«یا ذا الامن و الامان»

# امن سازی سیستم‌های کنترل و اتوماسیون صنعتی:
# با محوریت چالشهای پروتکل IEC 60870-5-104

# مقدمه‌ای از سامانه‌های کنترل صنعتی

- سامانه صنعتی
  مرکب از
  - سامانه‌های فناوری اطلاعات ⇦ هدف: تسهیل فرآیندهای تجاری و مدیریتی
  - سامانه‌های کنترل صنعتی[1]
    - متشکل از اجزای متعددی شامل حسگرها، محرک‌ها، واحدهای پردازش داده مانند کنترل کننده های منطقی قابل برنامه ریزی(PLC) و دستگاه های ارتباطی تشکیل می شوند.
    - وظیفه کنترل و هدایت فرایندها و اجزاء فیزیکی

- نفت و گاز
- برق
- آب
- پالایش و پتروشیمی
- حمل و نقل و خودرو
- فلزات (فولاد، مس و ...)
- داروسازی
- هوا فضا
- ....



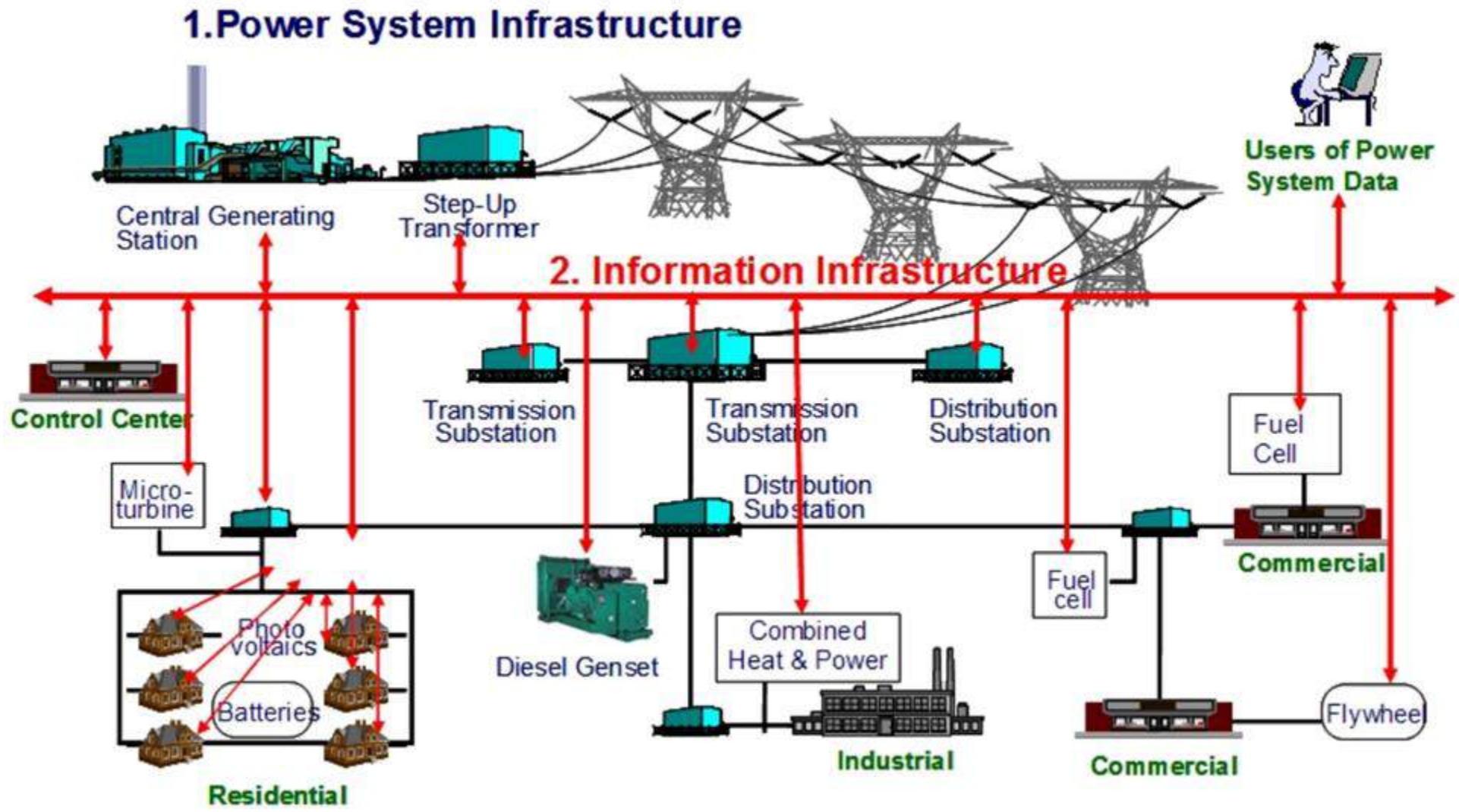



تبعات جبران ناپذیر ⇦

- اقتصادی
- سیاسی /بین المللی
- جانی / انسانی
- محیط زیست

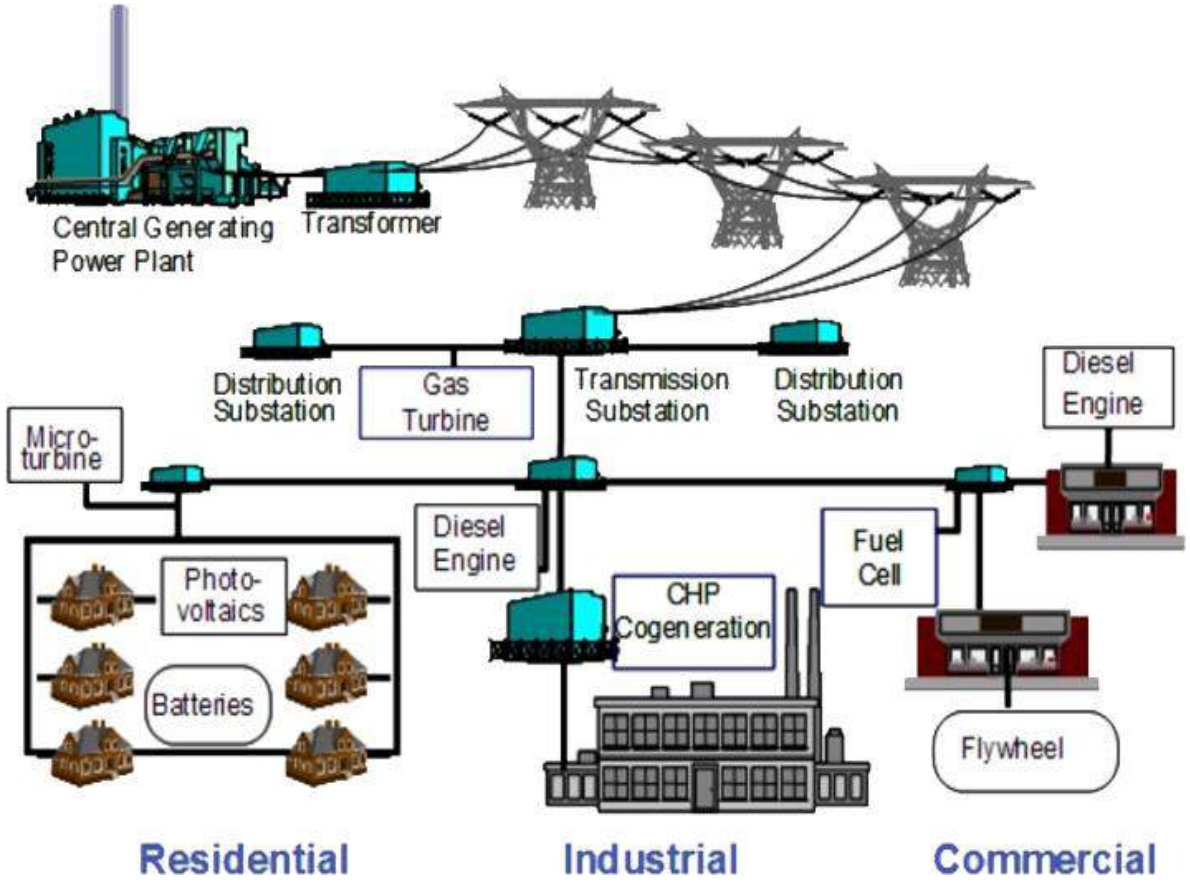
1.ICS: Industrial Control System(s)

# زیرساخت‌ها

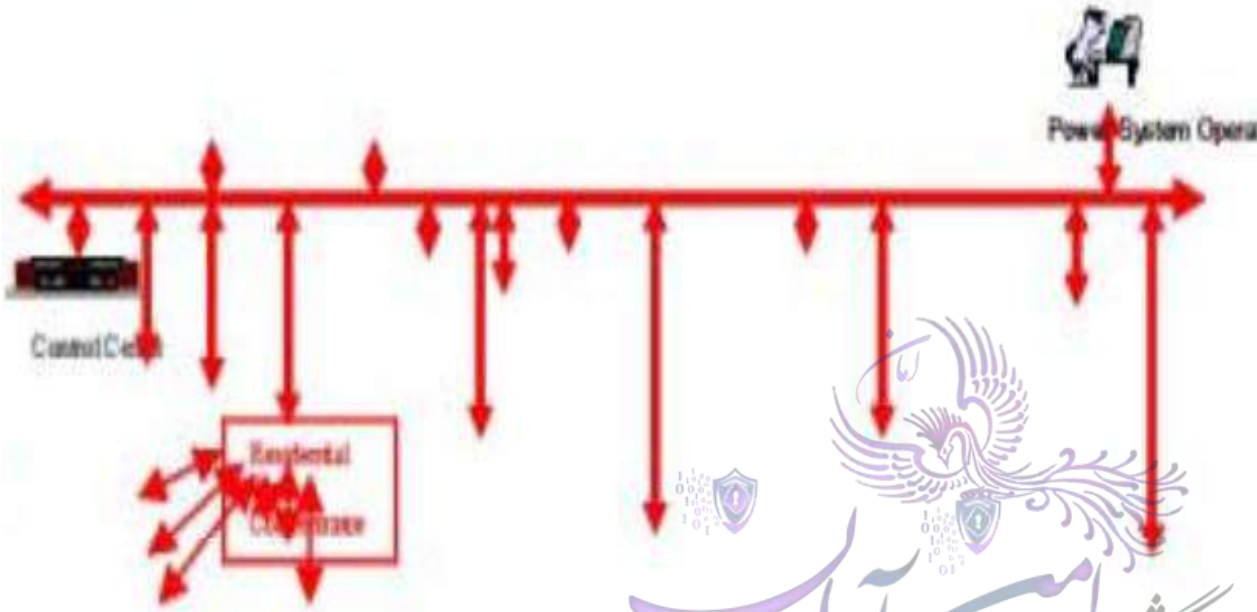

1.Power System Infrastructure
Central Generating Station
Step-Up Transformer
Users of Power System Data
2. Information Infrastructure
Control Center
Transmission Substation
Transmission Substation
Distribution Substation
Fuel Cell
Micro-turbine
Distribution Substation
Commercial
Fuel cell
Photo voltaics
Batteries
Diesel Genset
Combined Heat & Power
Industrial
Commercial
Flywheel
Residential

