Ar būtina rūpinti kibernetiniu saugumu Industry 4.0 kontekste?

Arvydas Žvirblis
Email: arvydas.zvirblis@smn.lt

Du pasauliai

IT - Skaitmeninis

Duomenys, galutinis vartotojas

Konfidencialumas, integralumas, prieinamumas

Prarandami pinigai

Dinaminis

Platus ryšių tinkas su išore

Standartizuotas

Greita plėtra

Lankstumas

Didelė greitaveika

OT - Fizinis

Kritiniai elementai, **procesai**, aplinka

Kontrolė, prieinamumas, integralumas, konfidencialumas

Prarandamos gyvybės

Deterministinis

Autonominis

Uždari standartai

Ilgas gyvavimo ciklas

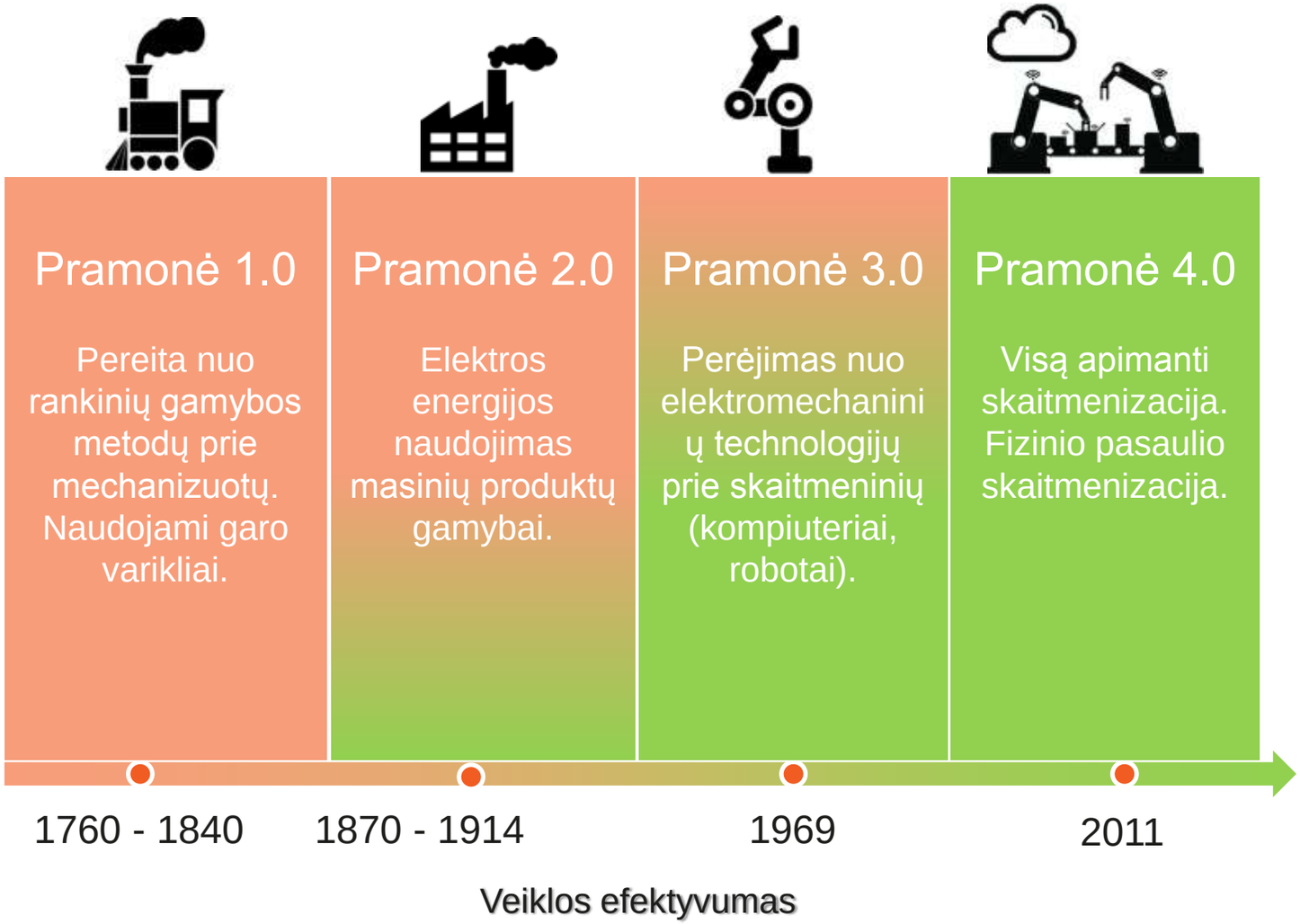
Aukštas patikimumas

Maža greitaveika

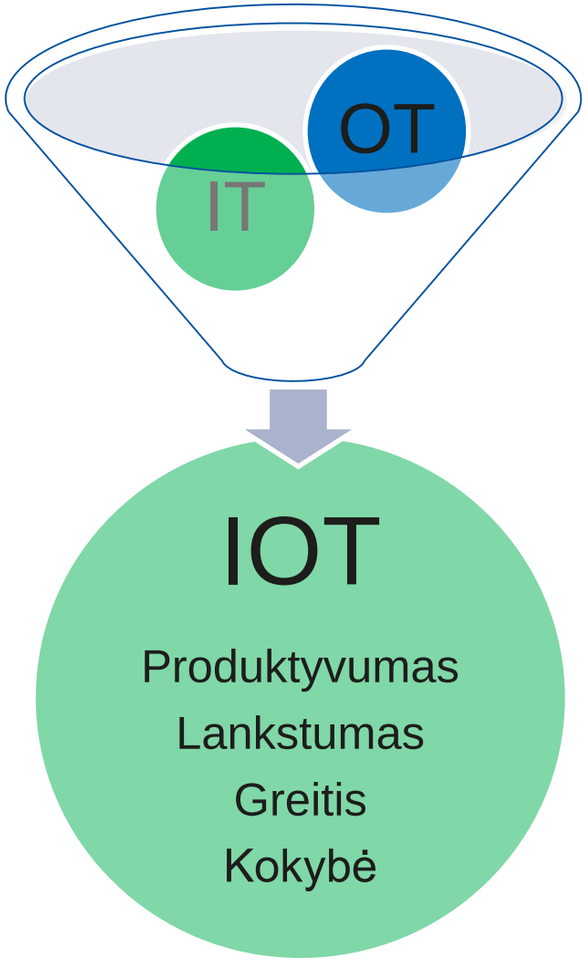
OT mitai #1

- OT naudoja uždarus kodus ir standartus
- Žinias apie OT turi tik mažas ratas specialistų ir OT niekam nėra įdomus
- OT veikia visiškai uždarose aplinkose
- OT veikia saugioje aplinkoje todėl protokolai gali būti paprasti ir nebūtina rūpintis saugumu
- Hackerių nedomina OT

