Ypatingos svarbos infrastruktūrų kibernetinis saugumas

Vytautas Butrimas
LR KAM KSITD vyr. patarėjas
Vytautas.Butrimas@kam.lt

2015 -01-29

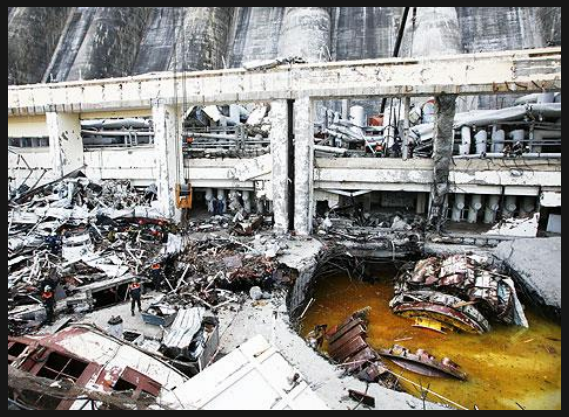
LT Mokslo Akademija

Ką turime saugoti?

- At tiktai informacinės sistemas ir kompiuterių tinklus?

"The Largest Cyber Attack In History Has Been Hitting Hong Kong Sites" - Parmy Olson , Forbes 2014-11-20

Kas sukelia šias nelaimes ?

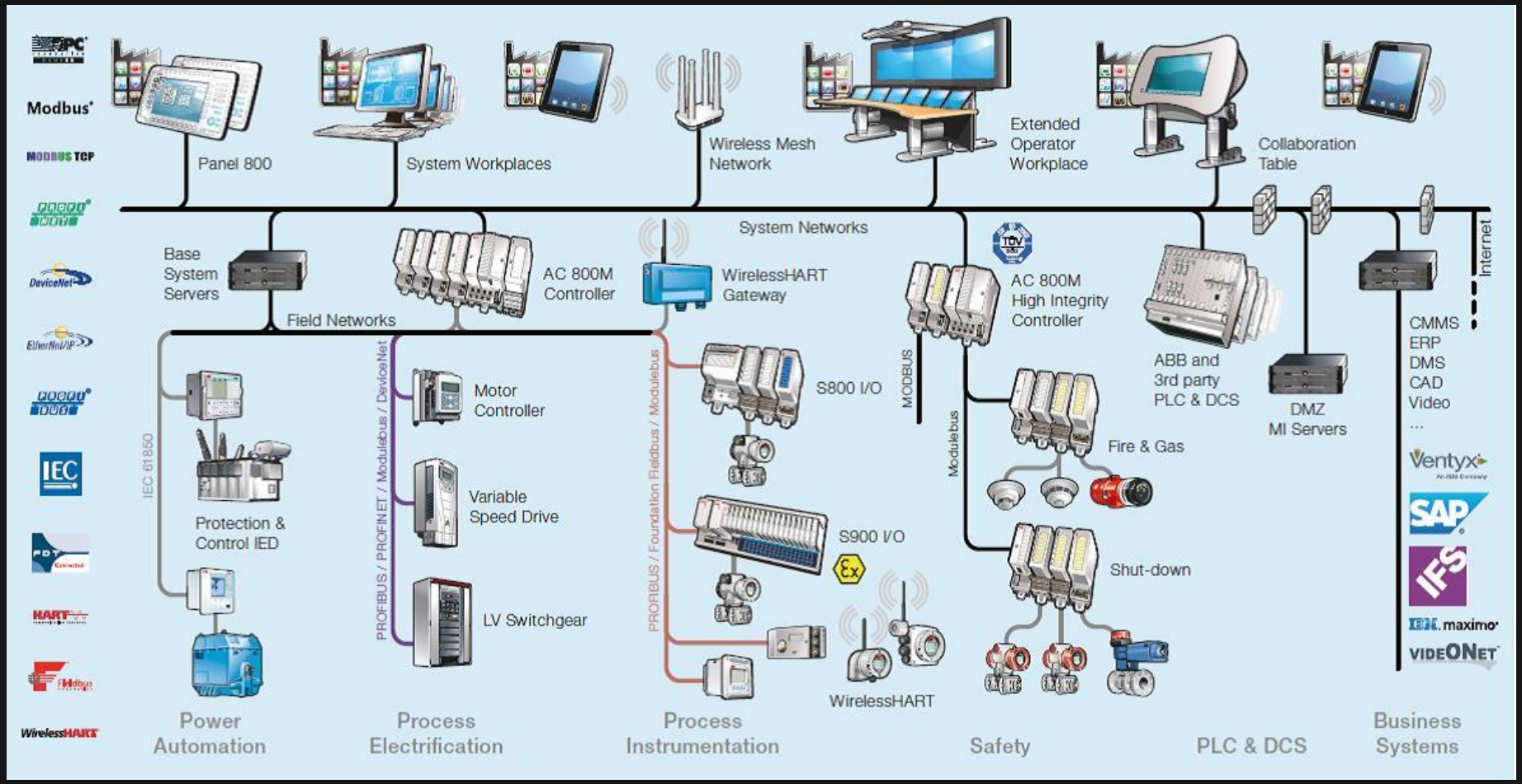


Ką turime saugoti?