# ادغام زیرساخت‌ها

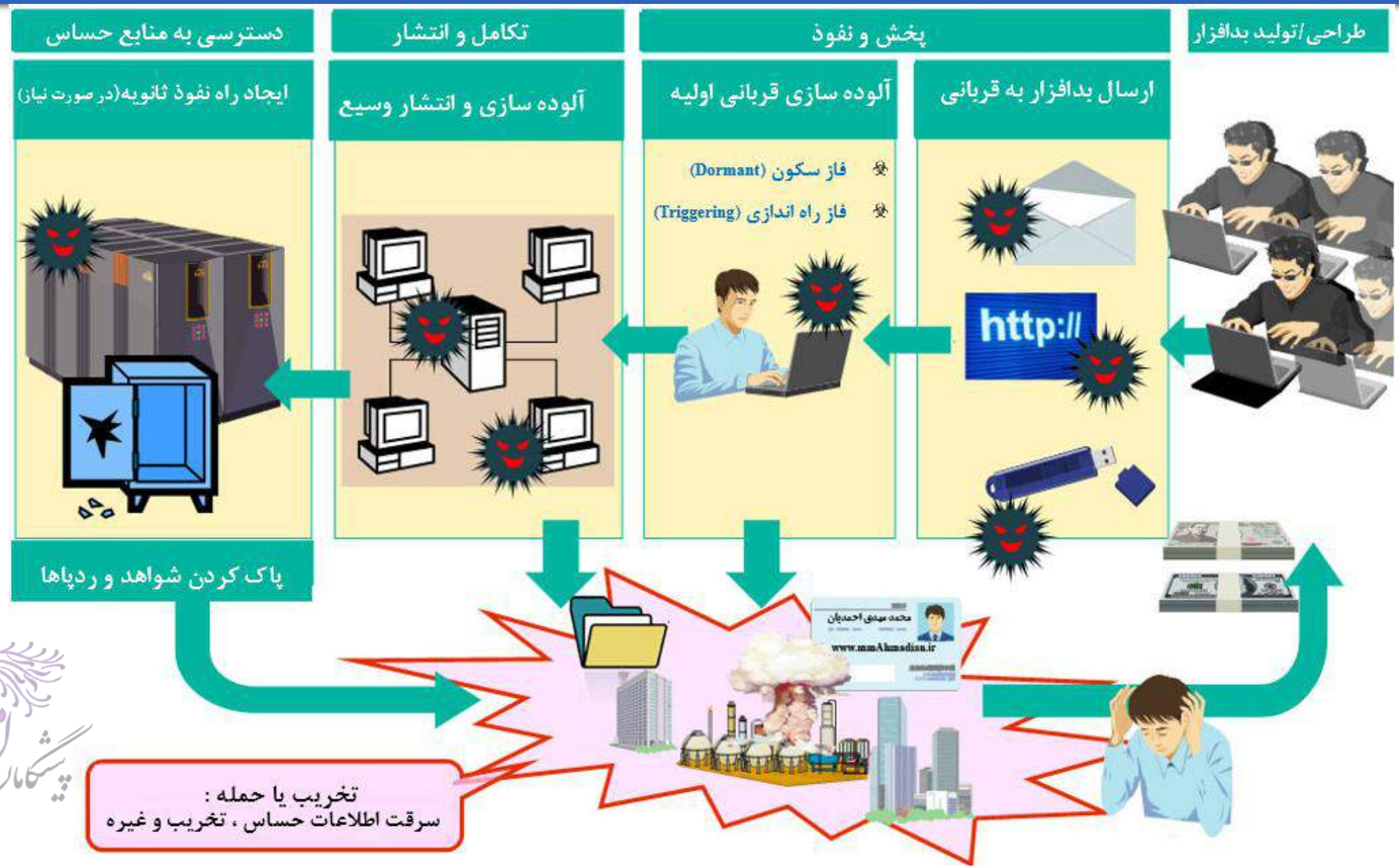
زیرساخت کنترل صنعتی



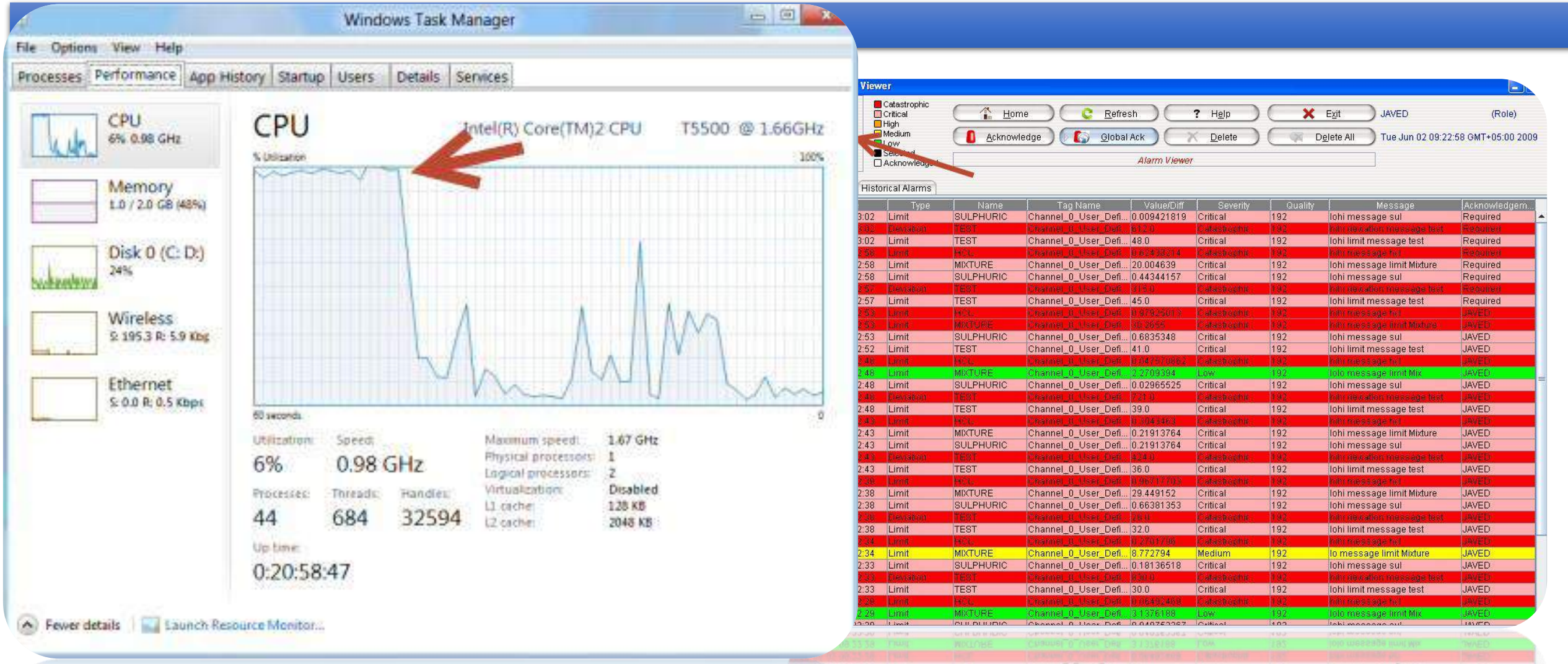

زیرساخت اطلاعاتی



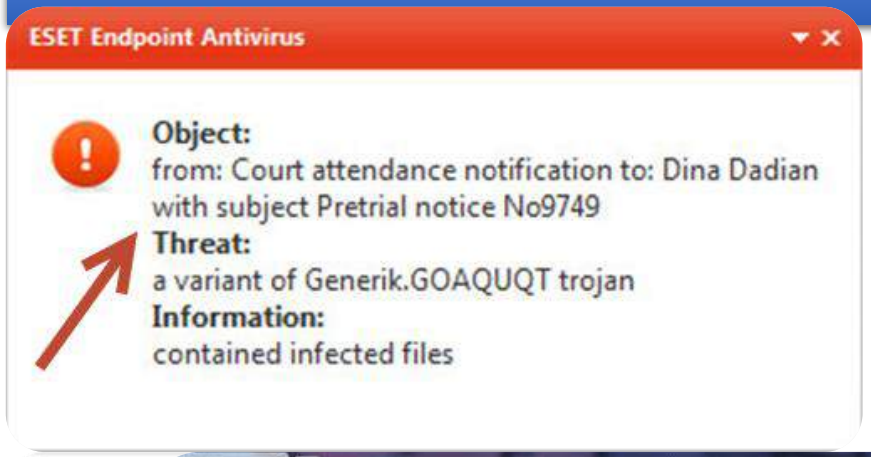
# نمونه تهدیدات

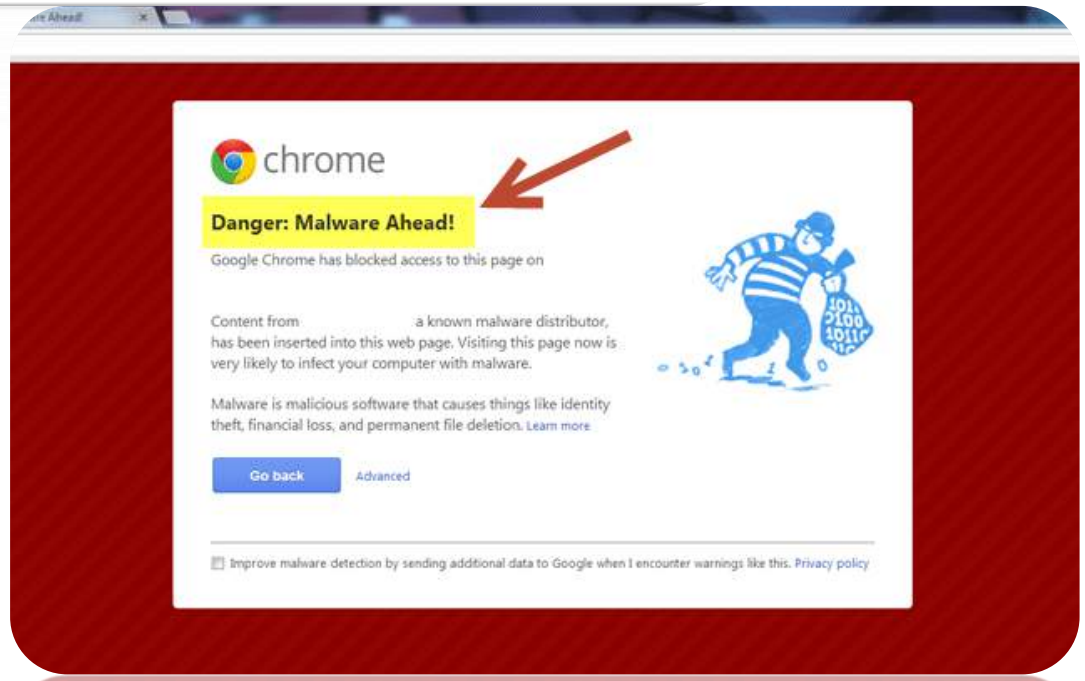


# نمونه تهدیدات

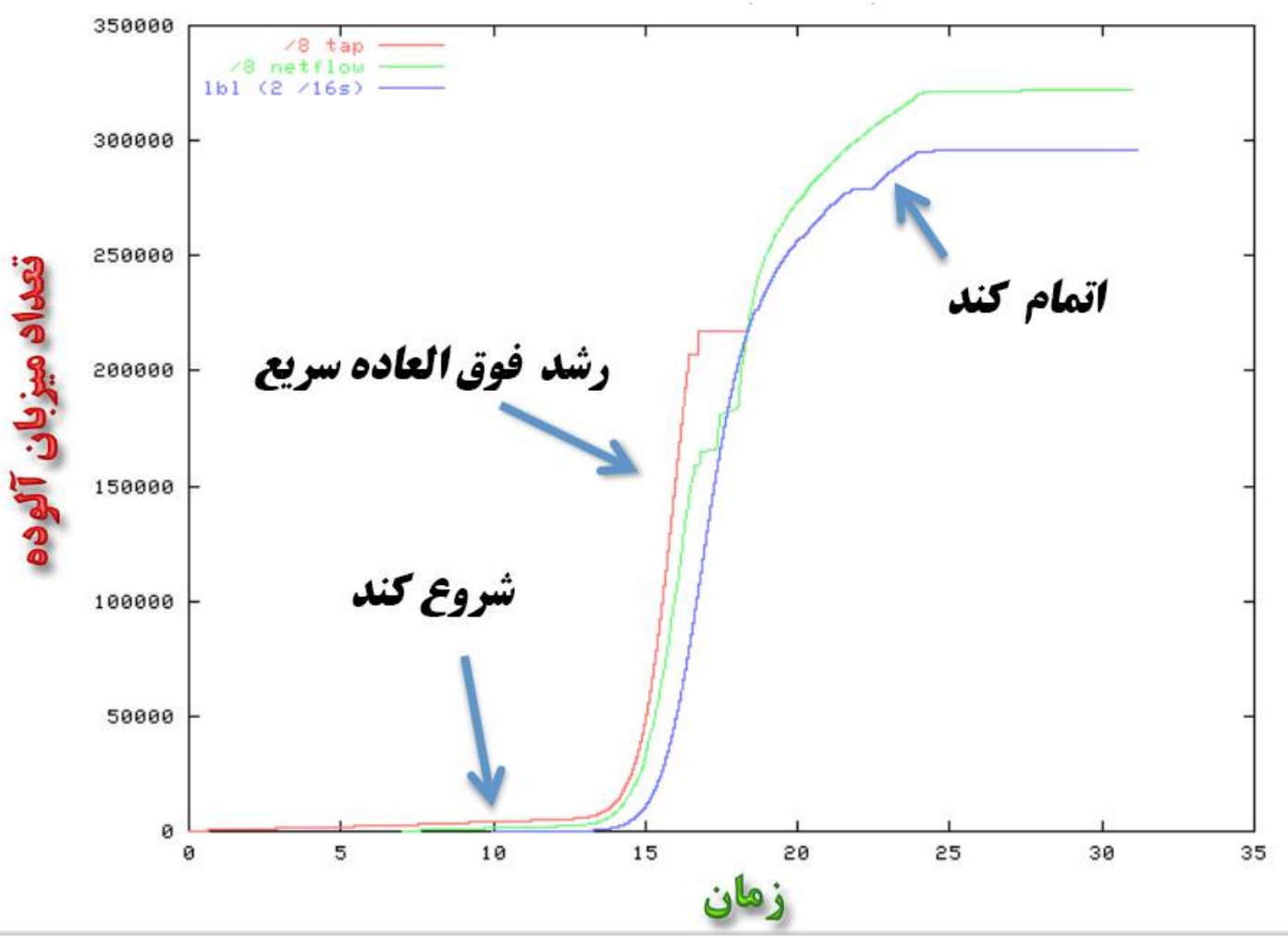


# نمونه تهدیدات



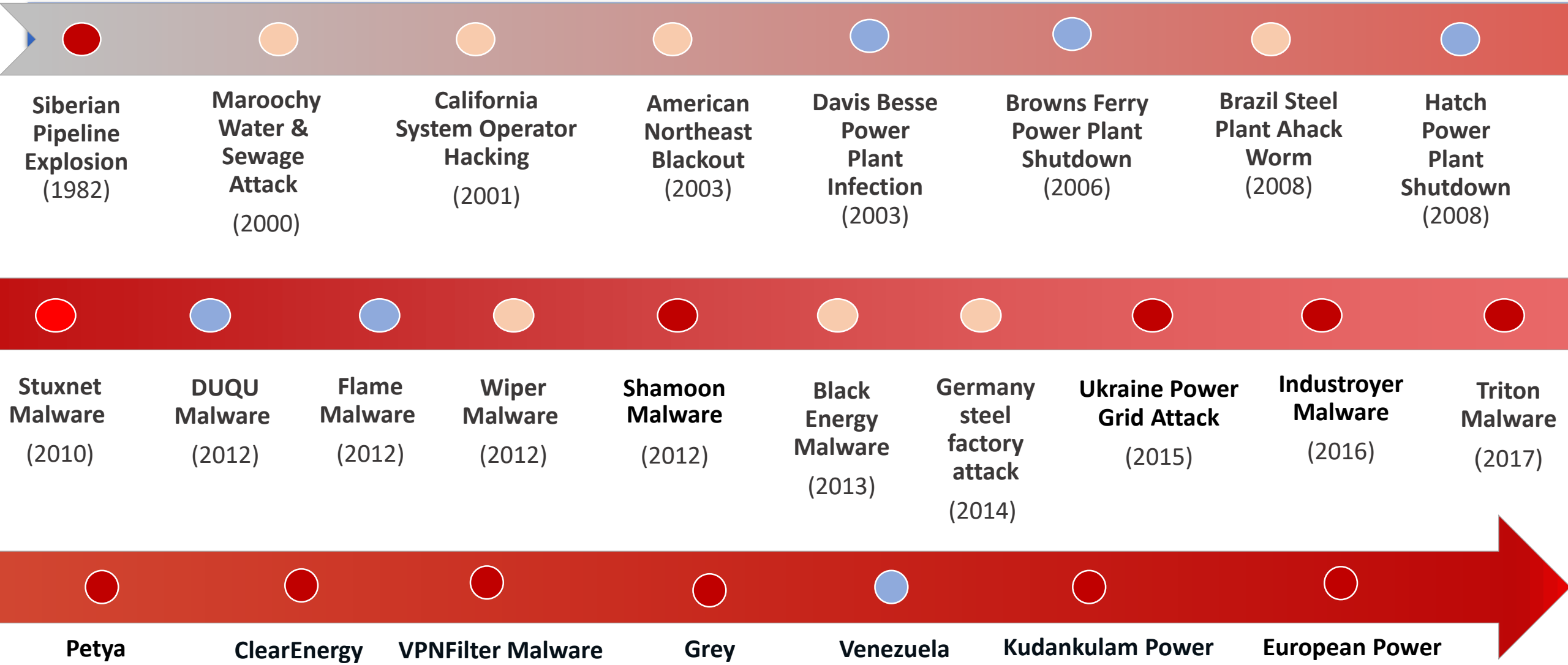

# نمونه تهدیدات



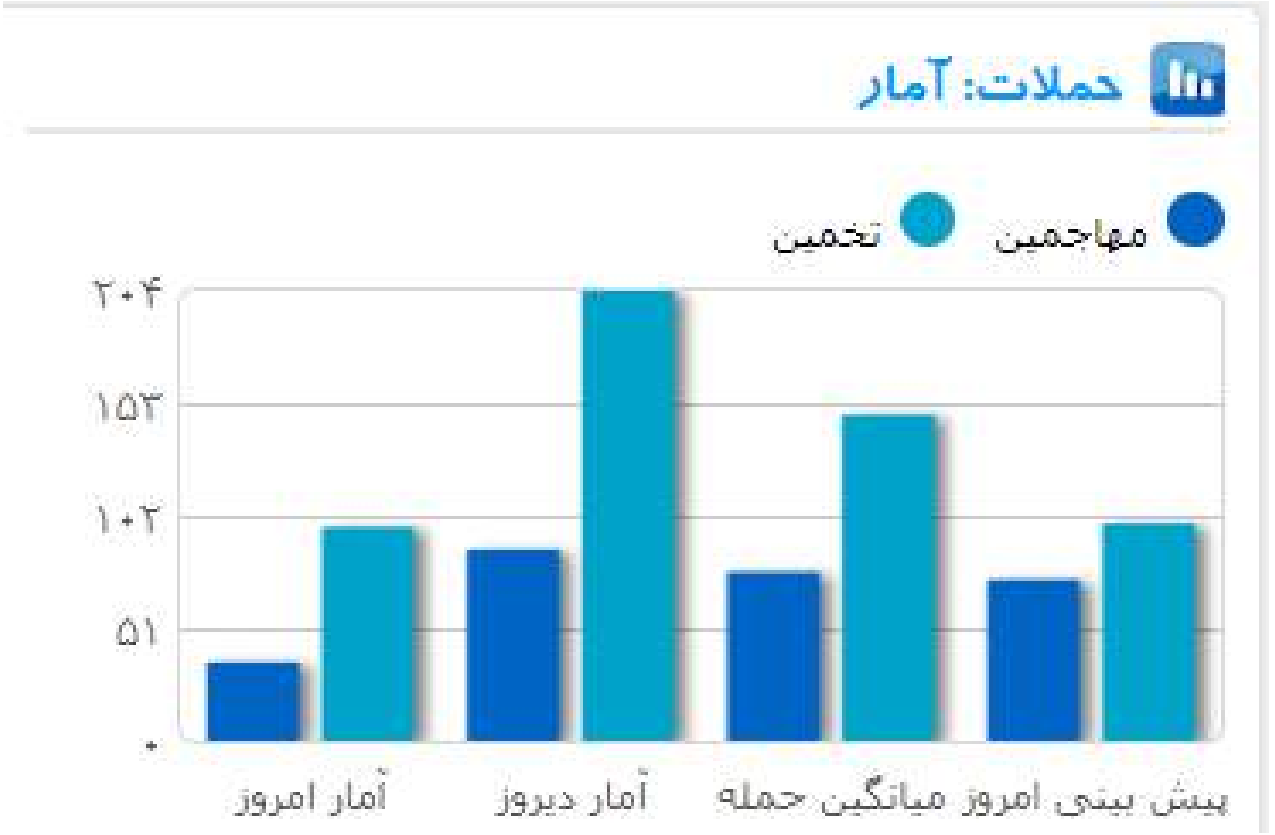
# IT / OT


دنیای فناوری اطلاعات و امکانات آن همانند کوهستان برفی زیبایی
است که اگر بدون شناخت قصد صعود از آن را داشته باشید، هر لحظه
امکان سقوط شما وجود دارد؛ پس اگر شناخت کافی از این کوهستان
زیبا ندارید، سعی کنید هر گام خود را دقیقاً در جایی بگذارید که یک
متخصص امنیتی قبلا آنجا گام گذاشته باشد و آن را بررسی کرده باشد.
محمد مهدی احمدیان / کتاب هنر امنیت

