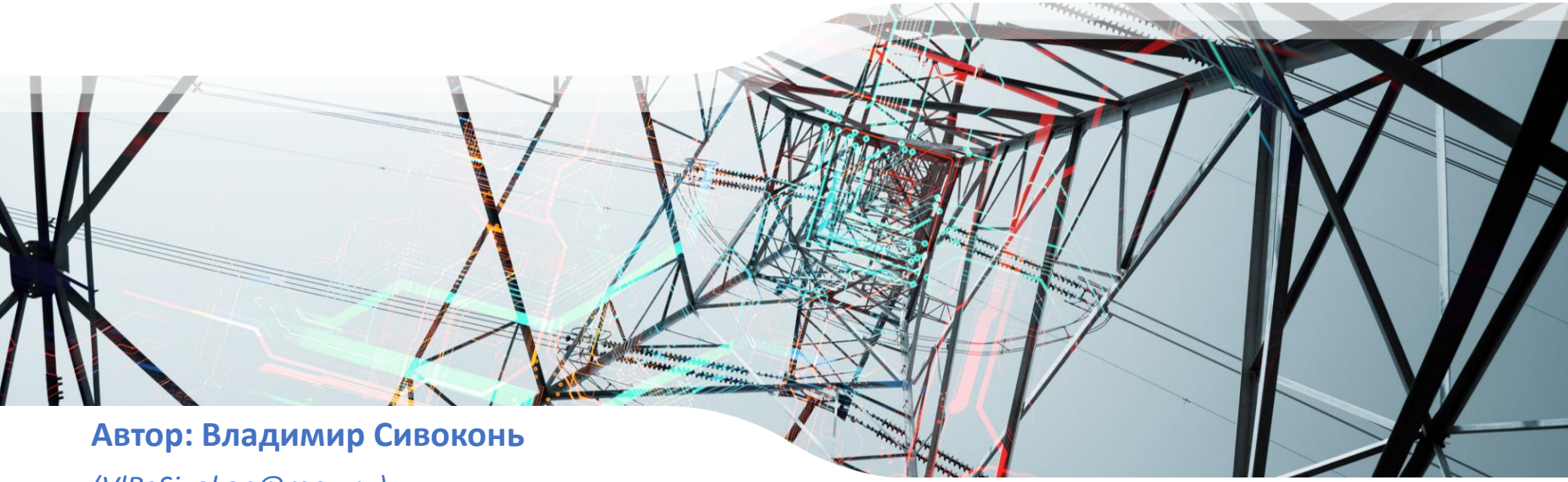
23 ежегодная конференция молодежного отделения ЯО России

Цифровые системы безопасности: всегда ли благо ?



Автор: Владимир Сивоконь

(VlPeSivokon@rasu.ru)

Компания: АО “РАСУ”

Нововоронеж , 12 октября 2018

Содержание

Определение безопасности (НП-001-15)
(проектированию цифровых систем нужно особое внимание)

Безопасность АС (ядерная и радиационная безопасность АС) - свойство АС обеспечивать надежную защиту персонала, населения и окружающей среды от недопустимого в соответствии с федеральными нормами и правилами в области использования атомной энергии радиационного воздействия.

Безопасность АС достигается **за счет качественного проектирования**, конструирования и изготовления оборудования, размещения, сооружения и эксплуатации АС посредством соблюдения требований федеральных законов, федеральных норм и правил в области использования атомной энергии, формирования и поддержания культуры безопасности, учета опыта эксплуатации и современного уровня развития науки, техники и производства.

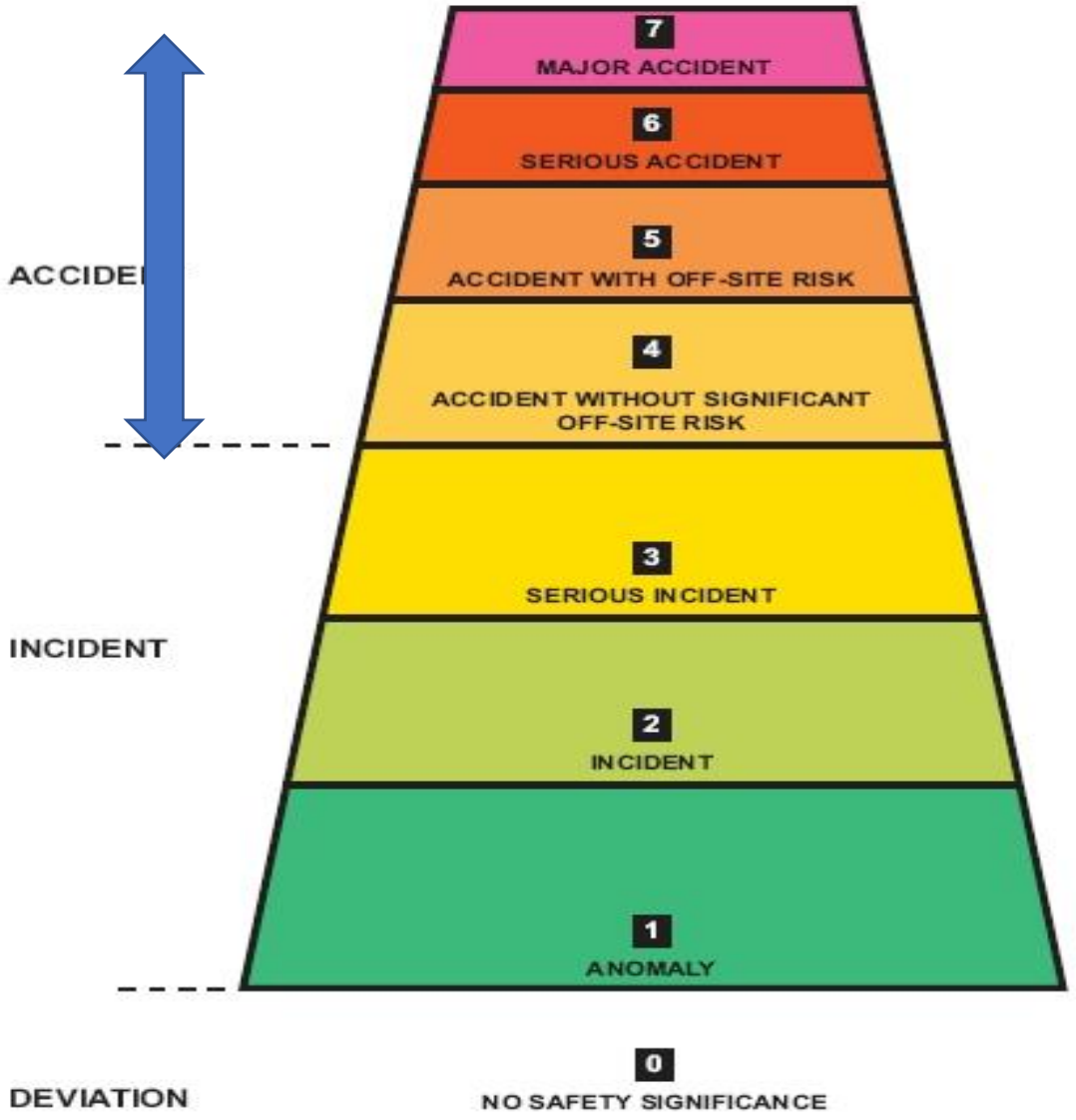
На практике это предотвращение аварий и минимизация числа и последствий инцидентов !

