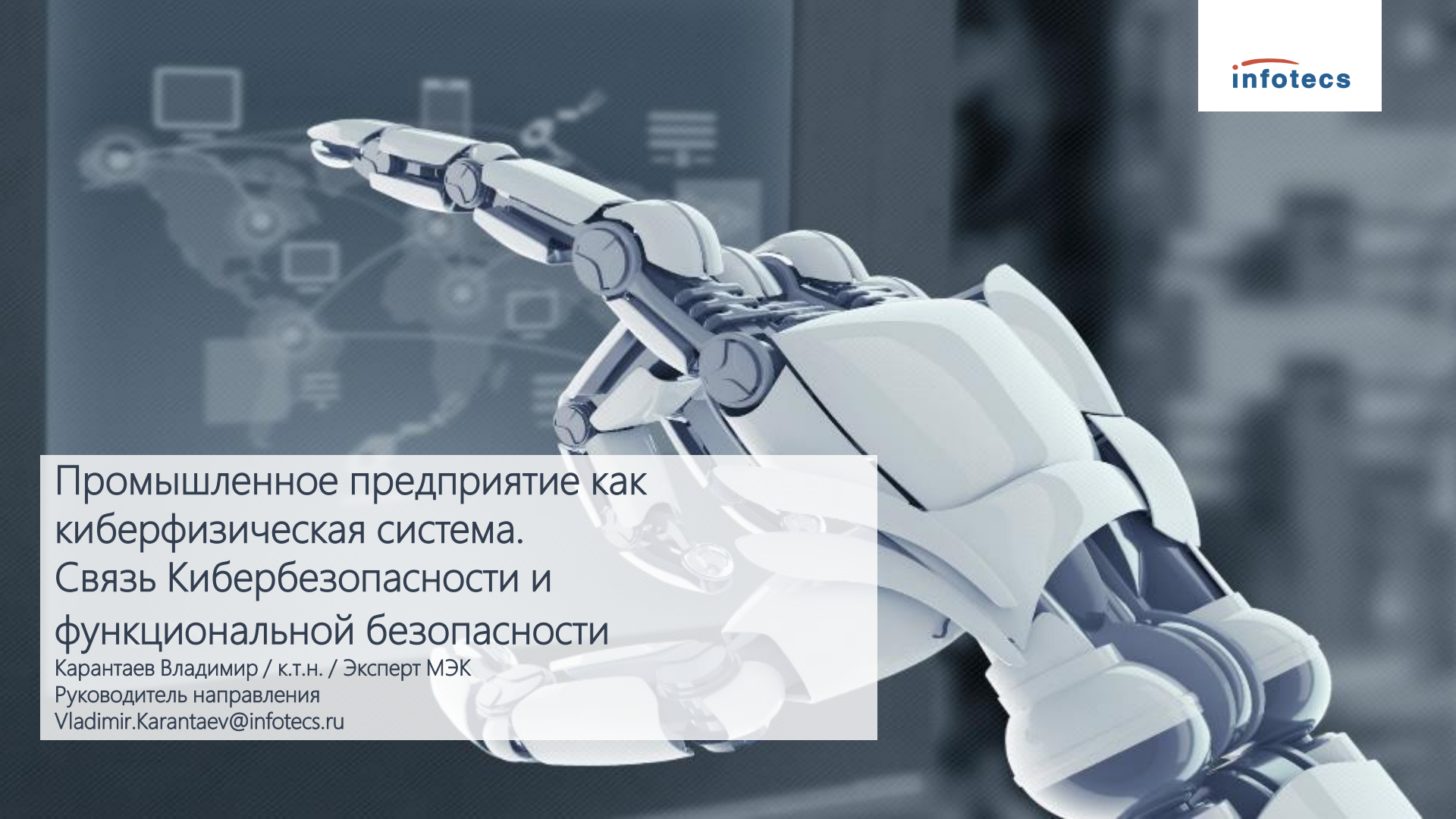


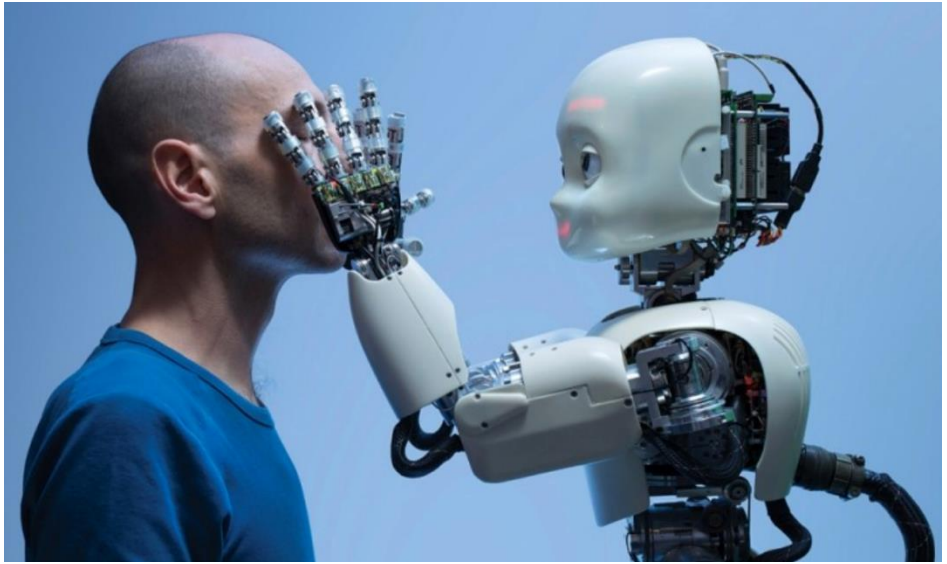
infotecs

Промышленное предприятие как киберфизическая система. Связь Кибербезопасности и функциональной безопасности

Карантаев Владимир / к.т.н. / Эксперт МЭК
Руководитель направления
Vladimir.Karantaev@infotecs.ru

Киберфизические системы

1. Робот не может причинить вред человеку или своим бездействием допустить, чтобы человеку был причинён вред.
2. Робот должен повиноваться всем приказам, которые даёт человек, кроме тех случаев, когда эти приказы противоречат Первому Закону.
3. Робот должен заботиться о своей безопасности в той мере, в которой это не противоречит Первому или Второму Законам.