- Ypatingos svarbos infrastruktūras
  - Tas, kuriose įvykus sutrikimui, susidaro pavojus šalies ekonomikai, žmonių gyvybei ir nacionaliniam saugumui.

Ką turime saugoti?

- Industrinių ir infrastruktūrinių procesų valdymo sistemas (PLC, DCS, SCADA)



IT “atėjimo” į YSI aplinką poveikis

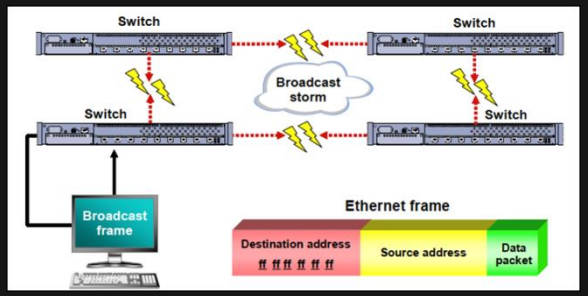
- IT technologijos leido efektyviau valdyti vis sudėtingesnes sistemas, tačiau kibernetinė aplinka tapo trapesnė.
- IT specialistai dominuoja YSI, įvesdami savo saugumo politiką pilnai neįvertindami naujos aplinkos ypatumų.
- Padidėjo netyčinių kibernetinių incidentų pramonės valdymo sistemų aplinkoje.

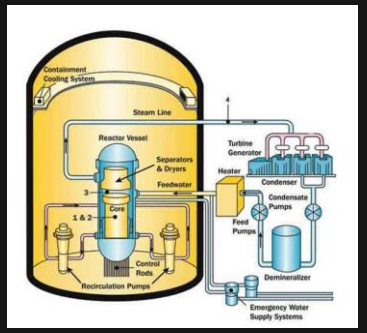
1971

Šiandien

YSI “netyčiniai” kibernetiniai incidentai

- “***A nuclear power plant in Georgia was recently forced into an emergency shutdown for forty-eight hours after a software update was installed on a single computer***”.
  - Hatch nuclear power plant near Baxley, Georgia 2008
- ***“..the root cause of the event was the malfunction of the VFD controller because of excessive traffic on the plant ICS network***.”
  - Brown’s Ferry Power Station Shutdown – 2006
- Žinios apie pažeidžiamumus, gali būti panaudojamos rengiant tyčinius išpuolius.





Kibernetinės grėsmės YSI

- Kibernetinis nusikalstamumas
- “Haktyvistų” veikla / “kibernetinis terorizmas?”
- Netyčiniai kibernetiniai incidentai
- Valstybės kenksminga veikla kibernetinėje erdvėje
  - Turi resursus, laiko, „licencijas“ ir visada pasieks tikslo

Valstybės kenksminga veikla kibernetinėje erdvėje
STUXNET (2006 – 201?)

- „Pirmas“ valstybės sukurtas kibernetinis ginklas, nutaikytas prieš kitos valstybės YSI.
- Sukėlė „matymo praradimą" ir „kontrolės praradimą„
  - Išjungė YSI įrangos apsaugos sistemas
  - Sužalojo įrangą kartu persiuntė operatoriams duomenis, kad vyksta „normalūs“ procesai.
- Patrauklus, palyginus „pigus“ , efektyvus, paneigiamas
- Daugiausia taikinių yra Europoje ir Š. Amerikoje

Valstybės kenksminga veikla kibernetinėje erdvėje

- STUXNET‘o sėkmė ir pavyzdys nukreipė dėmesį į YSI

Valstybės kenksminga veikla kibernetinėje erdvėje

- Irano energetikos sektorius (2009-?)
- Saudi Aramco 2012 (atpildas?)
- KPI: Havex, Sandworm, Black Energy, Regin, Cleaver 2014
  - Skanuoja SCADA energetikos, transporto ir gamybos sektorius
  - vyksta žvalgyba (RF?), ieškoma GE ir SIEMENS pagamintos įrangos

- Vokietijos BSI 2014 m. gruodžio ataskaita apie kibernetinę ataką, nutaikytą prieš plieno gamyklos SCADA (padaryta žala)

Dar nesate įtikinti dėl pavojaus ?

