Нов български университет

Сигурност в системите за управление на технологични процеси

Доц. Д-р Емил Стоилов

Департамент по Информатика на НБУ

София, май 2010

Съдържание

1. Кратък преглед на системите за управление на технологични процеси 3
   1.1 Действие на ICS 5
   1.2 Основни управляващи компоненти на ICS 6
   1.3 Мрежови компоненти на ICS 7
   1.4 SCADA системи 8
   1.5 DCS системи 10
   1.6 PLC системи 12
2. Различия между ICS и IT системите 13
3. Митове за сигурността в ICS 18
4. Заплахи и уязвимост на ICS системите 20
   4.1 Възможни заплахи за системите 20
   4.2 Потенциални пропуски в защитата на ICS. 21
      4.2.1 Пропуски в системата на политиките и процедурите 22
      4.2.2 Пропуски в хардуера и софтуера на ICS 23
      4.2.2.1 Пропуски в конфигурирането на ICS 23
      4.2.2.2 Пропуски в хардуера на ICS 24
      4.2.2.3 Пропуски в софтуера на ICS 25
      4.2.3 Пропуски в мрежите на ICS 26
         4.2.3.1 Пропуски в мрежовата конфигурация 26
         4.2.3.2 Пропуски в мрежовия хардуер 27
         4.2.3.3 Пропуски в периметъра на мрежата 27
      4.2.3.4 Пропуски в комуникационната система 28
      4.2.3.5 Пропуски в безжичните връзки 28
   4.3 Рискови фактори 29
5. Мрежова архитектура 30
   5.1 Свързване на полева мрежа с Интернет 30
      5.1.1 Тунелиране на протоколи 32
      5.1.2 Шлюзове (Gateways) 35
   5.2 Ethernet и възможност за работа в реално време 37
      5.2.1 Защо се стремим да използваме Ethernet като полева мрежа? 37
      5.2.2 Как да направим Ethernet подходящ за работа в реално време? 38
   5.3 Защитни стени (Firewalls) 39
   5.4 Логическо разделяне на управляващата мрежа. 43
      5.4.1 Защитна стена между корпоративната мрежа и управляващата мрежа 44
      5.4.2 Защитна стена и маршрутизатор между корпоративната мрежа и управляващата мрежа 45
      5.4.3 Защитна стена с демилитаризирана зона между корпоративната и управляващата мрежи 45
      5.4.4 Двойка защитни стени между корпоративната и управляващата мрежи 47
   5.5 Архитектура за ешелонирана защита (Defense-in-Depth Architecture) 48
   5.6 Основни политики реализирани със защитните стени на ICS 49
   5.7 Специфични въпроси при ICS защитните стени 51
      5.7.1 Сървъри за регистриране на събитията 51
      5.7.2 Отдалечен достъп до управляващата мрежа 51
   6. Литература 52

1. Кратък преглед на системите за управление на технологични процеси

Системите за управление в някои важни производствени отрасли са известни под общото наименование системи за управление на технологични процеси (Industrial Control Systems – ICS). Такива системи за управление обикновено се използват в производството на електроенергия, в управлението на водните системи, химическата индустрия, транспорта, както и в експерименталните и изследователски съоръжения на ядрените лаборатории. Те са от решаващо значение за правилното и надеждно функциониране на критично важни инфраструктури, които изцяло зависят от вградените в ICS компютърни системи. Критичната инфраструктура включва телекомуникациите, транспорта, енергетиката, банковото дело, финансите, водните ресурси, аварийните служби, селското стопанство, и други основни системи и услуги, които са от критично значение за сигурността, икономическия просперитет и социалното благоденствие на обществото. Критичната инфраструктура се характеризира със зависимости (физически, психически, географски и логически) и със сложност (множество от взаимно въздействащи се компоненти). Кибернетичните взаимозависимости са резултат от широко разпространената компютризацията и автоматизацията на инфраструктурите [1]. Смущения в критична инфраструктура могат пряко или косвено да засегнат други инфраструктури, да въздействат върху цели географски райони и да се отразят на националната икономика.

Макар ICS системите да имат много общи характеристики, те в значителна степен се различават помежду си. Условно можем да ги разделим на три главни групи [2]:

- Системи за събиране на данни, наблюдение и управление (Supervisory Control and Data Acquisition – SCADA)
- Разпределени системи за управление (Distributed Control Systems – DCS)
- Други управляващи системни конфигурации, изградени с програмируеми логически контролери (Programmable Logic Controllers – PLC).

В този раздел е направен преглед на SCADA, DCS и PLC системите, като са разгледани техни типични архитектури и компоненти. Представените схеми описват мрежови връзки и компоненти, които обикновено се срещат при всяка система, като целта е да се улесни разбирането на действието на тези системи. Реалните приложения на ICS могат да бъдат хибридни и разграничителната линия между SCADA и DCS системите да бъде размита, като са включени атрибути и на двете системи. Схемите в този раздел не са защитени ICS. Въпросите за сигурността и контрола на сигурността ще бъдат разгледани в следващите раздели.

SCADA системите са силно разпределени системи, които се използват за управление на географски отдалечени обекти. Тези обекти понякога са разпръснати на хиляди квадратни километри. Целта на системата е централизирано да събира данни за обектите, да обработва тази информация и да генерира управляващи въздействия. Типичните области на приложение на SCADA системите са железопътния транспорт, електропреносната мрежа, газопроводите и нефтопроводите, системата за разпределение на водните ресурси и др. В контролния център на SCADA системата се извършва централизирано наблюдение и контрол на състоянието на обектите и обработката на алармите, като информацията се предава по компютърна мрежа покриваща големи разстояния. На

базата на получената информация от отдалечените станции, автоматично или чрез оператор, се изработват управляващи команди, които се изпращат обратно към отдалечените устройства, често наричани полеви устройства. Полевите устройства извършват локални действия, като отваряне и затваряне на клапани и прекъсвачи, събиране на данни от сензорните системи и наблюдение за алармени състояния на околната среда.

DCS системите се използват в петролните рафинерии, в електроцентралите, в заводите на химическата, хранително-вкусовата и фармацевтичната промишлености, както и автомобилостроенето и други производства. Тези системи обикновено са на две нива. На долното ниво отделните подсистеми извършват локално управление и контрол на обектите, като се използват регулатори поддържащи процеса в границите на зададени от горното ниво стойности. Регулаторите обикновено са PID (с пропорционално, интегриращо и диференциращо действие) и най често са реализирани като PLC устройства. Настройката на тези устройства се извършва от горното ниво, което е отговорно за координацията на връзките между отделните подсистеми и за цялостната оптимизация на производството. Поради сравнителната близост на отделните подсистеми като комуникационна система обикновено се използват специализирани локални мрежи.

PLC са микропроцесорни устройства, които директно контролират промишлените съоръжения и процеси. С тези устройства е реализирана връзката към обектите във всички SCADA и DSC системи. Те често са и основни компоненти в по-малките системи за оперативно управление на дискретни системи, като например поточните линии в автомобилостроенето. PLC намират широко приложение в автоматизацията на всички промишлени процеси, както в непрекъснатите производства, така и в дискретните производства [3]. И двата вида производства (непрекъснати и дискретни) използват едни и същи системи за управление, сензори и мрежи. Понякога имаме и хибридни системи, със свойства характерни и за двата вида.

Въпреки че използват почти едни и същи структурни елементи, между отделните системи за управление съществуват и определени различия. За разлика от SCADA системите, където обектите са географски разпръснати, при DSC и PLC обектите са разположени в ограниченото пространство на един завод. Затова при тях в комуникациите се използват технологиите на локалните мрежи (Local Area Network – LAN), които обикновено са по-бързи и по-надеждни в сравнение с глобалните връзки, използвани в SCADA системите. В действителност SCADA системите са така проектирани, че да разрешават проблемите възникнали от закъсненията и загуба на данни, породени от различните използвани отдалечени връзки. При DSC и PLC системите се използват в по-голяма степен затворени контури с обратна връзка и управлението на производствения процес е много по-сложно отколкото в SCADA системите.

Тези различия могат да изглеждат твърде рафинирани за целта на това изследване, която е прилагането на IT технологии за сигурност в такива системи. Затова към SCADA, DSC и PLC системите ще се обръщаме по-нататък в текста с общото им наименование ICS, освен когато изрично не е подчертано друго (например полево устройство използвано в SCADA система).

1.1 Действие на ICS

За връзка на ICS с обекта на управление обикновено служи контролер (регулатор), както това е показано на Фиг.1. Представената схема е класическа и може да се намери във всеки учебник по автоматика. Поместването и тук е само с цел за изясняване на процеса.

Фиг.1 Свързване на контролера към управлявания процес

Ключовите елементи в схемата на Фиг.1 са следните:

- *Управляващ контур*. Управляващият контур представлява затворена верига включваща самият управляван процес, датчик за измерване състоянието на процеса, управляващо устройство (например PLC) и изпълнителен механизъм (например клапа, прекъсвач, превключвател). Контролираната променлива величина се измерва от датчика, предава се на контролера, който я интерпретира и сравнява с предварително зададена стойност, след което изработва управляващ сигнал за изпълнителния механизъм, за да може той да коригира стойността на тази величина. Тъй като процесът е под въздействието на външни смущения, управляващият контур работи непрекъснато.

- *Интерфейс човек-машина. (Human-Machine Interface – HMI)*. Операторите и инженерите използват HMI за да наблюдават процеса, да коригират настройките и параметрите на контролера и евентуално да променят алгоритмите за управление.

Чрез този интерфейс те имат достъп до информация за текущото състояние на процеса, както и до изменението на това състояние във времето.

- *Отдалечена диагностика и поддръжка*. Процедурите за отдалечена диагностика и поддръжка се използват за идентифициране, предотвратяване и отстраняване на повреди в управляващото оборудване.

За да поддържа функционирането на управляващите контури, HMI и отдалечената диагностика, една ICS система има съответно изградена многослойна мрежова архитектура и набор от мрежови протоколи. Много често локалните управляващи контури са каскадно свързани, като изходящите величини на един контур са входящи в друг. Тези величини се изчисляват на второто ниво на ICS като се организират управляващи контури от второ ниво. Характерно за всички контури в системата е, че те работят непрекъснато и цикълът на промяна на величините в тях варира от милисекунди до минути.

1.2 Основни управляващи компоненти на ICS

По-долу са описани функциите на основните управляващи компоненти на ICS:

- *Управляващ сървър (Control Server)*. В управляващия сървър се намира DSC или PLC софтуера, който е проектиран да комуникира с управляващите устройства на долното ниво на системата. Този софтуер има достъп до подчинените му модули по ICS мрежата.

- *SCADA сървър или главно терминално устройство (SCADA server, Master Terminal Unit – MTU)*. Това устройство управлява обмена на информация в цялата SCADA система. Отдалечените терминални възли, както и PLC устройствата разположени в терена, играят подчинена роля (slaves).

- *Отдалечен терминален възел (Remote Terminal Unit – RTU)*. Отдалеченият терминален възел е специално проектиран да събира информация и да управлява отдалечените SCADA станции. Това е полево устройство, обикновено снабдено с безжичен радио интерфейс и се използва в случаите, когато нямаме възможност за кабелна комуникация. Понякога контролерите PLC имат вградени функции на RTU и се използват като полеви устройства; в тези случаи те просто ще бъдат наричани RTU.

- *Програмируем логически контролер (PLC)*. PLC е микропроцесорно устройство (индустриален компютър), първоначално проектирано да извършва прости логически функции и да управлява електрически вериги (релета, превключватели, броячи). С развитието на изчислителната му мощност, PLC има вече възможност да управлява много по-сложни процеси и се превърна в основен елемент на SCADA и DSC системите. Съществуват и други устройства които се използват в терена, и които не са PLC, например регулатори и RTU. Те имат подобни управляващи функции, но са проектирани за специални приложения. В SCADA системите PLC често се използват като полеви устройства, понеже са по-икономични и с възможност за по-гъвкаво конфигуриране, отколкото RTU със специално предназначение.

- *Интелигентно електронно устройство (Intelligent Electronic Device - IED)*. IED е „умен" възел, състоящ се от датчик и изпълнителен механизъм, който възел събира данни, комуникира с други устройства, извършва обработка на събраните данни и локално управлява. В едно такова устройство могат да се намират например аналогов датчик, аналогов изход за изпълнителния механизъм, комуникационен модул и програмируема памет. В SCADA и DSC системите тези устройства се използват за автоматично регулиране на локално ниво.

- *Интерфейс човек-машина (HMI)*. HMI представлява софтуер и хардуер, който позволява на операторите да наблюдават управлявания процес, да променят настройките в него с цел оптимизация, а в извънредни ситуации да изключат автоматиката и да преминат към ръчно управление на процеса. HMI позволява на инженерите и операторите да променят зададени стойности и параметри, както и управляващите алгоритми на контролерите. HMI визуализира информация за състоянието на процеса, показва трендове на променливи, статистика, отчети и друга информация от която се нуждаят операторите, администраторите, мениджърите, бизнес партньорите, и другите упълномощени потребители. Мястото, платформата и самият интерфейс могат да бъдат най-различни в зависимост от приложенията. Например HMI е различен в контролния център, в лаптопа свързан безжично в локалната мрежа или в браузъра на всяка система свързана към Интернет.

- *Сървър за регистриране на събитията (Data Historian)*. Сървърът за регистриране на събитията представлява централизирана база данни, в която се записва цялата информация за процесите в ICS. Тази информация се използва за различни анализи, от статистически справки до планиране на корпоративно ниво.

- *Входно/Изходен сървър (I/O Server)*. I/O сървърът е компонент на управлението, който е отговорен за събирането, буферирането и достъпа до информация за процеса, която информация постъпва от подсистемите като PLC, RTU и IED. Физически този сървър може да се намира при управляващия сървър или на отделен компютър, използвайки отделна платформа. Сървърът взаимодейства с другите компоненти на управляващата система, като HMI и управляващия сървър.

1.3 Мрежови компоненти на ICS

На всяко ниво в йерархически изградената ICS има различни изисквания към компютърната мрежа. Използваните мрежови топологии в ICS системите могат в значителна степен да се различават от топологиите в модерните системи, използващи Интернет технологии и стратегии за корпоративна интеграция. Свързването на ICS мрежите с корпоративните мрежи позволява на управляващите процеса инженери да имат достъп до него от разстояние, без да се намират в управляващите зали. Ръководителите на корпоративно ниво също имат пряк достъп до данните за управляваните технологични процеси. По-долу са описани основните мрежови компоненти на една ICS, независимо от това какви топологии са използвани.

- *Полева (серийна) магистрала (Fieldbus)*. Полевата серийна магистрала свързва сензорите и другите полеви устройства към PLC, както и към други видове контролери. Използването на такава магистрала елиминира необходимостта от свързване от типа точка-точка по кабел PLC контролера с всяко едно полево

устройство. Сензорите комуникират с контролерите по Fieldbus използвайки специално създадени за целта протоколи.

- *Управляваща мрежа (Control Network).* Управляващата мрежа свързва горното (надзорно) ниво на управлението с управляващите модули на долното ниво.

- *Комуникационни маршрутизатори (Communications Routers)*. Маршрутизаторите са мрежови устройства, които прехвърлят информация между две мрежи. Такива устройства се използват в глобалните мрежи (Wide Area Network – WAN) или за връзка между LAN и WAN. В SCADA системите също се срещат, най-често при свързването на MTU и RTU.

- *Защитни стени (Firewalls)*. Защитните стени предпазват устройствата в една мрежа като наблюдават и контролират получаваните пакети да бъдат в съответствие с предварително избрана политика на филтриране. Те се използват в ICS системите за реализиране на стратегиите за разделяне и изолиране на отделни подмрежи.

- *Модеми (Modems)*. Модемите са устройства, които преобразуват серийните цифрови сигнали в сигнали подходящи за предаване по телефонна линия и обратно. Те често се използват в SCADA системите за серийна връзка между MTU и отдалечените полеви устройства. Чрез тях може да се получи и отдалечен достъп до SCADA, DSC и PLC системите. Този отдалечен достъп може да се използва за прихващане на управлението на такива системи, т.е. до промяна на управляващи параметри, както и за диагностични цели.

- *Точки за отдалечен достъп (Remote Access Points)*. Точките за отдалечен достъп са специални устройства разположени в отделни области на управляващата мрежа, позволяващи отдалечено свързване към нея. За примери тук могат да служат модемите за отдалечен достъп, както и безжичните точки за достъп към мрежата, които се използват за свързване на преносими компютри към нея.

1.4 SCADA системи

SCADA е система за автоматизация на процеси, която се използва за събиране на данни от сензори и други инструменти, намиращи се на значителни разстояния, и предаването на тези данни към едно централно място за целите на наблюдението и управлението на цялостния процес. Събраните данни се наблюдават на един или повече компютъра в управляващ център. На базата на събраната информация от отдалечените станции, автоматично или чрез оператор се генерират управляващи команди за отдалечените управляващи устройства, които често се наричат и полеви устройства.

Като цяло, една SCADA система включва следните компоненти:

- Полеви инструменти измерващи стойностите на различните величини на управлявания процес.

- Работно оборудване, свързано с тези инструменти.

- Локални управляващи устройства, които комуникират с полевите инструменти и работното оборудване и събират данните за процеса. Това са PLC, RTU, IED и различни регулатори (Process Automation Controller – PAC).

- Локална серийна магистрала (Fieldbus), свързваща локалните управляващи устройства с полевите инструменти и работното оборудване.

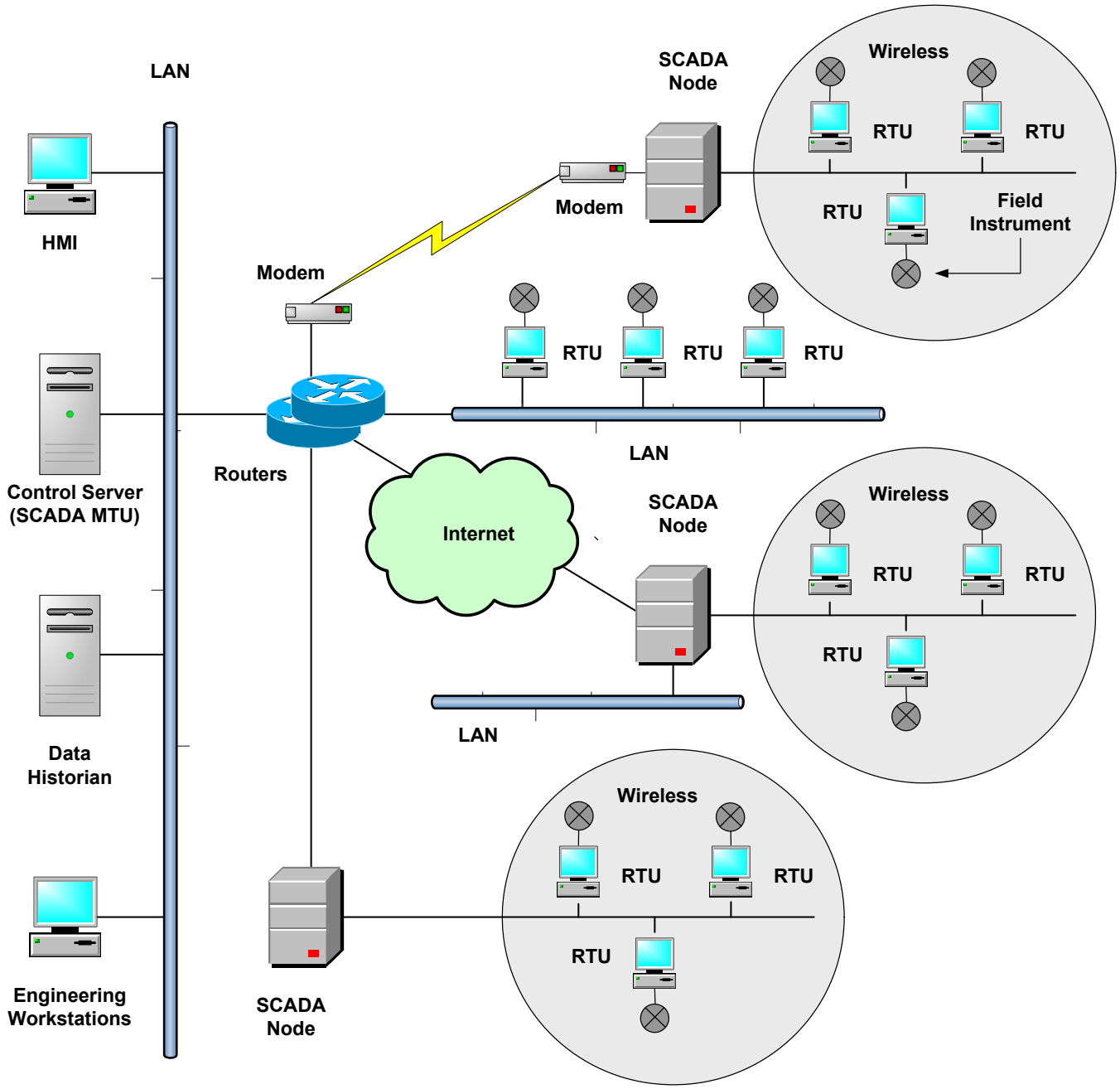
- Компютри в управляващия център, в които се съхраняват базите данни, на екраните на които се наблюдава процеса и където се изработват управляващите команди. Това са MTU, HMI, Data Historian, I/O Server, както и компютри с други, специфични функции.