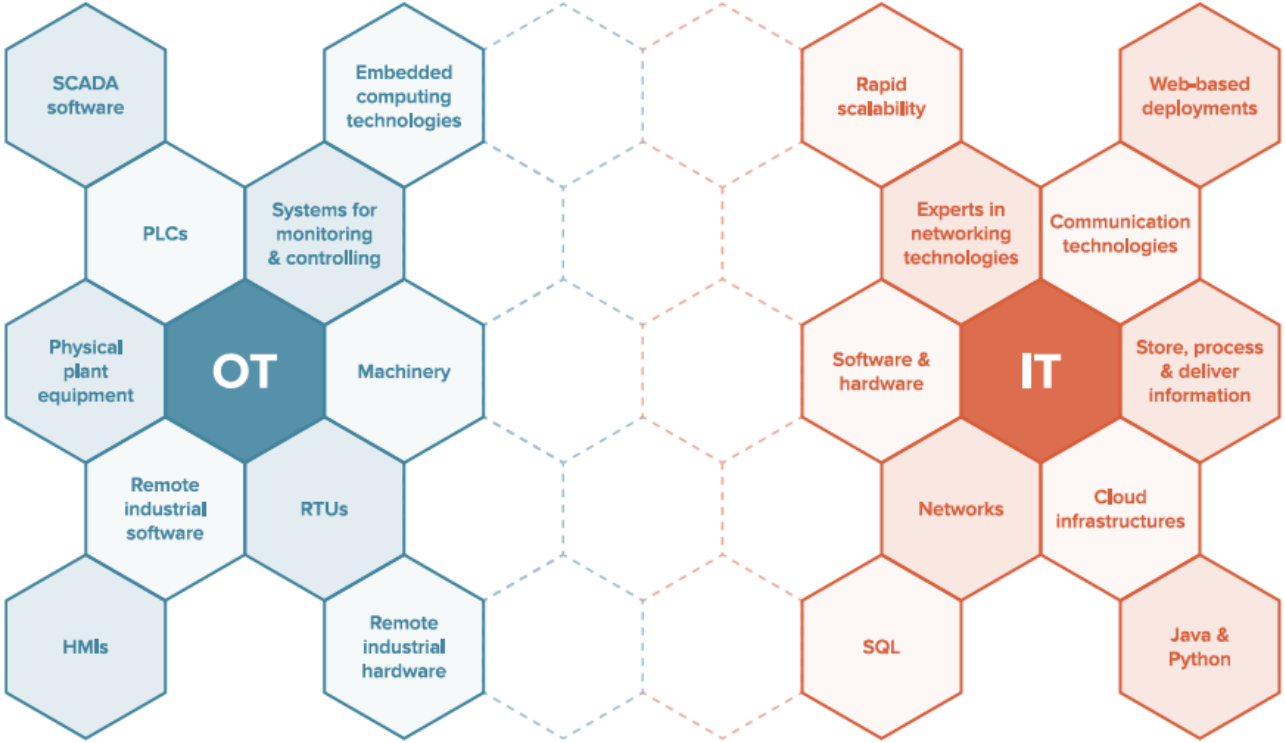


Три закона робототехники

Айзек Азимов

©2017, ОАО «ИнфоТеКС».

Operational technology + Information technology=IIoT