Что такое авария ?

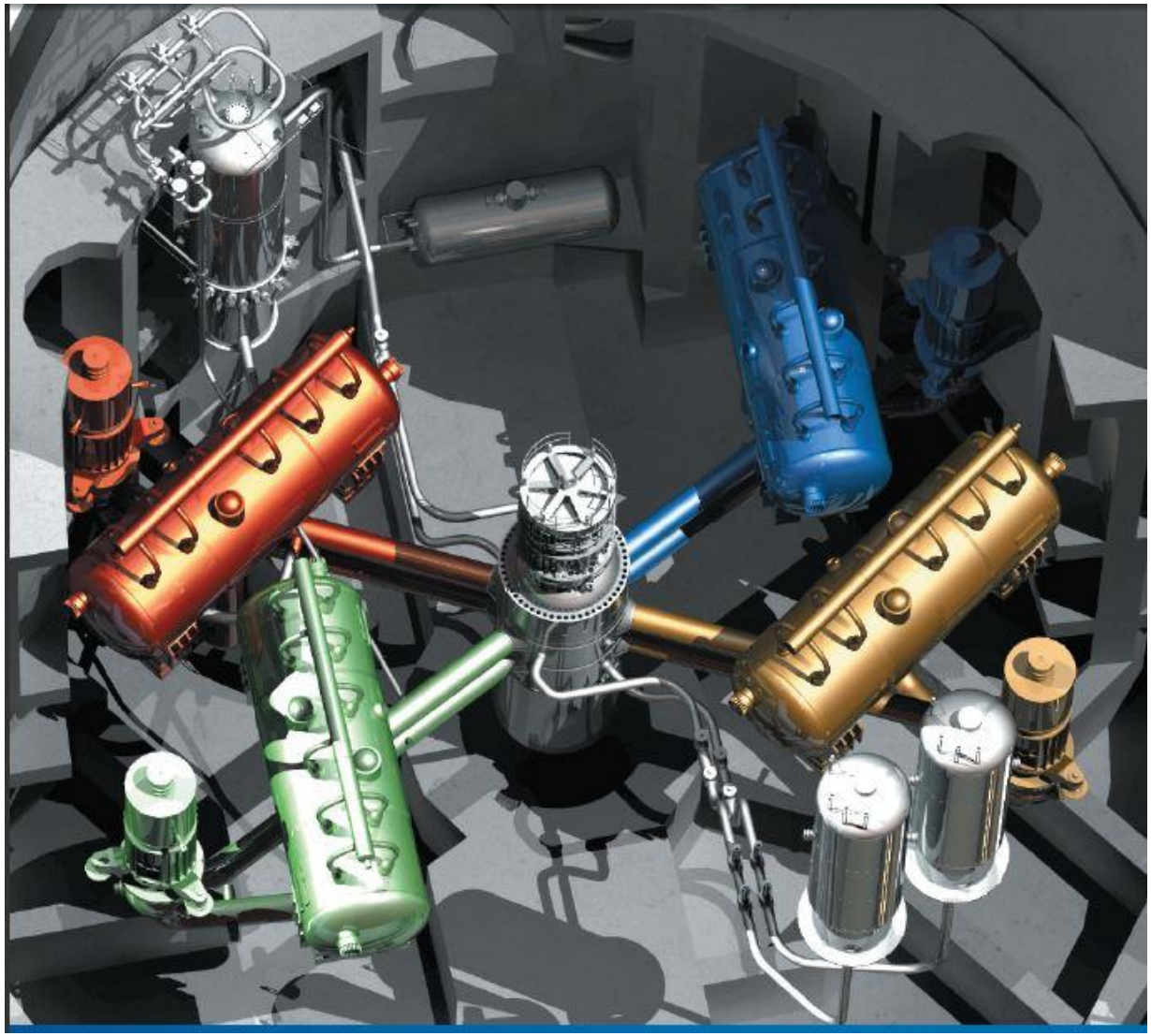
АВАРИЯ * - нарушение эксплуатации АС, при котором произошел выход радиоактивных веществ и/или ионизирующего излучения за предусмотренные проектом для нормальной эксплуатации границы в количествах, превышающих установленные пределы безопасной эксплуатации.

