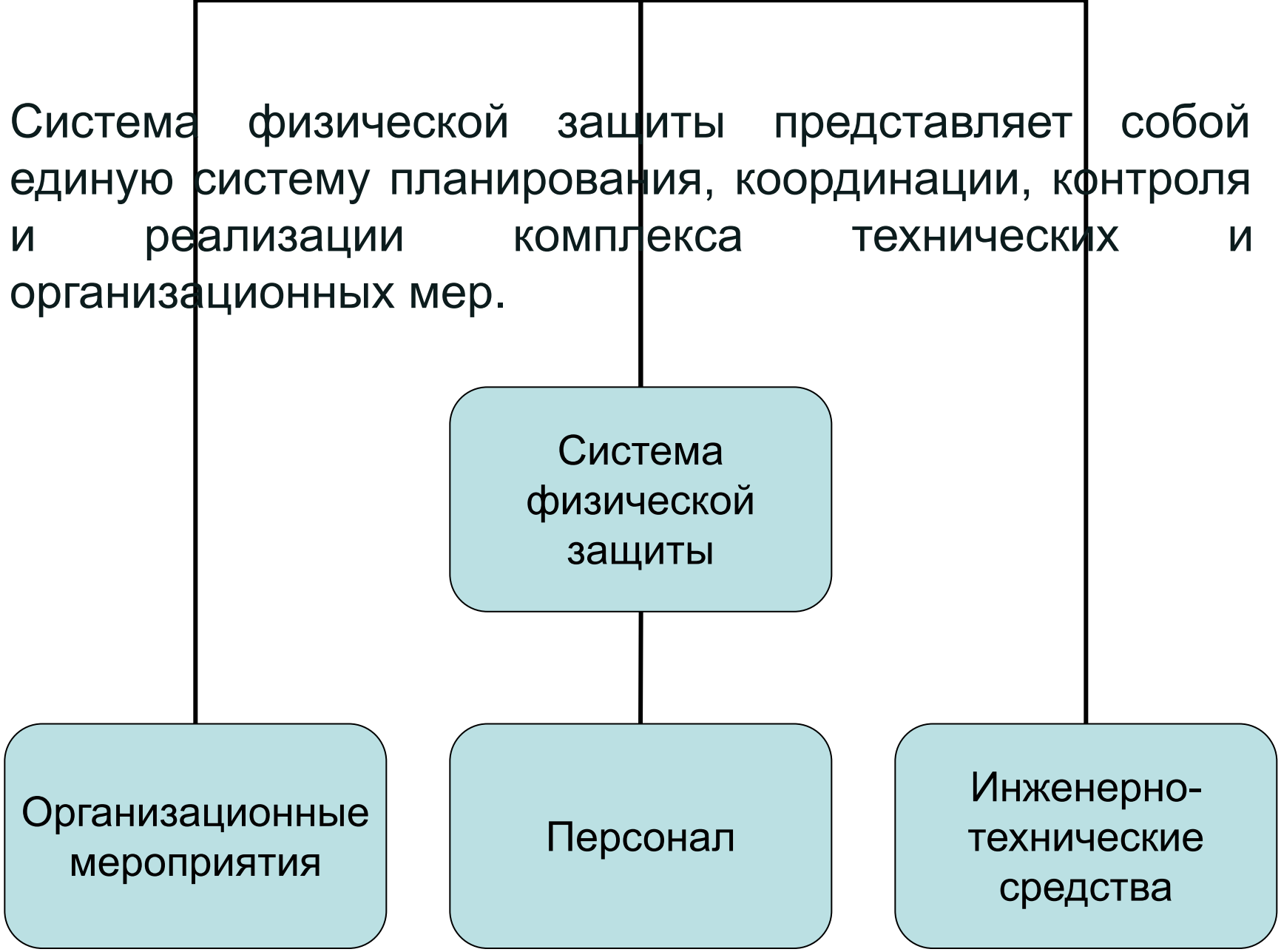
Защита объекта от физического несанкционированного доступа

Система физической защиты представляет собой единую систему планирования, координации, контроля и реализации комплекса технических и организационных мер.