- Комуникационна мрежа за предаване на дълги разстояния, свързваща RTU с MTU, използваща кабелни или безжични връзки.

На Фиг.2 е представена архитектурата на една интегрирана SCADA система, като е показано мястото на отделните елементи и връзките между тях. Схемата е най-обща, повече подробности могат да бъдат намерени например в [2}, където са разгледани различни топологии и схеми.

SCADA архитектурата поддържа TCP, UDP и други IP-базирани комуникационни протоколи, специализирани индустриални комуникационни протоколи като Profibus, Modbus TCP, Modbus над TCP или UDP [4] [5] [6], както и всякакви протоколи на радио, клетъчни и сателитни мрежи. В сложните SCADA системи срещаме голямо разнообразие от кабелни (телефонни линии с набиране, наети телефонни линии, оптични кабели, ADSL) и безжични (лицензирани радио канали, безжични локални мрежи – WLAN, клетъчни и сателитни връзки) преносни среди. Изборът зависи от редица фактори, които характеризират съществуващата комуникационна инфраструктура. Такива са например достъпните комуникации до отдалечените обекти, скоростите на предаване, бюджетът с който разполагаме, необходимостта от задоволяване на бъдещи потребности и т.н. Всички тези фактори влияят върху решението за избор на SCADA архитектурата. В реалния сват SCADA системите могат да следят и контролират от стотици до стотици хиляди входно/изходни точки като се използват голям брой I/O канали със скорости от 100 Kbps до близо 1 Mbps.

SCADA системите се развиха много бързо от специализирани хардуерно/софтуерни системи през 70-те години на миналия век до съвременните системи, които включват стандартни персонални компютри и операционни системи, TCP/IP комуникации, използване на Интернет като транспортна среда и др. С това възникнаха и нови проблеми свързани със сигурността на данните. В миналото тези системи бяха изолирани от останалите системи използващи информационни технологии (Information Technology – IT). Свързването им към Интернет е сравнително отскоро (началото на 1990 година) и е спорно сред специалистите. Много от тях смятат, че това не е добра идея. Независимо от това обаче, дори без връзката към Интернет, тези системи остават уязвими на вътрешни и външни атаки, при които се използва уязвимостта на стандартния софтуер (операционни системи, база данни, фирмени приложения).



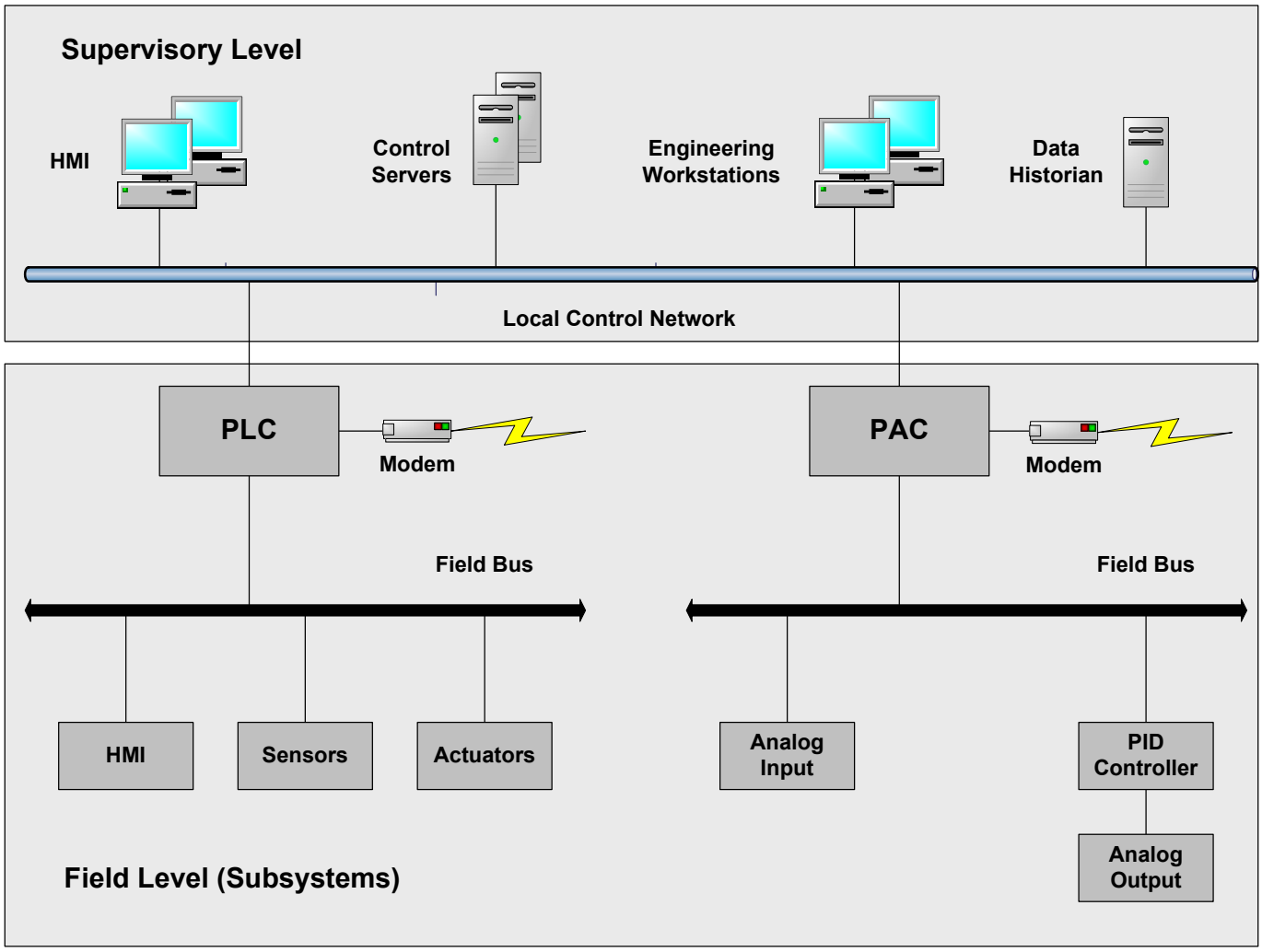
Фиг.2 Архитектура на интегрирана SCADA система

1.5 DCS системи

DCS се използват за управление на производствени процеси намиращи се в географска близост един до друг, като например в нефтопреработвателни заводи, електрически централи, химически и фармацевтични поточни линии. Управляваните производства са както непрекъснати, така и дискретни. Обикновено управляващата DCS е на две нива. На горното ниво се извършва координиране на действията на отделните управляващи подсистеми и оптимизация на цялостния процес [7]. На долното ниво са управляващите подсистеми, които се грижат за поддържане на зададените параметри в определените им граници. Такова разбиване на подсистеми намалява значително влиянието на възникнали грешки в една подсистема върху цялата система. В много съвременни приложения DCS

са свързани с корпоративната мрежа с цел наблюдение на производството, изготвяне на икономически анализи и доклади, както и за вземане на управленски решения в реално време.

На Фиг.3 са показани елементите на една примерна DCS система и тяхното свързване. Горното надзорно ниво (Supervisory Level) комуникира с контролерите намиращи се на долното ниво (Field Level) посредством локалната управляваща мрежа (Local Control Network). По нея управляващите сървъри отправят искания за данни и изпращат команди към разпределените контролери. Тези контролери пък от своя страна управляват изпълнителните механизми въз основа на получените от сървърите команди и на стойностите на измерените от сензорите величини.



Фиг.3 Архитектура на DCS система

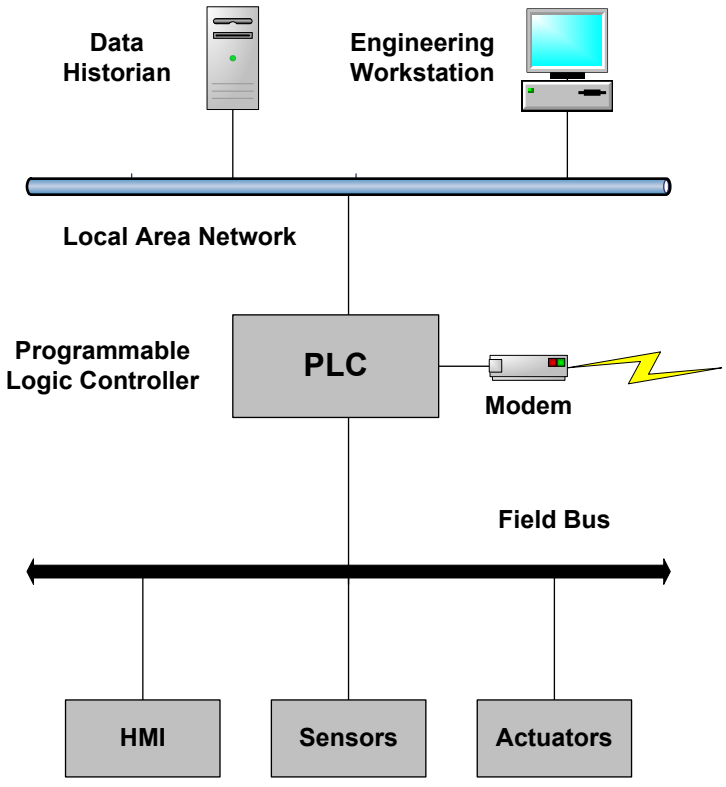
Управляващите процеса PLC могат да бъдат свързани с датчиците и изпълнителните механизми директно с кабели или като се използва полева магистрала. Възможни са много различни конфигурации. Например в показаната на Фиг.3 конфигурация PID регулаторът получава измерваната в процеса стойност по полевата магистрала и директно управлява изпълнителния механизъм, докато от PAC получава само зададената стойност [8]. Полевите магистрали елиминират необходимостта от окабеляване точка –

точка между всички елементи участващи в процеса на ниско ниво (датчици, регулатори, изпълнителни механизми). Освен това те позволяват по-голяма функционалност, включително диагностика в реално време и изпълнение на някои алгоритми, при което PLC не участват пряко във всяко действие. В управляващите мрежи и полевите магистрали се използват стандартизирани индустриални комуникационни протоколи, разработени от такива групи като Modbus и Fieldbus [6].

Освен двете показани на Фиг. 3 нива, могат да съществуват и други, междинни нива на управление. Например при по-големи DSC може да има нива за наблюдение на отделните подсистеми (цехове или поточни линии).

1.6 PLC системи

Програмируемите логически контролери се използват както в SCADA, така и в DCS системите като елементи от ниско ниво на йерархическата система, осигуряващи управляващи функции на това ниво и обратна връзка от процеса. При SCADA системите те предоставят същата функционалност, както RTU. В DCS системите PLC се използват като органи на местно управление, и работят под надзора на горните нива. Те могат да се използват и като елемент в малки самостоятелни конфигурации, където изпълняват главната роля (Фиг. 4).



Фиг.4 Малка управляваща система използваща PLC

PLC имат потребителска програмируема памет, в която да се съхраняват инструкции за изпълнение на конкретни функции, като входно/изходни операции за управление, логически функции, отчитане на времеинтервали, PID регулатори, аритметика, обработка и съхраняване на данни. В показаната на Фиг. 4 система управлението на

производствения процес се извършва от един PLC контролер с използване на полева магистрала. Достъпът до PLC става чрез програмен интерфейс намиращ се в работната станция, а данните се съхраняват в сървъра за регистриране на събитията. Трите устройства са свързани в локална мрежа.

2. Различия между ICS и IT системите

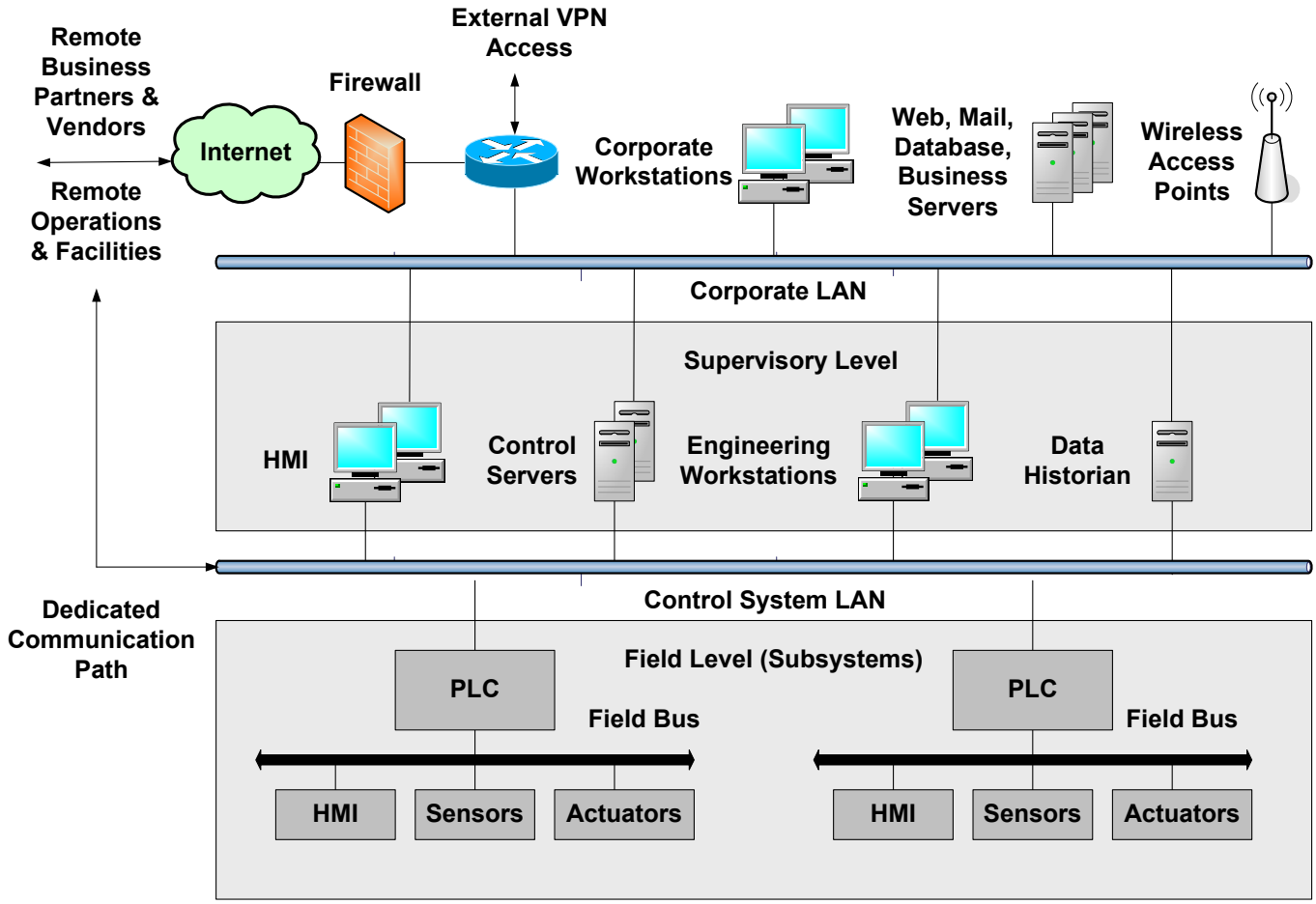
В миналото ICS системите бяха изградени от специално разработени хардуер, софтуер и мрежови протоколи. По този начин се осигуряваше отделянето на функциите по наблюдение и контрол от влиянието на външно свързаните към ICS компютърни мрежи. Акцентът беше поставен върху физическото разделяне на мрежите, и много малко внимание се отделяше на въпросите за сигурността на данните в процеса на проектирането. Предполагаше се, че данните са защитени, защото не са достъпни. Физическата сигурност (охрана, заключени врати, ограждания) беше основният метод осигуряващ достъпа до тези критично важни данни. С течение на времето разпространението на Интернет промени този модел. Много промишлени производства, включително и комуналните услуги, сега се възползват от наличието и гъвкавостта която предлагат обществените мрежи.

Връзката с Интернет предлага много удобства, включително отдалечен достъп и управление на системите, увеличение на производителността чрез използване на вериги за доставка и аутсорсинг, достъп до централизирани бази данни, използване на връзките между частните и обществени мрежи за търговски обмен. Значително се увеличи разнообразието и обемът на дейностите несвързани пряко с производството. Регулаторната рамка беше променена, нарасна броя на изискваните отчети и доклади, в администрацията стана задължително използването на стандартизиран софтуер. Корпоративното планиране и счетоводството се нуждаят от една страна от достъп до ресурсите на мрежата на ICS, а от друга страна използват достъпа до външни мрежи за сътрудничество с други фирми и актуализации на базите данни. Тези административни, комуникационни и други интерфейси представляват риск, за който мрежите на ICS не са проектирани. Това налага предприемането на нови ефективни мерки за опазване на сигурността на данните.

Особено незащитени са SCADA системите. В миналото техните мрежи бяха напълно отделени и използваха патентовани управляващи протоколи за работа със специализиран софтуер и хардуер. Впоследствие TCP/IP базираните системи започнаха все повече да се използват и намериха своето приложение в SCADA среда. Използването на новите информационни технологии (Information Technologies – IT) ни осигурява по-добра връзка и по добри възможности за отдалечен достъп. SCADA системите са високо ефективни и широко разпространени. Това прави техните мрежи потенциално уязвими към прекъсване на услугата, пренасочване на процеси и манипулиране на оперативни данни, което може да доведе до нарушения на обществената безопасност и смущения в доставките в критично важни инфраструктури.

Сближаването на техническото развитие, правителствените разпореждания и подобряването на производителността води до „отваряне" на инфраструктурата на системата за управление и увеличение на рисковете свързани с нейното използване.

На Фиг. 5 е представено едно възможно свързване на IT и ICS мрежите в една DCS система.



Фиг. 5 Свързване на DCS и IT системите в едно предприятие.