* Под термином "авария" всегда понимается событие, связанное с радиационными последствиями.

Международная шкала событий ИНЕС
The International Nuclear Event Scale (INES)



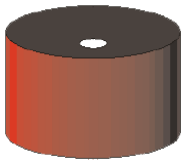
Как обеспечивается безопасность АЭС с ВВЭР



Принцип глубокоэшелонированной защиты (ГЭЗ) – фундаментальный принцип обеспечения безопасности АЭС

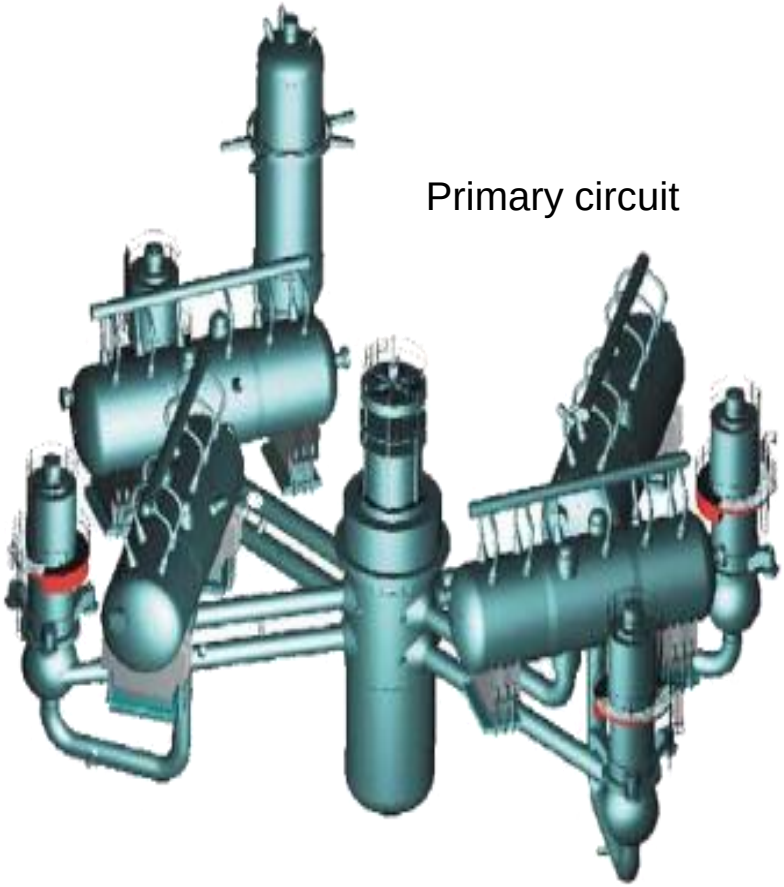
Пример реализации принципа глубокоэшелонированной защиты в физических барьерах АЭС