# نمونه حملات و رخدادها



# رصد رخدادهای سایبری

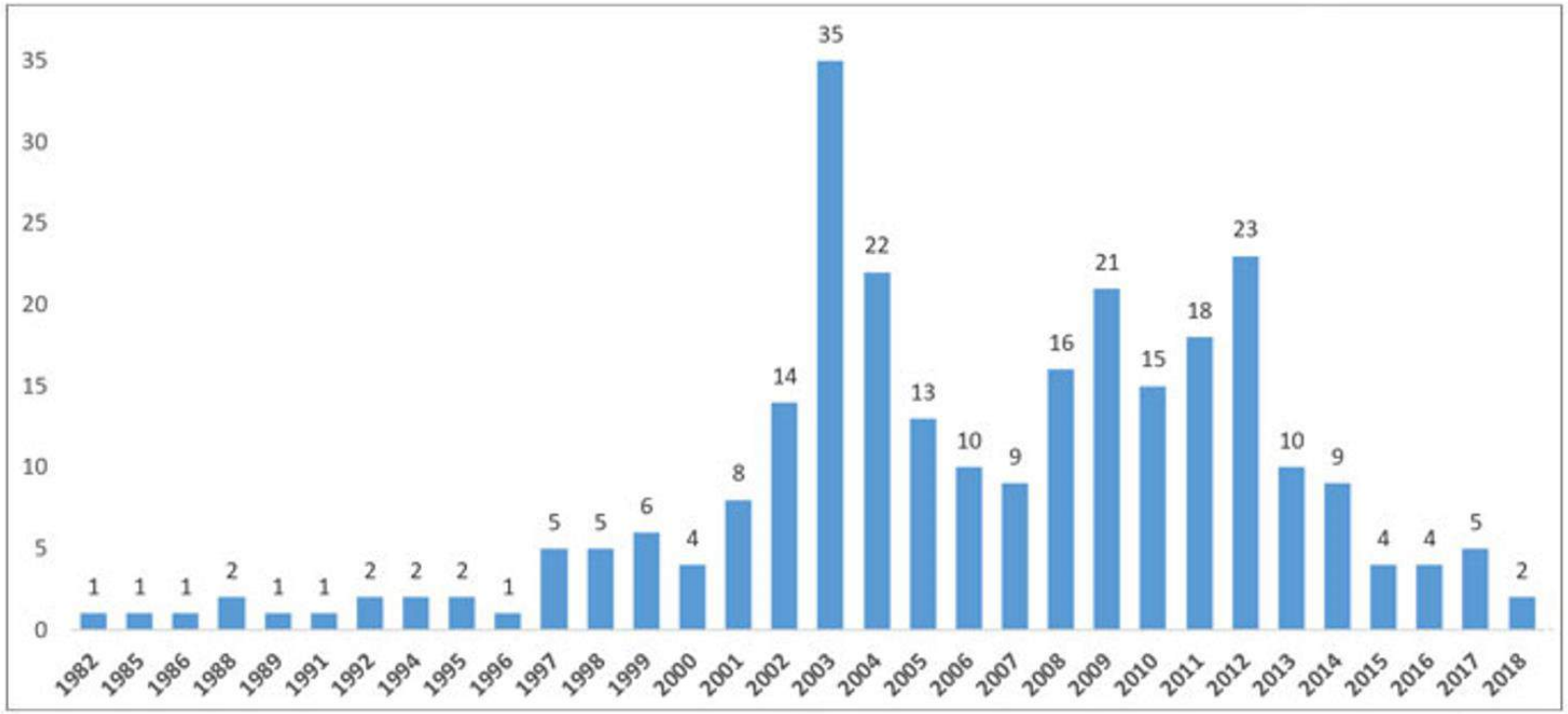



| آمار کل | مهاجم | نمایش |
|---|---|---|
| آمار کل | ۱۵۶۴۶۴ | ۳۰۲۶۷۵ |
| آمار امروز | ۳۶ | ۹۶ |
| آمار دیروز | ۸۶ | ۲۰۲ |
| در حال حمله | ۰ | |
| میانگین حمله | ۷۵ | ۱۴۶ |
| پیش بینی امروز | ۷۲ | ۹۷ |

مشاهده آمار به صورت تفصیلی

# آمار حملات و حوادث سایبری

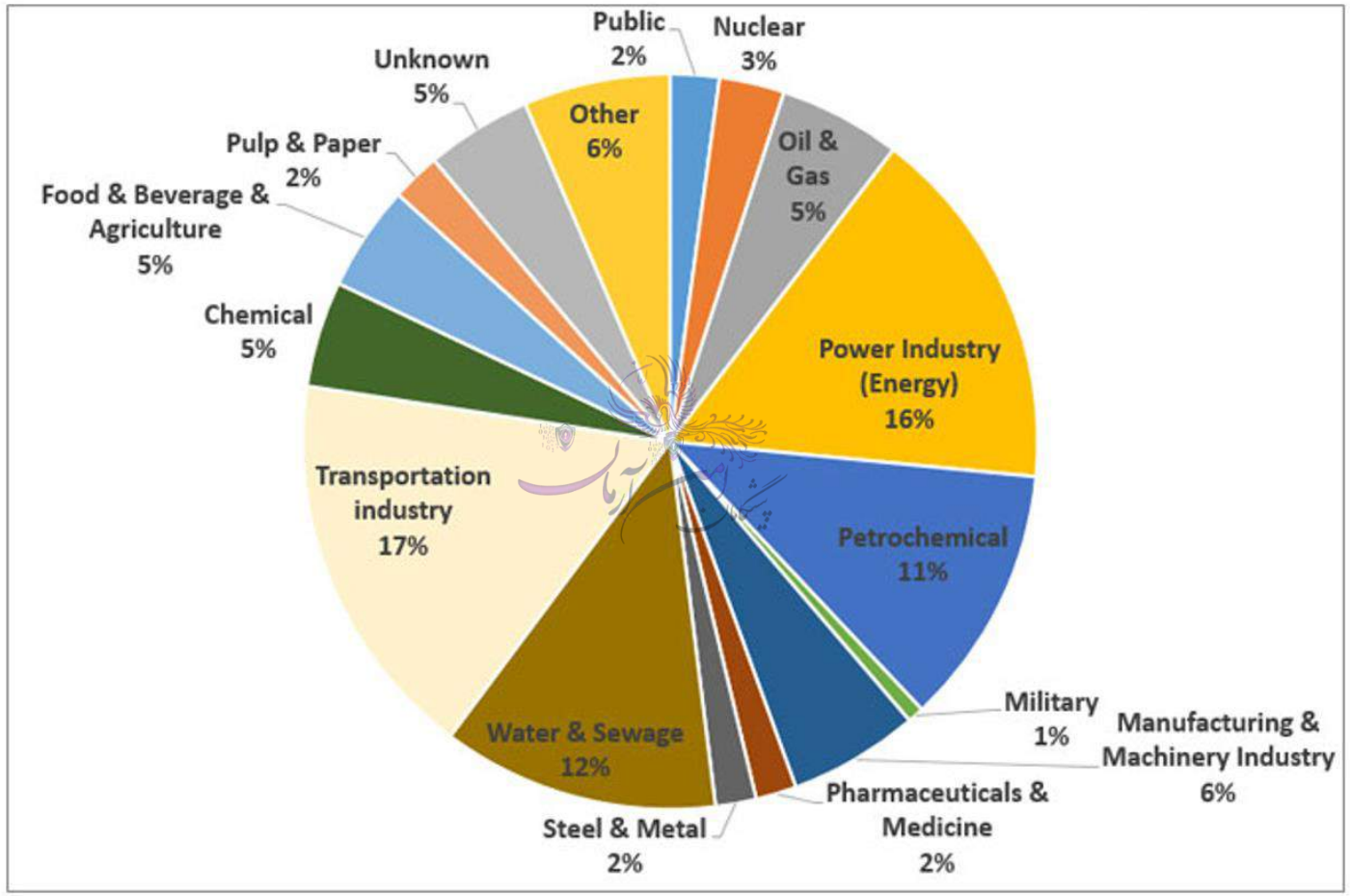
- تحلیل ۲۶۸ رخداد صنعتی
  - ۱۴۷ حمله
  - ۱۲۱ رخداد امنیتی غیرتهاجمی




Ref.: Ahmadian et al. Industrial Control System Security Taxonomic Framework with Application to a Comprehensive Incidents Survey, *International Journal of Critical Infrastructure Protection* (2020), doi:https://doi.org/10.1016/j.ijcip.2020.100356

# رصد رخدادهای سایبری

1. حمل و نقل
2. صنعت برق
3. پتروشیمی
4. آب و فاضلاب
5. نفت و گاز و ...




Ref.: Ahmadian et al. Industrial Control System Security Taxonomic Framework with Application to a Comprehensive Incidents Survey, *International Journal of Critical Infrastructure Protection* (2020), doi:https://doi.org/10.1016/j.ijcip.2020.100356

# از چالش‌های پروتکل‌های بسته تا چالش‌های پروتکل‌های باز

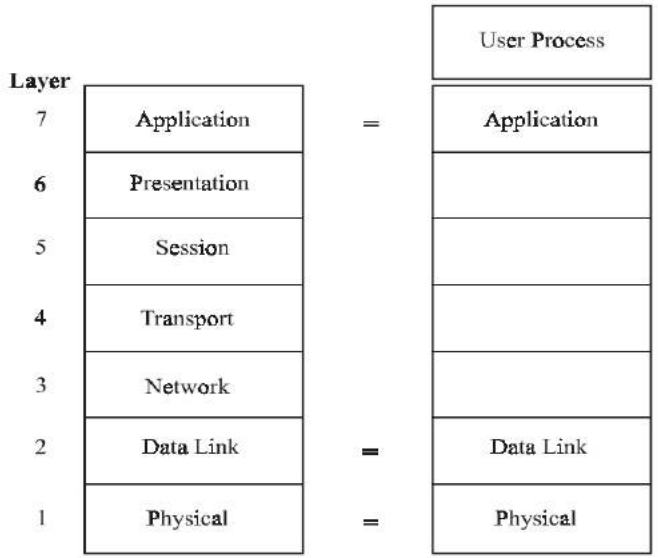
- راهبرد امنیت از طریق ایجاد ابهام (به واسطه پروتکل‌ها و واسط‌های اختصاصی) به تنهایی به سود آنها است( باور اشتباه )
- بررسی امنیتی تجهیزات و پروتکل‌های صنعتی بسته، دشوار است.

- گذر از سامانه‌های اختصاصی به معماری باز
  - ایستگاه کاری مهندسی مبتنی بر ویندوز
  - شبکه‌های TCP/IP
  - IEC61850
  - OPC
  - IEC 60870
  - ...

# پروتکل IEC 104(T104)

- IEC 60870-5-104
- در سال ۲۰۰۰ جهت سیستم‌های اسکادای برق طراحی شد(برای ارتباطات میان RTUها و RTUها با MTUها).
- هدف از این استاندارد، استفاده از داده‌های لایه کاربرد پروتکل ۶۰۸۷۰ -۵ روی شبکه‌های دیجیتال داده توسط پروتکل TCP/IPبود.

| Layer | Source | Selections |
|---|---|---|
| User Process | IEC 60870-5-101 | Application functions |
| Application | IEC 60870-5-101 | ASDUs and Application Information Elements. |
| Transport | TCP / IP Transport and network protocol suite | |
| Network | | |
| Link | | |
| Physical | | |



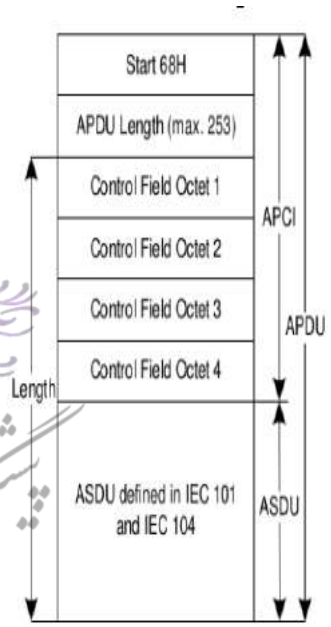

[۴۶]

# ساختار استاندارد ۶۰۸۷۰-۵-۱۰۴

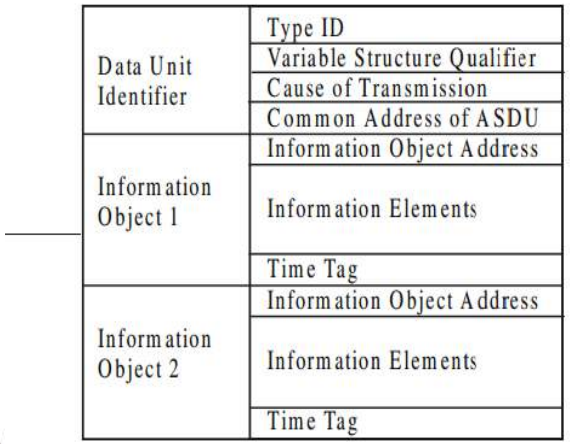
- در حالت کلی طول بسته T104متغیر است که با قالب فیلد کنترلی محدود می‌شود.