ICS системите имат много характеристики, които ги отличават съществено от традиционните IT системи, например съществуващите в тях рискове и възприетите приоритети. В някои ICS системи има значителен риск за здравето и безопасността на човешкия живот, за нанасяне на сериозни щети на околната среда, както и за сериозни финансови и производствени загуби. Изискванията за производителност и надеждност са различни. Използват се операционни системи и приложения които са необичайни за типичния IT поддържащ персонал. В резултат ICS и IT системите имат различни оперативни (и риск) профили:

- В една типична IT система поверителността на данните и тяхната непокътнатост обикновено са от основно значение. В ICS системите приоритет е устойчивостта на отказ в оборудването, водещ до застрашаване безопасността на човешкия живот и на общественото здраве, до разрушаване на инсталации, загуба на интелектуална собственост или повреждане на продукцията.

- Сигурността в IT системата е фокусирана върху защитата на работоспособността на IT активите и на информацията, съхранявана или предавана между тези активи. В някои конфигурации централно запазената и обработвана информация е критично важна и тя трябва да бъде по-добре защитена. При ICS крайните устройства (например PLC, операторските станции и контролери) трябва да бъдат старателно защитени, тъй като те са пряко отговорни за управлението на процеса.

- В управляващите системи времето за реакция е съществен фактор. Критериите за допустимо забавяне са продиктувани от конкретните инсталации. За Разлика от IT системите, в ICS не се преследва висока производителност и пропускателна способност на мрежата.

- Много ICS процеси са непрекъснати по своята природа, т.е. те изискват непрекъсната наличност на суровините. Неочаквано прекъсване на функционирането на управляващите системи в тях е неприемливо. Прекъсванията трябва да бъдат планирани с дни и седмици по-рано. Преди пускането на инсталацията се извършва предварително тестване за да се гарантира висока надеждност. В допълнение при неочаквани прекъсвания много управляващи системи не могат лесно да бъдат спрени и стартирани отново без това да доведе до унищожение или повреда на продукцията. В резултат използването на типични IT стратегии, като рестартиране на компютър, са обикновено неприемливи поради изискванията за висока надеждност, достъпност и възможност за поддръжка на ICS.

- Операционните системи и приложения използвани в ICS могат да не допускат обикновено използваните IT практики за сигурност. Унаследените ICS системи са особено уязвими от към достъпност на ресурси и временни задръжки. Управляващите мрежи често са по-сложни и изискват по-голям опит (например те се управляват от инженери, а не от IT персонал). Софтуерът и хардуерът трудно се поддават на усъвършенствания и надстройка. Много управляващи системи нямат вградени функции за защита като криптиране, регистриране на грешките и използване на пароли.

- Изчислителните ресурси на ICS (включително производителността на процесорите, обемите памет и операционните системи за работа в реално време) са много ограничени, и са проектирани така, че максимално да бъдат използвани за нуждите на управлението. Поради тази причина няма почти никаква възможност за включване на допълнителен софтуер за сигурност (като антивирусни програми, програми за откриване и блокиране на нарушители и др.). Срещат се и трудности с лицензите. Инсталирането на такива допълнителни програми без одобрението на производителя обикновено води до загуба на поддръжката от негова страна.

- Комуникационните протоколи и кабелите използвани в полевите магистрали на ICS системите обикновено са доста различни от тези, използвани в IT системите и често са специализирани и патентовани.

- IT компонентите имат продължителност на живот в границите от 3 до 5 години поради бързото развитие на технологията. При ICS, където технологията е разработвана специално за конкретните нужди на завода, жизненият цикъл често е от порядъка на 15 – 20 години, а понякога е и по-дълъг.

- Контролът за достъп към IT системите може да се осъществява без да се взема предвид връзката с потока от данни в дадения момент. При някои ICS системи, времето за отговор на системата при заявка от страна на оператора може да бъде критично. Така например, изискването на пароли за автентикация и авторизация не трябва да спира спешните действия към ICS. Информационният поток не трябва да бъде прекъсван и ограничаван от тежки физически проверки за сигурност.

- Обикновено в IT системите няма физическо взаимодействие с околната среда. При ICS съществуват много сложни взаимодействия между управляващите сигнали и физическото обкръжение. Поради тази причина всички функции по сигурността в ICS трябва да бъдат много строго тествани на самия обект, не само в лабораториите на производителя.

- Компонентите в IT системите са локални и има лесен достъп до тях. При ICS системите компонентите могат да бъдат отдалечени, изолирани, и да изискват съществени физически усилия за осигуряване на такъв достъп.

В Таблица 1 са резюмирани основните различия между ICS и IT системите засягащи тяхната сигурност [2].

Характеристики	IT системи	ICS системи
Изисквания за производителност	- Системите не работят в реално време. - Необходима е висока производителност. - Допустими са големи забавяния.	- Системите работят в реално време. - Непретенциозни изисквания за производителност. - Времето за отговор е критично. - Големи забавяния са недопустими.
Изисквания за наличност	- Отговори като рестартиране на системата са приемливи. - В зависимост от оперативните изисквания могат да бъдат толерирани кратки интервали на недостъпност на системата.	- Отговори като рестартиране на системата са неприемливи поради изискването за непрекъснат достъп до процеса. - Изискванията за наличност правят неизбежно използването на дублиращи системи. - Престоите трябва да бъдат планирани с дни и седмици предварително. - Необходимо е предварително изчерпателно тестване на извършените промени.
Изисквания за управление на риска	- Поверителността на данните и тяхната цялост е от първостепенно значение. - Устойчивостта на откази не е толкова важна. Моментният престой не е голям риск. - Голям рисков ефект има забавянето на бизнес операциите.	- Безопасността на човешкия живот е от първостепенно значение, след което следва защитата на технологичния процес. - Устойчивостта на откази е от съществено значение; дори и моментно прекъсване може да бъде неприемливо. - Голямо рисково въздействие оказват регулаторните несъответствия, ефектът върху околната среда, загубата на живот, оборудване или продукция.
Фокус на защитата в дадената архитектура	- Основната цел е опазване на IT активите, както и на информацията съхранявана или предавана между тези активи. - Централният сървър може да изисква по-сериозна защита.	- Основната цел е защитата на крайните устройства (PLC, операторски станции и DCS контролери). - Защитата на централния сървър също е от значение.
Непредвидими последици	- Решенията по сигурността са предназначени за типичните, често срещани IT системи.	- Инструментите за сигурност трябва да бъдат предварително тествани (например на подобни ICS системи), за да се гарантира, че те не застрашават нормалното функциониране на ICS.

Характеристики	IT системи	ICS системи
Критични времена за взаимодействие	- Времената за действие в непредвидени ситуации не са критични. - Достъпът до системите може да бъде ограничаван до степента необходима за гарантиране на сигурността.	- В извънредни ситуации отговорът на човека е от решаващо значение. - Достъпът до ICS следва да бъде строго контролиран, но не трябва да пречи или влияе на взаимодействието човек-машина.
Операционни системи	- IT системите са проектирани да използват типични операционни системи. - Процесите на изменения и подобрения в такива операционните системи са ясни и добре дефинирани, тъй че могат да бъдат използвани инструменти за автоматизирано зареждане на промените.	- Използват се различни специализирани операционни системи, често без вградени възможности за защита. - Софтуерните промени трябва да бъдат правени внимателно, обикновено от доставчиците. Използването на специализирани управляващи алгоритми може да изисква допълнителни промени в софтуера и хардуера.
Ограничения на ресурсите	- Системите са снабдени с достатъчно ресурси, за да посрещнат допълнителни приложения, като например програми за сигурност.	- Системите са проектирани за управление на промишлените процеси и могат да нямат достатъчно памет или изчислителни ресурси за да посрещнат допълнителни изисквания за сигурност.
Комуникации	- Стандартни комуникационни протоколи. - Главно кабелни връзки, с локални възможни за безжични връзки. - Стандартни и широко описани IT мрежови практики.	- Множество от фирмени, специализирани и стандартни протоколи. - Различни типове комуникационни връзки, включително наети линии и безжични мрежи (радио и сателитни). - Мрежите са сложни и понякога изискват експертизи от страна на управляващи процесите инженери.
Управление на извършваните промени	- Софтуерните промени се извършват своевременно при наличието на добри политики и процедури за сигурност. Често тези процедури са автоматизирани.	- Софтуерните промени трябва да бъдат старателно предварително тествани и да бъдат въвеждани постепенно в цялата система. - Престоите на ICS са планирани. - В ICS могат да се използват операционни системи, които вече не се поддържат.
Поддръжка на системите	- Възможна е поддръжка от различни фирми, с различен стил на действие.	- Поддръжката обикновено е от производителя на оборудването.
Живот на компонентите	- Продължителността на живота на изграждащите системата компоненти е в границите от 3 до 5 години.	- Продължителността на живота на изграждащите системата компоненти е в границите от 15 до 20 години.
Достъп до компонентите	- Компонентите обикновено са локални и леснодостъпни.	- Компонентите могат да бъдат отдалечени, изолирани, и да изискват съществени физически усилия за осигуряване на достъп до тях.

Таблица 1. Различия между IT и ICS системите

Като резултат от тези различия възниква необходимостта от създаване на нови, по-изтънчени стратегии за кибернетична сигурност. Това може да стане чрез обединение на управляващите ICS инженери, операторите и специалистите по IT сигурност в смесени колективи, където заедно могат да анализират възможните последици от инсталирането, действието и поддръжката на определени решения по сигурността. Значителна част от

този анализ трябва да бъде извършен преди прилагането на тези мерки, тъй като някои от тях със сигурност няма да доведат до очакваните резултати вследствие на различната ICS архитектура.

3. Митове за сигурността в ICS

Преминаването от първа към втора генерация ICS и свързването на тези системи с IT системите, както е показано на Фиг. 5, породи множество митове, които се разпространяват в публичното пространство, и се поддържат дори от някои специалисти.

Организациите по цял свят не желаят да поемат отговорността за собствената си сигурност. Вместо това те обвиняват недостатъците и несигурността на Интернет и поради невежество и погрешни убеждения твърдят, че сигурността е глобален проблем. Поради тази причина всички са виновни, но никога не се намира конкретен виновник. Ще започнем с четири мита, които са по-скоро на философско ниво [9]:

- *Мит първи: Световните лидери са отговорни за безопасността на Интернет.*

Интернет измамите нанасят щети за милиарди долари годишно. Дори компютърните системи на британското правителство са многократно атакувани от чужбина, така че министрите трябва да бъдат или гении в компютърния бранш, или да наемат хакери за защита на държавната тайна. Министър-председателят Гордън Браун дори създаде специална служба за защита на страната от терористични хакерски атаки и електронен шпионаж. Това стана поради опасенията, че компютърните системи на правителството и бизнеса са уязвими по отношение на онлайн атаки от враждебни страни и терористични организации. Полицията пък, и по специално нейното централно бюро за електронни престъпления (Police Central E-Crime Unit), потърси доброволци от IT индустрията за борба срещу престъпленията в кибернетичното пространство. Трябва да бъде казано много ясно: Правителството на Великобритания не разполага с финанси, ресурси и даже компетентност за да направи Интернет безопасно място за всички, които го ползват [9]. Естествено това важи и за всички останали правителства.

- *Мит втори: Имам защитна стена, следователно съм в безопасност*

Защитната стена не дава достатъчна защита поради самия си характер – тя отваря множество врати за потребителите към външния свят, и през тези отворени врати хакерите могат да получат достъп. Системите са проектирани главно да помогнат на потребителите да получат излаз навън от системата и в по-малка степен се обръща внимание на това какво може да премине в обратната посока. Хакерите се възползват от прости грешки в програмирането и от пропуските в сигурността.

- *Мит трети: Ние не извършваме финансови операции, следователно хакерите не се интересуват от нас.*

Защо да давате пари за научно-изследователска и развойна дейност, ако можете да откраднете произведението на някой друг? Кражбата на интелектуална собственост е „невидима” форма на бизнес кражба, в смисъл, че не винаги я осъзнаваме и тя може да мине незабелязано, но това ще струва на организацията много скъпо. За разлика от данните в кредитната карта, които лесно могат до бъдат идентифицирани на по-късен етап като откраднати, загубата на една фирма на информация за проекти, бизнес

планове, стратегии и т.н. може никога да не бъде проследена назад във времето и да доведе до изясняване на случаите.

- *Мит четвърти: Много е трудно да защитя своята система*

Програмистите носят отговорността за тестването на своя софтуер по отношение на неговата сигурност. Грешките могат да бъдат избегнати, като в процеса на създаване на програмния продукт се използват известните практики на сигурно кодиране. Има достъпни онлайн услуги, които ви позволяват да използвате специално разработен тестови софтуер. Това са автоматизирани програмни пакети, които ще извършат анализ на вашата програма на две нива (изходен и двоичен код). Те ще открият уязвимите за сигурността места и ще ви върнат точни и пълни заключения с указания за промените които трябва да направите. Можете също да упълномощите външни разработчици активно да изследват приложенията в тяхната работна среда вместо да закупувате всички необходими тестови установки.

Следват няколко мита, които са по скоро на техническо ниво и засягат архитектурата на изградените системи [10]:

- *Мит пети: ICS системата е сигурна, ако не я свързваме с Интернет*.

От Фиг. 5 непосредствено се вижда, че ICS системата е свързана с външния свят не само чрез Интернет. Връзката към корпоративната IT мрежа, както и използването на отдалечени връзки с модеми също могат да бъдат опасни.

- *Мит шести: Трябва да се фокусираме върху терористите.*

Пример който оборва тази теза. Управляващата мрежа и IT мрежата работят с един и същи протокол – TCP/IP. В управляваща станция са объркани IP адресите на PLC контролер и принтер. Измененията в конфигурационната програма на PLC, вместо да се заредят в контролера, се печатат върху принтера в счетоводството. За управлявания процес това може да има катастрофални последици, принтерът ще блокира или ще печата глупости.

- *Мит седми: Всички лоши момчета са в Интернет.*

Пример на инцидент оборващ тази теза: Инженер в главната квартира на фирмата зарежда програма в DCS графична станция, с която да получи данни директно от обекта. Новата програма претоварва DCS/PLC шлюзовете и операторите губят управлението на процеса.

- *Мит осми: IT отделът се грижи за сигурността на технологичния процес.*

Пример за инцидент: Недоволен служител на фирмата атакува PLC в друга област на завода, като използва полевата магистрала и променя паролата за достъп. Това води до блокиране на поддръжката и до прекратяване на технологичния процес.

- *Мит девети: Хакерите не разбират SCADA и PLC системите*.

Експеримент: Извършва се вътрешно тестване, като се поставя задача на хакер с никакви познания по PLC да разбие системата. Един час след откриване на устройството, всички комуникации към и от PLC са прекъснати.
С описанието на такива митове може да се продължава дълго. Изводът е еднозначен: трябва задълбочено да се изследват уязвимите места на ICS системите.

4. Заплахи и уязвимост в ICS системите

4.1 Възможни заплахи за системите

Както се убедихме от горните примери, заплахите за ICS могат да произлизат както от състезателни източници (враждебна правителствена политика, терористични групи, промишлен шпионаж , недоволни служители, злонамерени натрапници), така и от естествени източници (човешки грешки и инциденти, дефекти в оборудването, природни бедствия). За да бъдат ICS защитени от състезателни заплахи е необходимо да бъде изградена задълбочена стратегия за тяхната защита. По долу са изброени някои от възможните заплахи:

- *Хакери (Attackers).* Хакерите нахлуват в мрежите водени от тръпката на предизвикателството или просто за защита на реномето си в хакерската общност. Отдаленият достъп изисква значителни компютърни умения и познания. Атакуващите обикновено изтеглят скриптове и протоколи от Интернет и заразяват с тях избраните за жертва сайтове. Инструментите за атака стават все по-сложни и все по-лесни за използване. Много от хакерите не разполагат с необходимите качества за атакуване на трудни цели. Независимо от това, в световен мащаб, общността на хакерите представлява относително висока опасност за изолирани или кратковременни смущения с едновременно нанасяне на сериозни щети.

- *Паразитни мрежови оператори (Bot-network operators).* Паразитните мрежови оператори за разлика от хакерите овладяват няколко системи едновременно и извършват координирани атаки за разпространение на схеми за измама (phishing), спам (spam) и злонамерен софтуер (malware).

- *Престъпни групи (Criminal groups).* Специално организирани престъпни групи атакуват системите за парична печалба. Те използват схеми за измама, спам и злонамерен софтуер за извършване на кражба на самоличност и онлайн престъпления. Тези организации също представляват заплаха за големите индустриални страни и фирми със способността си да извършват промишлен шпионаж и парични кражби в големи размери, като за целта наемат талантливи хакери и финансират развитието на техните умения.

- *Терористи (Terrorists).* Терористите се стремят да унищожат, обезвредят или използват критични инфраструктури, с което заплашват националната сигурност, предизвиквайки масова смърт, отслабване на икономиката, на обществения морал и доверието. Терористите могат да използват измамнически схеми или злонамерен софтуер за събиране на чувствителна информация. Те могат да атакуват една цел за да се отвлече вниманието или ресурсите от други цели.

- *Чуждестранни разузнавателни служби (Foreign intelligence services).* Чуждестранните разузнавателни служби използват кибернетичното пространството като инструмент за събиране на информация и шпионаж. Много нации агресивно развиват военните си доктрини, програми и възможности. Тези възможности позволяват на едно лице със своите действия да доведе до сериозни последици като прекъсване на снабдяването, комуникациите и икономическата инфраструктура.

- *Вътрешни хора (Insiders)*. Недоволните вътрешни хора са основен източник на компютърни престъпления. Не е необходимо те задълбочено за познават технологията на атаките, тъй като разполагат с необходимата вътрешна информация и често имат неограничен достъп до системите. В тази група попадат също аутсорсинг доставчиците, както и служителите, които въвеждат случайно зловреден софтуер в системата.

- *Автори на злонамерен софтуер (Spyware/malware authors)*. Злонамерени физически лица или организации извършват нападения, като произвеждат и разпространяват Spywares и Malwares. Различни разрушителни компютърни вируси и червеи увреждат файлове и твърди дискове (например Melissa Macro Virus, Explore Zip worm, CIH (Chernobyl) Virus, Slammer, Blaster и др.).

- *Измамници (Phishers).* Измамниците са физически лица или малки групи, които използват различни схеми, опитвайки се да откраднат нечия самоличност или определена информация с цел парична печалба. Те не се ограничават само до измамническите схеми, а често използват и спам и злонамерен софтуер.

- *Спамери (Spammers).* Спамерите са физически лица или организации, които разпространяват нежелана електронна поща със скрита или невярна информация, за да продават продукти, да разпространят измамнически схеми или просто да нападнат определена организация.

4.2. Потенциални пропуски в защитата на ICS

За определяне на оптималната стратегия за защита, уязвимостта на ICS трябва да бъде изяснена от различни гледни точки. Например какви политики и процедури, софтуер, хардуер и мрежи се използват. Конкретната система за управление обикновено не е застрашена от всички тези фактори, но за нея могат да съществуват някои допълнителни специфични заплахи. Когато изследваме уязвимостта на определена система лесно можем да се подведем да изследваме само въпроси, които изглеждат технически интересни, но в крайна сметка имат по-ограничено ниво на въздействие. Необходимо е да се използва метод за оценка и класификация на риска. Рискът е функция на вероятността определен атакуващ елемент да използва конкретна специфична уязвимост, за да нанесе удар. Рискът за конкретна уязвимост се влияе от различни фактори, в т.ч. от:

- Мрежовата и компютърна архитектура,

- Инсталираните мерки за противодействие,

- Техническата трудност за нападение,

- Вероятността за откриване (например времето през което атакуващият може да остане в контакт със системата без да бъде разкрит),

- Последствията от инцидента,

- Разходите за отстраняване на щетите от инцидента.

Уязвимост в системите за управление обикновено се появява вследствие на непълна, неподходяща или несъществуваща документация за сигурност, включително за политиката и изпълнителните процедури. Документацията за сигурността заедно с необходимата подкрепа от страна на управляващия екип, е крайъгълен камък на всяка програма за сигурност. Корпоративната политика за сигурност може да намали уязвимостта чрез задължително изискване за използване на пароли и тяхната поддръжка, както и определяне на строги изисквания за включване на допълнителни устройства към мрежата (например модеми).