White Paper. IIoT: Combining the Best of OT and IT

©2017, ОАО «ИнфоТеКС».

Анализ рисков ИБ

infotecs

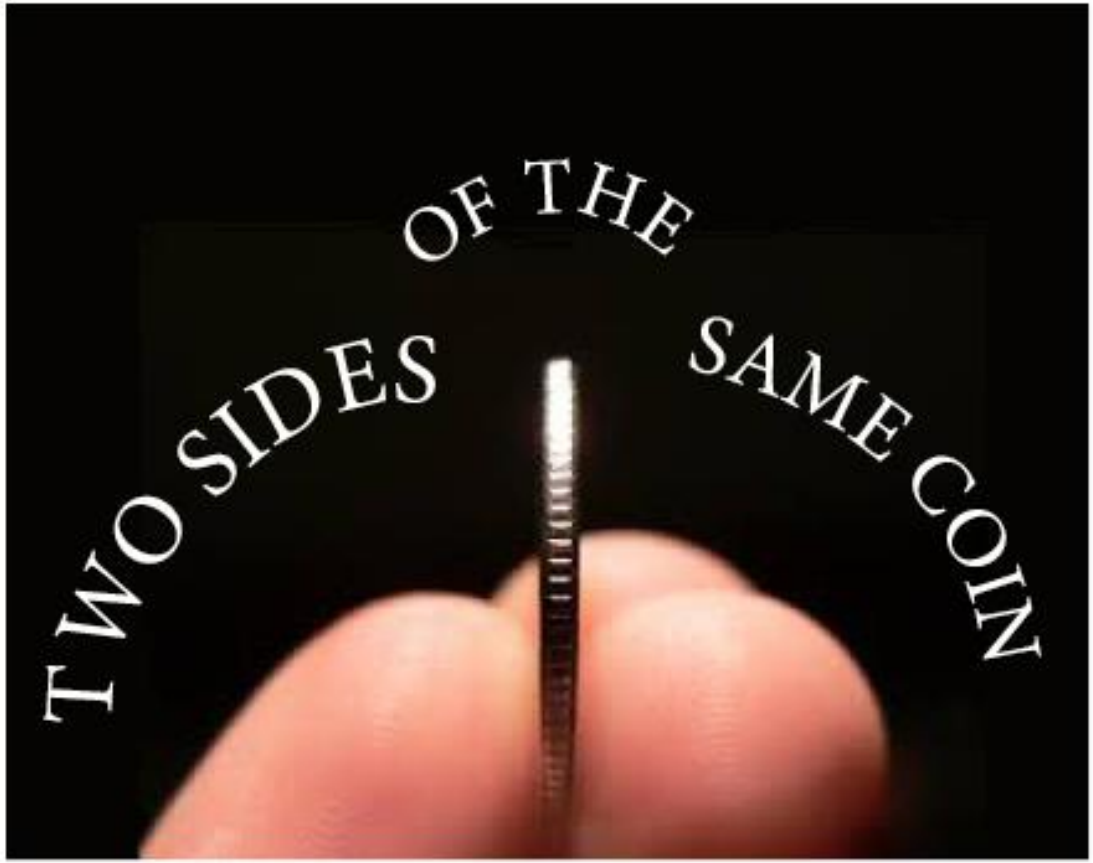
©2017, ОАО «ИнфоТеКС».