Персонал

СОТРУДНИКИ СЛУЖБЫ БЕЗОПАСНОСТИ:

Работники предприятия, обеспечивающие организацию и функционирование системы физической защиты (в т.ч. техническую поддержку и обслуживание)

СИЛЫ РЕАГИРОВАНИЯ (RESPONSE FORCES):

находящиеся на площадке или за ее пределами вооруженные лица, соответственно оснащенные и обученные для противодействия нарушителям

Цели системы физической защиты

Предотвратить успешное выполнение нарушителем (группой нарушителей) своих действий.

- *Несанкционированное проникновение на объект,*
- *Нанесение физического ущерба оборудованию или объекту в целом,*
- *Нарушение способности объекта выполнять свои задачи,*
- *Хищение материальных ценностей (материалов или информации).*

Функции системы физической защиты

Сдерживание (Deterrence)

Меры, превращающие объект в непривлекательную цель (труднопреодолимо, устрашающе и.т.д)

Цель - прекращение нарушителями подготовки к нападению или отказ от него.

Предупреждающие знаки, достаточное освещение, демонстрация наличия сигнализации, систем видеонаблюдения, опечатывание проходов и др.

! Измерить эффективность сдерживания невозможно.

Сдерживания неэффективно, при решимости нарушителей осуществить нападение.

Функции системы физической защиты

Обнаружение (Detection)

Выявление скрытой или открытой акции нарушителя по проникновению в пространство объекта.

Особо выделяются точки санкционированного доступа.

1. Системы охранных датчиков (как внешних, так и внутренних), видеонаблюдения, контроля доступа должны зарегистрировать нештатную ситуацию и выдать сигнал тревоги.

2. Полученный сигнал тревоги должен быть принят оператором или другим ответственным лицом.

Оценка тревожной ситуации должна производится не только на основе сигнала тревоги от датчика, но и с использованием другой доступной информации, например результатов видеонаблюдения и сообщений сил охраны.

Функции системы физической защиты

Задержка (Delay)

Замедление продвижения нарушителей к цели. Способы реализации задержки: использование физических барьеров, препятствий, замков, а также сил охраны.

Задержка до обнаружения при определении эффективности не учитывается, и относится к сдерживанию по причине того, что время такой задержки не может быть использовано для реакции на действия нарушителя.

Функции системы физической защиты

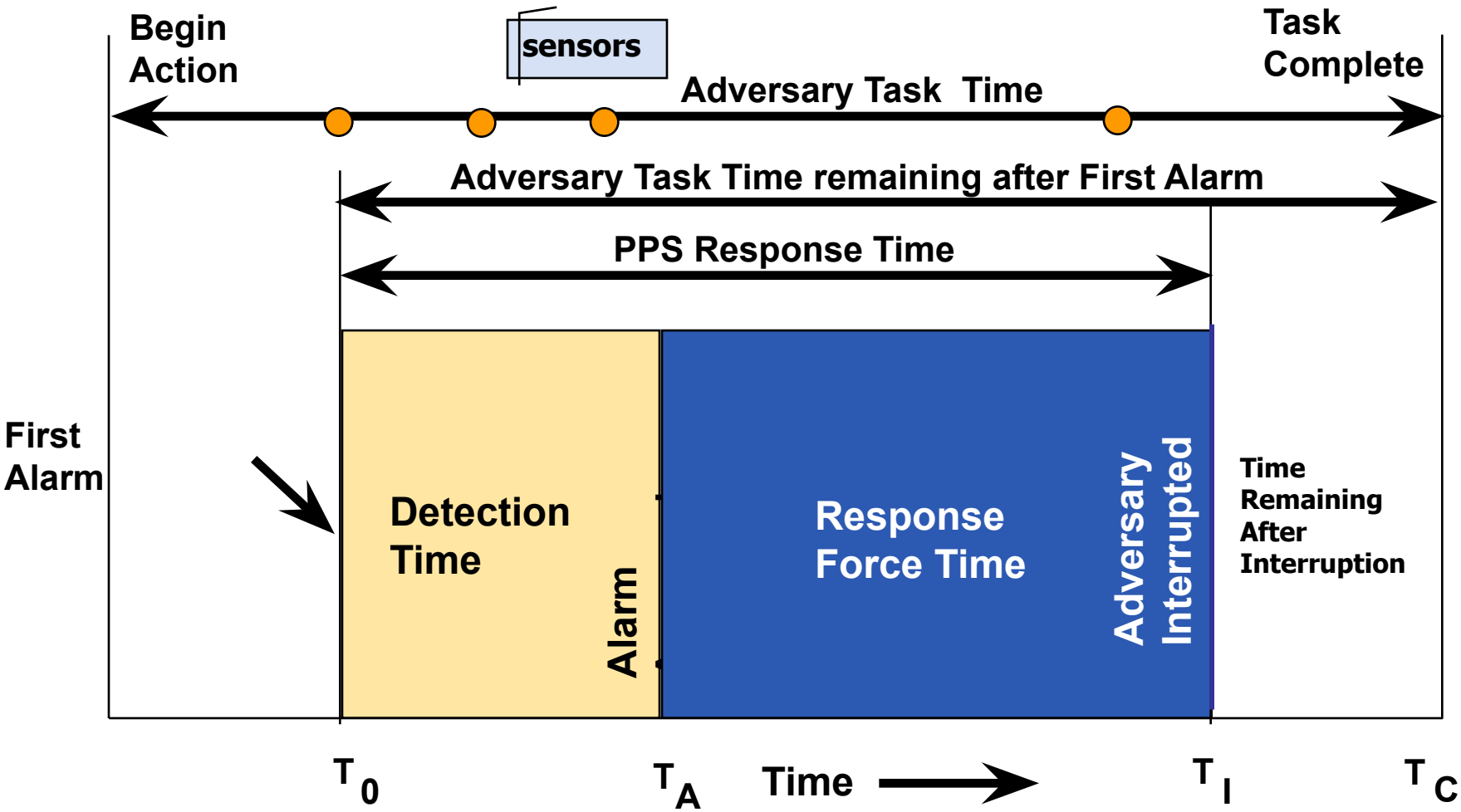
Реагирование (Response)