4. 2.1 Пропуски в системата на политиките и процедурите

По долу са подадени някои фактори влияещи върху уязвимостта на ICS като следствие от пропуски в използваните политики и процедури:

- *Неподходяща политика по сигурността.* Системите за управление често стават уязвими поради прилагане на неподходящи политики по сигурността или поради липса изобщо на политика по сигурността.

- *Липса на програма за обучение по сигурността.* Трябва да се разработи програма за обучение, която да поддържа персонала наясно с провежданата политика по сигурността, с последните използвани стандарти и с най-добрите практики в дадената област. Без тренировки за овладяване на специфичните процедури по сигурността не може да се очаква да бъде поддържана безопасна среда.

- *Използване на архитектури с недостатъчна сигурност.* Управляващите инженери исторически нямат тренировки за защита от външни намеси. Освен това някои от предлаганите продукти нямат разработени в достатъчна степен елементи по сигурността. В такава среда не може да се очакват адекватни действия от страна на персонала.

- *Специфични и документирани процедури.* При ICS често няма специфични и документирани процедури по сигурността. Такива процедури трябва да бъдат разработени. Те са корените на една разумна програма за сигурност.

- *Отсъствие или дефицит на указания за използване на оборудването.* Указанията за използване на оборудването трябва да бъдат осъвременени и лесно достъпни. Тези указания са неразделна част от процедурите за сигурност в случай на неизправност в ICS.

- *Липса на административни механизми.* Персоналът трябва да бъде държан отговорен за администрирането на документираните политики за сигурност и процедурите.

- *Малко или никакви проверки на сигурността на ICS.* Трябва да се провеждат независими одити по сигурността, да се разглеждат направените записи и да се оценява адекватността на предприетите действия в съответствие с възприетите политики и процедури. Одитите трябва да се използват за откриване на нарушения и за препоръки за промени в плана за сигурност.

- *Липса на план за възстановяване.* Планът за възстановяване е необходим в случай на големи хардуерни или софтуерни сривове. Липсата на конкретен план може да доведе до значително удължаване на престоя.

- *Липса на план за управление при промяна на конфигурацията.* Трябва да има план за контрол на процеса на промяна на хардуера, фирмуера, софтуера и документацията. Този план трябва да ни защитава преди, по време и след направени недостатъчни и неправилни модификации. Липсата на процедури за промяна на конфигурацията може да доведе до пропуски в сигурността и да подложи системата на риск.

4.2.2 Пропуски в хардуера и софтуера на ICS

Уязвимостта на ICS може да се дължи на неправилно конфигуриране или лошо поддържане на използваните технически платформи, включително хардуер, операционни системи (ОС) и приложения. Тази уязвимост може да бъде смекчена с прилагане на различен вид контрол за сигурност, например с използването на кръпки (patches) при операционните системи и приложенията, физически контрол на достъпа и софтуер за сигурност (антивирусен софтуер).

4.2.2.1 Пропуски в конфигурирането на ICS

- *Кръпките към ОС и приложния софтуер не са налични в момента на установяване на уязвимостта.* Поради сложността на софтуера и възможните модификации на операционните системи, направените промени трябва интензивно да бъдат тествани. Това е продължителна процедура и от установяването на системната грешка до последвалото разпространение на актуализирания софтуер се появява голям интервал от време, в който системата е уязвима.

- *Кръпките към ОС и приложния софтуер не се поддържат.* Трябва да бъдат разработени документирани процедури за поддръжка на системата от кръпки.

- *Кръпките към ОС и приложния софтуер са направени без изчерпателно изследване.* Това може да компрометира нормалното функциониране на ICS. Трябва да бъдат разработени документирани процедури за тестване на всяка нова кръпка.

- *Използват се конфигурации по подразбиране.* Използването на конфигурации по подразбиране често води до несигурно и ненужно отворени портове, улесняващи използването на допълнителни услуги и приложения.

- *Критични конфигурации не се помнят или не са архивирани.* Трябва да имаме достъпни процедури за възстановяване на конфигурацията и настройките на ICS.

Те ще бъдат използвани при случайна или вследствие на атака промяна на конфигурацията.

- *Използване на незащитени преносими устройства.* Ако чувствителни данни се съхраняват в явен вид на портативни устройства като лаптопи, и тези устройства са загубени или откраднати, системата за сигурност може да бъде компрометирана. За защитата са необходими различни политики, процедури и механизми.

- *Липса на адекватна политика за използване на пароли.* Политиката трябва да определи кога паролите да се използват, колко силни да бъдат те и как да бъдат поддържани. Без такава политика неконтролираният достъп към ICS е лесен. Политиката за използване на пароли трябва да бъде разработена като част от програмата за сигурност на ICS, като се разгледат възможностите за използване на по-сложни пароли.

- *Не се използват пароли.* За избягване на неоторизиран достъп, паролите трябва да се използват. Задължително е използването на пароли при влизане в системата (system login), включване и изключване на захранването (system power-on или system power-off) и системата за загасване на екраните (system screen saver).

4.2.2.2 Пропуски в хардуера на ICS

- *Незадоволително тестване при промяна в сигурността.* Много съоръжения на системата за управление, особено тези по-малките, нямат специализирани тестове и тяхната работоспособност и промените, които те въвеждат в системата на сигурността, се установяват в реално действащата система.

- *Недостатъчна физическа защита на критични системи.* Достъпът до контролния център, устройствата разположени в терена, портативните устройства, кабелажа, и останалите компоненти на ICS трябва да бъде контролиран. Много отдалечени обекти често не могат да бъдат физически наблюдавани.

- *Неоторизиран персонал има физически достъп до оборудването.* Физическият достъп до оборудването на управляващата система трябва да се ограничи само до необходимия персонал. Неразрешен достъп до оборудването може да доведе до физическа кражба или увреждане на данни и хардуер, неупълномощени промени в конфигурациите, прекъсване на физически връзки, както и незабележимо прихващане на данни.

- *Несигурен отдалечен достъп до компонентите на управляващата система.* Използването на модеми и други устройства, позволяващи на инженерите да упражняват отдалечен контрол над системите, трябва да бъде подложено на проверки за сигурност за предотвратяване на възможността неоторизиран персонал да получи достъп до тях.

- *Устройства използващи повече от един мрежови интерфейс за връзка.* Такива устройства, свързани към различни мрежи могат евентуално да позволят неоторизиран достъп и прехвърляне на данни от една мрежа в друга.

- *Работа в поле на електромагнитни импулси.* Хардуерът използван в управляващите системи е уязвим на електромагнитни и радиочестотни импулси. Влиянието на такива импулси се проявява от временни смущения в управлението до трайно увреждане на електрониката.

- *Липса на резервно захранване.* Без резервно захранване на критичните възли, отпадането на захранването на цялата система може да доведе до опасни последствия.

4.2.2.3 Пропуски в софтуера на ICS

- *Препълване на буферите.* Софтуерът използван в системата може да бъде чувствителен към препълване на буферите, което да бъде използвано за започване на различни атаки.

- *Инсталираните възможности на системата за сигурност не са разрешени по подразбиране.* Системата за сигурност е безполезна, ако тя не е активирана. Най малкото, в отделни моменти, системата трябва да бъде разпознавана като умишлено деактивирана.

- *Отказ от услуга (Denial of service - DoS).* Софтуерът може да бъде уязвим на атаки от типа DoS, което би довело до отказ на оторизиран достъп или до значително забавяне във функционирането на системата.

- *Неопределено реагиране при появата на недефинирани, не напълно дефинирани или „незаконни" условия.* Някои имплементации на софтуера са уязвими на увредени пакети, съдържащи полета с неочаквани или невъзможни стойности.

- *Използване на несигурни протоколи.* Distributed Network Protocol (DNP) 3.0, Modbus, Profibus и други протоколи са широко използвани в различни отрасли и информацията за тях е свободно достъпна. Те нямат вградени сериозни защитни възможности.

- *Използване на явен текст.* Пакетите на много протоколи съдържат информация в явен текст при предаване по кабела, което ги прави податливи на подслушване.

- *Разрешени са и се изпълняват ненужни услуги.* Много софтуерни платформи предлагат голямо разнообразие на мрежови услуги, които са разрешени по подразбиране. Ненужните услуги рядко се забраняват и могат да бъдат използвани при атака.

- *Софтуерът за откриване на натрапници (Intrusion Detection Software - IDS) не е инсталиран.* Това води до загуба на достъп до системата, прихващане, промяна и заличаване на данни. IDS софтуерът може да предотврати различни видове атаки, включително и DoS атаки, както и да определи атакуваните вътрешни компютри, които евентуално са заразени с червеи. IDS софтуерът трябва да бъде предварително тестван че не застрашава нормалното функциониране на системата.

- *Не се поддържат дневници (Logs).* Без правилното и точно поддържане на дневниците може да се окаже, че е невъзможно да се определи какво е причинило определено събитие в системата за сигурност.

- *Неоткрити инциденти.* Дневниците и другите елементи на сигурността, макар и инсталирани, често не се наблюдават в реално време. Това води до несвоевременно откриване на инциденти и до невъзможност за бързо противодействие.

4.2.3 Пропуски в мрежите на ICS

Уязвимостта на ICS може да бъде следствие на недостатъци, неправилно конфигуриране или лошо администриране на компютърната мрежа, както и на връзките с други мрежи. Намаляването или премахването на тази уязвимост се осъществява с различни видови контрол на сигурността, като използването на схема за ешелонирана защита (defense-in-depth), криптиране на мрежовите комуникации, ограничаване на потоците от мрежов трафик, и осигуряване на физически контрол за достъп до мрежовите компоненти.

4.2.3.1 Пропуски в мрежовата конфигурация

- *Използване на архитектура със слаби възможности за сигурност.* При разработването и модифицирането на мрежовата инфраструктура обикновено се вземат предвид изискванията за цена и функционални възможности, и се обръща по-малко внимание на потенциалните въздействия на промените върху сигурността. С течение на времето, по невнимание, са могли да бъдат въведени пропуски в сигурността на отделни елементи на инфраструктурата. Без саниране, тези пропуски могат да представляват „задна врата” към ICS.

- *Не се използват методи за управление на потока.* За директен достъп до мрежовите устройства е необходимо да се използват методи за управление на потока, например списъци за контролиране на достъпа (access control lists - ACL). Обикновено само мрежовите администратори имат достъп до тези устройства. Останалите подсистеми на ICS не трябва да имат достъп до мрежовите устройства.

- *Лошо конфигурирани устройства от гледна точка на сигурността.* Използването на конфигурации по подразбиране често води до ненужно отворени портове и осигуряване на услуги, които не са необходими за ICS. Неподходящо конфигурирани защитни стени и ACL в маршрутизаторите може да позволят ненужен трафик.

- *Конфигурацията на мрежово устройство не е запомнена или архивирана.* Трябва да имаме на разположение процедури за възстановяване на конфигурацията на мрежовите устройства в случай на нужда. При това тези процедури трябва да бъдат много ясно документирани.

- *Паролите не са кодирани.* Паролите предавани в явен текст са податливи на подслушване и могат повторно да бъдат използвани за неоторизиран достъп до мрежовите устройства. Такъв достъп може да доведе до нарушения във функционирането на ICS.

- *Паролите в мрежовите устройства не се променят дълго време.* Паролите трябва да се сменят редовно, така че дори и да се осъществи неоторизиран достъп, то той ще бъде за много кратко време.

- *Прилага се неподходящо контролиране на достъпа.* Неоторизираният достъп до мрежовите устройства и административните функции може да позволи на потребител да наруши функционирането и наблюдението на мрежата на ICS.

4.2.3.2 Пропуски в мрежовия хардуер

- *Недостатъчна физическа защита на мрежовото оборудване.* Достъпът до мрежовото оборудване трябва да бъде контролиран за предотвратяване на повреди и унищожаване.

- *Необезопасени физически портове.* Необезопасени USB и PS/2 портове могат да позволят физическо свързване към системата.

- *Прекъсване в управлението на околната среда.* Например увеличението на температурата може да доведе до прегряване на процесорите. В такава ситуация някои процесори ще спрат до функционират, други просто ще се стопят.

- *Различни хора имат достъп до оборудването и мрежовите връзки.* Физическият достъп до мрежовото оборудване трябва да бъде разрешен само за необходимия персонал. Погрешният достъп може да доведе до физическа кражба на данни или хардуер, неоторизирани промени в сигурността, прекъсване на мрежови връзки и т.н.

- *Ползване на външни мрежови услуги.* Не можем да си позволим ICS да стане зависима от външни за нея информационни услуги, например DNS, DHCP и т.н.. Такива услуги са по принцип ненадеждни и от време на време недостъпни.

- *Липса на резервни връзки в критични мрежи.* Липсата на резервни връзки в по-отговорните мрежи води до прекъсване на комуникациите при повреда дори само в една точка (single point of failure).

4.2.3.3 Пропуски в периметъра на мрежата

- *Няма дефиниран периметър за сигурност на мрежата.* Ако мрежата няма точно определен и дефиниран периметър за сигурност, не може да се гарантира че необходимите проверки са разгърнати и конфигурирани правилно. Това може да доведе до неоторизиран достъп до системата или до други проблеми.

- *Несъществуващи или неправилно конфигурирани защитни стени.* Липсата на правилно конфигурирани защитни стени позволява ненужни данни да преминават между различните мрежи, например между ICS и корпоративната мрежа. Това създава множество проблеми като разпространение на зловреден софтуер, прихващане на чувствителни данни, неоторизиран достъп и т.н.

- *Използване на мрежите на ICS за прекарване на друг вид трафик.* Изискванията към трафика в мрежите на ICS и към трафика с общо предназначение са различни.

4.2.3.4 Пропуски в комуникационната система

- *Неподходящи дневници на защитните стени и маршрутизаторите.* Без подходящите и точни дневници е невъзможно да се определи причината за нарушаване на сигурността и настъпилия инцидент.

- *Няма наблюдение на сигурността в ICS мрежата.* Без редовен мониторинг на сигурността някои инциденти могат да минат незабелязано и това да доведе до допълнителни увреждания. Освен това той служи за идентифициране на проблеми в сигурността, като например неправилно конфигуриране и аварии.

- *Не са идентифицирани критични за наблюдението и сигурността връзки.* Измамни или неизвестни връзки в ICS могат да отворят вратички за атаки.

- *Стандартни и добре документирани протоколи се използват в явен вид.* Недоброжелатели могат да наблюдават активността на ICS мрежата, като за целта използват протоколни анализатори или други помощни програми за декодиране на данните пренасяни с протоколи като Telnet, FTP, и NFS. Използването на такива протоколи улеснява провеждането на атаки срещу ICS.

- *Не се използва автентикация на потребителите, данните и устройствата или се използва нередовно.* Много протоколи в ICS нямат механизми за автентикация на всички нива. Без нея съществува потенциална възможност за неправомерни отговори, модификации и прихващане на данни.

- *Липса на проверка на целостта на данните.* В повечето индустриални протоколи няма вградена проверка на интегритета на данните. Недоброжелатели могат да манипулират необезпокоявани комуникациите. За осигуряване на интегритет в ICS могат да бъдат използвани протоколи от долните нива, например като IPSec, които предлагат такава защита на целостта на данните.

4.2.3.5 Пропуски в безжичните връзки

- *Недостатъчна (незадоволителна) автентикация между клиентите и точките за достъп (access points).* Необходимо е да бъде използвана силна взаимна автентикация между клиентите и точките за достъп за да се гарантира, че клиентите няма да се свързват с нерегламентирани точки за достъп разположени в близост от недоброжелатели, а също така, че външни хора няма да могат да се включат към безжичната мрежа на ICS.

- *Недостатъчна защита на данните между клиентите и точките за достъп.* Конфиденциалните данни между безжичните клиенти и точките за достъп трябва да бъдат защитени като се използва силно криптиране

4.3. Рискови фактори

Няколко фактора в момента допринасят за увеличаване на риска в ICS. Те са следните:

- *Използване на стандартизирани протоколи и технологии в ICS.* Производителите на ICS оборудване започнаха да отварят своите патентовани протоколи и да публикуват техните спецификации с цел други производители да започнат производствата на съвместими с тях възли и елементи. Организациите също предпочитат да преминат от патентовани системи към по-евтини стандартизирани технологии, като например MS Windows и UNIX-базирани операционни системи, както и да използват общите мрежови протоколи TCP/IP за да намалят разходите и да подобрят производителността. За тази еволюция към отворените системи допринася и OPC, протокол позволяващ взаимодействие между ICS и PC-базирани приложни програми. Преминаването към използване на този отворен протокол предлага много икономически и технически предимства, но също така и увеличава податливостта на ICS към атаки от страна на кибернетичното пространство.

- *Увеличение на взаимната свързаност.* ICS и корпоративната мрежа често са свързани помежду си като резултат от няколко последователни промени на практиката за управление на информацията. Изискването за отдалечен достъп насърчи много организации да изградят допълнителни връзки към ICS и да позволят на инженерите да наблюдават и управляват системата от разстояние. Много организации също добавят такива връзки между фирмената мрежа и мрежата на ICS за да могат хората вземащи решения да получат достъп до критични данни за състоянието на производството и да изпращат инструкции към персонала или разпространителите на продуктите. Първоначално това се правеше с потребителски софтуер или чрез използването на OPC сървър/шлюз, но в последните десет години това се постига с използване на TCP/IP мрежа и стандартни IP приложения за обмен на данни , като например FTP и XML. При това тези връзки се осъществяват без пълно разбиране за съответните рискове за сигурността. В допълнение корпоративните мрежи често са свързани с корпоративните мрежи на партньорите и с Интернет. От друга страна в ICS също все повече се използват глобални мрежи и Интернет като преносна среда за техните отдалечени станции и индивидуални устройства. Това интегриране на ICS с корпоративните и обществени мрежи в значителна степен увеличава възможността за достъп до уязвимите места на ICS. Ако не се приложат подходящи мерки за контрол, цялата мрежова архитектура на ICS, на всички нейни нива, става уязвима за множество кибернетични атаки.

- *Несигурни и измамнически връзки.* Много от производителите на ICS оборудване доставят системи с dial-up модеми с цел да осигурят отдалечен достъп и да облекчат техническия персонал. Отдалечената връзка е за достъп до системата и е на ниво администратор. Недоброжелатели, използващи прости компютърни програми, прозвъняват последователно телефонните номера, откриват модемите, и използвайки софтуер за разкриване на паролите получават достъп до системата. Използваните пароли за отдалечен достъп обикновено са еднакви за всички имплементации за конкретния производител и често не са променяни от потребителите. Случва се организациите по недоглеждане да оставят такива връзки отворени за отдалечена диагностика, поддръжка и наблюдение. Все повече

управляващите системи използват безжични комуникации, което ги прави уязвими. Много от връзките между ICS и корпоративните мрежи изискват интегриране на системи с различни комуникационни стандарти, което от една страна представлява върхът на инженерната практика, но от друга води до проблеми в сигурността.

- *Публичност на информацията.* С цел да се подпомогне развитието на софтуера и да се увеличат продажбите, информацията за проектиране, поддръжка, начини на свързване и използвани протоколи е широко достъпна в Интернет. Производителите на ICS оборудване продават развойни системи за създаване на управляващ софтуер. Налице са и голям брой бивши работници, производители, доставчици и други, които имат достатъчно познания за начините на функциониране на системите за управление.

5. Мрежова архитектура

Преди за разгледаме въпросите как да изградим архитектурата на една ICS система, така че да отговаря на изискванията за сигурност, трябва да отговорим на въпроса възможно ли е изобщо да бъдат свързвани полевите мрежи с Интернет? Трябва да бъде решен транспортния проблем на свързването, след което да се заемем със сигурността.