Mūsų YSI įranga „matoma“ Internete: „Project Shine“

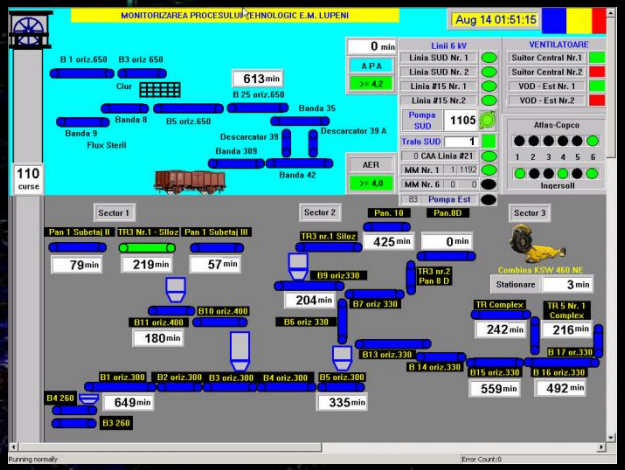
Countries Identified with Total Count Results

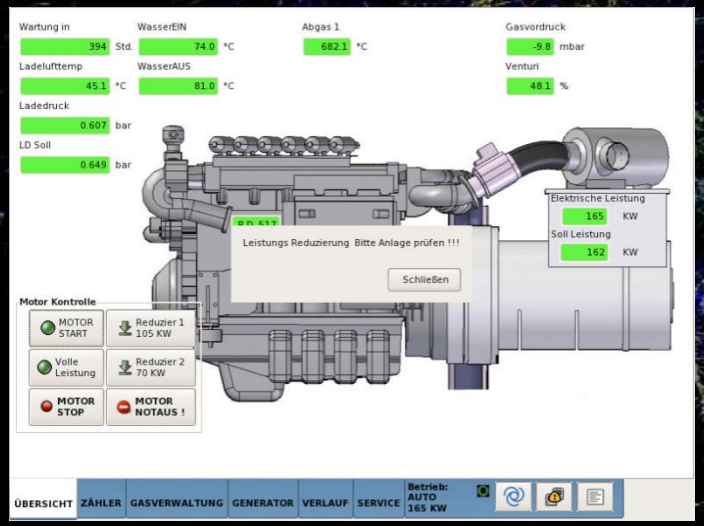
There were 211 countries identified based on the IP addresses harvested from the search terms discovered. Outlined below is each country with total count per country. The total count is 2,186,971.

Afghanistan	165	Cameroon	136	Ghana	300	Lichtenstein	0
Aland Islands	79	Cape Verde	22	Gibraltar	312	Lithuania	1951
Albania	192	Cayman Islands	59	Greece	9287	Luxembourg	1172
Algeria	1068	Central African	4	Greenland	175	Macau	472
American Samoa	74	Chile	5993	Grenada	37	Macedonia	616
Andorra	49	China	112114	Guadeloupe	129	Madagascar	83
Angola	241	Colombia	15801	Guam	141	Malaysia	8832
Anguilla	40	Comoros	7	Guatemala	508	Malawi	68
Anonymous Proxy	88	Congo	89	Guernsey	77	Mali	92
Antigua and Barbuda	63	Cook Islands	10	Guinea	126	Maldives	105
Argentina	12634	Costa Rica	6477	Guyana	17	Martinique	135
Armenia	2487	Cote d'Ivoire	81	Haiti	144	Malta	363
Aruba	375	Croatia	11439	Honduras	413	Mauritania	30
Asia/Pacific Region	74	Cuba	143	Hong Kong	11702	Mauritius	179
Australia	20083	Curacao	209	Hungary	6871	Mayotte	7
Austria	14027	Cyprus	1948	Iceland	1159	Mexico	39904
Azerbaijan	922	Czech Republic	13955	India	41309	Moldova	416
Bahamas	196	Denmark	9992	Indonesia	7182	Monaco	88
Bahrain	275	Djibouti	32	Iran	3260	Mongolia	209
Bangladesh	955	Dominica	1410	Iraq	362	Montenegro	121
Barbados	204	Dominican Republic	1402	Ireland	4891	Morocco	1459
Belarus	807	Ecuador	2663	Isle of Man	79	Mozambique	271
Belgium	8863	Egypt	5342	Israel	11894	Myanmar	8
Belize	418	El Salvador	338	Italy	62266	Nambia	0
Benin	33	Equatorial Guinea	12	Jamaica	1186	Nepal	112
Bermuda	262	Estonia	1571	Japan	34013	Netherlands	29349
Bhutan	51	Ethiopia	28	Jersey	91	New Caledonia	82
Bolivia	3344	Europe	338	Jordan	2106	New Zealand	2783
Bonaire	29	Faroe Islands	56	Kazakhstan	2111	Nicaragua	204
Bosnia & Herzegovina	772	Fiji	77	Kenya	1282	Nigeria	1850
Botswana	109	Finland	14444	Korea	99856	Norway	28544
Brazil	62376	France	56827	Kuwait	1203	Oman	230
Brunei Darussalam	121	French Guiana	35	Kyrgyzstan	338	Pakistan	2980
Bulgaria	3369	French Polynesia	218	Lao People	77	Palestinian Territory	765
Burkina Faso	100	Gabon	60	Latvia	2093	Panama	2427
Burundi	10	Gambia	54	Lebanon	779	Papua New Guinea	90
Canada	62712	Georgia	483	Liberia	22	Paraguay	228
Cambodia	321	Germany	280248	Libya	55	Peru	2708