Fuel pellet

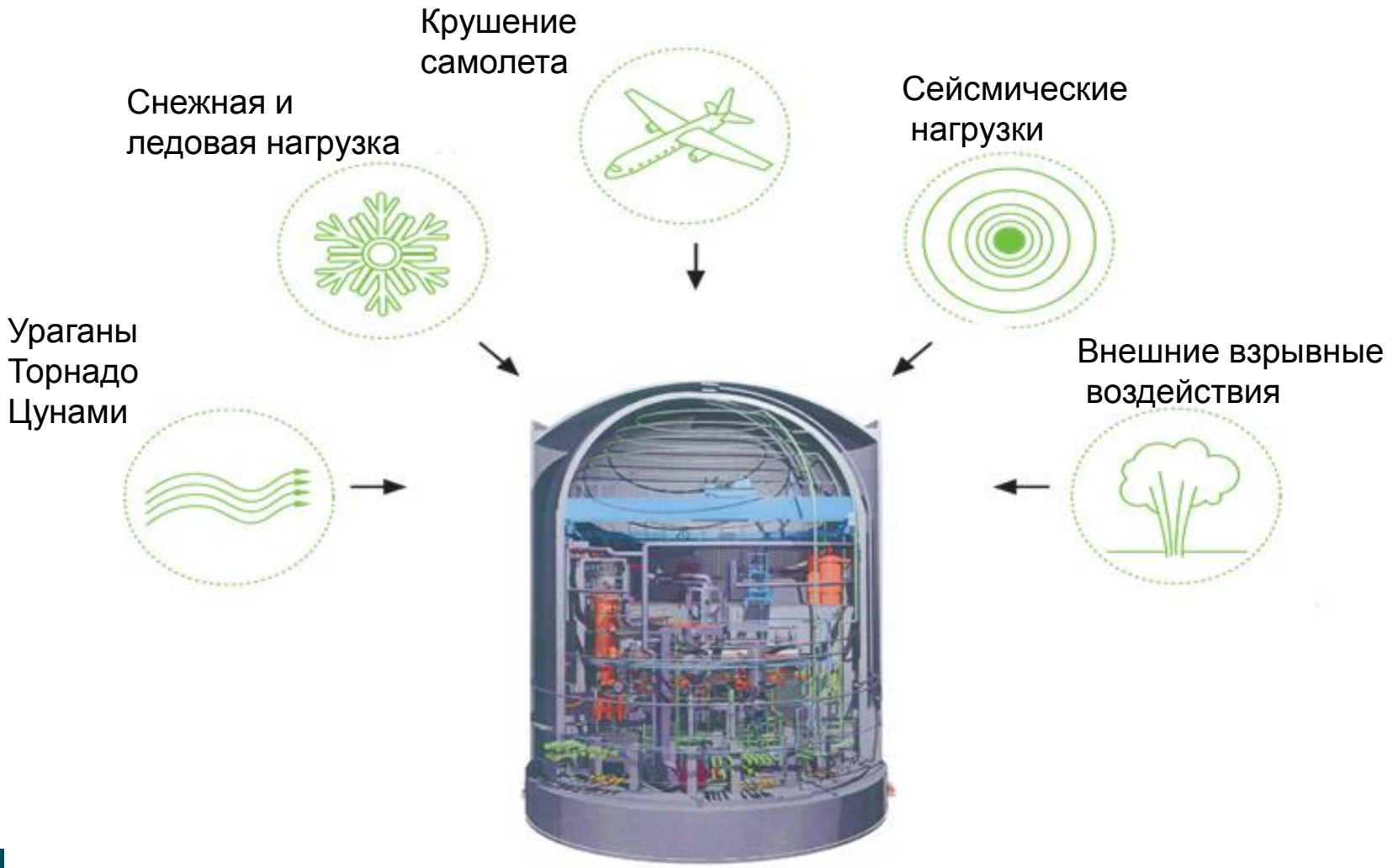


Fuel element

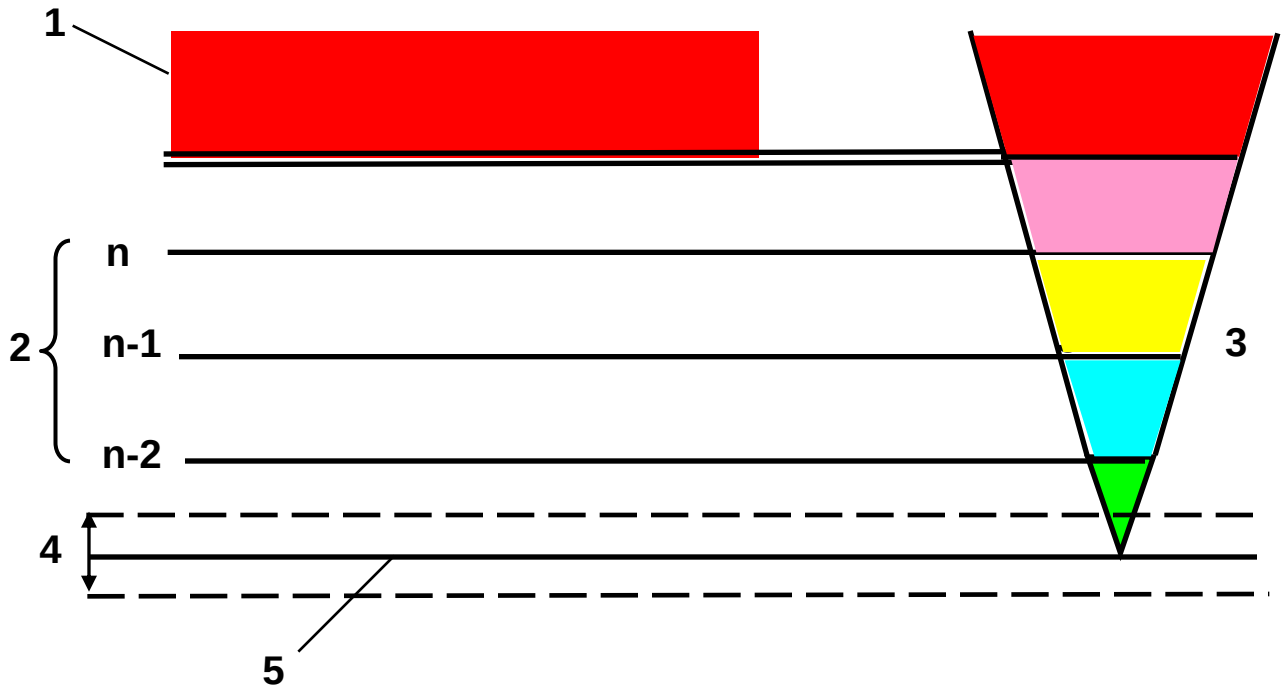
Primary circuit



Реализация принципа глубокоэшелонированной защиты в физических барьерах АЭС (продолжение)



С 80-х годов СКУ АЭС тоже строятся по принципу ГЭЗ (впервые внедрено на немецких PWR фирмой KWU)



1 – Зона АЗ (УСБ); 2 – Прогрессирующие уровни ПЗ;
3 – Защитные действия с возрастающей эффективностью;
4 – Диапазон регулирования; 5 – Уставка регулятора.