Функция реагирования состоит из действий, предпринимаемых силами реагирования для воспрепятствования успеху нарушителя. Реагирование трактуется как прерывание действий нарушителя.

Прерывание может быть определено как прибытие достаточного количества персонала сил реагирования в соответствующее место для остановки нарушителя и предполагает передачу им точной информации о нарушителе, а также их развертывание.

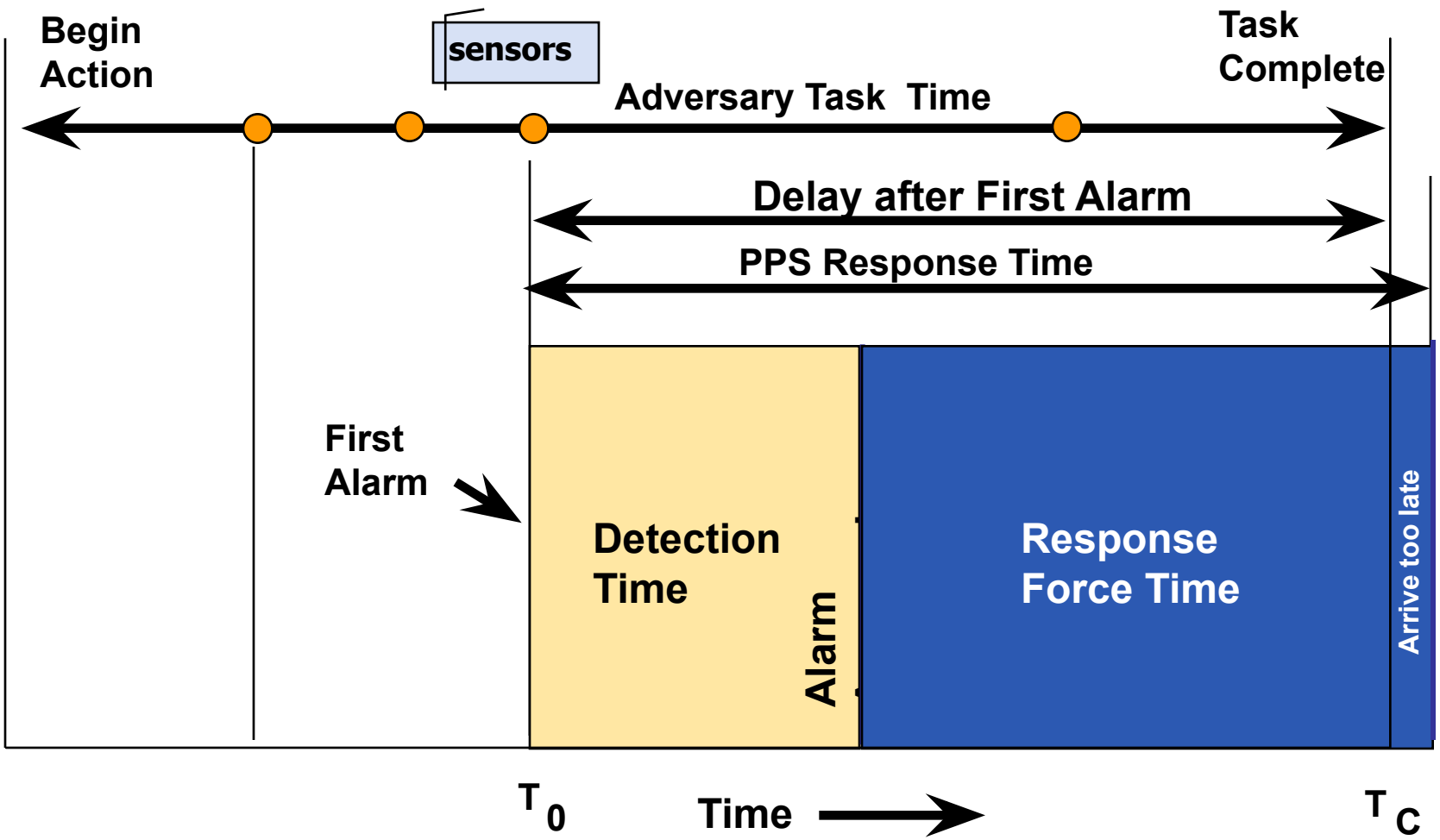
Временной график действий СФЗ

Adversary and PPS Timelines

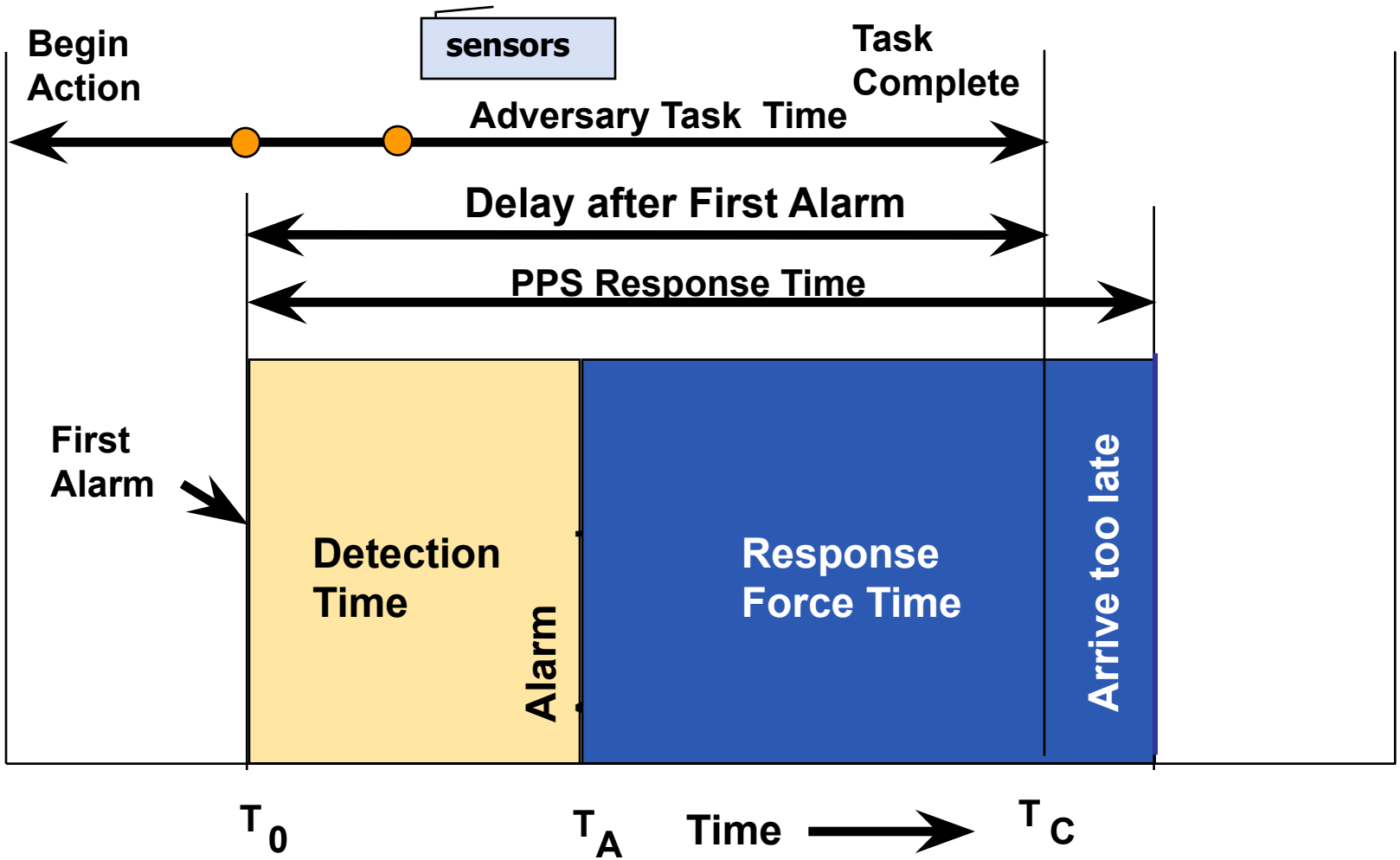


Time before First Alarm is not Delay

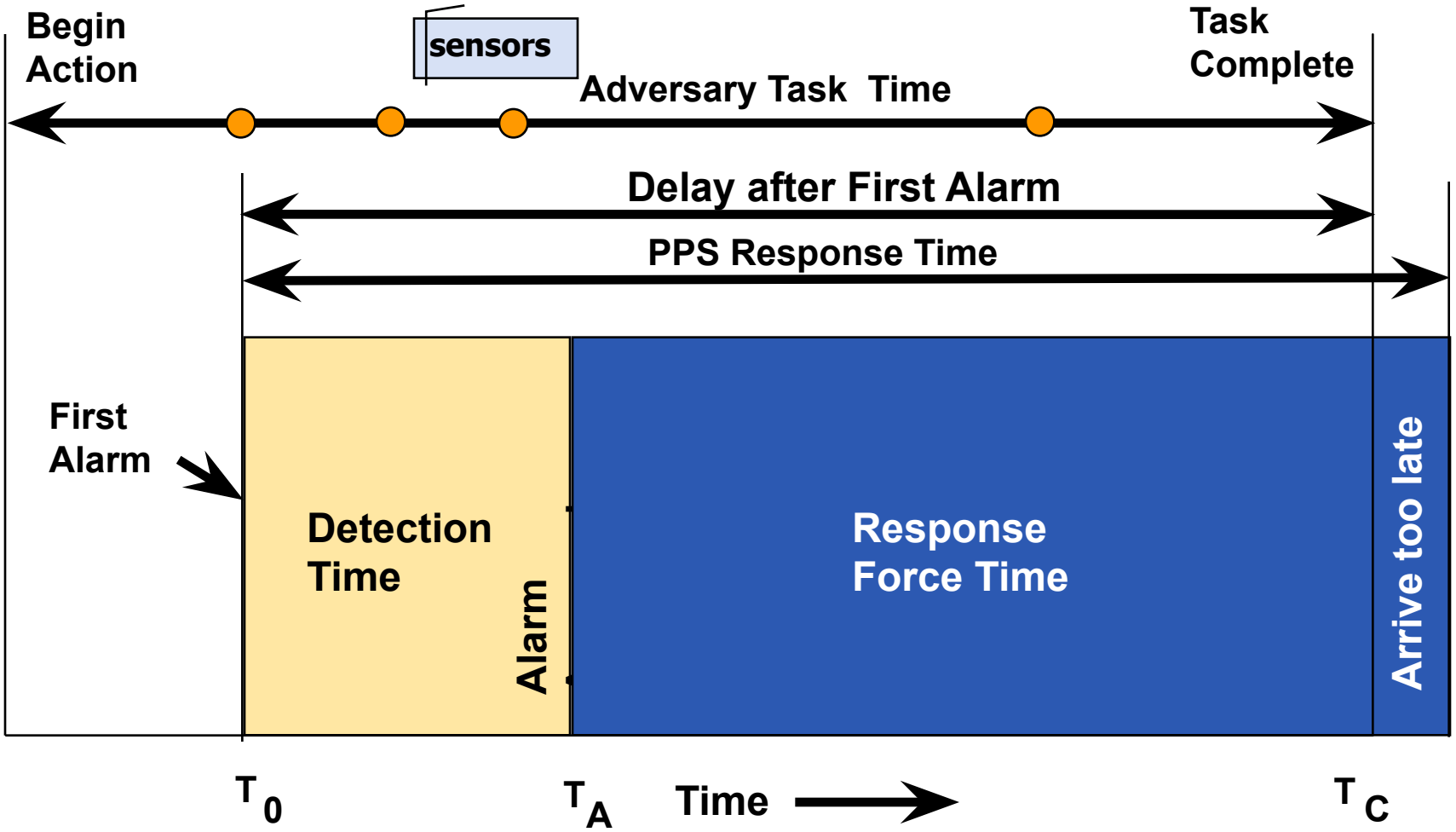
Late Detection



Insufficient Delay



Slow Response



Принципы построения СФЗ.

Направлены на обеспечение способности СФЗ противостоять НСД с учетом перечня угроз и моделей нарушителя.

- Зональное построение;
- Равнопрочность;
- Обеспечение надёжности и живучести;
- Адаптивность;
- Регулярность контроля функционирования;
- Адекватность.

Зональное построение