Уязвимости на разных уровнях

- **Уязвимости на уровне системного программного обеспечения:**
  - Базовая система ввода-вывода (BIOS);
  - Операционная система .
- **Уязвимости на уровне прикладного программного обеспечения:**
  - Программные средства (ПС) общего назначения;
  - ПС специального назначения;
  - ПС профессионального уровня.
- **Уязвимости используемых телекоммуникационных протоколов:**
  - МЭК 60870-5-104;
  - MMS, GOOSE, SV;
  - PTP, SMTP.

©2017, ОАО «ИнфоТеКС».

Информационная безопасность и функциональная безопасность



©2017, ОАО «ИнфоТеКС».

Используемые методы

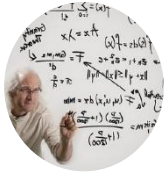
Общая теория систем и системный анализ

Вербализация

Формальные методы

Мозговой штурм

Экспертные оценки

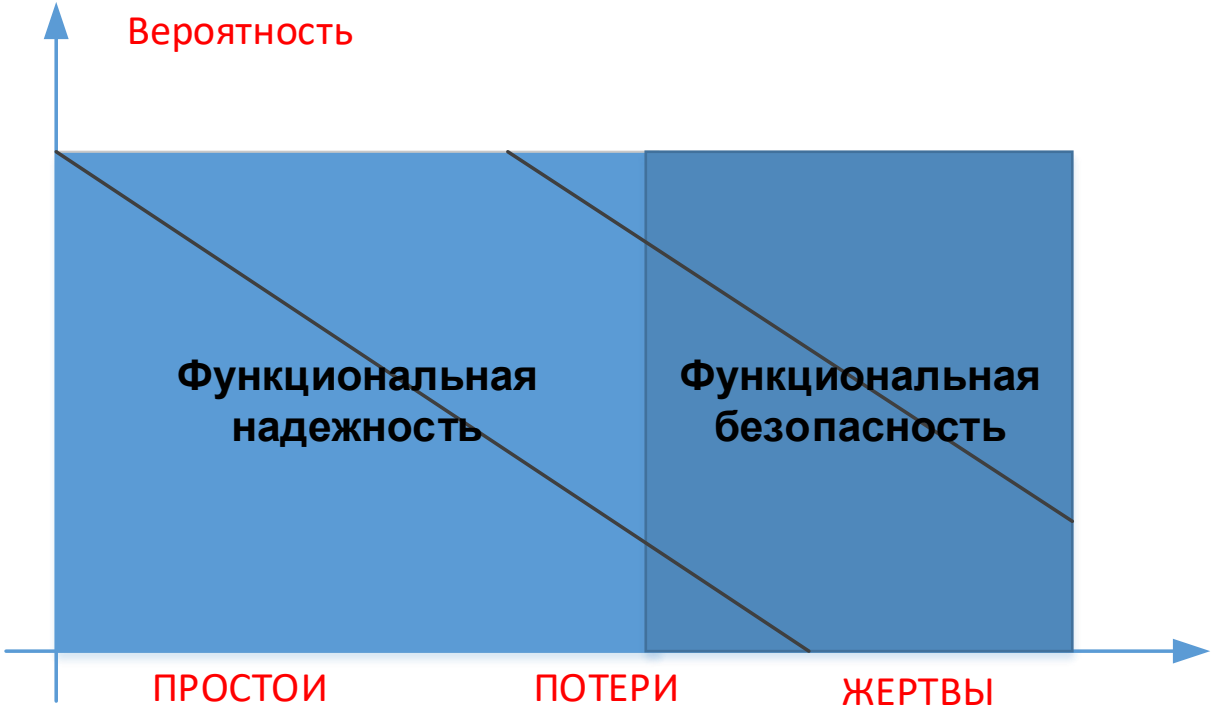


Математическая логика

Аналитические методы

©2017, ОАО «ИнфоТеКС».

Функциональная надежность и функциональная безопасность



On the definition of functional reliability

D.Eng.Sc. I. Shubinsky

©2017, ОАО «ИнфоТеКС».

Как мы можем оценить надежность?

Аварии могут быть индикатором надежности промышленных систем.

©2017, ОАО «ИнфоТеКС».