5.1 Свързване на полева мрежа с Интернет

Ако се вярва на съвременните рекламни и маркетингови статии, свързването на полевите мрежи с Интернет е въпрос, който трябва да бъде решен от инженерите по автоматизация. За простота по-долу ще разгледаме връзката между полева мрежа като Fieldbus и Интернет. Направените разсъждения обаче са верни и за връзка между произволна автоматизирана система използваща специализирана мрежа и IT мрежа базирана на използването на Internet Protocol (IP), т.е. това може да бъде и Интранет. Това което непрекъснато се рекламира като голямата полза от такава връзка, всъщност се свежда до две основни, но взаимно преплетени предимства: осигуряване на отдалечен достъп до системите за автоматизация и обещание за интеграция на данните от процеса с по-лесна за тяхното използване среда. С други думи, има две причини, поради които свързването на полевите мрежи с Интернет могат да бъдат полезни:

- *Разширяване на физическите размери на една автоматизирана система*. Предимно по исторически причини, разширяването на една типична полева мрежа не може да бъде осъществено, поради ограничената дължина на нейните сегменти и липсата на маршрутизиращи възможности. Ако е налична инфраструктурата на Интернет, то тя може да се използва като един вид гръбнак, за да свържете отдалечените сегменти на инсталацията.

- *Осигуряване на вертикална интеграция*. В областта на автоматизацията, този широко използван термин означава доставяне на информацията от автоматизираната управляваща система в локалната мрежа на предприятието, където тя може да бъде използвана не само за събиране на данни, но също така и за нуждите на стратегически операции, като управление и планиране на ресурсите.

Особено втората причина в момента е във фокуса на значителните усилия свързани с нарастващото използване на Ethernet в управляващите системи. Въпреки това следва да се отбележи, че идеята за вертикална интеграция не е нова. Корените и датират от 1980

година, когато беше разработена концепцията за компютърно интегрирано производство (Computer-Integrated Manufacturing – CIM). Разработеният йерархически модел на пет нива във вид на пирамида [11] всъщност е ранен опит за структуриране на информационния поток в рамките на предприятието. Съществуват много различни начини за представяне на тази пирамида, при това отделните нейни нива се срещат с различни наименования в зависимост от областите на приложение. Но крайната цел винаги е била една и съща: да се получи прозрачен обмен на данни между йерархически разположените мрежи.

Първите опити за реализиране на концепцията CIM бяха напразни, главно поради технологични причини. От една страна протоколите за комуникация вътре в управляващата система (например Manufacturing Automation Protocol – MAP [12] с неговата пълна реализация на OSI модела) бяха твърде сложни. От друга страна развитието на микроелектрониката все още не беше достатъчно, за да осигури необходимите изчислителни ресурси на разумна цена. Затова интегрирането на полевата мрежа в CIM се оказа почти невъзможно. В допълнение Fieldbus системите бяха в много ранен етап на своето развитие. Следователно от мрежова гледна точка нямаше връзка между първоизточника на данни за процеса и вече съществуващите локални корпоративни мрежи.

Големият скок напред в интеграцията дойде с успеха на Интернет и по-точно с изобретяването на World Wide Web (WWW). Докато в областта на полевите мрежи, въпреки продължителния и тромав процес на стандартизация [13] [14], съществува голямо разнообразие от подходи, светът на корпоративните мрежи е доминиран от IP и от разработените за него приложения.

Причината поради която старата идея за вертикална интеграция се възобновява в последните години е по-скоро психологическа. Интернет и неговите основни технологии са на разположение (и използвани) от дълго време. Появата обаче на уеб браузера стимулира приемането на Интернет повсеместно и осигури господстващата му роля. От потребителска гледна точка уеб браузерът позволява достъп до отдалечени данни в почти тривиален начин. Затова не е учудващо, че лесната навигация чрез хипертекст документи се възприе в автоматизацията като модел за отдалечен достъп до данни. Вследствие на това много решения за свързване между Fieldbus и Интернет се базират на технологията WWW и на интерфейса на уеб браузер. Впечатлението обаче, че достъпът да полевите мрежи през Интернет става винаги по един и същи начин, е измамно. Потребителският интерфейс е само едната страна на проблема; използваните механизми и структурите от данни са другата страна. Всъщност когато става въпрос за връзка между полеви мрежи и IP базирани мрежи има едно изненадващо разнообразие от възможности, дори в толкова стандартна като Интернет среда.

От архитектурна гледна точка има два подхода за осъществяване на връзка Fieldbus – Интернет, като и двата се използват в практиката:

- Използване на тунел за преминаване на един протокол през друг
- Използване на шлюз (gateway) за преобразуване на протоколите и услугите.

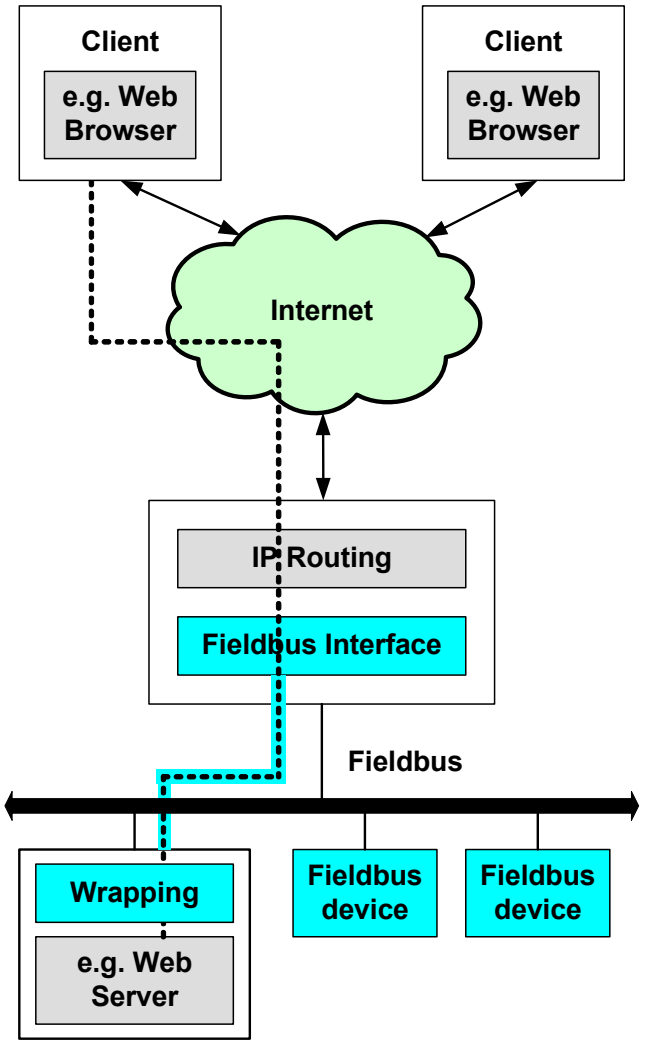
По отношение на топологията, двата подхода са много подобни. И при двата трябва да има една централна точка за достъп между мрежите. Това което ги различава е начина на

обработка на информацията от тази връзка, или по точно, как обработката се разпределя между устройствата включени в комуникацията.

5.1.1 Тунелиране на протоколи

В комуникационните мрежи тунелирането по същество означава, че рамките на един протокол просто са поместени (скрити) в полето за данни на рамките на друг протокол. При това не се променя тяхното съдържание. Тунелният подход в разглеждания контекст попада в две категории:

Най разпространеното решение е IP пакетите да се вградят в съобщенията на полевата мрежа. По този начин се отваря и канал за протоколите от по-горни слоеве, необходими например за директен уеб достъп до полевите устройства [15]. Тази възможност наскоро бе включена в няколко Fieldbus системи – ход който трябва да бъде разглеждан главно във връзка с дискусията за използване на Ethernet в процесите на автоматизацията. На пръв поглед IP тунелирането дава лесен начин на постигане на вертикална интеграция, както е показано на Фиг. 6. Полевите устройства извършват IP-базирани услуги, като например уеб сървър, осигурявайки данни за съответните приложения в Интернет, които имат директен достъп до устройствата.



Фиг. 6 Структура на IP тунелиране през Fieldbus

При по внимателно вглеждане обаче във Фиг. 6 се вижда, че интеграцията не е толкова лесна. В тази структура има няколко критични момента:

- *Изчислителни ресурси на полевото устройство*. Първо, полевото устройство като крайна точка на тунела трябва да бъде в състояние да извършва всички дейности свързани с пълния IP протокол и допълнителните протоколи, необходими за приложенията. Второ, необходима е памет за конкретната приложна програма, до която ще имаме достъп по IP. За използваните днес вградени (embedded) системи, това може да не е проблематично, тъй като разполагаме с набор от олекотени протоколи (обикновено за сметка на подробно описание на грешките). Във всеки случай това изисква използване на допълнителен хардуер в устройствата и може да бъде икономически фактор, особено при прости устройства, като датчици или изпълнителни механизми.

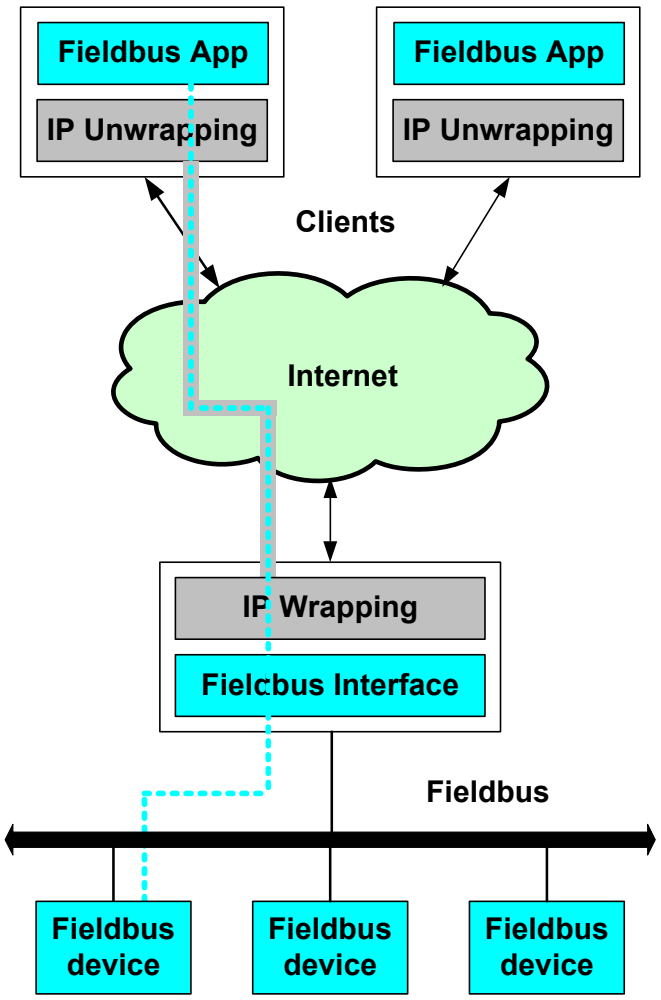
- *Управление на трафика в точката за достъп*. Възелът, който свързва IP-базираната мрежа и полевата мрежа трябва да опакова IP пакетите и да ги препрати по полевата мрежа към съответните полеви възли, където те да бъдат разопаковани. От тази гледна точка устройството за достъп трябва да работи като IP маршрутизатор. Нещо повече, то трябва да изгради таблица за съответствие между IP връзките и съответните полеви комуникационни канали. Това изисква адресно преобразуване от полевата страна на точката за достъп. От страната на Интернет, адресно преобразуване може да се наложи, ако адресите в полевата мрежа не са публични такива, а са частни, което е обичайната практика при конфигурирането на такива мрежи. Точката за достъп трябва да работи като защитна стена с просто маскиране и транслация на мрежови адреси (Network Address Translation – NAT). С изключение на случая, когато полевите адреси са публични, полевата мрежа като цяло е достъпна през един единствен IP адрес и разграничаването между отделните устройства (например уеб сървъри), скрити зад NAT става с използването на портове. Услугите вече не са достъпни чрез добре познатите стандартни портове (well-known ports), а през специални такива, които разбира се трябва да бъдат по подходящ начин конфигурирани.

- *Производителност*. IP пакетите са големи (до 1500 байта), докато съобщенията в полевите мрежи обикновено са оптимизирани само за предаване на малки порции данни. Вкарването на IP пакетите в малките полета на полевите съобщения изисква разделянето на IP пакетите, или т.н. фрагментиране. Това фрагментиране води до удължаване на времето за предаване. Типичен пример тук е мрежата Interbus [16], където IP трафика може да бъде прекарван по полевата мрежа, като се използва канала за предаване на параметри. Този канал е с малък капацитет от 8 байта на цикъл (при това един от байтовете е служебен), за да не се пречи на предаването на управляващите съобщения транспортирани в реално време. В зависимост от големината на мрежата и нейната скорост, един цикъл трае няколко милисекунди. Непосредствено се вижда, че за една секунда могат да бъдат прекарани не повече от 2 до 3 IP пакета. Изводът е, че при тунелиране на IP през полева мрежа, производителността изключително много зависи от особеностите на полевата мрежа.

Вторият начин за тунелиране работи в обратната посока. Fieldbus съобщенията са опаковани в пакети на протокола IP (или протокол от по-горно ниво, например TCP, в зависимост от това как е изграден тунела) и се изпращат на отдалечения възел на

мрежата (Фиг.7). От гледна точка на вертикалната интеграция, недостатъкът на този подход е очевиден. Fieldbus данните трябва да бъдат интерпретирани при клиента, което изисква специфично за дадената полева мрежа приложение, или най-малкото присъствие на опитен потребител със задълбочени познания по конкретната автоматизирана система.

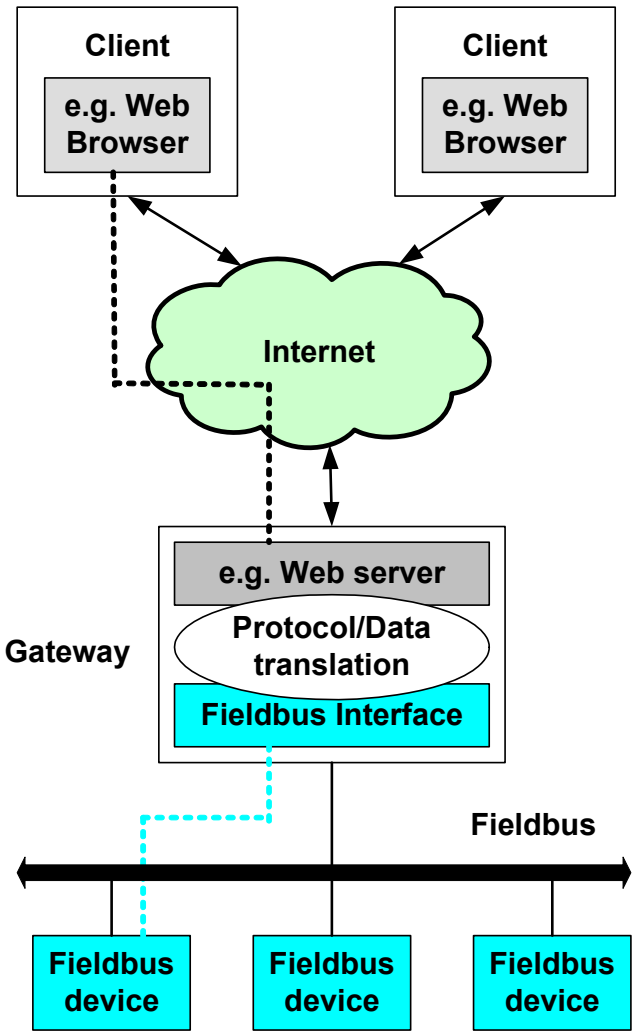
Този подход не отговаря на изискванията за удобство на потребителя, залегнали в идеята за вертикално интегриране. В реалния свят прекарването на Fieldbus съобщения през тунел в Интернет по скоро се използва за свързване на отдалечени части на инсталацията. Намира широко приложение при автоматизацията на сградни инсталации [17]. Тук трябва да отбележим, че при връзката между два Fieldbus сегмента през тунел в Интернет трябва да се справим с времеви проблеми породени от закъсненията необходими за обработка на пакетите в IP мрежата. Следователно този метод може да се използва, само ако полевите протоколи нямат строги времеви ограничения.



Фиг. 7 Структура на Fieldbus тунелиране през IP мрежа.

5.1.2 Шлюзове (Gateways)

За да се изгради връзка между Fieldbus и Интернет може да се използва и алтернативен подход, а именно централната точка за достъп да се оформи като шлюз. От едната страна шлюзът е пълноправен участник в комуникацията във Fieldbus мрежата, а от другата страна е достъпен с IP базирани механизми през Интернет (Фиг. 8). Това което е различно, е начинът на обработка на информационния поток. При подхода с IP тунелиране, клиентът се свързва директно към сървъра, който се намира в полевото устройство. Точката за достъп само препраща IP трафик. При използването на шлюз, точката на достъп играе ролята на посредник (proxy) и представлява мрежата Fieldbus и данните в нея пред външния свят. Тя извлича данни от полевите устройства като използва обичайните за Fieldbus комуникационни методи, и е комуникационен партньор адресиран от клиента.



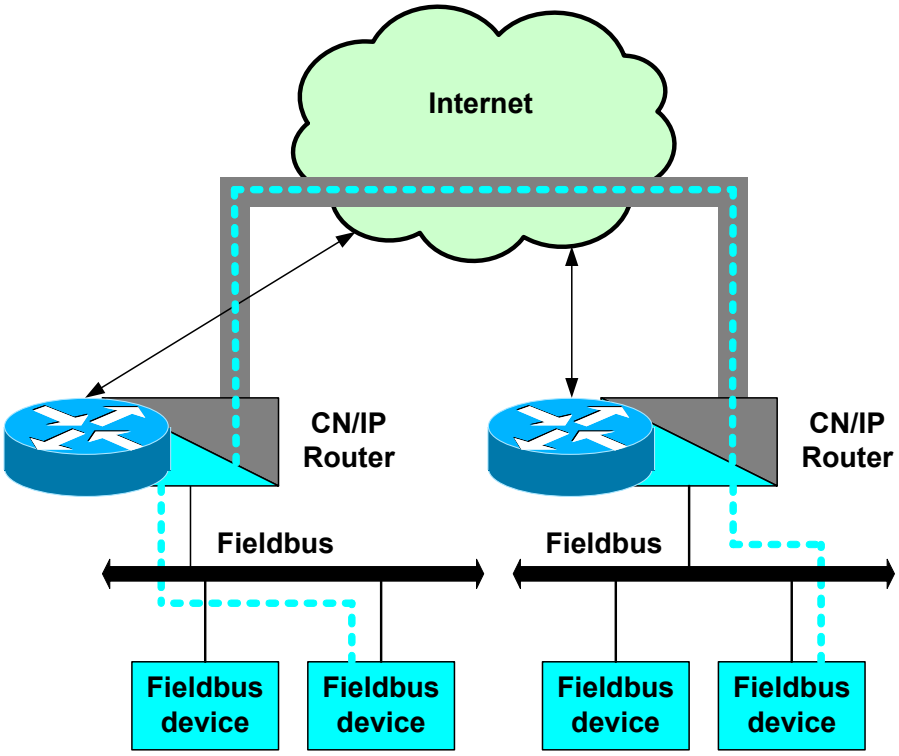
Фиг. 8 Топология на свързване с използване на шлюз

За разлика от тунелния подход, където всяко полево устройство трябва да осигури и поддържа данните на индивидуална основа, обработката на информацията за Интернет клиента е централизирана в шлюза. Това му позволява да има цялостна и последователна представа за автоматизираната система, което е безспорно предимство.