جدول ۴: ساختار تشریحی پی‌آیند بسته IEC 60870-5-104

| بایت/بیت | ۷ | ۶ | ۵ | ۴ | ۳ | ۲ | ۱ | ۰ | | |
|---|---|---|---|---|---|---|---|---|---|---|
| ۰ | بایت آغاز (0x68) | | | | | | | | APCI | APDU |
| ۱ | طول APDU (حداکثر ۲۵۳) | | | | | | | | | |
| ۲ | فیلد کنترلی ۱ | | | | | | | | | |
| ۳ | فیلد کنترلی ۲ | | | | | | | | | |
| ۴ | فیلد کنترلی ۳ | | | | | | | | | |
| ۵ | فیلد کنترلی ۴ | | | | | | | | | |
| ۶ | شناسایی نوع (TypeID) | | | | | | | | ASDU | |
| ۷ | تعداد اشیا (NumIX) | | | | | | | SQ | | |
| ۸ | علت انتقال (COT) | | | | | | P/N | T | | |
| ۹ | آدرس منبع (ORG) | | | | | | | | | |
| ۱۰ | فیلدهای آدرس ASDU (Addr) | | | | | | | | | |
| ۱۱ | (بایت دوم) | | | | | | | | | |
| ۱۲ | فیلدهای آدرس اشیا اطلاعاتی(IOA) | | | | | | | | | |
| ۱۳ | (بایت دوم) | | | | | | | | | |
| ۱۴ | (بایت سوم) | | | | | | | | | |
| ۱۵ | اطلاعات شیء | | | | | | | | | |
| ... | | | | | | | | | | |
| ... | | | | | | | | | | |
| ... | | | | | | | | | | |
| n-1 | | | | | | | | | | |
| n | | | | | | | | | | |

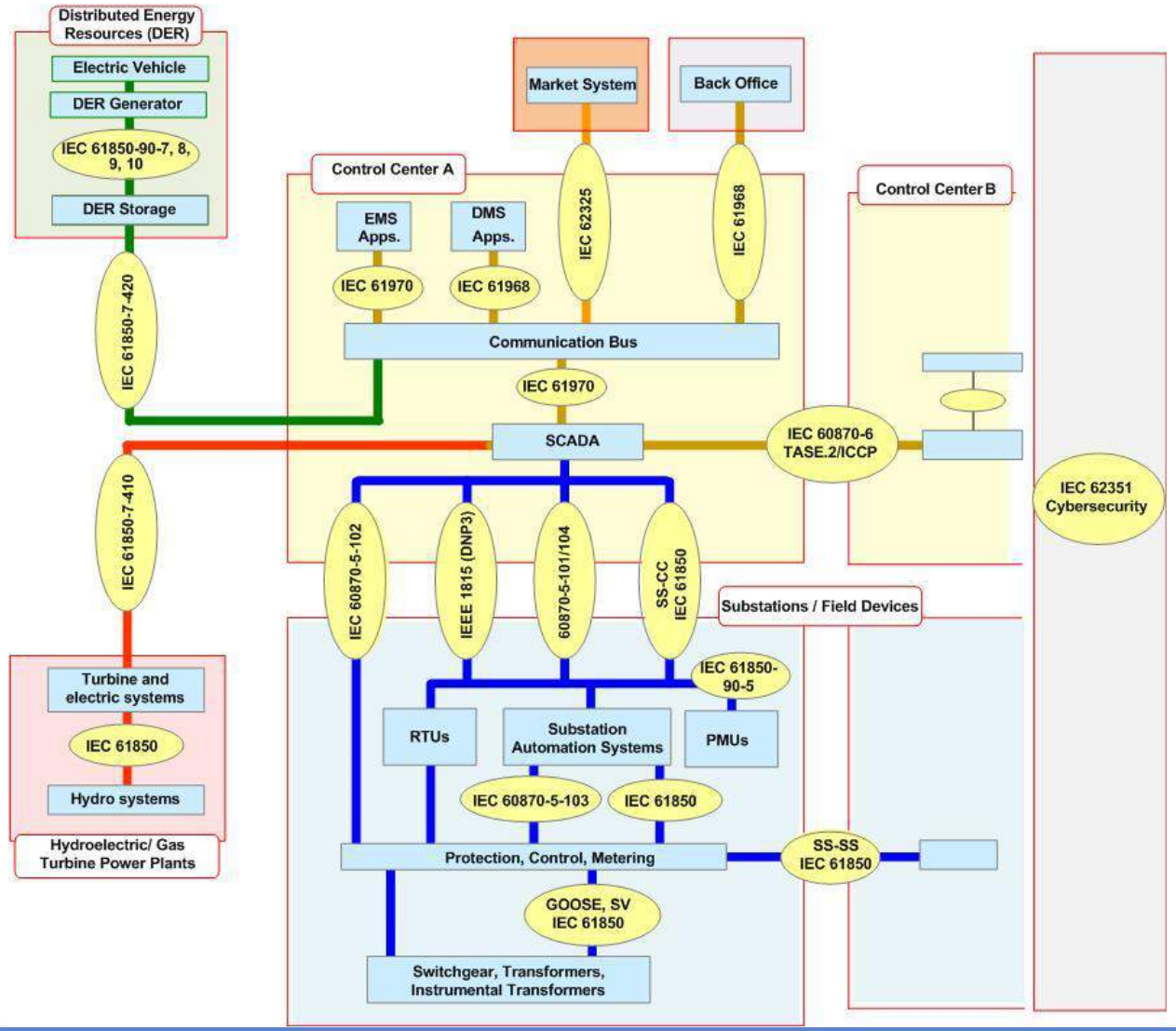



شکل ۱۴: ساختار پی‌آیند بسته IEC 60870-5-104




IOA:Information object address fields

# نمای کاربردی IEC 104(T104)

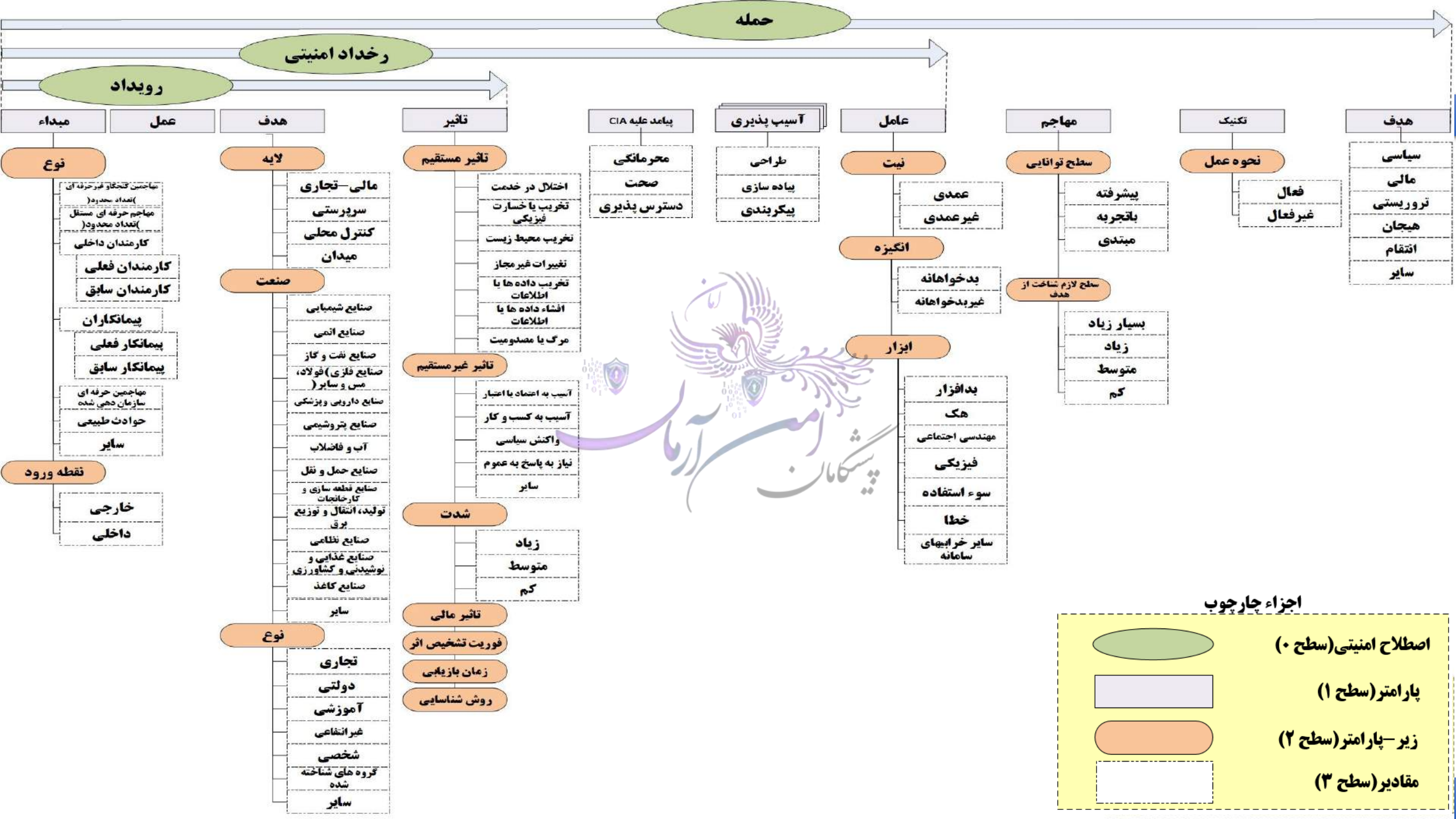



[۴۶]

# آسیب پذیری‌های طراحی IEC 104(T104)

- فقدان مکانیزم تصدیق هویت( V1)
- فقدان مکانیزم‌های رمزنگاری ( V2)
- فقدان برچسب زمانی( V3)
- فقدان مکانیزم تضمین صحت داده و فیلد چکسام ( V4)
- فقدان مکانیزم‌های امنیتی توکار در لایه کاربرد و پیوند داده ( V5)
- محدودیت پهنای باند ارتباطی ( V6)

[۴۶]

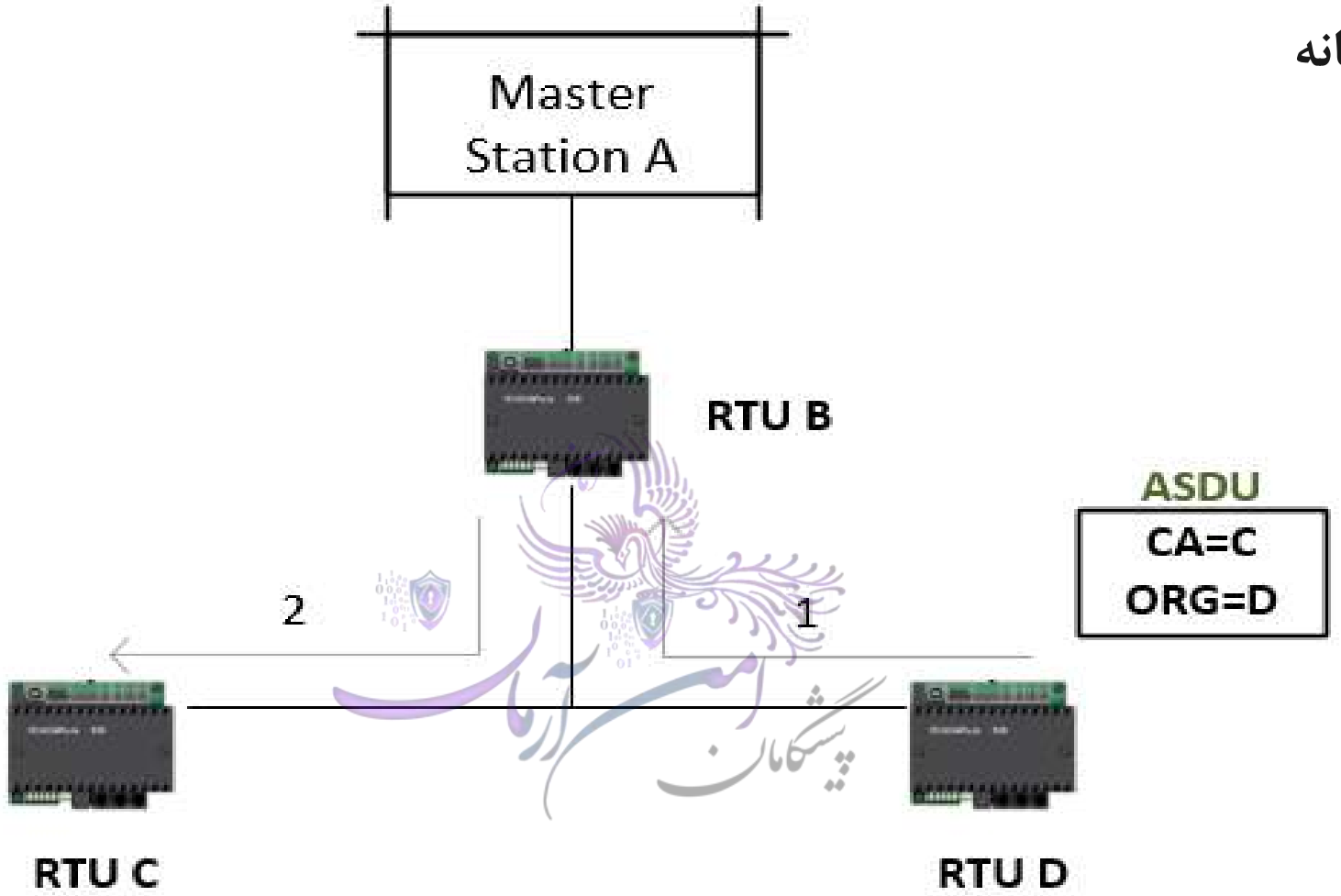

حمله
رخداد امنیتی
رویداد
مبداء
عمل
هدف
تاثیر
پیامد علیه CIA
آسیب پذیری
عامل
مهاجم
تکنیک
هدف
نوع
مهاجمین کنجکاو غیرحرفه ای (تعداد محدود)
مهاجم حرفه ای مستقل (تعداد محدود)
کارمندان داخلی
کارمندان فعلی
کارمندان سابق
پیمانکاران
پیمانکار فعلی
پیمانکار سابق
مهاجمین حرفه ای سازمان دهی شده
حوادث طبیعی
سایر
نقطه ورود
خارجی
داخلی
لایه
مالی–تجاری
سرویس دهی
کنترل محلی
میدان
صنعت
صنایع شیمیایی
صنایع انرژی
صنایع نفت و گاز
صنایع فلزی (فولاد، مس و سایر)
صنایع دارویی و پزشکی
صنایع پتروشیمی
آب و فاضلاب
صنایع حمل و نقل
صنایع قطعه سازی و کارخانجات
تولید، انتقال و توزیع برق
صنایع نظامی
صنایع غذایی و نوشیدنی و کشاورزی
صنایع کاغذ
سایر
نوع
تجاری
دولتی
آموزشی
غیرانتفاعی
شخصی
گروه های شناخته شده
سایر
تاثیر مستقیم
اختلال در خدمت
تخریب یا خسارت فیزیکی
تخریب محیط زیست
تغییرات غیرمجاز
تخریب داده ها یا اطلاعات
افشاء داده ها یا اطلاعات
مرگ یا مصدومیت
تاثیر غیرمستقیم
آسیب به اعتماد یا اعتبار
آسیب به کسب و کار
واکنش سیاسی
نیاز به پاسخ به عموم
سایر
شدت
زیاد
متوسط
کم
تاثیر مالی
فوریت تشخیص اثر
زمان بازیابی
روش شناسایی
محرمانگی
صحت
دسترس پذیری
طراحی
پیاده سازی
پیکربندی
نیت
عمدی
غیرعمدی
انگیزه
بدخواهانه
غیربدخواهانه
ابزار
بدافزار
هک
مهندسی اجتماعی
فیزیکی
سوء استفاده
خطا
سایر خرابیهای سامانه
سطح توانایی
پیشرفته
باتجربه
مبتدی
سطح لازم شناخت از هدف
بسیار زیاد
زیاد
متوسط
کم
نحوه عمل
فعال
غیرفعال
سیاسی
مالی
تروریستی
هیجان
انتقام
سایر
اجزاء چارچوب
اصطلاح امنیتی(سطح ۰)
پارامتر(سطح ۱)
زیر–پارامتر(سطح ۲)
مقادیر(سطح ۳)