Определение функциональной надежности

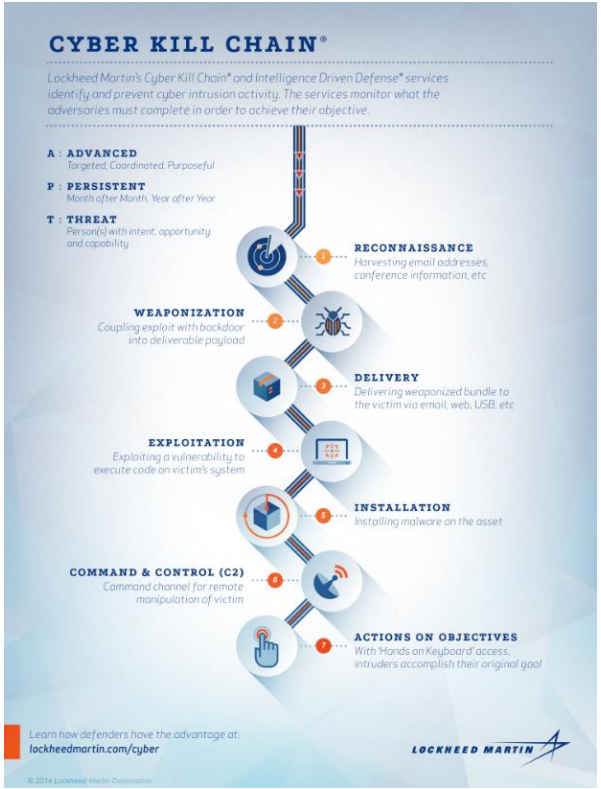
On the definition of functional reliability

D.Eng.Sc. I. Shubinsky

2017, ОАО «ИнфоТеКС».

Kill Chain View

Reconnaissance	Firewall	IDS	VPN	
Weaponization	Threat Intelligence			
Delivery	DNS Security	E-mail Security	Web Security	IDS
Exploitation	Firewall	IDS	Network Antivirus	
Installation	Host Firewall	Host Antivirus	Host VPN	
Command & Control	DNS Security	Web security	IDS	
Actions on Objectives	Anomaly analytics			



http://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html

©2017, ОАО «ИнфоТеКС».

FUNCTIONAL SAFETY INTERPRETATION

Стандарты приборных систем безопасности процессов
(безопасность функциональная)

ГОСТ Р МЭК 61511
Разработчики систем безопасности (проектировщики, пользователи систем безопасности)

ГОСТ Р МЭК 61508
Изготовители и поставщики технических устройств
(Системное оборудование, КИП, ИМ)

Оценка риска процесса, определение приемлемого риска, HAZOP → Распределение функций безопасности по слоям защиты, оценка частоты запросов на SIF → Определение уровня полноты безопасности (SIL) функций безопасности ПАЗ