Принцип работы систем безопасности ВВЭР и западных PWR (IAEA TR-374)

Тип реактора АЭС (PWR and WWER)

Параметры, по которым можно определить ПИС:								Постулируемые исходные события (ПИС)	Требуемые действия:						
	x				x		x	Большая течь в первом контуре реактора	x	x	x	x			x
	x		x	x		x		Течь в главном паропроводе вне контаймента (ЗО)	x				x	x	x
	x		x	x		x	x	Течь в главном паропроводе внутри контаймента	x				x	x	x
	x	x		x				Остановка нескольких ГЦН	x						x
				x		x		Остановка питательных насосов	x				x		x
x	x							Неуправляемое извлечение органов регулирования	x						x
Нейтронный поток велик	DNB низкое (dT высокое)	Скорость ГЦН низкая	Давление первогокоонтура	Высокое давление в ПГ	Низкое давление в ПГ	Низкий уровень в ПГ	Высокое давление в ЗО		Аварийный останов РУ	Изоляция здания	Впрыск насосами ВД	Впрыск насосами НД	Аварийная пит. вода	Паропровод и пит.вода	Останов ТГ
Инициирующие критерии								Система защиты (УСБ) / Испол-ительные системы	Функции безопасности						
								Обеспечивающие системы безопасности							

Вид БПУ блока 3 Калининской АЭС после внедрения рекомендаций МАГАТЭ при вводе в эксплуатацию

Фрагмент панелей безопасности КАЭС-3

Новые вызовы и подходы к обеспечению безопасности атомной энергетики

В последние годы, начиная с 2010, многие страны, развивающие атомную энергетику, и международные организации, связанные с этой отраслью, активно пересматривают нормативную базу в сторону повышения требований по ядерной безопасности АЭС.

Это вызвано в первую очередь двумя основными причинами:

- **тяжелой аварией на АЭС Фукусима в марте 2011 года;**
- **массовым повреждением центрифуг обогатительного производства в Иране в 2010 году новым типом компьютерного вируса, способного фатально поражать промышленные контроллеры, в том числе в АСУ ТП АЭС.**

Отражение новых вызовов безопасности в требованиях к системам управления АЭС и СБ, в частности

Разработанные и разрабатываемые в мире новые требования в части АСУ ТП АЭС касаются в основном следующих вопросов:

- **Повышению надежности и отказоустойчивости систем важных для безопасности**
- **Уточнению концепции глубокоэшелонированной защиты с учетом допущения отказа систем безопасности по общей причине (ООП)**
- **Обеспечению высокой степени разнообразия систем безопасности для борьбы с ООП;**
- **Обеспечению кибербезопасности СБ и АСУ ТП в целом**

Основные изменения в требованиях к системам безопасности АЭС

- ✓ Недоверие западноевропейских регулирующих органов к очень высокой надежности любых программируемых систем безопасности (отчет WENRA)
- ✓ Постулированная многими регулирующими органами необходимость учета множественных отказов, в том числе в системах безопасности (разделение уровня 3 ГЭЗ на 3a и 3b, пояснения последуют)
- ✓ Требование наличия на уровне 3b упрощенной дополнительной диверсной системы (ДДСЗ), выполняющей роль минимизации рисков при отказе СБ на уровне 3a, «диверсной» по отношению к СБ и выполненной предпочтительно на «жесткой логике» (пояснение последует)
- ✓ Возрастание риска и серьезности киберугороз и, как следствие, потребность в новых технических решениях в системах безопасности и АСУ ТП в целом для устранения или минимизации последствий этой проблемы

Усовершенствованная концепция глубокоэшелонированной защиты (ГЭЗ)

- В нормах МАГАТЭ по безопасности АЭС, принятых МАГАТЭ в 2012 и детализированных в рабочей группе западноевропейских регулирующих органов (RHWG WENRA) в 2013, предложена усовершенствованная Концепция ГЭЗ, ориентированная на дальнейшее повышение безопасности АЭС.
- Введено четкое разделение между средствами и условиями действия подуровней защиты в 3а и 3б ГЭЗ. Главное - наличие на уровне 3b упрощенной дополнительной «диверсной» системы защиты (ДСЗ), минимизирующей риски при отказе СБ на уровне 3а

Усовершенствованная структура глубокоэшелонированной защиты в СКУ (1)

Уровни защиты в глубину	Цель/задача	Основные средства	Радиационные последствия	Категории режимов эксплуатации станции и **соответствующие подсистемы АСУ ТП**
Уровень 1	Предупреждение нарушений нормальной эксплуатации и отказов	Консервативный подход и высокое качество при строительстве и эксплуатации, управление основными параметрами станции в установленных пределах	Радиационное воздействие за территорией станции отсутствует (ограничено допустимыми пределами эксплуатации по выбросам)	Нормальные условия эксплуатации **Автоматические регуляторы (АРМР и т.п.)**
Уровень 2	Управление нарушениями нормальной эксплуатации	Системы управления и предупредительной защиты		Ожидаемые эксплуатационные события **Предупредительная защита**

Усовершенствованная концепция (WENRA-2013) глубокоэшелонированной защиты в СКУ (2)

Уровни защиты в глубину		Цель/задача	Основные средства	Радиационные последствия	Категории режимов эксплуатации станции и соответствующие подсистемы АСУ ТП
Уровень 3	3.a	Управление аварией для ограничения радиационных выбросов и защита от условий расплавления активной зоны[1]	Система защиты реактора, системы безопасности, аварийные инструкции	Радиационное воздействие за территорией станции отсутствует или незначительно	Постулируемые единичные исходные события **СБ (АЗ-УСБТ)**
	3.b		Дополнительные функции безопасности, аварийные инструкции		Рассматриваемые исходные события с множественными отказами **ДСЗ (DAS) и дополнительные аварийные инструкции и меры**