В допълнение полевите устройства не се нуждаят от специално оборудване за обработка на IP базираните данни и услуги.

За изчерпателност следва да се отбележи, че шлюзът по принцип позволява и комуникация в обратната посока. Затова полевите устройства могат също да получат достъп до ресурси в Интернет, т.е. различни Fieldbus мрежи да получат достъп до корпоративната локална мрежа през съвместими шлюзове. Това обаче няма съществено практическо приложение.

Специален случай на протоколно тунелиране е свързването на два отдалечени Fieldbus сегмента, като се използва един IP-базиран гръбнак. Този подход стана популярен в инженерната практика напоследък [18]. Характеристиките и особено производителността на гръбнака са от съществено значение. По-специално настройката на IP канала свързващ управляващите възли или мрежи оказва директно влияние върху свойствата на системите и моделирането на мрежа с такава топология не е проста задача.



Фигура 9 EIA-852 конфигурация

За изграждането на тунела и за обмен на данни между крайните точки се изисква специализиран протокол. Стандартът EIA-852 е проектиран специално за тази цел и се радва на все по-голяма популярност [19]. Той описва елементите на системата, комуникационните протоколи и управляващите механизми за установяване на IP канал с управляващи устройства и маршрутизатори (Фиг.9). Устройствата в една EIA-852 система трябва да бъдат или напълно IP базирани, или обикновени Fieldbus устройства които се свързват към IP мрежата посредством Control Network/IP (CN/IP) тунелни маршрутизатори, както е показано на горната фигура.

ETA-852 устройствата комуникират директно помежду си (peer-to-peer), като използват оригиналните управляващи протоколи без да има нужда от шлюзове. Данните на

оригиналния протокол се капсулират в пакетите на UDP (User Datagram Protocol) и се маршрутизират да съответните получатели в IP канала. Предпочитането на UDP пред TCP като транспортен протокол има някои предимства. Първо, избягват се тежките процедури при установяване на сесия, Второ, TCP гарантира доставката чрез препредаване. Поради изискванията за работа в реално време на управляващите приложения, едно такова повторно предаване ще бъде вече закъсняло във времето и безпредметно. И трето, мрежовите управляващи протоколи имат техни, собствени схеми за препредаване когато това е необходимо. С течение на времето се оказа, че EIA-852 като тунелен протокол е едно реално и работещо решение.

От направените по-горе разсъждения могат да се извлекат следните изводи:

- Тунелирането на IP протокол през протоколите на Fieldbus е с малка производителност и води до нарушаване на изискванията за работа в реално време.

- Създаването на шлюзове за връзка между двата типа системи също обаче среща трудности. Инженерите и програмистите създаващи шлюза трябва да познават в тънкости както протоколите от седемслойния модел на OSI, използвани в IT системите, така и на протоколите от трите слоя (физически, канален и приложен [11]) използвани в системите за управление. И докато програмисти запознати с IT системите се обучават в университетите и могат да се намерят, то програмисти запознати с управляващите системи и можещи да програмират специализираните микропроцесорни устройства няма на пазара. Те трябва да се обучават с години, за да могат да бъдат полезни при създаването на конкретните програми.

Една от насоките за решаване на възникналите проблеми е да бъдат модифицирани протоколите в управляващите системи така, че от една страна да се държат например като Ethernet за протоколите от горните нива, а от друга страна да запазят възможностите си за работа в реално време, т.е. да гарантират времето на доставка. При такъв подход можем в значителна степен да приложим разработените вече за IT системите механизми за пренос на данни и защита на информацията.

5.2 Ethernet и възможност за работа в реално време

5.2.1 Защо се стремим да използваме Ethernet като полева мрежа?

Операциите на ниво Fieldbus предполагат възможност за предаване на ограничен във времето трафик между датчиците, контролерите и изпълнителните механизми. Ethernet не е проектиран да поддържа такъв тип трафик и някои от неговите характеристики, например недетерминистичният арбитражен механизъм, създава сериозни проблеми при използването му за тази цел. Защо тогава да го използваме? В много статии се разглеждат различни аргументи за и против [20], [21], [22], [23]. Например в [21] се изтъкват следните предимства:

- Използваните интегрални схеми са евтини поради масовото производство.

- Интегрирането с Интернет е лесно (TCP/IP над Ethernet е широко разпространен, което позволява да се използват различни приложни протоколи, като FTP и HTTP)

- Напоследък наблюдаваме силно нарастване на скоростите на предаване – от 10 Mbps до 1000 Mbps и повече.

- Поради естествената си съвместимост с комуникационните протоколи на локалните мрежи от по-горните нива на системите за управление, обмена на информация с централните диспечерски пунктове е улеснен.

- Ethernet има достатъчно широка честотна лента, за да бъде използван за последните мултимедийни приложения, например предаване на образ от терена.

- Наличие на технически грамотни хора запознати с този протокол.

- Наличие на достъпно тестово оборудване от различни източници.

- Това е изпитана технология, добре стандартизирана, с много производители, без последици от несъвместимост.

От друга страна най-често срещаният аргумент срещу използването на Ethernet като полева мрежа е прилагането в него на конкурентния, недетерминистичен арбитражен механизъм CSMA/CD. Потенциално лекарство тук е използването на комутируем (switched) Ethernet, с който можем да заобиколим появата на колизии и да работим в пълен дуплекс.

Избягването на колизиите обаче не прави Ethernet детерминистичен: например ако много съобщения едновременно пристигнат в комутатора и всички те са насочени към един конкретен порт, то буферите на този порт могат да се запълнят и да бъдат загубени съобщения. Затова в този случай е необходима някаква координация от по-високото ниво. Освен това ограниченото време за доставка не е единственото изискване към Fieldbus. Някои други фактори, често споменавани в литературата, са: използване на приоритетни съобщения, ефективно обслужване на периодичен и непериодичен трафик, както и наличието на много къси пакети. Ясно е, че дори и комутируем Ethernet, не дава отговори на всички тези изисквания.

5.2.2 Как да направим Ethernet подходящ за работа в реално време?

Дотук разгледахме предимствата и недостатъците на използването на Ethernet за комуникация в реално време и по-специално на използването му като Fieldbus. По принцип, Ethernet сам по себе си, не може да изпълни всички изисквания, наложени на една полева мрежа. По отношение обаче на използването му в реално време бяха разработени няколко подхода. Много от тях се базират на изменение на CSMA/CD схемата, като се въвежда по-горен слой за контролиране на предаването, който слой да елиминира, или поне да намали, колизиите при достъпа до преносната среда. Други подходи предлагат модифициране на самата схема CSMA/CD така, че когато все пак се случат колизии, да сработи детерминистичен алгоритъм за тяхното разрешаване за да се гарантира времето за доставка в най-лошия случай. Сред многото различни подходи целящи да направят Ethernet подходящ за работа в реално време можем да различим следните групи:

- CSMA/CD базирани протоколи [11], [24], [25]
- Модифицирани CSMA протоколи [11], [26], [27]
- Методи за достъп с управляващ маркер (Token Passing) [28], [29], [30]
- Методи за достъп с времеделение (Time Division Multiple Access) [31], [32], [33]
- Методи главен/подчинен (Master/Slave) [34], [35]
- Комутируем (Switched) Ethernet [21], [36], [37], [38].

Всеки един от тези методи намира своето приложение. Комутируемият Ethernet изглежда най-перспективен при съвременното развитие на технологията. В [21] са разгледани и някои други проблеми при този метод, като забавянето на пакетите в комутаторите, малкото на брой опашки за различните приоритетни нива и т.н. Тези проблеми обаче са основно технологични и се очаква да бъдат отстранени в близко бъдеще. Прилагането на комутируемия Ethernet значително облекчава липсата на детерминизъм при CSMA/CD като метод на достъп и отваря път за ефективно прилагане на Ethernet в реално време.

5.3 Защитни стени

При проектирането на мрежовата архитектура, обикновено се препоръчва мрежите на ICS и корпоративната мрежа да бъдат свързани по някакъв начин, но да бъдат разделени, не само поради съображенията за сигурност, но и защото мрежовият трафик в тези две мрежи е коренно различен. Например Интернет, FTP, електронна поща и други услуги се разрешават в корпоративната мрежа, но не трябва да бъдат допускани в ICS мрежата. Процедурите за промяна на мрежовото оборудване, на софтуера и неговото конфигуриране в корпоративната мрежа могат да бъдат не особено строги. От друга страна, ако се допусне мрежовият трафик на ICS да преминава през корпоративната мрежа, то той може да бъде прихванат и подложен на атака, например на DoS. Благодарение на едно такова разделение, проблемите на сигурността и производителността на корпоративната мрежа не би трябвало да оказват голямо влияние върху ICS мрежата.

Връзката между двете мрежи представлява съществен риск за сигурността, затова трябва да се обърне специално внимание както на нейното проектиране, така и на самото изпълнение. Препоръчително е мрежите да бъдат свързани с колкото се може по-малко връзки (ако е възможно само една връзка) като се използват защитни стени и демилитаризирани зони (Demilitarized Zone - DMZ). От тази гледна точка показаните връзки на Фиг. 5 не са добре проектирани.

DMZ е отделен мрежови сегмент, към който директно е свързана защитната стена. В този сегмент се разполага сървър, където се намират данните на ICS, до които корпоративната мрежа трябва да има достъп. Достъп до други данни на ICS, които се намират извън този сървър, корпоративната мрежа няма. При това достъпът до сървъра е само през защитната стена.

Мрежовите защитни стени са устройства или системи, които контролират потока на мрежовия трафик между мрежи с различни изисквания за сигурност. В повечето

публикации са описани приложения на защитни стени в контекста на връзката към Интернет и използването на протоколния комплект TCP/IP. Независимо от това, защитни стени могат да бъдат използвани и в системи, където няма необходимост от връзка към Интернет. В много корпоративни мрежи се използват защитни стени за ограничаване на достъпа до вътрешни мрежи обслужващи по-чувствителни данни и функции, например до мрежите на личен състав и счетоводството.

Защитните стени често се комбинират с други технологии, най вече маршрутизиращи, като функциите по защитата могат да бъдат неразделна част от тези други технологии. Така например технологията за преобразуване на адреси (Network Address Translation – NAT) понякога се разглежда като технология на защитна стена, а тя всъщност е технология за маршрутизиране. Много защитни стени включват и функции за филтриране на съдържанието на пакетите с цел прилагане на конкретни политики на организацията, които политики не са пряко свързани със сигурността. Някои защитни стени включват и технологии за предотвратяване на проникванията (Intrusion Prevention System – IPS), с които могат да се открият атаки и да се предотвратят повреди в системата.

Различаваме три основни категории защитни стени [39]:

- *Защитни стени за филтриране на пакети (Packet Filtering Firewalls)*. Често този основен вид защитна стена се нарича филтър на пакети. По същество това е маршрутизиращо устройство, което контролира достъпа до системата от адреси и комуникационните сесии. Контролът на достъпа се управлява от набор от директиви. Обикновено филтърът на пакети работи в мрежовия слой на OSI модела. Този тип защитна стена проверява мрежовата информация във всеки пакет, като например IP адресите, и сравнява дали тази информация отговаря на множеството зададени критерии. В зависимост от пакета и критериите, защитната стена може да отхвърли пакета, да го препрати в дадена мрежа, или да изпрати съобщение на първоизточника на пакета. Предимствата на този тип защитни стени са ниската цена и слабото влияние върху производителността на мрежата, тъй като се анализират само едно или няколко полета в заглавната част на пакета (header).

- *Защитни стени за проверка на състоянието на връзките (Stateful Inspection).* Подобрението на защитните функции на филтъра на пакети може да стане чрез проследяване на състоянието на връзките и блокиране на пакетите, които се отклоняват от очакваното състояние. Това се постига, като се използва и информацията от транспортния слой. Пакетите се прихващат в мрежовия слой и се проверяват дали те изпълняват набора от директиви на защитната стена. Допълнително обаче се следят и състоянията на връзките, които се поддържат в отделна таблица. Тази таблица е различна за различните приложения, но обикновено включва IP адресите на източника и местоназначението, номерата на използваните портове и информация за състоянието на връзката. При TCP трафик имаме три състояния: установяване на връзка (initializing), използване на установена връзка (established), и прекратяване на връзка (terminating). Защитната стена проверява определени полета в хедърите на TCP пакетите и следи за състоянието на всяка връзка. Всеки нов пакет се сравнява със състоянието на връзката в таблицата за да се определи дали състоянието на пакетите не противоречи на очакваното състояние. Програмата на защитната стена много добре познава тънкостите на TCP и UDP протоколите и ще блокира всеки пакет дори и при минимално отклонение в съответния автомат на състоянията. Например

защитните стени проверяват такива атрибути, като поредните номера в TCP хедърите и отхвърлят пакетите, които не са от поредицата. Когато защитната стена предоставя и NAT услуги, в таблицата често се включва и NAT информация.

Понеже някои протоколи, например UDP, са без установяване на връзка, тяхното състояние не може да бъде определено от транспортния слой, така както е при TCP. За такива протоколи се проследяват само IP адресите и портовете на източника и местоназначението. DNS отговор от външен източник ще бъде разрешен, само ако преди това през защитната стена е преминала заявка за DNS услуга от вътрешния източник. Тъй като защитната стена не може да определи кога една сесия е приключила, дадена входна точка в таблицата на състоянията се отстранява след изтичане на определен конфигуриран таймаут. Ако защитната стена работи на приложно ниво, то тя е в състояние да прекрати DNS сесията след получаване на DNS отговора. По същия начин се действа и при NTP протокола Когато става въпрос за ICS приложения, към защитната стена могат да бъдат предявени още изисквания под формата на допълнителен набор от директиви.

- *Приложни прокси защитни стени изградени върху шлюзове (Application-Proxy Gateway Firewalls).* Тази категория защитни стени проверява пакетите в приложния слой и филтрира трафика въз основа на специфични правила наложени от специфичните приложения (например браузъри) или протоколи (например FTP). Предлаганата степен на сигурност е висока, но обикновено тези стени са бавни и оказват значително влияние върху производителността на мрежата. Това може да бъде неприемливо при ICS мрежи.

В ICS системите, защитните стени най-често се разполагат между мрежата на ICS и корпоративната мрежа. Подходящо конфигурирани, те могат значително да ограничат нежелания достъп към и от компютрите в управляващата система. Могат също така потенциално да подобрят условията в управляващата мрежа, като премахнат ненужният трафик от нея. Когато са правилно проектирани, конфигурирани и с необходимата поддръжка, обособените хардуерни защитни стени могат да допринесат значително за повишаване на сигурността на управляващата система.

Защитните стени ни предоставят множество инструменти за прилагане на политики за сигурност, които иначе не биха могли да бъдат реализирани с наличните на пазара устройства за управление. Тези инструменти ни дават възможност за:

- Блокиране на всички съобщения (с изключение на специално разрешените) между незащитената корпоративна LAN и защитените ICS мрежи. Блокирането се основава на IP адресите на източника и местоназначението, на използваните портове и услуги. Блокирането важи както за входни (inbound), така и за изходни (outbound) пакети, което е полезно при ограничаването на комуникации с висока степен на риска, като например електронна поща.

- Автентикация за всички потребители, стремящи се да получат достъп до ICS мрежата. Съществува възможност за гъвкав избор на различни нива на защита и различни автентикационни методи, включително прости и сложни пароли, многофакторни автентикационни технологии, биометрични данни и смарт карти.

- Прилагане на упълномощен достъп само до определени устройства. Потребителите могат да бъдат ограничени да се свързват в управляващата мрежа само с устройства, до които трябва да имат достъп вследствие на преките си служебни задължения. Това намалява възможността те умишлено или случайно да получат достъп до управляващи устройства, за които не са упълномощени. Използването на този механизъм от друга страна може да пречи на обучението и да затормозява тренировъчния процес.

- Записване на информационния поток за нуждите на управлението на трафика, за анализи и за откриване на нерегламентирано проникване.

- Прилагане на оперативни политики, които са подходящи за ICS, но са неуместни за една IT мрежа, като забрана на електронна поща, използване на лесни за запомняне потребителски имена и групови пароли.

- Лесно прекъсване на достъпа до мрежата в случай на сериозни кибернетични атаки към нея.

В мрежовата архитектура се срещат и компютърно-базирани защитни страни, както и малки самостоятелни хардуерни защитни стени, които стоят пред или работят в отделните управляващите устройства. Използването на индивидуални (персонални) защитни стени създава значително административно натоварване, особено при промяна на тяхната конфигурация.

Компютърно-базираните защитни стени за сървъри и персоналните защитни стени за настолните и преносими персонални компютри предоставят допълнително ниво на сигурност при атаки по мрежата. Тези защитни стени са софтуерни, намират се в компютрите които защитават и всяка една от тях наблюдава и контролира мрежовия трафик към и от дадения компютър. Те предоставят по-детайлна защита в сравнение с мрежовите защитни стени, и по-добре отговарят на специфичните нужди на дадения компютър.

Компютърно-базираните защитни стени обикновено са достъпни като част от операционните системи на сървърите, например Linux, Windows, Solaris, BDS и Mac OS X Server, но могат да произхождат и от трети производители и да бъдат инсталирани допълнително. Конфигурирането на компютърно-базираната стена да позволява само необходимия трафик към сървъра осигурява защита срещу злонамерени дейности от всички останали компютри, включително и от тези които се намират в същата подмрежа или в други вътрешни подмрежи неразделени със защитни стени. Ограничаването на изходящия трафик на един сървър може да бъде използвано за противодействие на някои злонамерени програми, пречейки да бъдат заразявани и други компютри. Компютърно-базираните защитни стени обикновено извършват регистриране на събитията и често разрешават достъпа само от определени адреси и за конкретни приложения. Много от тях действат и като IPS, т.е. след подозрение за мрежова атака предприемат действия за противопоставяне на хакера и за предотвратяване на повреда в компютъра.

Персоналната защитна стена е софтуер, който работи на настолен или преносим компютър с потребителски насочена операционна система, например Microsoft Windows. Този софтуер изпълнява същите функции като компютърно-базираната защитна стена на сървъра, само интерфейсът е по-различен и естествено по-лесно разбираем за

обикновения потребител. Така се изгражда допълнително ниво на сигурност, особено за преносимите персонални компютри. Персоналната защитна стена обикновено не работи самостоятелно, а в пакет с други програми за сигурност.

Някои персонални защитни стени имат възможност за използване на различни профили (конфигурации) в зависимост от мястото където се намира компютъра, например профил за работа в мрежата на организацията и профил за работа при отдалечен достъп. Това е особено важно когато даден компютър се намира в ненадеждна външна мрежа, защото в профила му за такъв вид работа мрежовата активност ще бъде значително ограничена.

В допълнение към традиционното филтриране с проверка на състоянието на връзките, много персонални защитни стени могат да бъдат конфигурирани да позволяват комуникация въз основа на създадени списъци на разрешени сфери на приложение (например уеб браузъри да контактуват с уеб сървъри), и да не разрешават комуникация между други приложения. Такива защитни стени наричаме приложно-базирани защитни стени *(*application-based firewalls).

Управлението на персоналните защитни стени трябва да бъде централизирано, като се изгради ефективна система за създаване, разпространение и прилагане на политиките за достъп на всички потребители и групи. Така се гарантира, че политиката за сигурност на организацията ще бъде винаги в сила. Независимо от това дали персоналната защитна стена се управлява централно от администратора или от индивидуалния потребител, всички предупреждаващи съобщения, които се издават от стената, трябва да се показват на екрана на потребителя.

Има няколко въпроса, които трябва да бъдат разгледани при използването на защитни стени в ICS мрежи, а именно:

- Допълнителните закъснения в комуникациите на управляващата система, които са генерирани от защитните стени

- Липсата на опит в проектирането на подходящ набор от директиви за промишлени приложения. Защитните стени в ICS мрежите трябва да бъдат конфигурирани така, че да не позволяват входящ и изходящ трафик по подразбиране, т.е. в тези системи конфигурациите по подразбиране много често трябва да бъдат променяни.