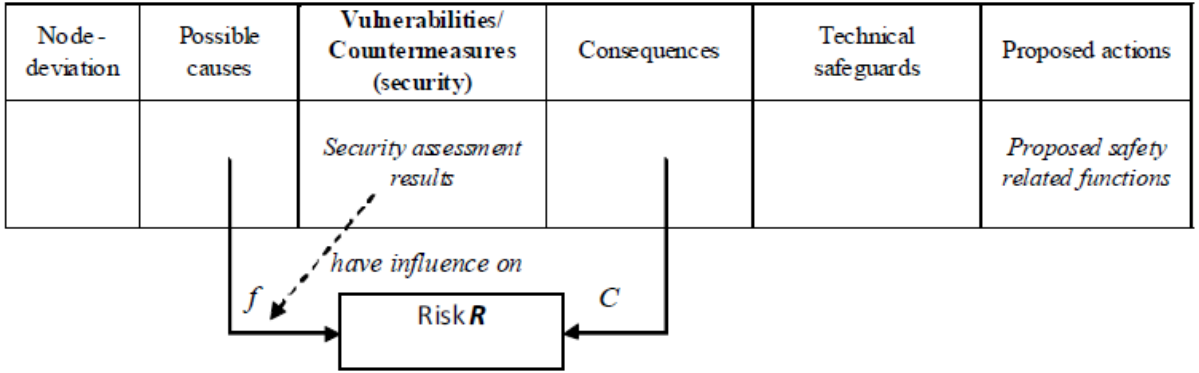
Оценка вероятности отказов аппаратных средств

Достижение назначенного уровня SIL для программного обеспечения

©2017, ОАО «ИнфоТеКС».

HAZOP и ИБ

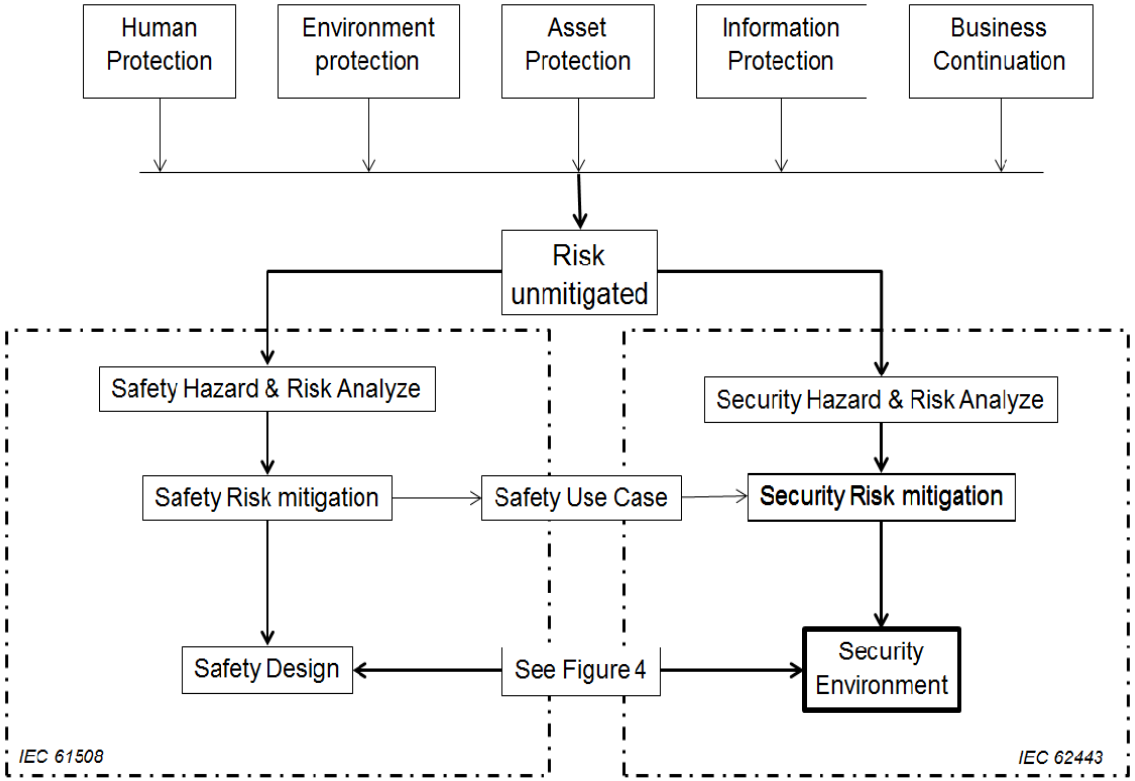
IEC 61511 Edition 2.0 «Safety instrumented system for the process industry sector»