# حملات فنی به فیلدهای T104

| فیلد | نوع حمله |
|---|---|
| بایت آغاز (0x68) | تخریب غیر فیزیکی($V_4$)، ممانعت از کیفیت خدمات($V_1$, $V_4$)، دست کاری غیر مجاز ($V_1$,$V_4$) |
| طول APDU | تخریب غیر فیزیکی ($V_4$)، استراق سمع منفعل($V_2$)، ممانعت از کیفیت خدمات ($V_1$,$V_4$)، دست کاری غیرمجاز ($V_1$,$V_4$)، داده‌ای($V_1$,$V_4$)، می‌تواند پیش زمینه‌ی حمله‌ی تزریق بسته شود ($V_1$,$V_4$)، می‌تواند پیش زمینه‌ی حمله‌ی ربایش جریان کنترلی شود ($V_1$,$V_4$)، مردی در میان غیر فعال ($V_1$)، مردی در میان فعال ($V_1$)، جعل هویت ($V_1$) |
| فیلد کنترلی ۱ | استراق سمع منفعل ($V_2$)، تخریب غیر فیزیکی ($V_4$)، ممانعت از کیفیت خدمات ($V_1$,$V_4$)، دست کاری غیر مجاز ($V_1$,$V_4$) |
| فیلد کنترلی ۲ | استراق سمع منفعل ($V_2$)، تخریب غیر فیزیکی ($V_4$)، ممانعت از کیفیت خدمات ($V_1$,$V_4$)، دست کاری غیر مجاز ($V_1$,$V_4$) |
| فیلد کنترلی ۳ | استراق سمع منفعل ($V_2$)، تخریب غیر فیزیکی ($V_4$)، ممانعت از کیفیت خدمات ($V_1$,$V_4$)، دست کاری غیر مجاز ($V_1$, $V_4$) |
| فیلد کنترلی ۴ | استراق سمع منفعل ($V_2$)، تخریب غیر فیزیکی ($V_4$)، ممانعت از کیفیت خدمات ($V_1$,$V_4$)، دست کاری غیر مجاز ($V_1$,$V_4$) |
| شناسه نوع (TypeID) | استراق سمع منفعل ($V_2$)، تخریب غیر فیزیکی ($V_4$)، ممانعت از کیفیت خدمات ($V_1$,$V_4$)، دست کاری غیر مجاز ($V_1$,$V_4$)، تزریق بسته ($V_1$,$V_4$)، می‌تواند پیش زمینه‌ی حمله‌ی ربایش جریان کنترلی ($V_1$,$V_4$)، مردی در میان غیر فعال ($V_1$)، مردی در میان فعال ($V_1$) |
| تعداد اشیا (NumIX) | تخریب غیر فیزیکی ($V_4$)، ممانعت از کیفیت خدمات ($V_1$,$V_4$)، دست کاری غیر مجاز ($V_1$,$V_4$)، تزریق بسته ($V_1$,$V_4$)، می‌تواند پیش زمینه‌ی حمله‌ی ربایش جریان کنترلی ($V_1$,$V_4$) |
| SQ | تخریب غیر فیزیکی ($V_4$)، ممانعت از کیفیت خدمات ($V_1$,$V_4$)، دست کاری غیر مجاز ($V_1$,$V_4$)، می‌تواند پیش زمینه‌ی حمله تزریق بسته ($V_1$,$V_4$)، می‌تواند پیش زمینه‌ی حمله‌ی ربایش جریان کنترلی ($V_1$,$V_4$) |
| علت انتقال (COT) | استراق سمع منفعل ($V_2$)، تخریب غیر فیزیکی ($V_4$)، ممانعت از کیفیت خدمات ($V_1$,$V_4$)، دست کاری غیر مجاز ($V_1$,$V_4$)، می‌تواند پیش زمینه‌ی حمله تزریق بسته ($V_1$,$V_4$)، می‌تواند پیش زمینه‌ی حمله‌ی ربایش جریان کنترلی ($V_1$,$V_4$) |
| P/N | تخریب غیر فیزیکی ($V_4$)، ممانعت از کیفیت خدمات ($V_1$,$V_4$)، دست کاری غیر مجاز ($V_1$,$V_4$) |
| T | تخریب غیر فیزیکی ($V_4$)، دست کاری غیر مجاز ($V_1$,$V_4$) |
| آدرس منبع (ORG) | استراق سمع منفعل ($V_2$)، تخریب غیر فیزیکی ($V_4$)، ممانعت از کیفیت خدمات ($V_1$,$V_4$)، دست کاری غیر مجاز ($V_1$,$V_4$)، مردی در میان غیر فعال ($V_1$,$V_4$)، شنود فعال ($V_1$,$V_4$)، مردی در میان فعال ($V_1$,$V_4$)، جعل هویت ($V_1$,$V_4$)، ارسال مجدد پیام($V_1$, $V_3$) |
| فیلدهای آدرس مشترک ASDU (CA) | استراق سمع منفعل ($V_2$)، تخریب غیر فیزیکی ($V_4$)، ممانعت از کیفیت خدمات ($V_1$,$V_4$)، دست کاری غیر مجاز ($V_1$,$V_4$)، مردی در میان غیر فعال ($V_1$,$V_4$)، شنود فعال ($V_1$,$V_4$)، مردی در میان فعال ($V_1$,$V_4$)، جعل هویت ($V_1$,$V_4$)، ارسال مجدد پیام ($V_1$,$V_3$) |
| فیلدهای آدرس اشیا اطلاعاتی (IOA) | استراق سمع منفعل ($V_2$)، تخریب غیر فیزیکی ($V_4$)، ممانعت از کیفیت خدمات ($V_1$,$V_4$)، دست کاری غیر مجاز ($V_1$,$V_4$)، مردی در میان غیر فعال ($V_1$,$V_4$)، شنود فعال ($V_1$,$V_4$)، مردی در میان فعال ($V_1$,$V_4$)، جعل هویت ($V_1$,$V_4$)، ارسال مجدد پیام ($V_1$,$V_3$) |
| سایر فیلدها | تخریب غیر فیزیکی ($V_4$)، دست کاری غیر مجاز ($V_1$,$V_4$) |

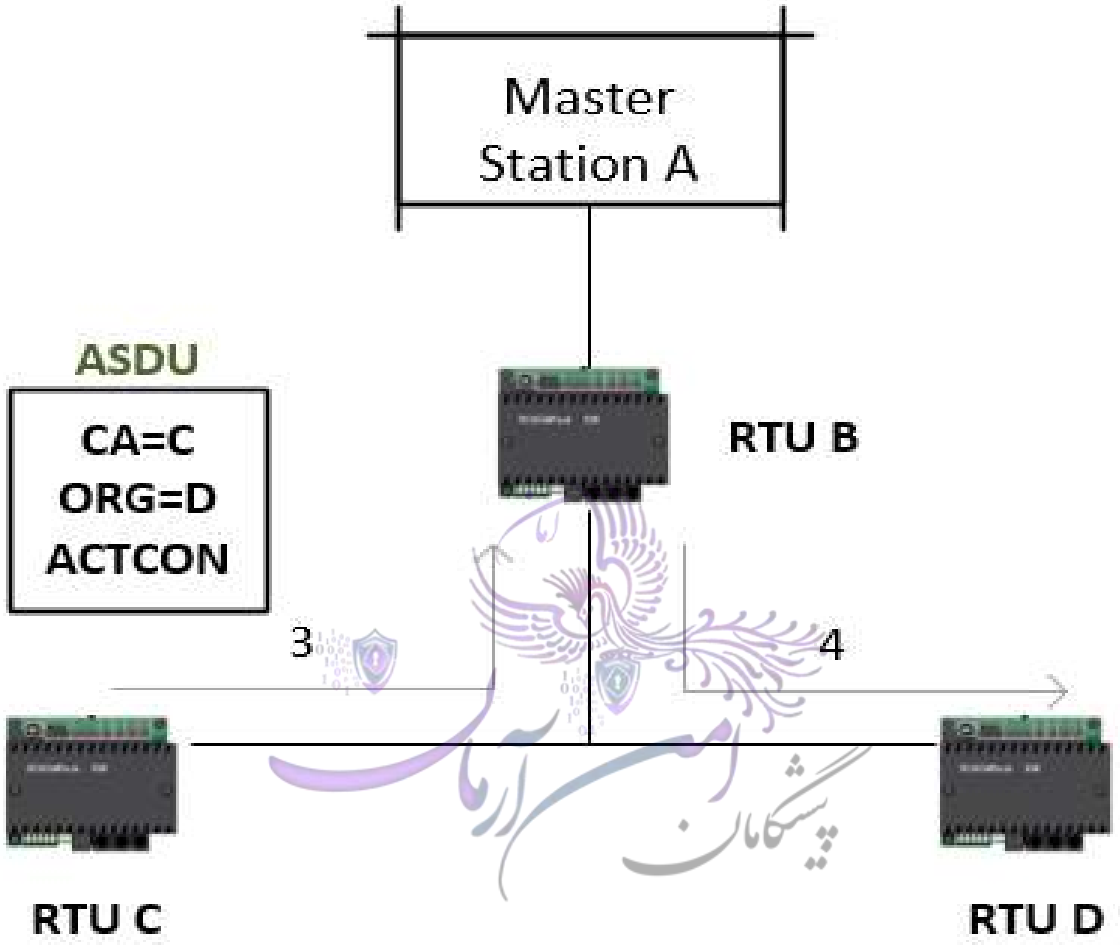
# فقدان برچسب زمانی

- ارسال دستور کنترلی از RTU حالت دوگانه



# فقدان برچسب زمانی

- ارسال ASDUتائید عمل به RTU



# آسیب‌پذیری‌های پیاده‌سازی و عملیاتی(IEC 104(T104

- **آسیب پذیری CVE-2008-2474**
  - BoFدر واحد پردازنده ارتباطی ABB PCU 400
  - امکان اجرای کد دلخواه را از طریق بسته‌های دست کاری شده می‌دهد.
  - این آسیب پذیری داری منشأ تهدید غیرطبیعی، محل تهدید خارجی، عامل تهدید غیرانسانی است و ویژگی امنیتی دسترس‌پذیری را نقض می‌نماید.
  - زمینه ساز حملات فنی
    - سرریز بافر در پشته، ممانعت از خدمات، اجرای کد دلخواه و تخریب حافظه می‌شود.

# آسیب‌پذیری‌های پیاده‌سازی و عملیاتی(IEC 104(T104

- IDS RTU 850 Version: NC851
- IDS RTU 850 Version: NC853
- IDS RTU 850 Version: NC854
- IDS RTU 850 Version: NC856
- IDS RTU 850 Version: EC86A

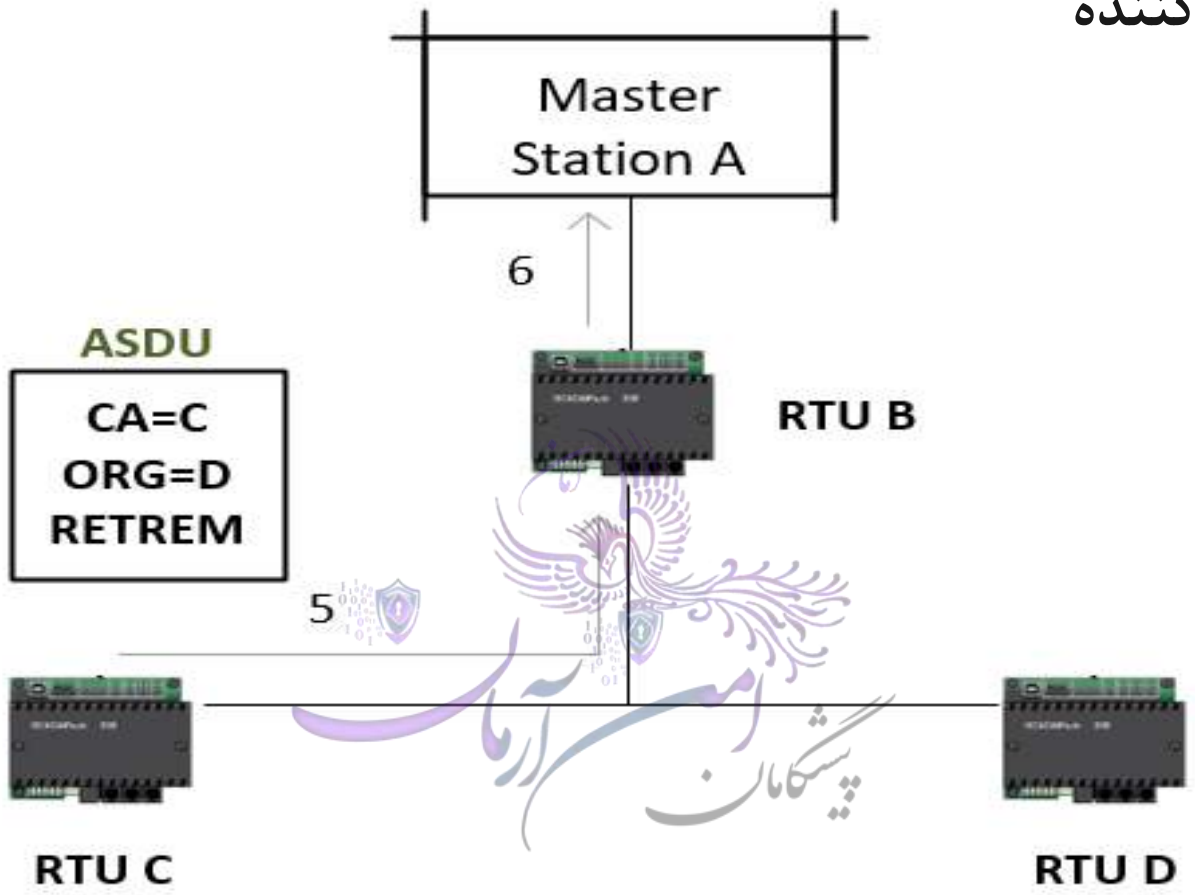
- **آسیب پذیری CVE-2015-3939**
  - دسترسی به گواهینامه‌هایی جهت ارتقا سطوح دسترسی در IDS RTU 850
  - تغییر فایل‌ها از طریف واسط سرویس داخلی
  - این آسیب پذیری داری منشأ تهدید غیرطبیعی، محل تهدید خارجی، عامل تهدید غیرانسانی است و ویژگی امنیتی محرمانگی را نقض می‌نماید. این
  - زمینه ساز حملات فنی نقض کنترل دسترسی، مرور سامانه، پیمایش مسیر، ارتقا مجوزها می‌شود.

# آسیب‌پذیری‌های پیاده‌سازی و عملیاتی(IEC 104(T104

- **آسیب‌پذیری‌های ارتباطی در بکارگیری رسانه غیرقابل اطمینان**
  - در صورتی استفاده از رسانه‌های ارتباطی رادیویی یا کابل‌های زوج سیم به هم تابیده باشد و این رسانه‌های در برابر تداخل امواج و فرکانس‌ها ایمن نشده باشند
  - می‌بایست امکان تداخل فرکانس توسط عوامل عمدی و غیر عمدی در آن‌ها بررسی شود.