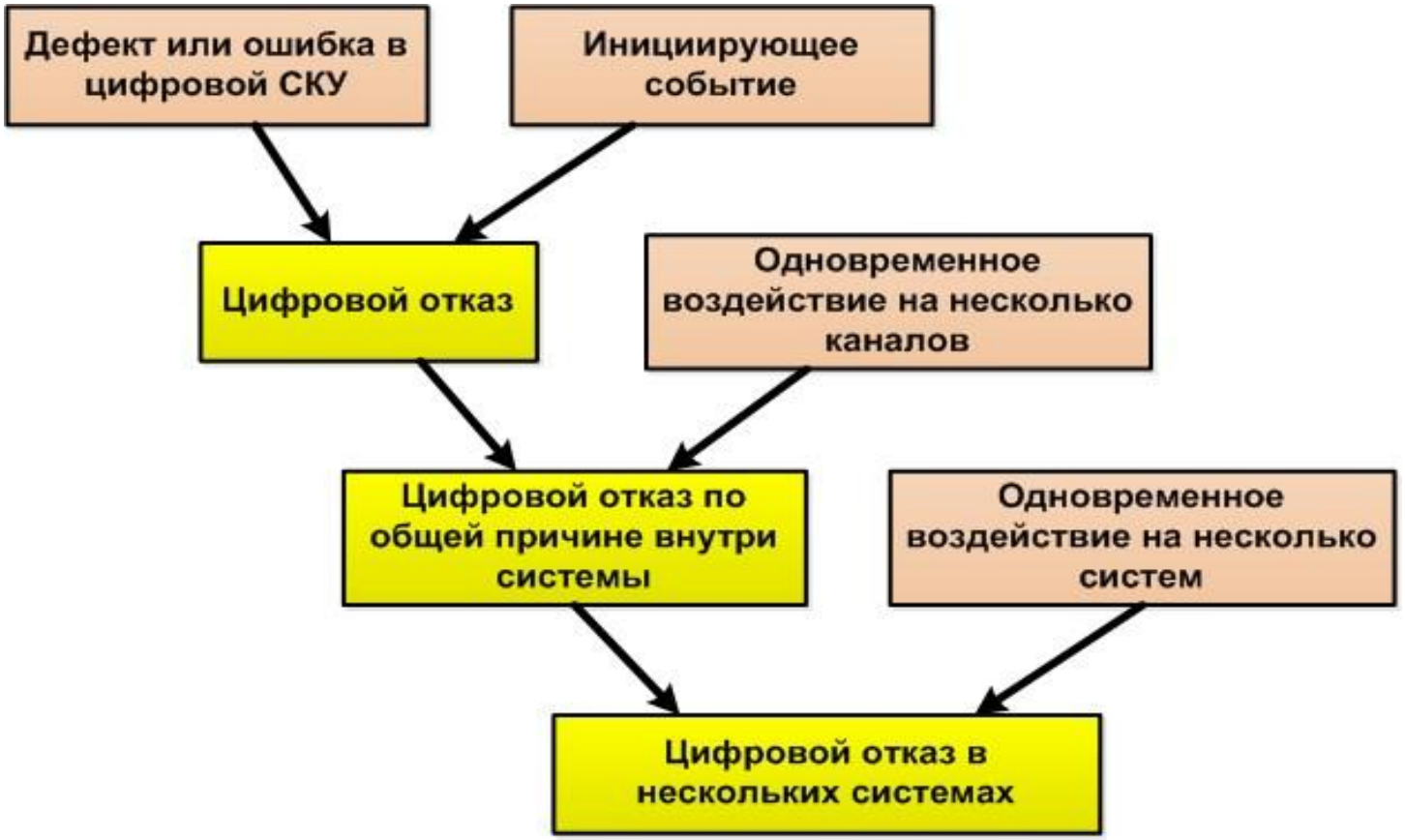
Усовершенствованная концепция (WENRA-2013) глубокоэшелонированной защиты в СКУ (3)

Уровни защиты в глубину	Цель/задача	Основные средства	Радиационные последствия	Категории режимов эксплуатации станции и соответствующие подсистемы АСУ ТП
Уровень 4	Управление авариями с расплавлением зоны для ограничения радиоактивных выбросов	Дополнительные средства безопасности для предотвращения расплавления зоны. Управление авариями с расплавлением зоны (тяжелые аварии)	Радиационные воздействие вне площадки может потребовать защитных мер в пространстве и времени	Постулируемые аварии с расплавлением зоны (кратко- и долго-срочные) **СКУ ЗПУ, ПАМС**
Уровень 5	Ослабление радиационных последствий от значительных выбросов рад. материалов	Аварийное реагирование за пределами площадки	Защитные меры от радиационного воздействия вне площадки	Снижение радиационных последствий **ПАМС, кризисные центры, ЕГАСКРО**

Основные принципы разработки систем безопасности

- Надежность (особенно актуальна для цифровых программируемых систем);
- Разнообразие;
- Разделение и Независимость;
- Отказоустойчивость;
- Избыточность (резервирование);
- Стойкость к условиям окружающей среды;
- Правило 30-ти минут;
- Принцип безопасного отказа;
- Бесперебойность питания;
- Способность передать управление в РПУ при невозможности использования БПУ.

В цифровых системах управления особенно опасен риск возникновения ООП



Риск ООП (отказов по общей причине) должен быть определен. При этом следует учитывать типичные условия возникновения ООП в цифровых СКУ.