Защищенная зона - территория объекта. Окружена физическими барьерами. Постоянно охраняется. Доступ ограничивается и контролируется.

Внутренняя зона - **охраняемая зона, находящаяся внутри защищенной зоны объекта**.

Особо важная зона - охраняемая зона, находящаяся во внутренней зоне.

Правило двух (трех) лиц...

КП П

КП П

КП П

Принципы построения СФЗ.

- Зональное построение;
- Равнопрочность;
- Обеспечение надёжности и живучести;
- Адаптивность;
- Регулярность контроля функционирования;
- Адекватность.

Равнопрочность

- Состоит в обеспечении требуемого уровня эффективности СФЗ для всех выявленных в процессе анализа уязвимости типов нарушителей, способов совершения НСД и маршрутов движения;
- Уровень эффективности СФЗ должен уточняться при создании и совершенствоании СФЗ с учетом категории ЯО и критерия «эффективность-стоимость».
- Равнопрочность должна обеспечиваться по всему периметру охраняемой зоны, включая контролируемые проходы и КПП.

Принципы построения СФЗ.

- Зональное построение;
- Равнопрочность;
- Обеспечение надёжности и живучести;
- Адаптивность;
- Регулярность контроля функционирования;
- Адекватность.

Обеспечение надежности и живучести

- СФЗ должна быть способна выполнять задачи в штатных и чрезвычайных ситуациях;
- В составе комплекса ИТСФЗ необходимо выделять группы технических средств отдельных охраняемых зон. Для управления этими группами должны организовываться локальные ПУ;
- Должно быть организовано резервирование элементов СФЗ, в т.ч. компенсационными мероприятиями.

Принципы построения СФЗ.

- Зональное построение;
- Равнопрочность;
- Обеспечение надёжности и живучести;
- Адаптивность;
- Регулярность контроля функционирования;
- Адекватность.

Адаптивность

- СФЗ должна иметь возможность адаптироваться к изменениям:
  - Угроз и моделей нарушителя;
  - В кофигурации объекта и границ охраняемых зон;
  - Видов и способов охраны;
  - Размещения ПФЗ.
- Создание дополнительных рубежей;
- Различные способы постановки и снятия с охраны;
- Не должны создаваться препятствия функционированию ЯО – адаптивность к технологическим особенностям ЯО.

Принципы построения СФЗ.

- Зональное построение;
- Равнопрочность;
- Обеспечение надёжности и живучести;
- Адаптивность;
- Регулярность контроля функционирования;
- Адекватность.

Регулярность контроля функционирования

- Проведение учений и проверок;
- Оценка эффективности;
- Постоянный дистанционный контроль состояния и работоспособности технических средств.

Принципы построения СФЗ.

- Зональное построение;
- Равнопрочность;
- Обеспечение надёжности и живучести;
- Адаптивность;
- Регулярность контроля функционирования;
- Адекватность.

Адекватность

- Принятые на ЯОО организационные, административные и технические мероприятия должны соответствовать принятым угрозам и моделям нарушителя.
- Обеспечивается:
  - Проведением анализа уязвимости;
  - Категорированием ЯО, ПФЗ;
  - Выбором структуры и состава ИТСФЗ;
  - Определением способов охраны и обороны;
  - Проведением оценки эффективности;
  - Возможностью применения компенсационных мер.