Figure 32.

Su SHODAN Jūs netgi "užrištomis akimis" rasite YSI internete





Kibernetinio saugumo politikos iššūkiai

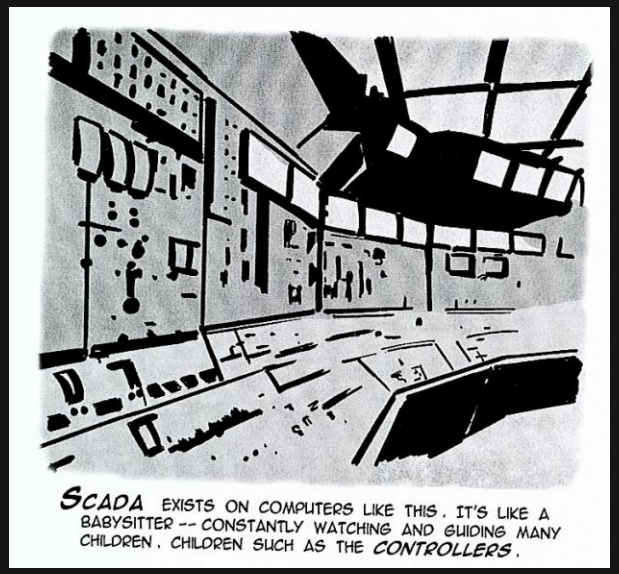
- Trūksta supratimo
  - Dominuoja IT saugumo mąstymo tipas ir per mažai supratimo apie YSI
  - Per daug orientuota į e-nusikaltimus, DDOS, BOTNET
  - “Nesąmonė, mūsų sistemos neturi prisijungimo prie interneto”

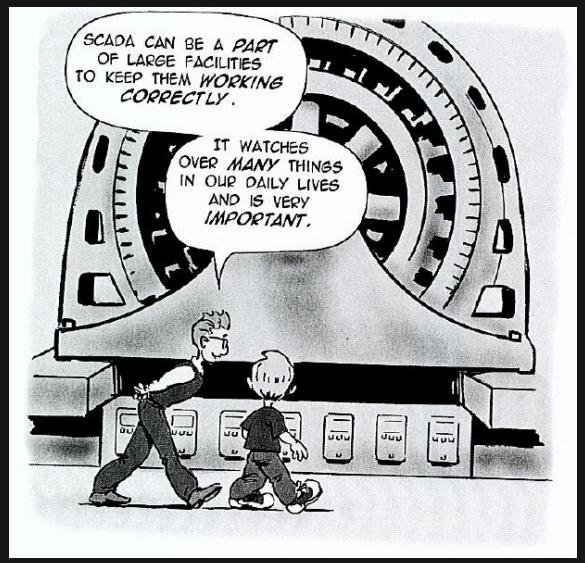

Dėkoju už dėmesį, klausimai?

Kuo labiausiai reikia rūpintis YSI aplinkoje? „matymo praradimą" ir „kontrolės praradimą„

SCADA?!! KAS YRA SCADA?!!