Хардуерните защитни стени изискват постоянна поддръжка и архивиране. Наборът от директиви трябва непрекъснато да бъде преразглеждан, за да се гарантира, че той осигурява адекватна защита при непрекъснато променящите се заплахи за сигурността. Системните параметри (например обема на паметта предназначена за регистрационните файлове) трябва да бъдат непрекъснато наблюдавани, за да сме уверени, че защитната стена изпълнява своите задачи по събирането на данни и може да се разчита на нея в случай на нарушаване на сигурността. Необходимо е наблюдение на защитните стени в реално време, за да можем бързо да открием инцидент и да предприемем необходимите действия за неговото преодоляване.

5.4 Логическо разделяне на управляващата мрежа

Както вече беше подчертано, ICS мрежите и корпоративните мрежи трябва да бъдат разделени с цел подобряване на сигурността в тези мрежи. В този раздел се описват

няколко възможни архитектури на такова разделяне, като са изяснени предимствата и недостатъците на всяка една от тези архитектури.

Компютрите свързани към различни мрежи позволяват прехвърляне на трафик от едната мрежа в другата. На тези компютри трябва да бъде извършена и проверката на сигурността, т.е. да бъдат инсталирани защитни стени. Следователно, във всички връзки между управляващата мрежа и корпоративната мрежа трябва да се използват защитни стени.

5.4.1 Защитна стена между корпоративната мрежа и управляващата мрежа

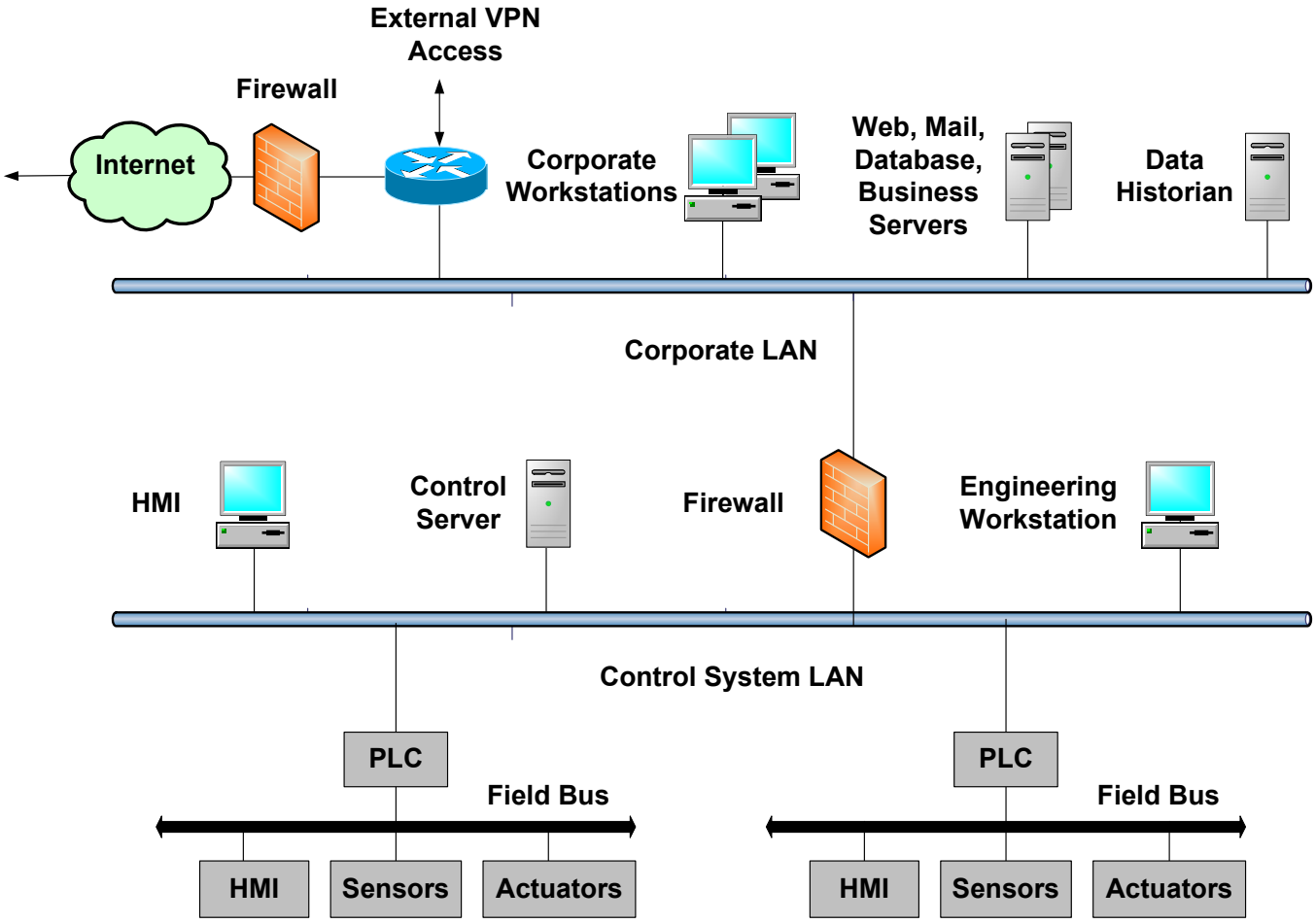
Значително подобрение на сигурността можем да постигнем, като поставим проста 2 портова защитна стена между двете мрежи (Фиг. 10). Такава стена обикновено предлага филтриране с проверка на състоянието на връзките на TCP пакетите и приложни посреднически (proxy) услуги за протоколите от приложния слой, като FTP, HTTP и SMTP. Едно подходящо конфигуриране на тази защитна стена може значително да намали възможността за успешна външна атака към управляващата мрежа.

За съжаление, в тази архитектура остават все още неразрешени въпроси. Ако сървърът за регистриране на събитията (Data Historian) се намира в корпоративната мрежа, (както е на Фиг.10) защитната стена трябва да му осигури достъп до устройствата намиращи се в управляващата мрежа. Пакет изпратен от злонамерен софтуер или просто от неправилно конфигуриран компютър в корпоративната мрежа може да бъде пропуснат от защитната стена и ще бъде препратен към PLC устройство.

От друга страна, ако сървърът се намира в управляващата мрежа, защитната стена трябва да осигури достъп до него на всички компютри от корпоративната мрежа. Обикновено това става със съобщения от приложния слой, като заявки на Structured Query Language (SQL) или на Hypertext Transfer Protocol (HTTP). Недостатъци в програмата на сървъра за регистриране могат да доведат до неговото компрометиране. Един път този сървър компрометиран, всички останали възли в управляващата мрежа са уязвими на червеи и интерактивни атаки.

Друг проблем е, че подправени пакети могат да бъдат изпратени в управляващата мрежа, при което съществува вероятност скрити данни да бъдат тунелирани обратно през разрешените протоколи. Например, ако HTTP пакети са разрешени за преминаване през защитната стена, тогава при случайно заразяване на HMI или преносим компютър на управляващата мрежа с вирус от типа троянски кон, тези устройства вече ще бъдат контролирани от отдалечено място и накарани да изпращат данни (например прихванати пароли).

В заключение, архитектурата е значително подобрение спрямо свързването без защитна стена, но тя изисква използване на набор от директиви на защитната стена, който набор трябва да позволява пряка комуникация между корпоративната мрежа и управляващите устройства. Като резултат са възможни евентуални нарушения в сигурността, ако системата не се проектира и наблюдава внимателно.



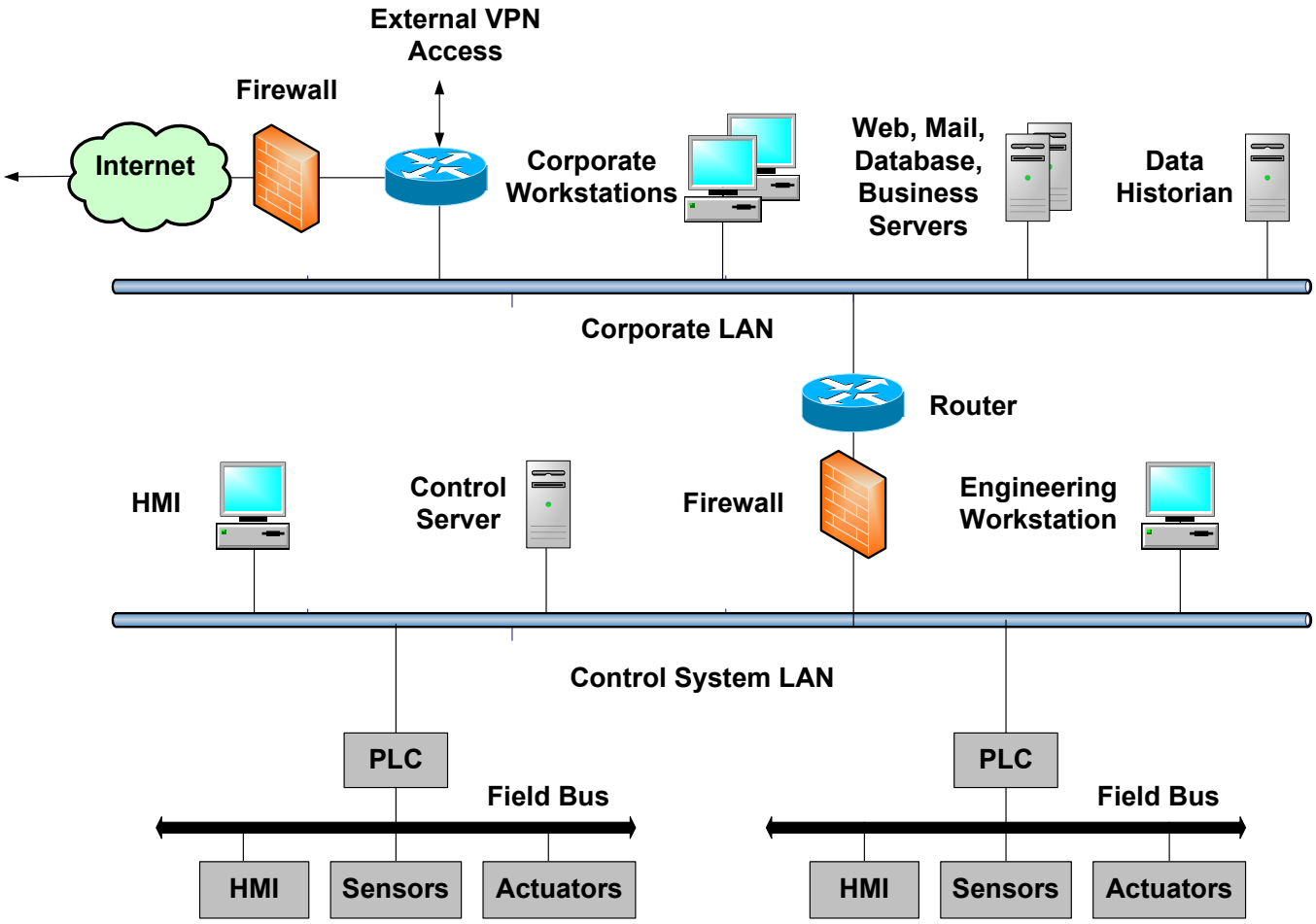
Фиг.10 Защитна стена между корпоративната мрежа и управляващата мрежа.

5.4.2 Защитна стена и маршрутизатор между корпоративната мрежа и управляващата мрежа

В малко по-изтънчената архитектура показана на Фиг.11 се използва комбинация от маршрутизатор и защитна стена. Маршрутизаторът е преди защитната стена и предлага основния пакет услуги за филтриране, докато защитната стена извършва по-сложните проверки, и е изградена или като стена за проверка на състоянието на връзките, или като стена използваща прокси технология. Този тип дизайн е много популярен при стените за свързване към Интернет, тъй като позволява бързият рутер да се справи успешно с по-голяма част от входящите пакети, особено при случай на DoS атака, като с това намалява натоварването на защитната стена. Тя също така предлага подобрена ешелонирана защита, тъй като имаме две различни устройства, които противникът трябва да преодолее [40].

5.4.3 Защитна стена с демилитаризирана зона между корпоративната и управляващата мрежи

Значително подобрение се постига, когато се използва защитна стена с възможност за създаване на DMZ между корпоративната и управляващата мрежи. Всяка DMZ има обикновено няколко основни компонента, като например сървър за регистриране на събитията, безжична точка на достъп, сървър за отдалечен достъп и т.н.

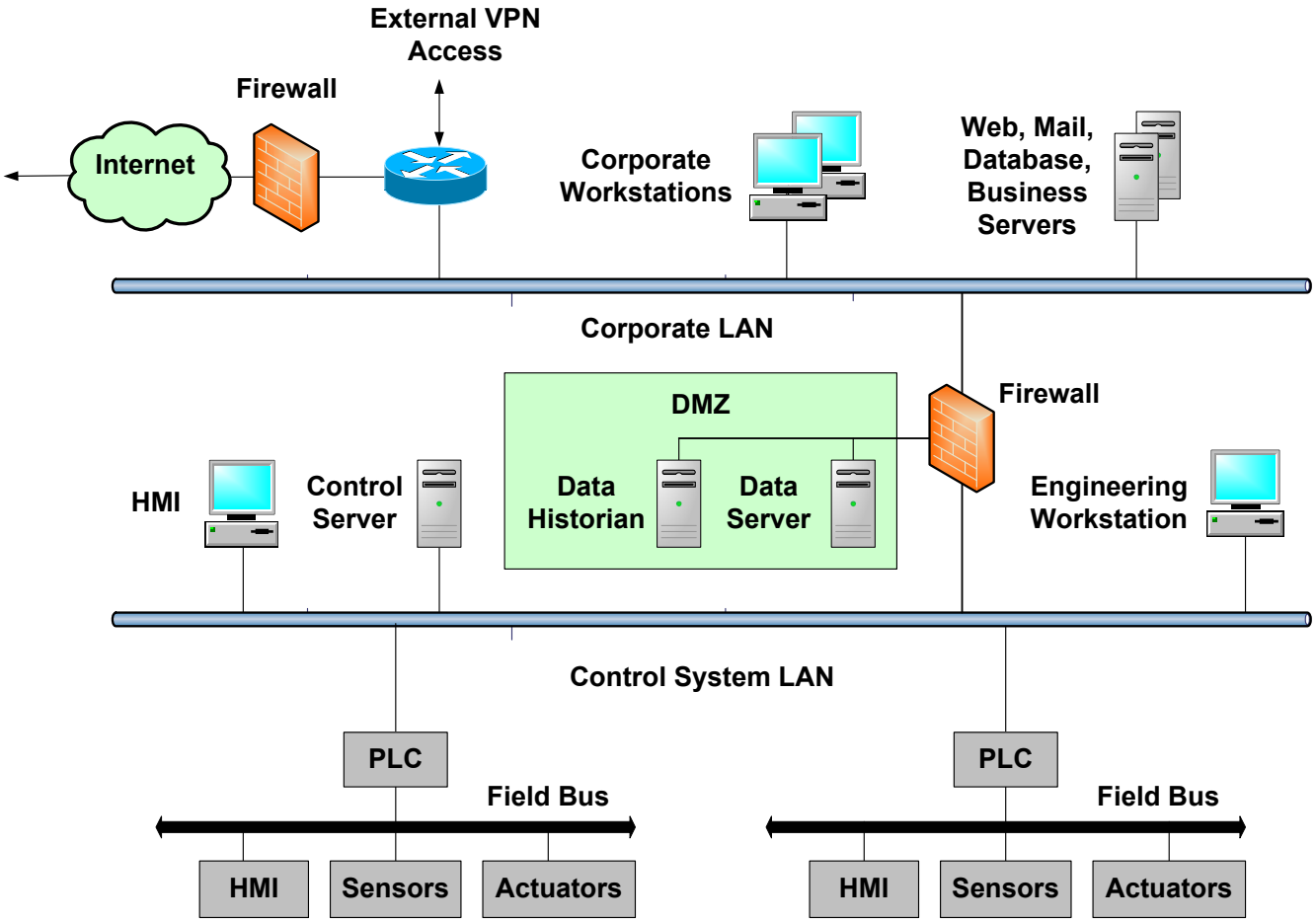


Фиг. 11 Защитна стена и маршрутизатор между корпоративната мрежа и управляващата мрежа

Създаването на DMZ изисква защитната стена да има три или повече интерфейса. Единият от тези интерфейси се свързва към корпоративната мрежа, вторият към управляващата мрежа, а останалите интерфейси се свързват към устройства за общ достъп или рискови устройства, като например сървър за регистриране на събитията, или безжични точки за достъп до DMZ мрежата. На Фиг.12 е даден пример за такава архитектура.

С поставянето в DMZ на компоненти на управляващата система, които трябва да са достъпни от страна на корпоративната мрежа, отпада изискването за директни комуникационни пътища от корпоративната до управляващата мрежа. Всеки такъв път реално свършва в DMZ. Повечето защитни стени позволяват няколко демилитаризирани зони, като може де се зададе какъв тип трафик да преминава между зоните.

Както се вижда от Фиг.12 защитната стена може да блокира произволен пакет от корпоративната мрежа да влезе в управляващата мрежа, както и да контролира трафика между останалите зони. С добре планиран набор от правила може да се постигне ясно разделяне между мрежите, като се гарантира малък или никакъв трафик между корпоративната и управляващата мрежа.



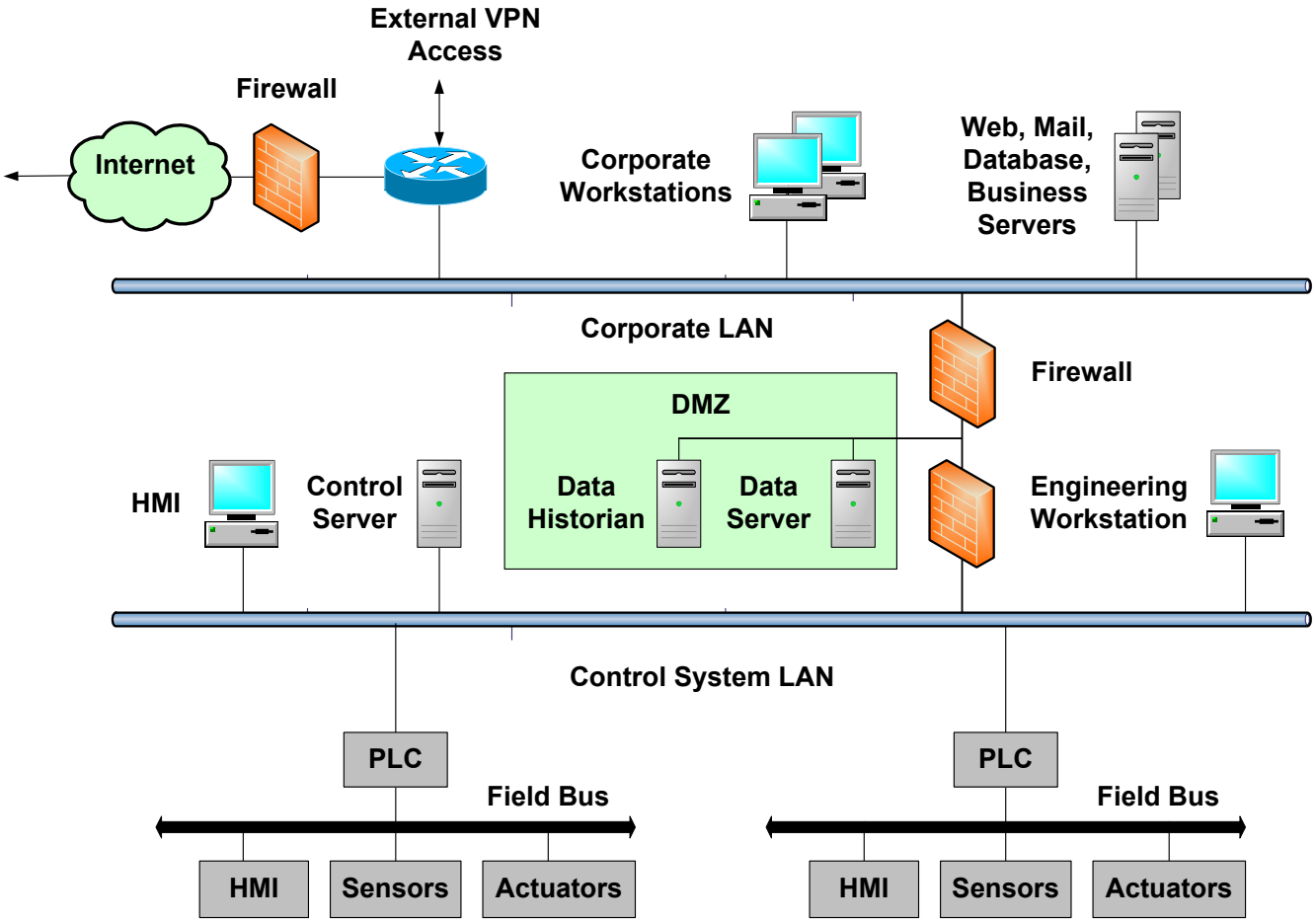
Фиг.12 Защитна стена с демилитаризирана зона между корпоративната и управляващата мрежи

Ако в управляващата система се използват различни сървъри по сигурността, например сървър за управление на кръпките (patch management server) и антивирусен сървър (antivirus server), то те трябва да се намират в DMZ. Един сървър може да изпълнява и двете функции. Желателно е антивирусният продукт избран за защита на ICS да бъде различен от антивирусния продукт използван в корпоративната мрежа. В случай че определен вирус успее да премине през единия продукт, то съществува голяма вероятност вторият продукт да го задържи.