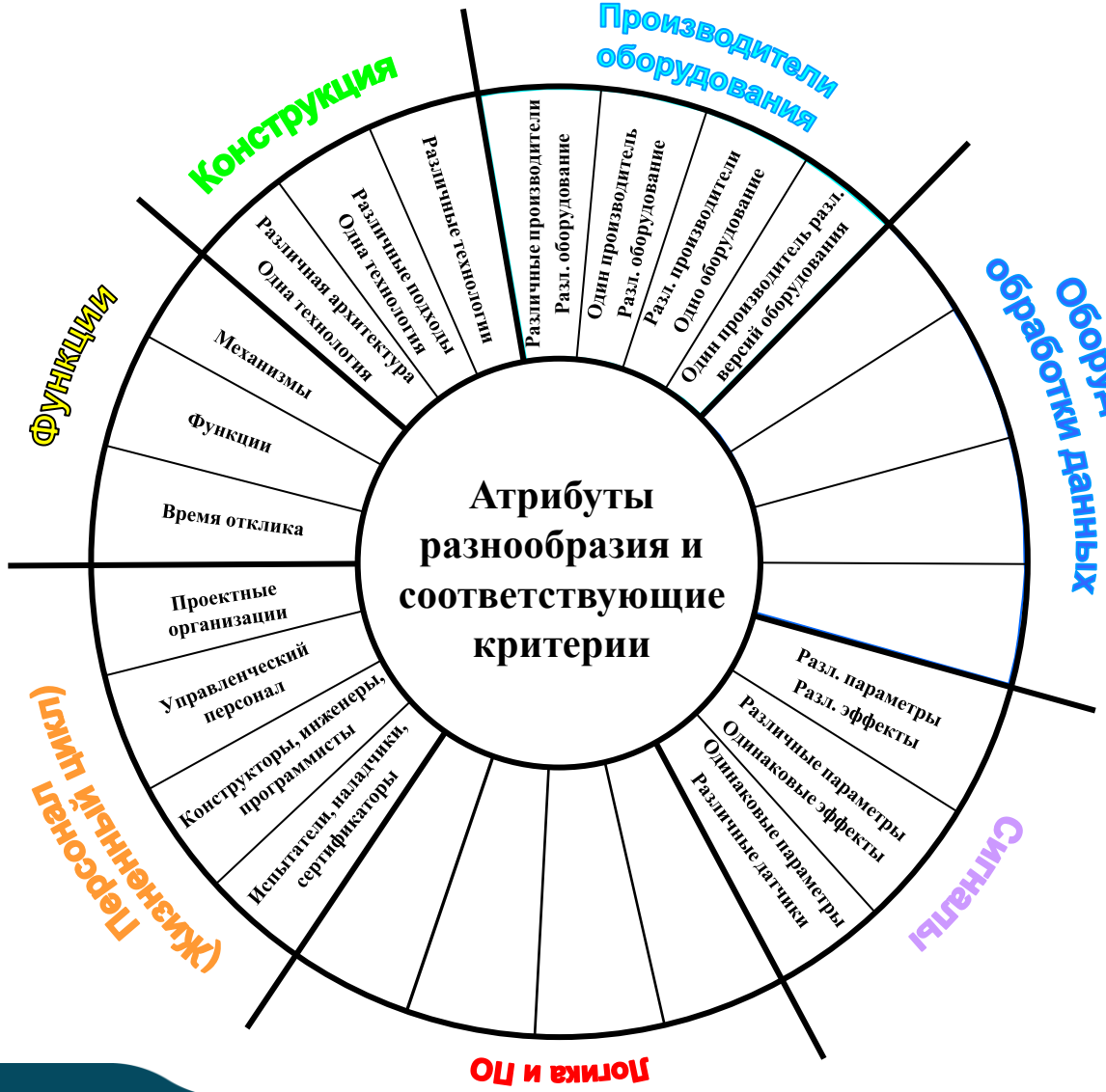
О надежности программируемых СКУ и, в частности, систем безопасности АЭС

Из отчета «Общая позиция семи Европейских ядерных регуляторов и организаций, осуществляющих их техническую поддержку»: Пункт 1.13.2.2 Ограничения по заявляемой надежности

- Заявления об очень высокой надежности ПО не может быть доказано современными методами. Поэтому должно быть принято решение ограничить заявляемую надежность компьютерных систем. Обзор стандартов в атомной отрасли показывает, что к заявлениям о надежности компьютерных систем выше, чем 10 E-4 по вероятности отказа на требование надо относиться с большой осторожностью