- Tai yra industriniams ir infrastruktūriniams procesams valdyti pritaikytos sistemos, kurios surenka technologinių procesų informaciją, ją apdoroja, vizualizuoja, analizuoja ir kontroliuoja.
- „ SCADA ….Ji panaši į vaikų auklę – nuolat prižiūri ir auklėja vaikus. Vaikai kaip reguliatoriai“



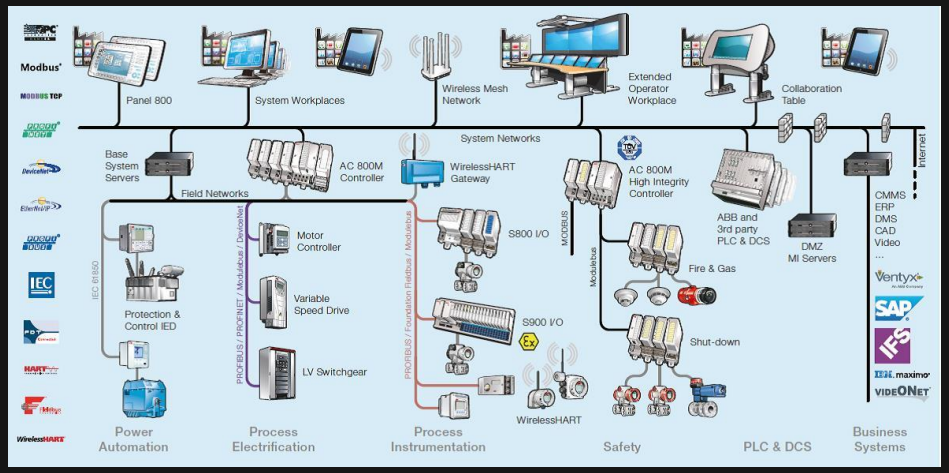


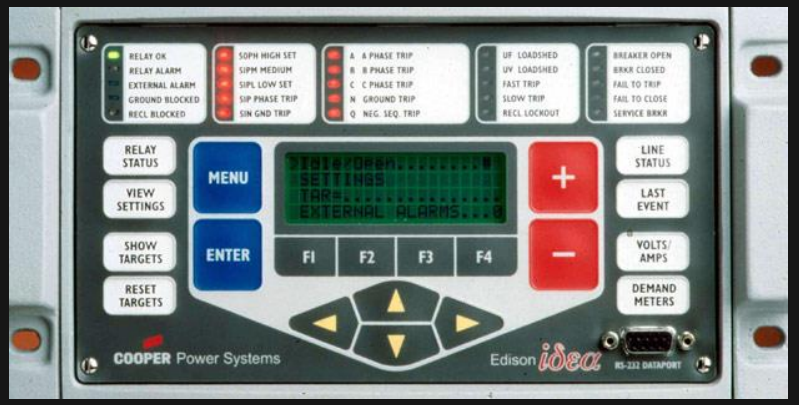
Ar visos Fukušimos pamokos buvo išmoktos ?

"At least one diesel generator, its fuel, and related switch gear could be housed in a room at **sufficiently high elevation and/or in a water-proof room** to preserve onsite AC power **in case of tsunamis or floods**." – MIT 2011 Report, NSP-TR-025 Rev. 1

Kur kreiptis dėl pagalbos įvykus kibernetiniam įvykiui YSI?

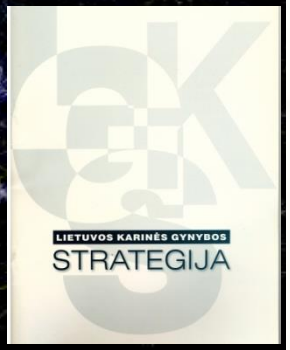
- Izraelio „CYBERGYM“ ☑
- JAV *Industrial Control Systems* ICS-CERT ☑
- Lietuvoje (CERT-LT, LKPB NEETV, NKSC) ☐ ?

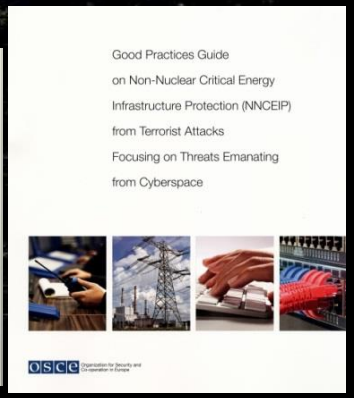




Vytautas Butrimas

- PWCG, LR RIM / KAM
  - 24 m. darbo ITT ir saugumo politikoje
  - Kibernetinio saugumo pratybų dalyvis
    - NATO CMX 2012
    - X 14
    - NATO Energetikos CoE TTX 2014
- Autorius
  - 15+ straipsnių/ knygos skyrių
  - Indėlis ruošiant pasaulio KS apžvalgos ataskaitą





Ką turime saugoti?

- At tiktai...
  - Informacines sistemas ir kompiuterių tinklus?
  - Konfidencialumą, vientisumą ir prieinamumą?
  - Interneto svetaines?
  - Ypatingos svarbos „informacinę“ infrastruktūrą?
  - Tik tiek?