# آسیب‌پذیری‌های پیاده‌سازی و عملیاتی IEC 104(T104)

- نظارت بر اطلاعات برگشت یافته به ایستگاه کنترل‌کننده



# مسائل درگیر در طراحی مکانیزم احراز اصالت

- IEC/TS 62351
  - ۵-۶۲۳۵۱
  - ۳-۶۲۳۵۱

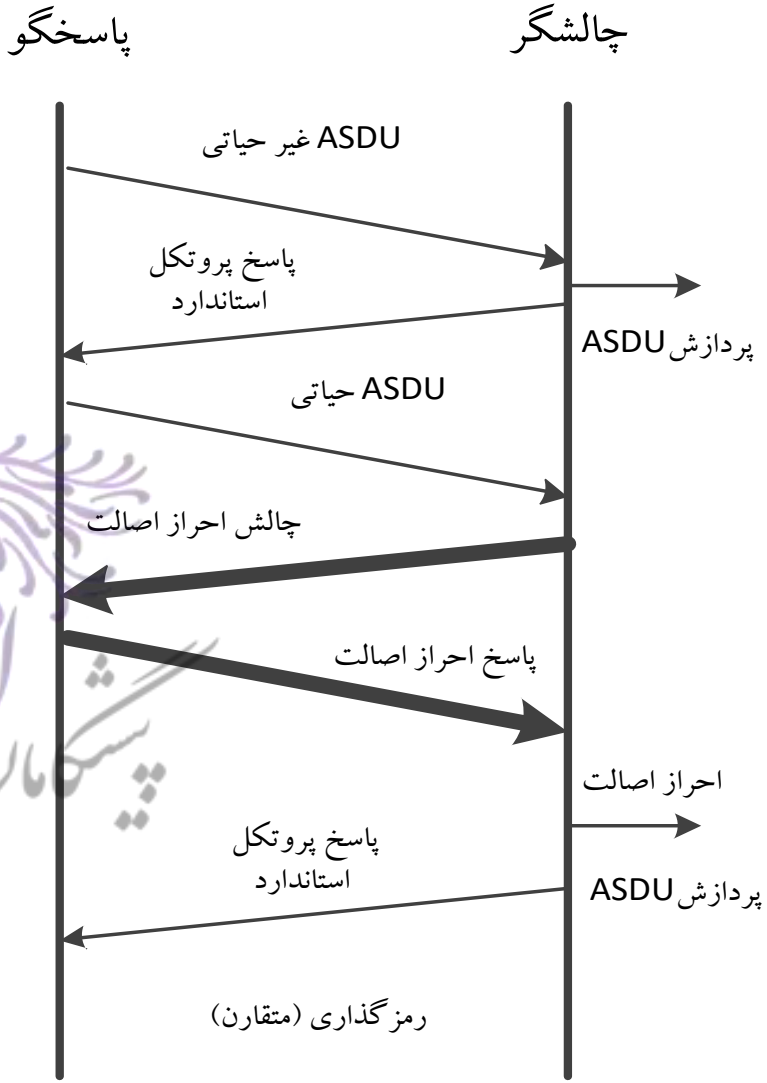
- ارتباطات نامتقارن
- مبتنی بر پیام بودن
- دنباله‌ی اعداد ضعیف یا فقدان دنباله اعداد
- توان پردازش محدود
- پهنای باند محدود
- عدم دسترسی به سرور احراز اصالت
- چکسام محدود
- سایت‌های از راه دور
- رسانه غیرقابل اطمینان

# مکانیزم طراحی امن

- پروتکل چالش و پاسخ
- مفهوم MACکه هر دو ایستگاه کنترل‌کننده و کنترل شونده بر اساس ASDUیا پیام پروتکل محاسبه می‌شود، باید احراز اصالت شوند.

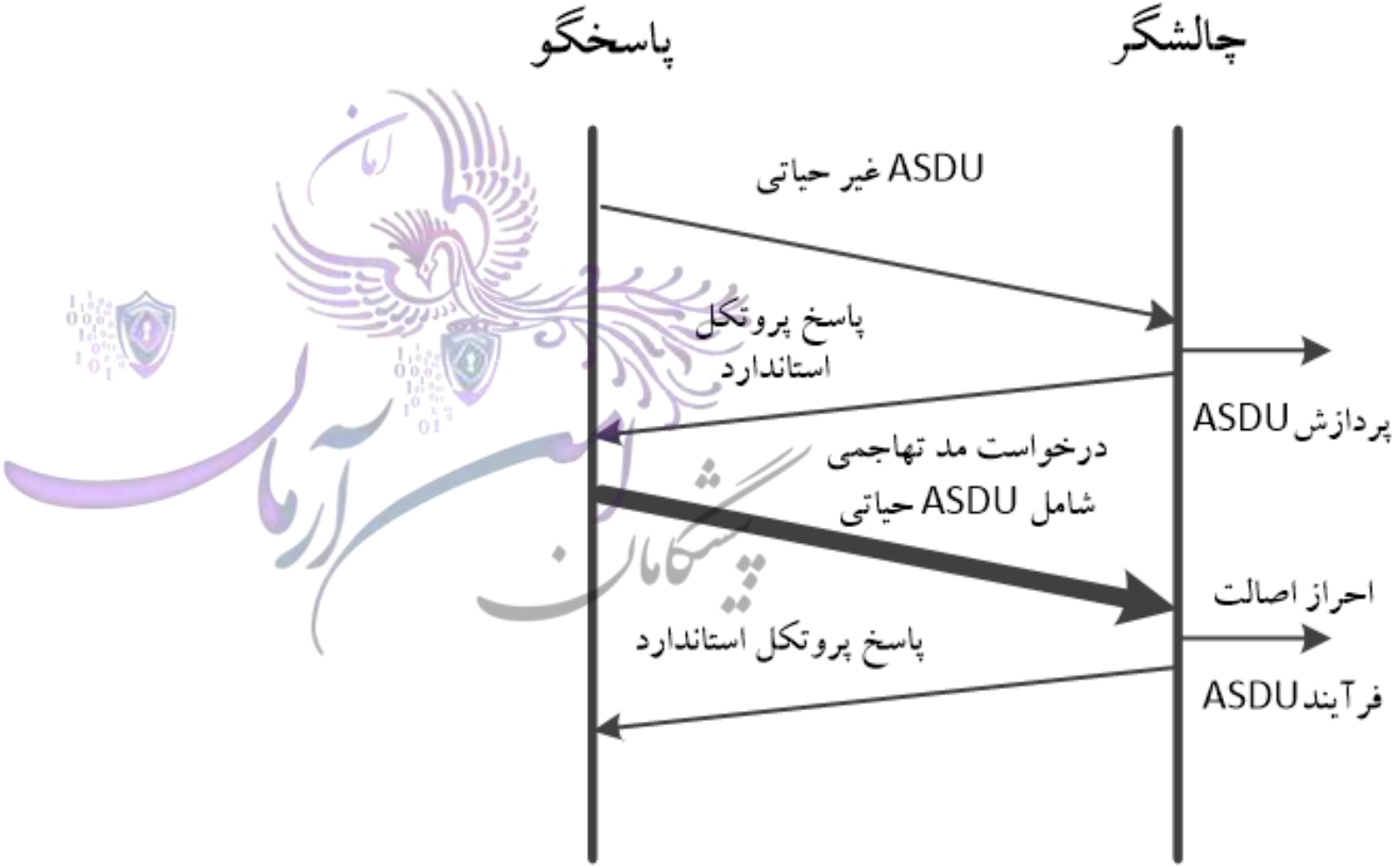
- این مفهوم مسئولیت امنیت در دستگاهی را که نیاز به احراز اصالت دارد فراهم می‌کند و در شبکه‌های متنوعی مانند شبکه‌های کنترل صنعتی شرایط کاربردی مناسبی را فراهم می‌سازد.
- این مفهوم امکان داشتن ارتباط غیر امن را در صورت لزوم ممکن می‌نماید و پهنای باند و نیازهای پردازشی را در این شرایط کاهش می‌دهد.

# نمونه چالش موفق ASDUحیاتی

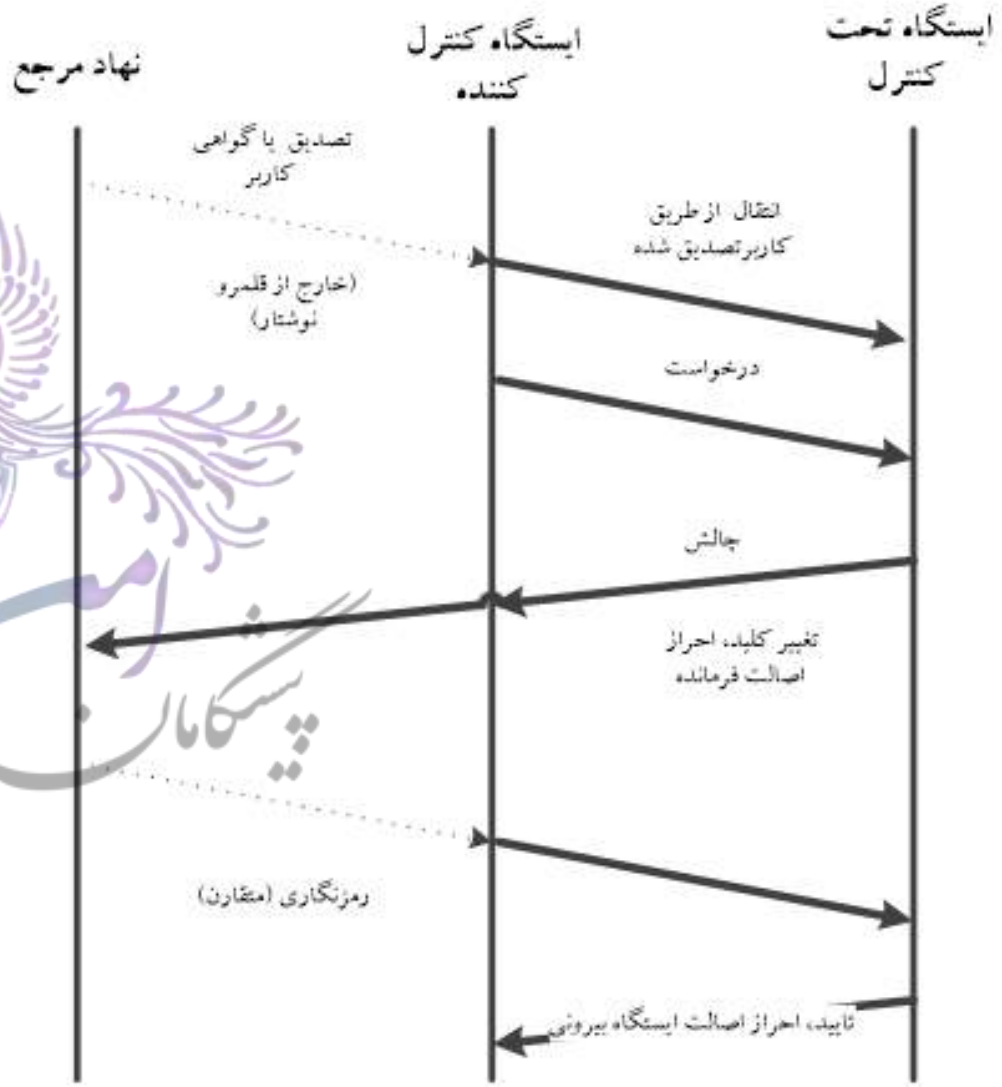


# احساس کاذب امنیت

# نمونه‌ای از درخواست مد تهاجمی موفق



# تعامل بین مرجع و ایستگاه‌ها در مدیریت کلید



# مقادیری که باید به فیلد COT اضافه شوند

| مقدار جدید | علت انتقال |
|---|---|
| ۱۴ | احراز اصالت |
| ۱۵ | نگه‌داری کلید نشست احراز اصالت |
| ۱۶ | نگه‌داری نقش کاربر و کلید به‌روزرسانی |

# مقادیری که باید به فیلد شناسه نوع اضافه شوند

| نوع | شماره | توضیح |
|---|---|---|
| S_IT_TC_1 | <۴۱> | برچسب زمانی برای آمار و گزارش‌های امنیتی |
| S_CH_NA_1 | <۸۱> | چالش احراز اصالت |
| S_RP_NA_1 | <۸۲> | پاسخ احراز اصالت |
| S_AR_NA_1 | <۸۳> | درخواست احراز اصالت مد تهاجمی |
| S_KR_NA_1 | <۸۴> | درخواست وضعیت کلید نشست |
| S_KS_NA_1 | <۸۵> | وضعیت کلید نشست |
| S_KC_NA_1 | <۸۶> | تغییر کلید نشست |
| S_ER_NA_1 | <۸۷> | خطای احراز اصالت |
| S_US_NA_1 | <۹۰> | تغییر وضعیت کاربر |
| S_UQ_NA_1 | <۹۱> | درخواست تغییر کلید به‌روزرسانی |
| S_UR_NA_1 | <۹۲> | پاسخ تغییر کلید به‌روزرسانی |
| S_UK_NA_1 | <۹۳> | تغییر کلید به‌روزرسانی متقارن |
| S_UA_NA_1 | <۹۴> | تغییر کلید به‌روزرسانی نامتقارن |
| S_UC_NA_1 | <۹۵> | تائید تغییر کلید به‌روزرسانی |

# بدافزار Win32/Industroyer

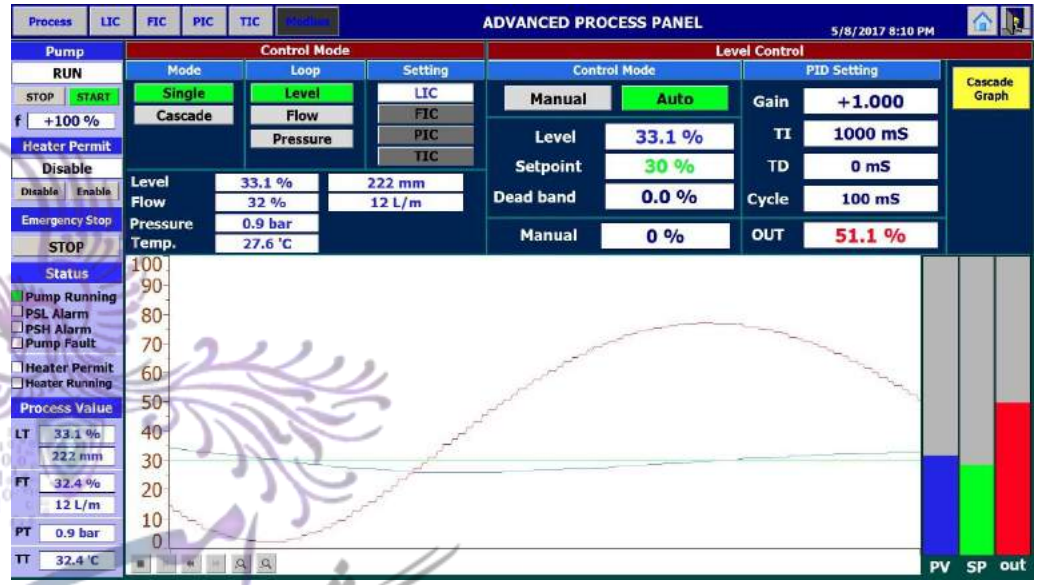
باج افزار ClearEnergy (۲۰۱۷) | **بدافزار Win32/Industroyer (۲۰۱۶)** | ... | بدافزار Havex (۲۰۱۴) | بدافزار TeamSpy (۲۰۱۳) | بدافزار MiniDuke (۲۰۱۳) | بدافزار Red October (۲۰۱۳) | بدافزار NetTraveler (۲۰۱۳)

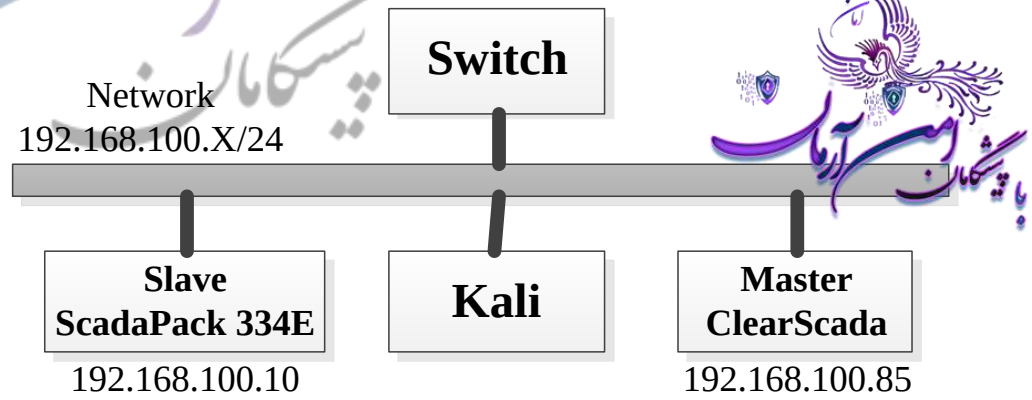
| | |
|---|---|
| **شناسه‌ها :** | • Win32/Industroyerz (ESET)<br>• Crashoverride (DRAGOS)<br>• Alert TA17-163A(US-CERT) |
| **هدف:** | • ICSهای شبکه برق(تولید، انتقال و توزیع )<br>• اوکراین |
| **پروتکل‌های هدف:** | • **IEC101**<br>• **IEC104**<br>• **IEC61850**<br>• **OPC DA** |
| **عملیات مخرب :** | • **قابلیت‌های درب پشتی**<br>• **ماژول امحاء داده**<br>• **ماژول DoS** |