Основният недостатък на тази архитектура е, че ако компютър в DMZ е компрометиран, то той може да служи за започване на атака на управляващата мрежа, като се използва приложния трафик позволен за преминаване от DMZ към мрежата. Този риск може да бъде значително намален, ако се положат съгласувани усилия за втвърдяване на политиките за защита на сървърите в DMZ, и едновременно с това, ако правилата на защитната стена позволяват осъществяване на връзка между DMZ и управляващата мрежа само по инициативата на управляващи устройства в тази мрежа. Друг недостатък на архитектурата е, че тя е твърде сложна, трудно се конфигурира, а освен това защитните стени с много портове са скъпи. В критично важни системи обаче, тези недостатъци могат да бъдат компенсирани със значителното подобряване на сигурността [40].

5.4.4 Двойка защитни стени между корпоративната и управляващата мрежи

Архитектурата от Фиг.12 може да бъде леко изменена, като между корпоративната мрежа и управляващата мрежа използваме двойка защитни стени, както е показано на Фиг. 13.



Фиг.13 Двойка защитни стени между корпоративната и управляващата мрежи

Общите сървъри, като например сървърът за регистриране на събитията, са разположени между двете защитни стени в мрежа подобна на демилитаризираната зона. Както и в описаните по-рано архитектури, първата защитна стена блокира определени пакети да преминават към управляващата мрежа или сървърите в DMZ. Втората защитна стена предотвратява нежелан трафик от компрометиран сървър в DMZ да проникне в управляващата мрежа, както и предпазва управляващата мрежа от влияние на трафика в DMZ върху нея.

Ако се използват защитни стени от два различни производителя, това решение предлага определени предимства. При него групата от управляващи специалисти и групата от IT специалисти имат ясно разграничени отговорности върху устройствата, които те управляват. Всяка от групите може да управлява своята защитна стена независимо. Основният недостатък на архитектурата с две защитни стени е високата цена и сложното управление. Предимствата са ярко изразени в системи със строги изисквания за сигурност и в системи при които е необходимо недвусмислено разграничаване на функциите на управляващите екипи.

5.5 Архитектура за ешелонирана защита (Defense-in-Depth Architecture)

От направените дотук разсъждения може да се направи извода, че една ICS система не може да бъде защитена с една софтуерна програма или технология, дори и да намерим изключително оригинално решение. Необходима ни е многослойна стратегия, включваща в себе си поне два (а най-добре и повече) взаимно препокриващи се механизми за сигурност. Такава стратегия се нарича ешелонирана защита (defense-in-depth), и тя помага в случай на провал на някой от механизмите за сигурност да сведем загубите до минимум. Архитектурата на ешелонираната защита включва използването на защитни стени, създаването на демилитаризирани зони, възможности за откриване на опити за проникване (intrusion detection), прилагане на ефективни политики за сигурност, програми за обучение и механизми за отговор при инциденти. Освен това ефективната стратегия за защита изисква задълбочено познаване на възможните начини за атакуване на ICS. Те включват използването на:

- Задни вратички и пролуки в параметъра на мрежата
- Пропуски в често срещаните протоколи
- Атакуване на полеви устройства
- Атакуване на базите данни
- Прихващане на комуникационни съобщения и др.

С разработването на такава стратегия за ешелонирана защита се занимава специално изградена комисия по препоръчителни практики за защитата на управляващи системи (Control Systems Security Program (CSSP) Recommended Practices) [41]. Допълнителни документи, които обхващат специфични въпроси и свързаните с тях предпазни мерки са включени в цитирания сайт. Там се дават и насоки за разработване на ешелонирани системи за организации, които използват управляващи мрежи, и същевременно поддържат информационна архитектура на няколко нива, която архитектура изисква:

- поддръжка на различни полеви устройства, събиране на телеметрични данни, и/или управление на технологични процеси,
- достъп до съоръжения с използване на отдалечени връзки и модеми,
- поддържане на обществени услуги за клиенти или извършване на корпоративни операции.

5.6 Основни политики реализирани със защитните стени на ICS

След като се установи архитектурата за ешелонирана защита, трябва точно да се определи какъв трафик да преминава през защитните стени. Много управленски екипи настояват конфигурирането на защитните стени да спре всякакъв трафик, с изключение на абсолютно необходимия за работата. Реалността обаче е доста по-сложна. Какво означава „абсолютно необходим за работата" и как точно се отразява влиянието на позволения трафик върху сигурността? За много организации например позволяването на SQL трафик през защитната стена е абсолютно необходим за работата на сървъра за

регистриране на събитията. За съжаление SQL е и разпространител на червея Slammer. Много важни протоколи използвани в промишлените приложения, като HTTP, FTP, OPC/DCOM, Ethernet/IP и MODBUS/TCP са значително уязвими по отношение на сигурността. По-долу са дадени някои правила за конфигуриране на индустриални защитни стени:

- Входящият трафик към управляващата мрежа трябва да бъде блокиран. Достъпът до устройствата на управляващата система трябва да става през DMZ.

- Изходящият трафик от управляващата мрежа трябва да бъде ограничен само до крайно необходимите комуникации.

- Целият изходящ трафик от управляващата мрежа към корпоративната мрежа трябва да бъде ограничен на принципа за точно съответствие между адресите на източника и местоназначението, на използваните портове и протоколи.

В допълнение към тези правила защитната стена трябва да бъде конфигурирана с изходящ филтър за спиране съмнителни IP пакети да напускат управляващата мрежа или DMZ. На практика това се постига чрез сравняване на IP адресите на изходящите пакети и съответния мрежови адрес на интерфейса на защитната стена. Целта е да се предотврати управляващата мрежа да стане източник на фалшифицирани пакети, които често се използват в DoS атаките. По този начин защитната стена е конфигурирана да препраща IP пакети само ако тези пакети имат верен адрес на източника в мрежата за управление или DMZ мрежата. И накрая, достъпът до Интернет през управляващите устройства трябва да се избягва, или най-добре изобщо да се забрани.

Следните правила трябва да се смятат като препоръчителни за общия набор от директиви на една промишлена защитна стена:

- Основното правило трябва да бъде, че всичко е забранено, нищо не е позволено (deny all, permit none).

- Разрешаването на портове и услуги за прехвърляне на трафик между управляващата мрежа и корпоративната мрежа трябва да става след анализ и даване на разрешение за всеки един случай поотделно.

- Всички разрешаващи (permit) правила трябва да са само за конкретни IP адреси и TCP/UDP портове, като се проверява състоянието на връзките ако е необходимо.

- Трафикът до определен адрес или диапазон от адреси може (а понякога и трябва) да бъде забранен напълно.

- Директният трафик между управляващата мрежа и корпоративната мрежа трябва да бъде прекъснат. Целият трафик трябва да има като крайна точка устройство в DMZ.

- Целият изходящ трафик от управляващата мрежа към корпоративната мрежа трябва да бъде ограничен само между конкретни устройства (адреси), за конкретни портове и услуги.

- На устройствата в управляващата мрежа не трябва да бъде разрешен достъп до Интернет.

- Управляващата мрежа не трябва да бъде пряко свързвана с Интернет, дори и през защитна стена.

- Трафикът за управление на самата защитна стена трябва да се извършва по отделна защитена мрежа, или по общата мрежа, но по кодиран канал с най-малко два автентикационни параметъра. Този трафик трябва да бъде ограничен до специфични адреси и портове.

5.7 Специфични въпроси при ICS защитните стени

В този раздел са разгледани по подробно два допълнителни проблема: мястото на сървъра за регистриране на събитията и възможностите за отдалечен достъп до управляващата мрежа.

5.7.1 Сървъри за регистриране на събитията

Съществуването на сървъри, които се използват едновременно от корпоративната мрежа и от управляващата мрежа, оказва значително влияние върху избора на защитната стена и нейното конфигуриране. Когато имаме комуникационна система с три отделни зони, поставянето на сървъра за регистриране на събитията в DMZ е очевидно, но в системи с две зони въпросът е доста по-сложен. Разполагането на този сървър в корпоративната мрежа означава, че много от несигурните протоколи, като MODBUS/TCP или DCOM, трябва да бъдат разрешени през защитната стена и всяко управляващо устройство, изпращащо данни към сървъра, се вижда в корпоративната мрежа. От друга страна разполагането на сървъра в управляващата мрежа означава, че на други, също съмнителни протоколи, като HTTP и SQL, трябва да се разреши достъпа през защитната стена, и сега имаме сървър, който е достъпен за всеки потребител в двете мрежи.

Най-доброто решение е да се избере архитектура с три зони, като в управляващата мрежа се сложи устройство за събиране на данни, а сървърът за регистриране на събитията се постави в DMZ. Но дори и това решение понякога е проблематично. Достъпът на голям брой потребители от корпоративната мрежа до сървъра за регистриране на събитията в DMZ може да подложи на изпитание производителността на защитната стена. Едно потенциално решение е да се инсталират два сървъра: един в управляващата мрежа, който да събира данните от управляващите устройства, и втори в корпоративната мрежа, който да е копие на първия и да отговаря на клиентските заявки. Тук трябва да бъде решен въпроса със синхронизацията на сървърите във времето. Трябва да се направи и отвор в защитната стена за директна комуникация сървър – сървър, но ако това се направи внимателно рискът ще бъде незначителен.

5.7.2 Отдалечен достъп до управляващата мрежа

Друг проблем при проектирането на промишлените защитни стени е осигуряването на отдалечен достъп на потребителите и/или доставчиците на оборудването (vendors) до управляващата мрежа. От всички потребители искащи достъп до управляващата мрежа от отдалечено място трябва да се изисква силна автентикация с подходящ механизъм, например с използване на маркери (token-based authentication).

Персоналът използващ отдалечен достъп, свързващ се по Интернет или по телефонни линии с модеми, трябва да използва при връзката си към корпоративната мрежа криптирани протоколи, като например виртуални частни мрежи (VPN) или защитен HTTP с вградени мощни многофакторни механизми за автентикация. Веднъж вече свързани към корпоративната мрежа, от тях трябва да се изисква втора автентикация при опит да минат през защитната стена, и тя пак трябва да бъде по някаква многофакторна схема базирана на маркери, за да получи накрая този персонал достъп до управляващата мрежа. За организациите, които не позволяват никакъв управляващ трафик да преминава през корпоративната мрежа, това ще изисква каскадиране, или решения с двойно тунелиране, като например използване на VPN базирана на Transport Layer Security (TLS) вътре във VPN базирана на IPSec.

6. Литература

[1] Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependences. *IEEE Control Systems Magazine, 21(6),* 11-25.

[2] Guide to Industrial Control Systems (ICS) Security, NIST Special Publication 800-82 Final Public Draft, September 2008.

[3] Frazer, Roy, *Process Measurement and Control - Introduction to Sensors, Communication Adjustment, and Control,* Prentice-Hall, Inc., 2001.

[4] International Electrotechnical Commission, EIC 61158, Digital Data Communications for Measurement and Control: Fieldbus of Use in Industrial Control Systems, 2003.

[5] Schneider Automation, Modbus Messaging on TCP/IP Implementation Guide, May 2002, http://www.modbus.org.

[6] Berge, Jonas, *Fieldbuses for Process Control: Engineering, Operation, and Maintenance*, ISA, 2002.

[7] Erickson, Kelvin, and Hedrick, John, *Plant Wide Process Control,* Wiley & Sons, 1999.

[8] Salvatore Cavalieri, *Foundation Fieldbus: History and Features,* in the Industrial Communication Technology Handbook, Edited by Richard Zurawski, 2005.

[9] Richard Kirk, *The Four Myths of Cyber Security*, http://www.networksecurityedge.com/content/four-myths-cyber-security

[10] Eric Byres, John Kay, Joel Carter, *Myths and Facts Behind Cyber Security of Industrial Control*, http://www.pimaweb.org/conference/april2003/pdfs/MythsAndFactsBehindCyber Security.pdf

[11] Thilo Sauter, *Fieldbus Systems: History and Evolution*, in the Industrial Communication Technology Handbook, Edited by Richard Zurawski, 2005.

[12] D.J. Damsker, Assessment of Industrial Data Network Standards, IEEE Tran. Energy Conversion, 3, 199-204, 1988.

[13] M. Felser and T. Sauter, *The fieldbus war: history or short break between battles?*, in IEEE International Workshop on Factory Communication Systems (WFCS), Vasteras, Sweden, August 2002, pp.73-80.

[14] J.P. Thomesse, *Fieldbuses and interoperability*, Control Engineering Practice, 7, 81-94, 1999.

[15] M. Wollschlaeger, *Framework for Web integration of factory communication systems*, in IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Antibes Juan-les-Pins, France, October 2001, pp. 261-265.

[16] M. Volz*, Quo vadis Layer 7?* The Industrial Ethernet Book, Issue 5, spring 2001,

[17] S. Soucek, T. Sauter, and T. Rauscher, *A scheme to determine QoS requirements for*

control network data over IP, in 27th Annual Conference of the IEEE Industrial Electronics Society (IECON), Denver, CO, 2001.
[18] F.L. Lian, I.R. Moyne, and D.M. Tilbury, *Performance evaluation of control networks: Ethernet, ControlNet and DeviceNet,* IEEE Control Systems Magazine, 21, 2001.
[19] *EIA-852 draft, Tunneling of Component Network Data over IP Channels*, April 2000.
[20] P. Pedreiras, L. Almeida, *Approaches to enforce real-time behavior in Ethernet,* http://www.iestcfa.org/books/ict_pedreiras.htm
[21] Decotignie, J-D. *A perspective on Ethernet as a Fieldbus*. Proceedings of the 4th FeT'2001 International Conference on Fieldbus Systems and their Applications, Nancy, France, 2001.
[22] Varadarajan, S., Chiueh, T., *EtheReal: A Host-Transparent Real-Time Fast Ethernet Switch*. Proceedings of the 6th International Conference on Network Protocols, Austin, USA, 1998.
[23] Lo Bello, L., O. Mirabella. *Design issues for Ethernet in Automation*. Proceedings of the 4th FeT'2001 International Conference on Fieldbus Systems and their Applications, Nancy, France, 2001
[24] Kweon, S-K., K. G. Shin, Q. Zheng. *Statistical Real-Time Communication over Ethernet for Manufacturing Automation Systems*. Proceedings of the 5th IEEE Real-Time Technology and Applications Symposium. June 1999.
[25] Andrew S. Tanenbaum. *Computer Networks*, 4th Edition". Prentice Hall. September 2002.
[26] LeLann, G, N. Rivierre. *Real-Time Communications over Broadcast Networks: the CSMA-DCR and the DOD-CSMA-CD Protocols.* INRIA Report RR1863. 1993.
[27] Malcolm, N., W. Zhao. *Hard Real-Time Communications in Multiple-Access Networks*. Real Time Systems 9, 75-107. Kluwer Academic Publishers. 1995.
[28] Malcolm, N., W. Zhao, *The Timed-Token Protocol for Real-Time Communications*, IEEE Computer 27(1), January 1994.
[29] Venkatramani, C., T. Chiueh. *Supporting Real-Time Traffic on Ethernet*. Proceedings of IEEE Real-Time Systems Symposium. San Juan, Puerto Rico. December 94.
[30] Martínez, J., Harbour, M., Gutiérrez, J. *A Multipoint Communication Protocol Based on Ethernet for Analyzable Distributed Applications*, Proc. of the 1st Int. Workshop on Real-Time LANs in the Internet Age, RTLIA'02, Vienna, Austria. Published by Edições Politema, Porto, Portugal, 2002.
[31] Kopetz, H., Damm, A., Koza, C., Mulazzani, M., Schwabl, W., Senft, C., Zainlinger, R. *Distributed Fault-Tolerant Real-Time Systems: The MARS approach*, IEEE Micro, 9(1). February 1989.
[32] Schabl, W., Reisinger, J., Grunsteidl, G. *A Survey of MARS*. Vienna University of Technology, Austria. Research Report Nr. 16/89. October 1989.
[33] Willig A. *A MAC Protocol and a Scheduling Approach as Elements of a Lower Layers Architecture in Wireless Industrial LANs*. Proceedings of WFCS '97 (IEEE Int. Works. On Factory Communication Systems). Barcelona, Spain. October, 1997.
[34] *ETHERNET Powerlink protocol*, available at www.ethernet-powerlink.org
[35] Pedreiras, P., Gai, P., Almeida, L.*The FTT-Ethernet Protocol: Merging Flexibility, Timeliness and Efficiency*, Proceedings of the 14th Euromicro Conference on Real-Time Systems. Vienna, Austria. IEEE Press, 2002.
[36] Jasperneit, J., P. Neumann. *Switched Ethernet for Factory Communication*. Proceedings of ETFA2001 – 8th IEEE International Conference on Emerging Technologies and Factory Automation. Antibes, France. October 2001.
[37] Hoang, H. Jonsson, M., Hagstrom, U., Kallerdahl, *A. Switched Real-Time Ethernet with Earliest Deadline First Scheduling - Protocols and Traffic Handling*. Proceedings of WPDRTS 2002, the 10th Intl. Workshop on Parallel and Distributed Real-Time Systems. Fort Lauderdale, Florida, USA. April 2002.

[38] Varadarajan, S., Chiueh, T. *EtheReal: A Host-Transparent Real-Time Fast Ethernet Switch*. Proceedings of the 6th International Conference on Network Protocols, Austin, USA. October 1998.
[39] Karen Scarfone, Paul Hoffman, *Guidelines on Firewalls and Firewall Policy*, NIST Special Publication 800-41.
[40] *NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks,* National Infrastructure Security Coordination Centre, London, 2005, http://www.cpni.gov.uk/docs/re-20050223-00157.pdf
[41] *CSSP Recommended Practices*, http://csrp.inl.gov/