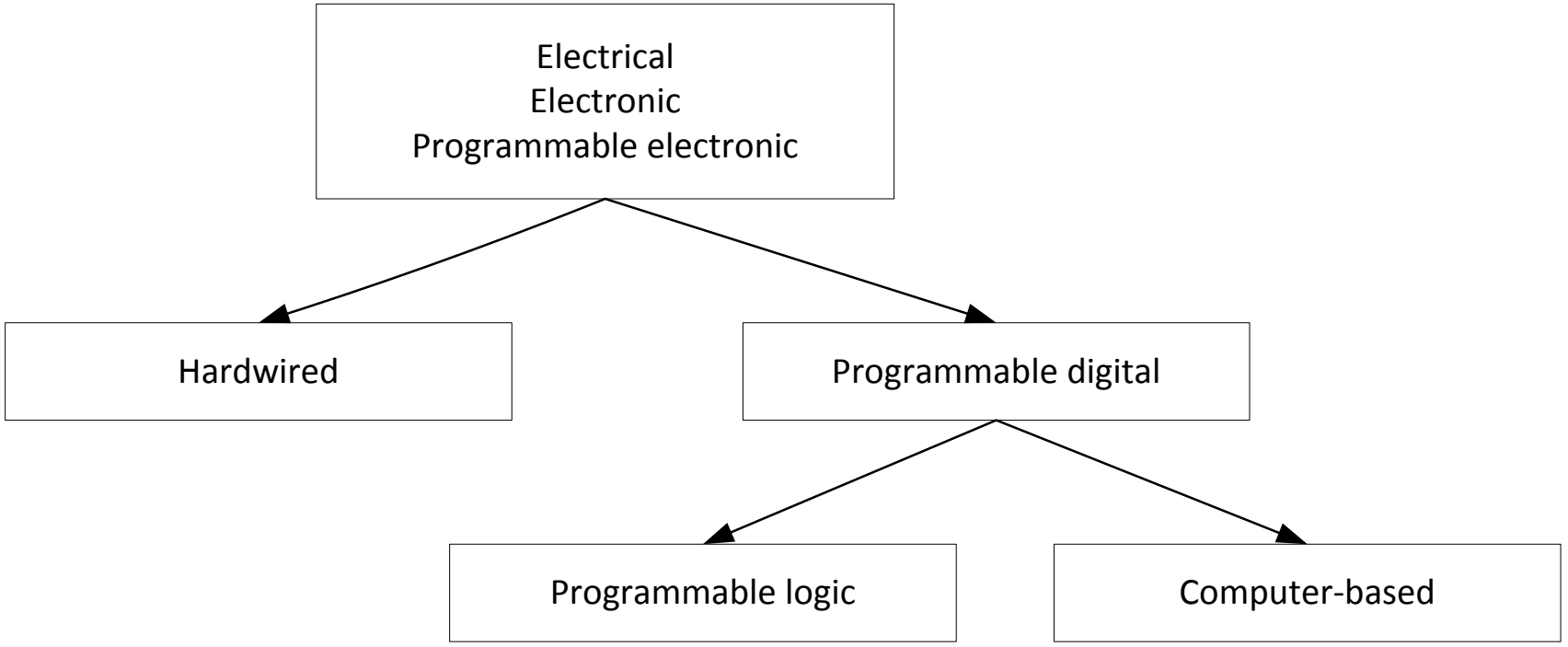
- Вывод: в СБ АЭС обязательно должен быть использован принцип разнообразия, например, путем сочетания программируемых и непрограммируемых технических средств

Атрибуты и критерии разнообразия в универсальной терминологии



Технологическое разнообразие – основной подход к выбору тех. средств для систем разного уровня ГЭЗ

Основные технологии, используемые в СКУ АЭС
(IAEA TECDOC -1848. Criteria for Diverse Actuations Systems, 2018)



Подход к выбору ТС на основе разнообразия в технологиях: СБ - тип 1 и 2, ДДСЗ - тип 3

№	Характеристика	Тип 1 Программируемые средства (PLC)	Тип 2 Однократно программируемые микросхемы (FPGA, PLD)	Тип 3 Жесткая логика (Логика на базе электронных схем)
1	Вычислительная мощность (реализация сложных функций)	**Очень высокая**	Высокая	**Низкая** (для сложных алгоритмов)
2	Надежность (в области малых вероятностей отказа)	**Неизвестная (считается не достаточно высокой для СБ)**	**Очень высокая**	Высокая
3	Уязвимость к кибератакам	**Очень высокая**	Низкая (возможна только при изготовлении)	**Отсутствует**
4	Самодиагностика	**Очень высокая**	Высокая	**Низкая** (требуются дополнительные устройства)
5	Модифициру-мость	**Очень высокая**	Высокая	**Низкая**
6	**Сложность лицензирования**	**Очень высокая !!!**	Высокая	**Низкая !!!**

Выводы

Без цифровых систем безопасности на современных блоках большой мощности уже невозможно обойтись, так как только они позволяют осуществлять необходимую защиту по параметрам, вычисляемым по сложным формулам. Это необходимо для максимального использования мощности ядерного реактора без нарушения пределов безопасности.

Кроме того, цифровые СБ обладают очевидными преимуществами такими как:

- Точность вычислений и измерений
- Глубокая самодиагностика
- Высокая помехозащищенность
- Простота реконфигурирования
- И другие

Выводы (2)

Тем не менее применение цифровых СБ вносит новые риски отказов СБ по общей причине и риски отказа в прохождении лицензирования у регулирующего органа из-за:

- Трудности (практически невозможности) полной проверки их программного обеспечения
- Уязвимости к вирусным атакам
- Отсутствия общепринятых для них методик расчета надежности

Выводы (3)

Поэтому современная тенденция использования цифровых СБ заключается в их конструировании в соответствии с принципами разнообразия и независимости, в комбинировании их с аналогами, реализованными на других технологиях (пример ТПТС-СБ, разработки ФГУП «ВНИИА»), и/или в дополнении их на случай отказа более простыми средствами, реализованными на «жесткой логике»:

- ДДСЗ - в России
  (дополнительная диверсная система защиты)
- DAS- за рубежом
  (diverse activation system)

Цифровые СБ АЭС эффективны и перспективны только тогда, когда они правильно спроектированы и интегрированы в систему управления АЭС

У нас нет другого пути, как обеспечить безопасность атомных станций на всех этапах их жизненного цикла !

Спасибо за внимание!