**قابلیت‌ها :**

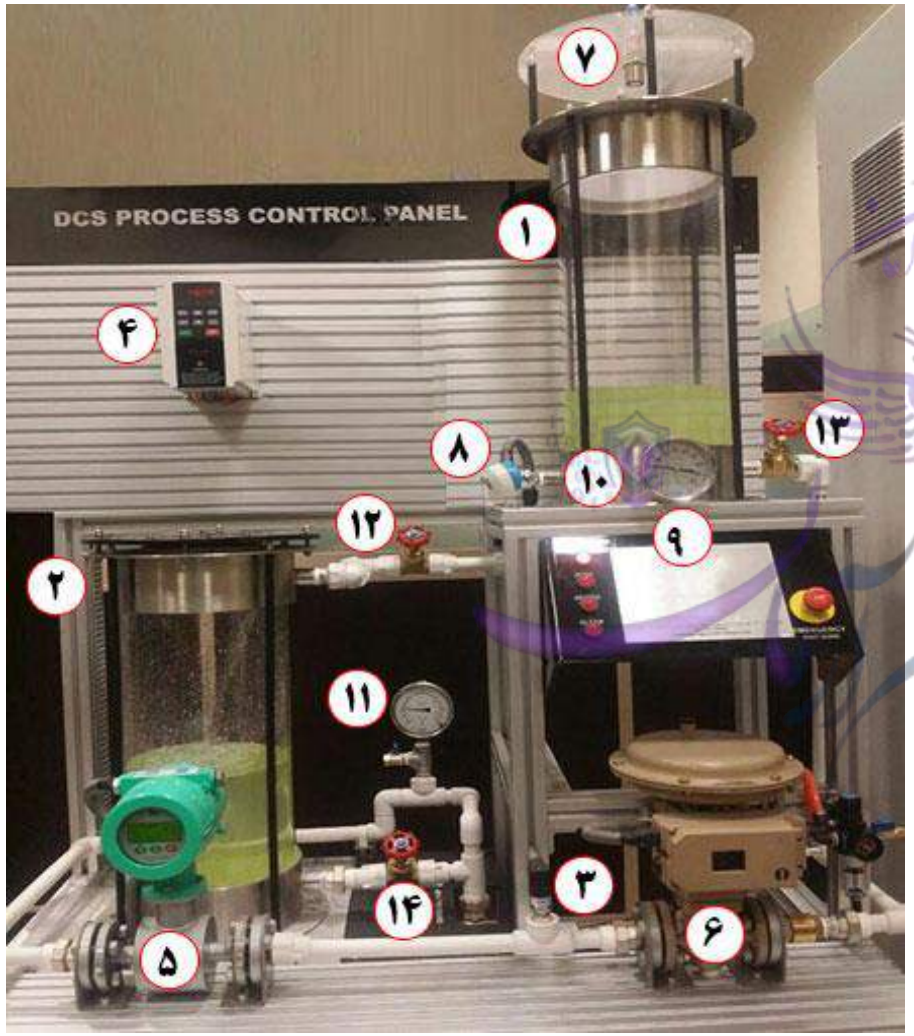
- ارسال دستورهای معتبر به RTUها
- منع خدمات تجهیزات فیلد دارای ارتباطات سریال درگاه COMویندوزی
- پویش شبکه از طریق پروتکل های متعدد: از جمله OPC
- بهره جویی از آسیب پذیری‌های منع خدمات در رله‌های زیمنس (خاموش شدن رله)
- ماژولی امحای داده برای از بین بردن داده‌های سامانه‌های ویندوزی

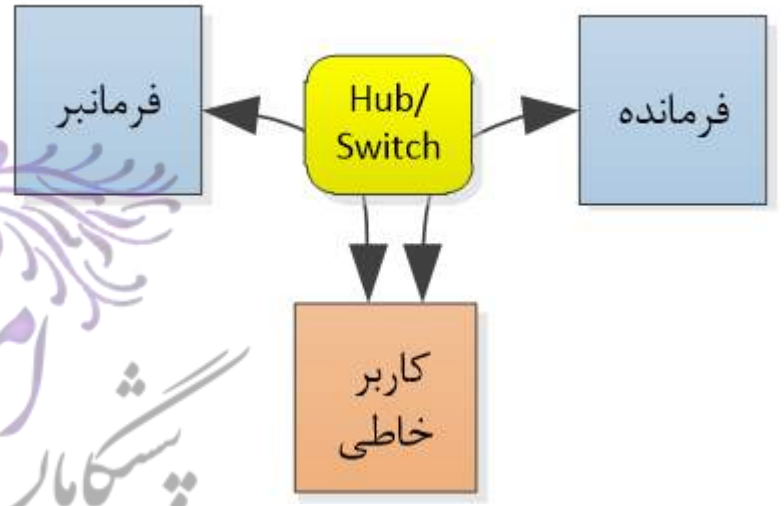
# بستر آزمایش و ارزیابی

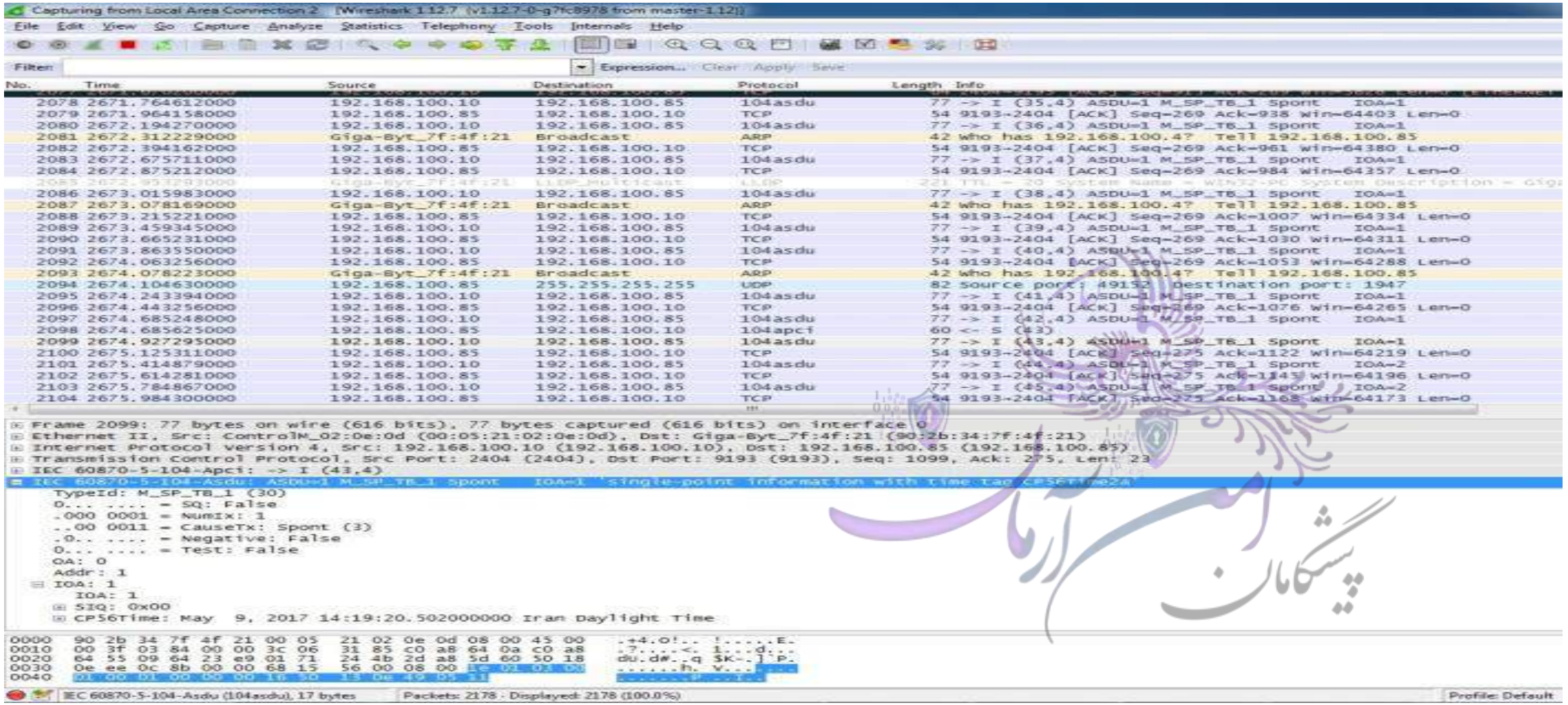



# حمله جعل ARP موفق



# ترافیک


Capturing from Local Area Connection 2 [Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
2078 2671.764612000 192.168.100.10 192.168.100.85 104asdu 77 -> I (35,4) ASDU=1 M_SP_TB_1 Spont IOA=1
2079 2671.964158000 192.168.100.85 192.168.100.10 TCP 54 9193→2404 [ACK] Seq=269 Ack=938 Win=64403 Len=0
2080 2672.194270000 192.168.100.10 192.168.100.85 104asdu 77 -> I (36,4) ASDU=1 M_SP_TB_1 Spont IOA=1
2081 2672.312229000 Giga-Byt_7f:4f:21 Broadcast ARP 42 Who has 192.168.100.4? Tell 192.168.100.85
2082 2672.394162000 192.168.100.85 192.168.100.10 TCP 54 9193→2404 [ACK] Seq=269 Ack=961 Win=64380 Len=0
2083 2672.675711000 192.168.100.10 192.168.100.85 104asdu 77 -> I (37,4) ASDU=1 M_SP_TB_1 Spont IOA=1
2084 2672.875212000 192.168.100.85 192.168.100.10 TCP 54 9193→2404 [ACK] Seq=269 Ack=984 Win=64357 Len=0
2086 2673.015983000 192.168.100.10 192.168.100.85 104asdu 77 -> I (38,4) ASDU=1 M_SP_TB_1 Spont IOA=1
2087 2673.078169000 Giga-Byt_7f:4f:21 Broadcast ARP 42 Who has 192.168.100.4? Tell 192.168.100.85
2088 2673.215221000 192.168.100.85 192.168.100.10 TCP 54 9193→2404 [ACK] Seq=269 Ack=1007 Win=64334 Len=0
2089 2673.459345000 192.168.100.10 192.168.100.85 104asdu 77 -> I (39,4) ASDU=1 M_SP_TB_1 Spont IOA=1
2090 2673.665231000 192.168.100.85 192.168.100.10 TCP 54 9193→2404 [ACK] Seq=269 Ack=1030 Win=64311 Len=0
2091 2673.863550000 192.168.100.10 192.168.100.85 104asdu 77 -> I (40,4) ASDU=1 M_SP_TB_1 Spont IOA=1
2092 2674.063256000 192.168.100.85 192.168.100.10 TCP 54 9193→2404 [ACK] Seq=269 Ack=1053 Win=64288 Len=0
2093 2674.078223000 Giga-Byt_7f:4f:21 Broadcast ARP 42 Who has 192.168.100.4? Tell 192.168.100.85
2094 2674.104630000 192.168.100.85 255.255.255.255 UDP 82 Source port: 49152 Destination port: 1947
2095 2674.243394000 192.168.100.10 192.168.100.85 104asdu 77 -> I (41,4) ASDU=1 M_SP_TB_1 Spont IOA=1
2096 2674.443256000 192.168.100.85 192.168.100.10 TCP 54 9193→2404 [ACK] Seq=269 Ack=1076 Win=64265 Len=0
2097 2674.685248000 192.168.100.10 192.168.100.85 104asdu 77 -> I (42,4) ASDU=1 M_SP_TB_1 Spont IOA=1
2098 2674.685625000 192.168.100.85 192.168.100.10 104apci 60 <- S (43)
2099 2674.927295000 192.168.100.10 192.168.100.85 104asdu 77 -> I (43,4) ASDU=1 M_SP_TB_1 Spont IOA=1
2100 2675.125311000 192.168.100.85 192.168.100.10 TCP 54 9193→2404 [ACK] Seq=275 Ack=1122 Win=64219 Len=0
2101 2675.414879000 192.168.100.10 192.168.100.85 104asdu 77 -> I (44,4) ASDU=1 M_SP_TB_1 Spont IOA=2
2102 2675.614281000 192.168.100.85 192.168.100.10 TCP 54 9193→2404 [ACK] Seq=275 Ack=1145 Win=64196 Len=0
2103 2675.784867000 192.168.100.10 192.168.100.85 104asdu 77 -> I (45,4) ASDU=1 M_SP_TB_1 Spont IOA=2
2104 2675.984300000 192.168.100.85 192.168.100.10 TCP 54 9193→2404 [ACK] Seq=275 Ack=1168 Win=64173 Len=0
Frame 2099: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface 0
Ethernet II, Src: ControlM_02:0e:0d (00:05:21:02:0e:0d), Dst: Giga-Byt_7f:4f:21 (90:2b:34:7f:4f:21)
Internet Protocol Version 4, Src: 192.168.100.10 (192.168.100.10), Dst: 192.168.100.85 (192.168.100.85)
Transmission Control Protocol, Src Port: 2404 (2404), Dst Port: 9193 (9193), Seq: 1099, Ack: 275, Len: 23
IEC 60870-5-104-Apci: -> I (43,4)
IEC 60870-5-104-Asdu: ASDU=1 M_SP_TB_1 Spont IOA=1 'single-point information with time tag CP56Time2a'
TypeId: M_SP_TB_1 (30)
0... .... = SQ: False
.000 0001 = NumIx: 1
..00 0011 = CauseTx: Spont (3)
.0.. .... = Negative: False
0... .... = Test: False
OA: 0
Addr: 1
IOA: 1
IOA: 1
SIQ: 0x00
CP56Time: May 9, 2017 14:19:20.502000000 Iran Daylight Time
0000 90 2b 34 7f 4f 21 00 05 21 02 0e 0d 08 00 45 00 .+4.O!.. !.....E.
0010 00 3f 03 84 00 00 3c 06 31 85 c0 a8 64 0a c0 a8 .?....<. 1...d...
0020 64 55 09 64 23 e9 01 71 24 4b 2d a8 5d 60 50 18 dU.d#..q $K-.]`P.
0030 0e ee 0c 8b 00 00 68 15 56 00 08 00 .....h. V...
0040 01 00 01 00 00 00 10 50 15 0e 49 05 11 .......P ..I..
IEC 60870-5-104-Asdu (104asdu), 17 bytes
Packets: 2178 · Displayed: 2178 (100.0%)
Profile: Default

# منابع جهت مطالعه بیشتر

پروتکل کنترل صنعتی IEC 60870-5-104 از منظـر امنیـت سایبری، ۱۳۹۷

# منابع جهت مطالعه بیشتر


- احمدیان محمد مهدی، شجری مهدی. شناسایی چالش‌های امنیتی پروتکل IEC۶۰۸۷۰-۵-۱۰۴ و بررسی راه‌کارهای موجود. ۱. ۱۳۹۷; ۷ (۲) :۱۵-۳۰

URL: http://monadi.isc.org.ir/article--۱-۱۲۳fa.html

- احمدیان، محمدمهدی و همکاران،۱۳۹۶،شناسایی تهدیدات و آسیب پذیری های امنیتی پروتکل کنترل صنعتی IEC 60870-5-104،چهاردهمین کنفرانس بین المللی انجمن رمز ایران،