Journal of Polish Safety and Reliability Association/Security aspects in functional safety analysis

©2017, ОАО «ИнфоТеКС».

Методология



IEC TC 65: Industrial Process measurement, control and automation

IEC TR 63069 ED1

©2017, ОАО «ИнфоТеКС».

Как снизить риски?

1. Приказ ФСТЭК России №31

Мера: Обеспечение безопасной разработки

2. ГОСТ Р ИСО/МЭК 27034-1. Безопасность приложений

3. ГОСТ Р 56939-2016 «Разработка безопасного программного обеспечения».

4. Методические рекомендации по обновлению сертифицированных средств защиты информации

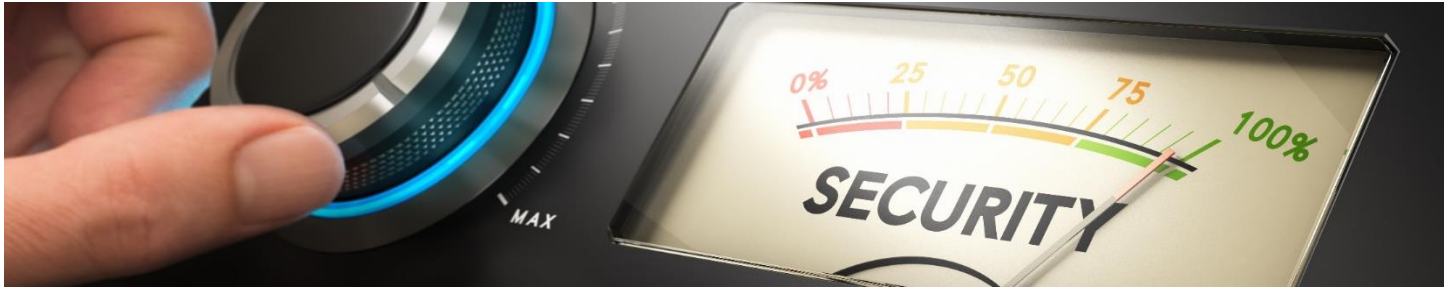
©2017, ОАО «ИнфоТеКС».

ViPNet SIES: Криптография

- Создание и проверка электронной подписи (ЭП).
- Вычисление/проверка имитовставки для блока данных.
- Вычисление хэш-функции для блока данных.
- Шифрование/расшифрование блока данных.

- Работа с ключами.
- Работа с сертификатами.

- Аппаратная криптография на базе смарт-карты для сценариев без требований к временным задержкам или с требованиями на уровне скорости реакции оператора
- Программно-аппаратная криптография для сценариев со средней производительностью.
- Программная и программно-аппаратная криптография с для сценариев в M2M-системах.



©2017, ОАО «ИнфоТеКС».

Выводы:

- Важной задачей является задача разработки инженерных методик расчета функциональной надежности.
- Системы должны разрабатываться исходя из анализа угроз функциональной надежности и информационной безопасности.
- В условиях необходимости удовлетворять комплексу требований по функциональной надежности, безопасности, наличия требований по быстродействию телекоммуникационных протоколов, оптимальности затрат реализация концепции «secure by design» (встроенных средств защиты информации в промышленных системах автоматизации), требований безопасной разработки – выглядит наиболее перспективно.

©2017, ОАО «ИнфоТеКС».

infotecs

Давайте пообщаемся!

Карантаев Владимир / к.т.н. / Эксперт МЭК
Руководитель направления
Vladimir.Karantaev@infotecs.ru / +7 915 221 15 96