URL: https://civilica.com/doc/781741

# جمع بندی

- معرفی مختصری از T104
- شناخت جوانب امنیتی
- آسیب‌پذیری‌ها (مراحل طراحی، پیکربندی و پیاده سازی)
- اهم حملات شناسایی شده
  - استراق سمع
  - ممانعت از کیفیت خدمات
  - دست کاری غیرمجاز
  - تزریق بسته
- بهره گیری از محیط آزمایشی مناسب
- نکات امن سازی

## عناوین برخی دوره‌های تخصصی تئوری – عملی امنیت سایبر صنعتی قابل ارائه در صنعت برق

| عنوان | مدت دوره (ساعت) |
|---|---|
| ارتقاء امنیت سایبری سامانه‌های کنترل صنعتی در صنایع برق و زیرساخت‌های حساس، حیاتی و مهم حوزه انرژی | ۲۴–۳۲ |
| ارتقاء امنیت سایبری سامانه‌های کنترل صنعتی و اتوماسیون حوزه توزیع برق | ۳۲ |
| ارتقاء امنیت سایبری سامانه‌های کنترل صنعتی و اتوماسیون حوزه انتقال برق | ۳۲ |
| ارتقاء امنیت سایبری سامانه‌های کنترل صنعتی و اتوماسیون حوزه تولید برق | ۳۲ |
| ارتقاء امنیت سایبری سامانه‌های کنترل صنعتی و اتوماسیون صنعتی در شرکت مدیریت شبکه برق ایران و مراکز دیسپاچینگ | ۳۲ |

| عناوین برخی دوره‌های تخصصی امنیت سایبر صنعتی قابل ارائه در سایر صنایع | |
|---|---|
| عنوان | مدت‌زمان دوره (ساعت) |
| ارتقاء امنیت سایبری سامانه‌های کنترل صنعتی در صنایع و زیرساخت‌های آب و فاضلاب و شرکت‌های تابعه | ۳۲-۲۴ |
| پدافند غیرعامل و امنیت سایبری در سامانه‌های کنترل و اتوماسیون صنعتی | ۱۶-۸ |
| پدافند غیرعامل، حفاظت اطلاعات و افشاء اطلاعات سایبر-فیزیکی در سامانه‌های کنترل و اتوماسیون صنعتی | ۸-۴ |
| الزامات امنیت در سامانه‌های کنترل صنعتی و اسکادا (مطابق سرفصل‌های SANS ICS 410) | ۴۰ |
| امنیت سایبری سامانه‌های کنترل صنعتی در صنایع نفت، گاز و پالایشگاه و زیرساخت‌های حساس، حیاتی و مهم این حوزه | ۳۲-۲۴ |
| ارتقاء امنیت سایبری سامانه‌های کنترل صنعتی در صنایع پتروشیمی و زیرساخت‌های حساس، حیاتی و مهم این حوزه | ۳۲-۲۴ |
| ارتقاء امنیت سایبری سامانه‌های کنترل صنعتی در صنایع مس و فولاد و زیرساخت‌های حساس، حیاتی و مهم این حوزه | ۳۲-۲۴ |
| ارتقاء امنیت سایبری سامانه‌های کنترل صنعتی در صنایع حمل‌ونقل و زیرساخت‌های حساس، حیاتی و مهم این حوزه | ۳۲-۲۴ |

# فیلم کوتاه از بخش‌های عملی  تست نفوذ و امن سازی پروتکل IEC 104

## جهت مشاهده:

به کانال آپارات یا یوتیوب ما مراجعه نمایید:

Subscribe to our YouTube Channel

Link(YouTube)
https://www.youtube.com/channel/UCbxxf39UnwDgbfTu1-bL2Qg

Link(آپارات)
https://aparat.com/v/qykRN

# مشاهده رزومه امان

**جهت مشاهده** به وب‌سایت به آدرس ذیل مراجعه نمایید:

AmanSec.ir

## حوزه‌های فعالیت:

**امنیت سایبری سامانه‌های کنترل و اتوماسیون صنعتی، اسکادا، DCS، دیسپاچینگ،ESD، تله متری**

| | |
|---|---|
| مدیریت مخاطرات (ریسک) امنیت سایبری سامانه‌های کنترل و اتوماسیون صنعتی | ★★★★★★★★★★ |
| آموزش تخصصی امنیت سایبری سامانه‌های کنترل صنعتی واسکادا | ★★★★★★★★★★ |
| طراحی و پیاده‌سازی معماری امن صنعتی مطابق با استانداردهای خارجی و داخلی | ★★★★★★★★★☆ |
| مشاوره در اجرای راهکارهای امنیت سایبری سامانه‌های کنترل و اتوماسیون صنعتی | ★★★★★★★★★☆ |
| ارزیابی مخاطرات سایبری سامانه‌های کنترل صنعتی و زیرساخت‌های حیاتی | ★★★★★★★★★☆ |
| تحلیل آسیب‌پذیری‌ها، تهدیدات و تست نفوذ در سامانه‌های صنعتی | ★★★★★★★★☆☆ |
| مدل‌سازی امنیتی سامانه‌های سایبر- فیزیکی | ★★★★★☆☆☆☆☆ |

# سایر مراجع


1. Chikuni, E., Dondo, M., *"Investing the Security of Power System SCADA"*, Conference proceedings, AFRICON, Sept. 2007.
2. Thomas, Roshan K., Alvaro A. Cardenas, and Rakesh B. Bobba, *"First Workshop on Cyber-Physical Systems Security and PrivaCy (CPS-SPC): Challenges and Research Directions"* Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, ACM, 2015.
3. Clarke, Gordon R., Reynders D., and Wright E., *Practical modern SCADA protocols: DNP3, 60870.5 and related systems*. Newnes, 2004.
4. Cheah, Zi Bin. *Testing and Exploring Vulnerabilities of the Applications Implementing IEC 60870-5-104 Protocol*, Master Thesis,KTH University,Stockholm, Sweden, 2008.
5. Robinson, M., *"The SCADA threat landscape. In: First International Symposium for ICS & SCADA Cyber Security Research"*, In: First International Symposium for ICS & SCADA Cyber Security Research. Leicester, U.K., 30–41, 2013.
6. Morris, T. H. and Gao, W., *"Industrial control system cyber attacks"*, In: First International Symposium for ICS & SCADA Cyber Security Research. Leicester, U.K., 22–29, 2013.
7. Morris, T., Vaughn, R., and Dandass, Y. S., *"A testbed for SCADA control system cybersecurity research and pedagogy"*, In: Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research, CSIIRW ’11. New York, NY, USA, 27:127, 2011.
8. Pietre-Cambacedes, L., Tritschler, M., and Ericsson, G. N., *"Cybersecurity myths on power control systems: 21 misconceptions and false beliefs"*, IEEE Trans. Power Del., 26 (1). 161–172, 2011.

# سایر مراجع


9. Samineni, N. R., Barbhuiya, F. A., and Nandi, S., *"Stealth and semi-stealth MITM attacks, detection and defense in IPv4 networks"* In: 2012 2nd IEEE International Conference onParallel Distributed and Grid Computing (PDGC), 364–367, 2012.
10. Bruschi, D., Ornaghi, A., and Rosti, E., *"S-ARP: A secure address resolution protocol"*, In: Computer Security Applications Conference, Proceedings. 19th Annual. 66–74, 2003.
11. Yang, Y., *"Man-in-the- middle attack testbed investigating cyber-security vulnerabilities in smart grid SCADA systems. In: International Conference on Sustainable Power Generation and Supply"*, (SUPERGEN 2012), 1–8, 2012.
12. Gao, W., *"On SCADA control system command and response injection and intrusion detection"*, In: eCrime Researchers Summit (eCrime). 1–9, 2010.
13. Timorin, A., atimorin/PoC2013 Available from https://github.com/atimorin/PoC2013, 2013.
14. Dondossola, G., *"ICT resilience of power control systems: Experimental results from the CRUTIAL testbeds"*, In: IEEE/IFIP International Conference on Dependable Systems Networks, DSN 09, 554–559, 2009.
15. Maynard, P., McLaughlin, K., Haberler, B., *"Towards understanding man-in-the-middle attacks on iec 60870-5-104 scada networks"*, InProceedings of the 2nd International Symposium on ICS & SCADA Cyber Security Research, pp. 30-42, 2014.
16. Pidikiti, Samanth, D., *"SCADA communication protocols: vulnerabilities, attacks and possible mitigations"*, CSI transactions on ICT1.2, 135-141, 2013.

**با تشکر از حسن توجه شما**

**جهت استفاده از خدمات مشاوره‌ای ، اجرای پروژه‌های مدیریت مخاطرات و امن‌سازی، برگزاری دوره‌های آموزشی، سمینارها، سخنرانی‌ها و ...**
**از طریق راه‌های ذیل با ما در ارتباط باشید:**

**تلفن تماس**

(۰۲۱) ۸۸۳۷۹۰۸۲

**پست الکترونیک**

info(at)AmanSec.ir

**ساعت کاری**

شنبه - پنج شنبه

۸ صبح تا ۸ شب

**آدرس**

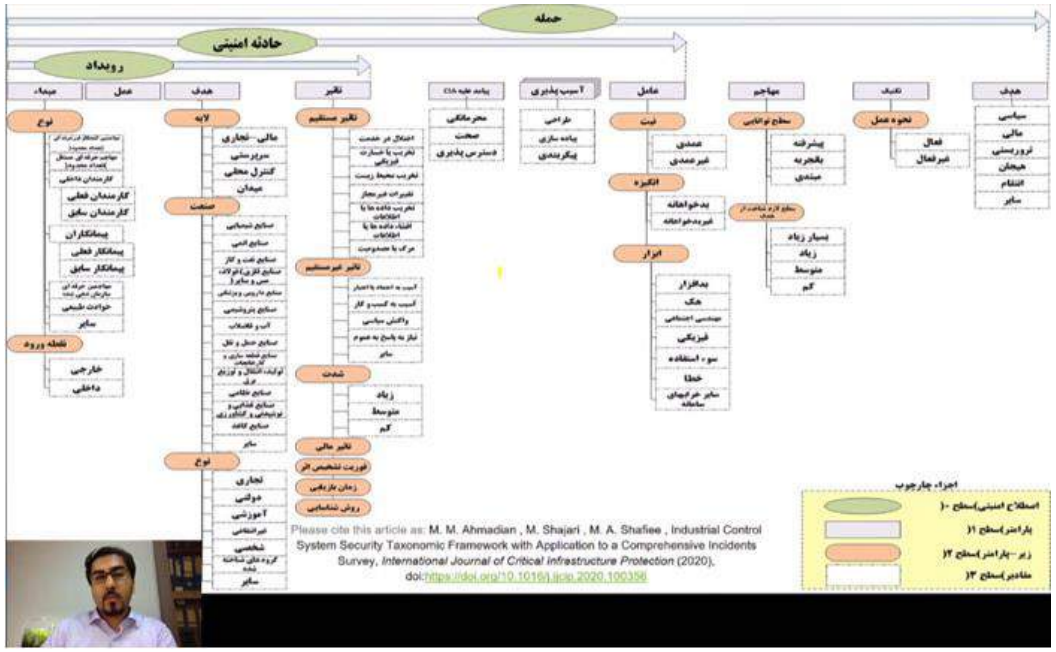
تهران، شهرک قدس، انتهای(غربی) بلوار شهید دادمان، پژوهشگاه نیرو ، مرکز توسعه فناوری

صنعت برق و انرژی (ساختمان رویش) (مرکز رشد) ، طبقه ۱-

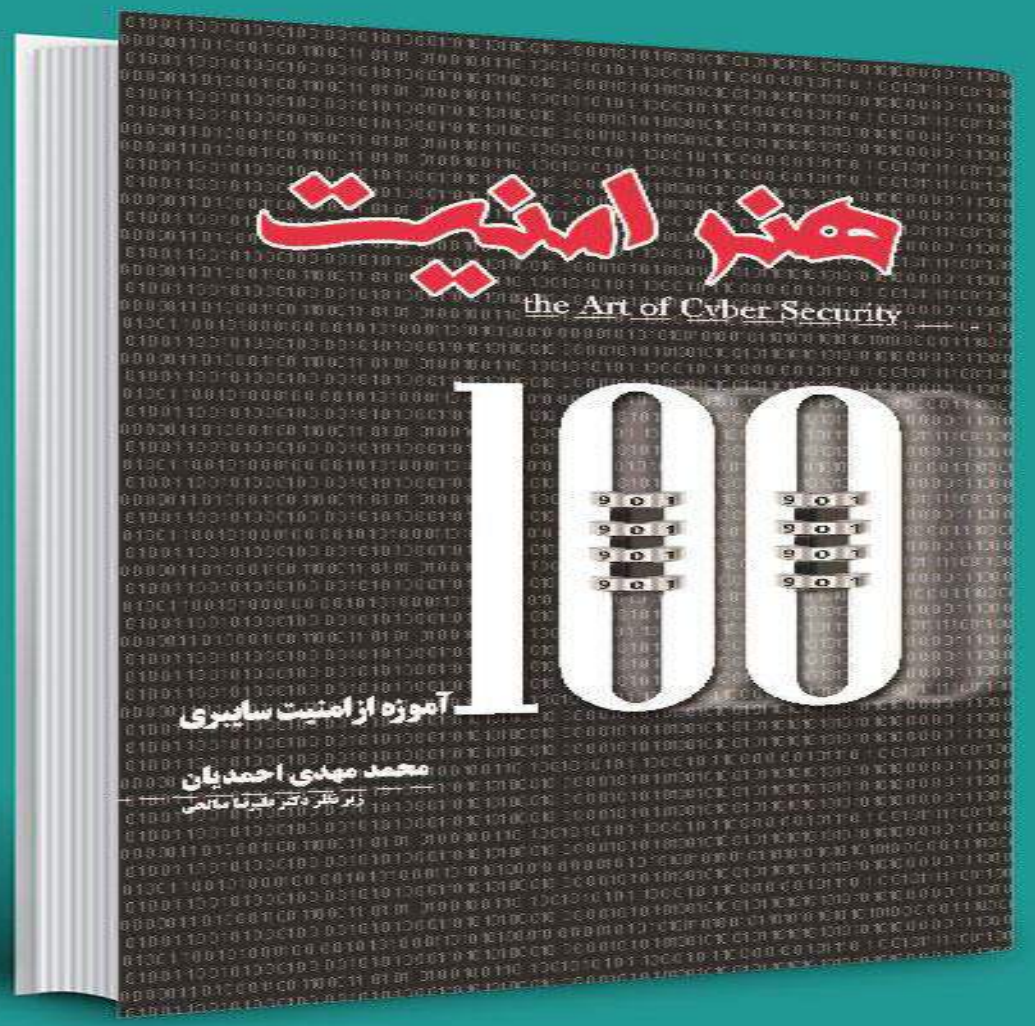
# مشاهده/دانلود رایگان فیلم آموزشی طبقه بندی رخدادهای امنیت سایبری
# سیستم های کنترل صنعتی و اسکادا


آدرس فیلم در آپارات: لینک
www.aparat.com/v/h0s8N

آدرس فیلم در YouTube: لینک



# دانلود رایگان کتاب «هنر امنیت؛۱۰۰ آموزه از امنیت سایبری» از لینک‌های ذیل:




- دانلود کتاب از ResearchGate: لینک
- دانلود کتاب از google drive: لینک
- دانلود کتاب از طاقچه : لینک
- دانلود کتاب از گیسوم : لینک
- دانلود کتاب از سایت ناشر محترم: لینک

# دانلود رایگان کارت‌های آگاهی بخشی و حساس‌سازی امنیت سایبری از لینک ذیل:

- دانلود از وبلاگ: لینک








«یا ذا الامن و الامان»

# قبل از اینکه هکرها شما را پیدا کنند

پیشگامان امن آرمان به شما کمک می کند تا

# متخصصین امنیتی را پیدا کنید.

امن آرمان؛ امنیت و آرامش

AmanSec.ir

@Aman_Sec