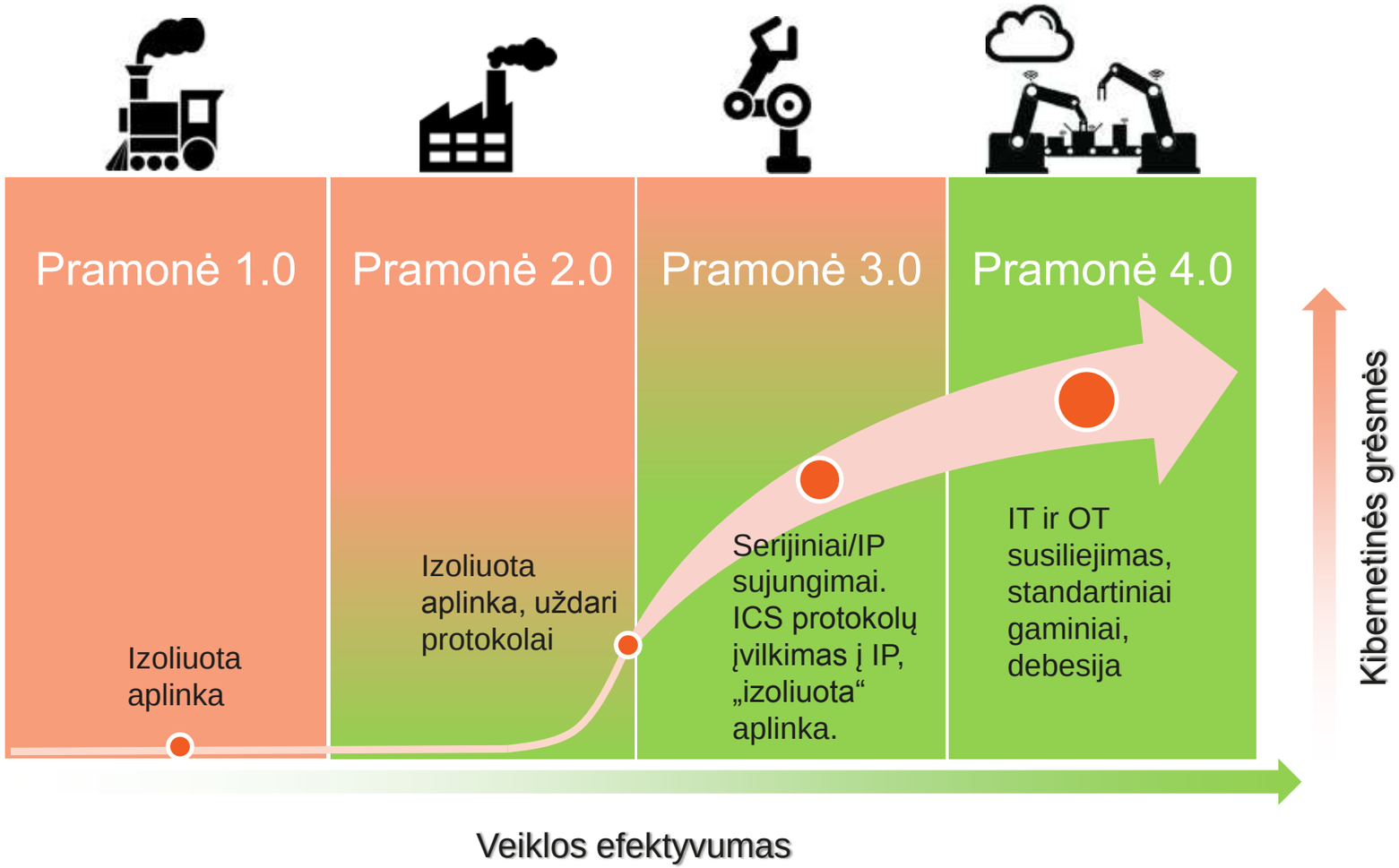
Pramonės revoliucijos



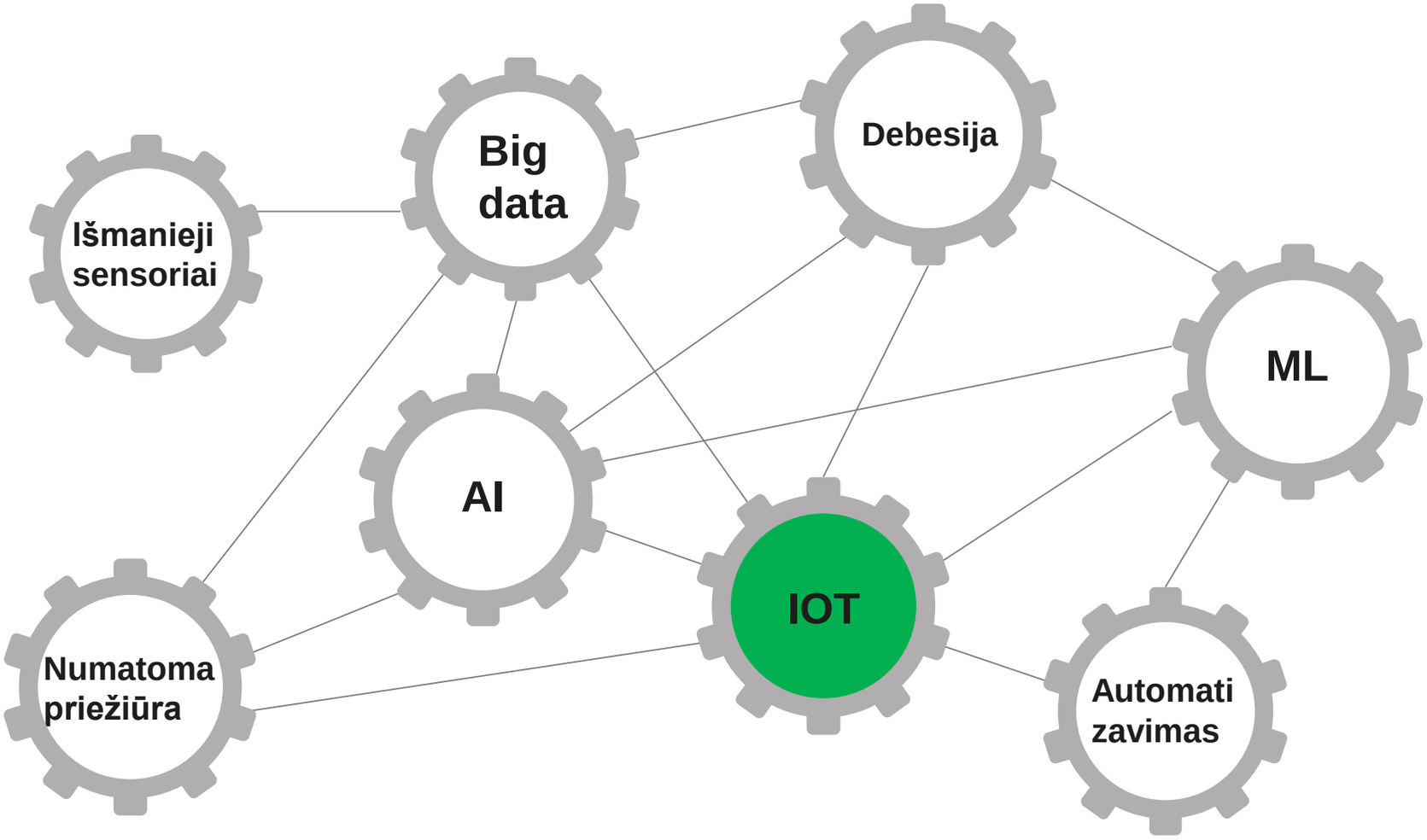
Pramonės revoliucijos



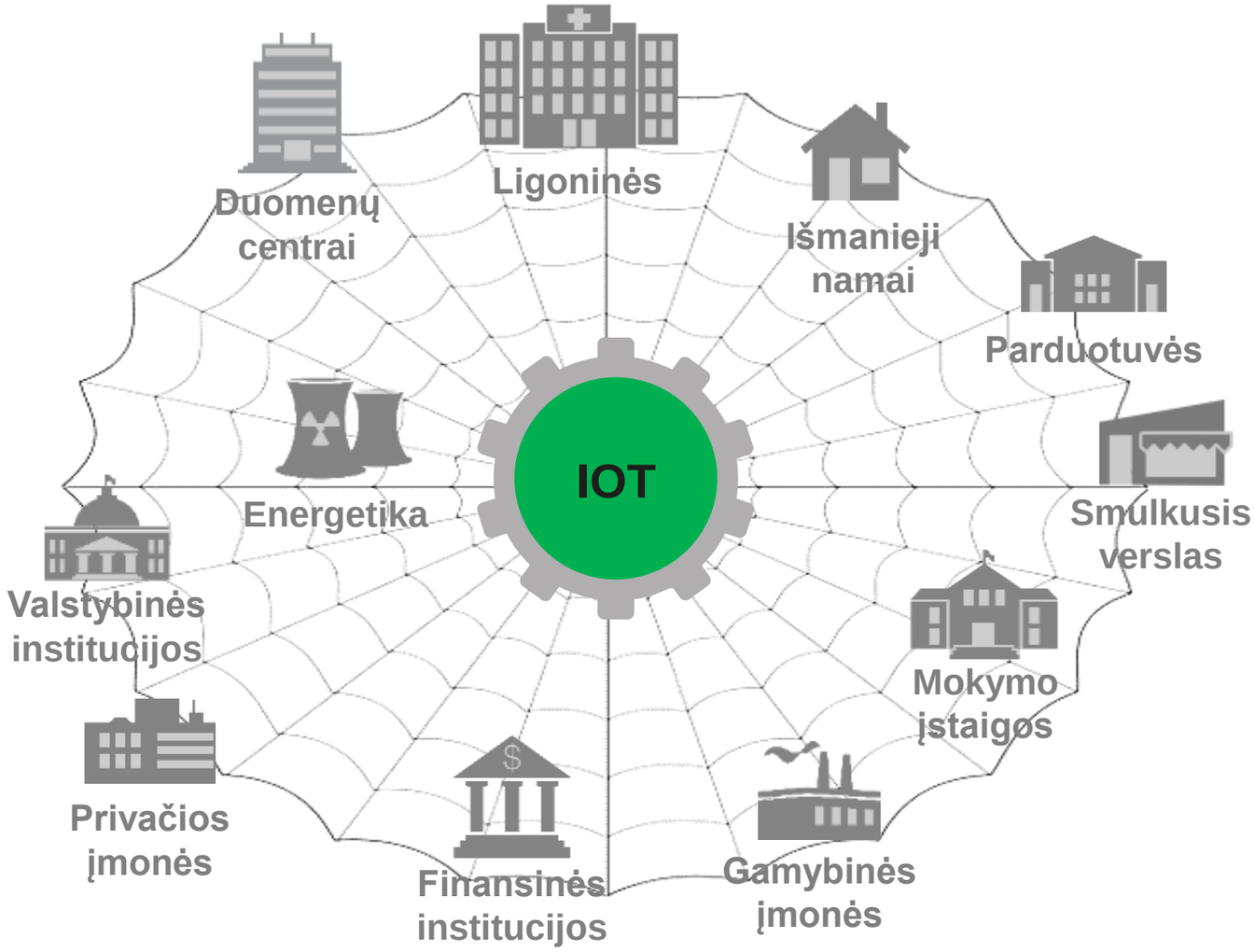
Grėsmių pokytis



Grėsmių pokytis



Grėsmių pokytis



OT trūkumai didinantys riziką

- Ilgas įrangos gyvavimo ciklas
- Naudojama įranga ir protokolai nebuvo kuriami galvojant apie saugumą
- Sudėtingas, o kartais neįmanomas įrangos atnaujinimas. Atnaujinimai daromi retai arba nedaromi.
- Dėl sistemų jautrumo negali būti pilna apimtimi pritaikomi IT pasaulio saugumo sprendimai
- OT darbuotojai neturi IT žinių
- IT darbuotojai neturi OT žinių
- Ryšys su IT pasauliu

OT mitai #2

- OT naudoja uždarus kodus ir standartus
  - OT vis labiau naudoja komercinių (COTS) aparatinių, programinių produktų, protokolų
  - Vis plačiau naudojamas atvirasis kodas
- Žinias apie OT turi tik mažas ratas specialistų ir OT niekam nėra įdomus
  - Daug informacijos apie konkrečius OT sprendimus (dokumentacija, aprašymai) galima rasti internete
- OT veikia visiškai uždarose aplinkose
  - OT tiesiogiai arba netiesiogiai pajungti prie išorinių tinklų (pvz. Internetas), net valdomi iš namų naudojant planšetes

"We back up our data on sticky notes because sticky notes never crash."

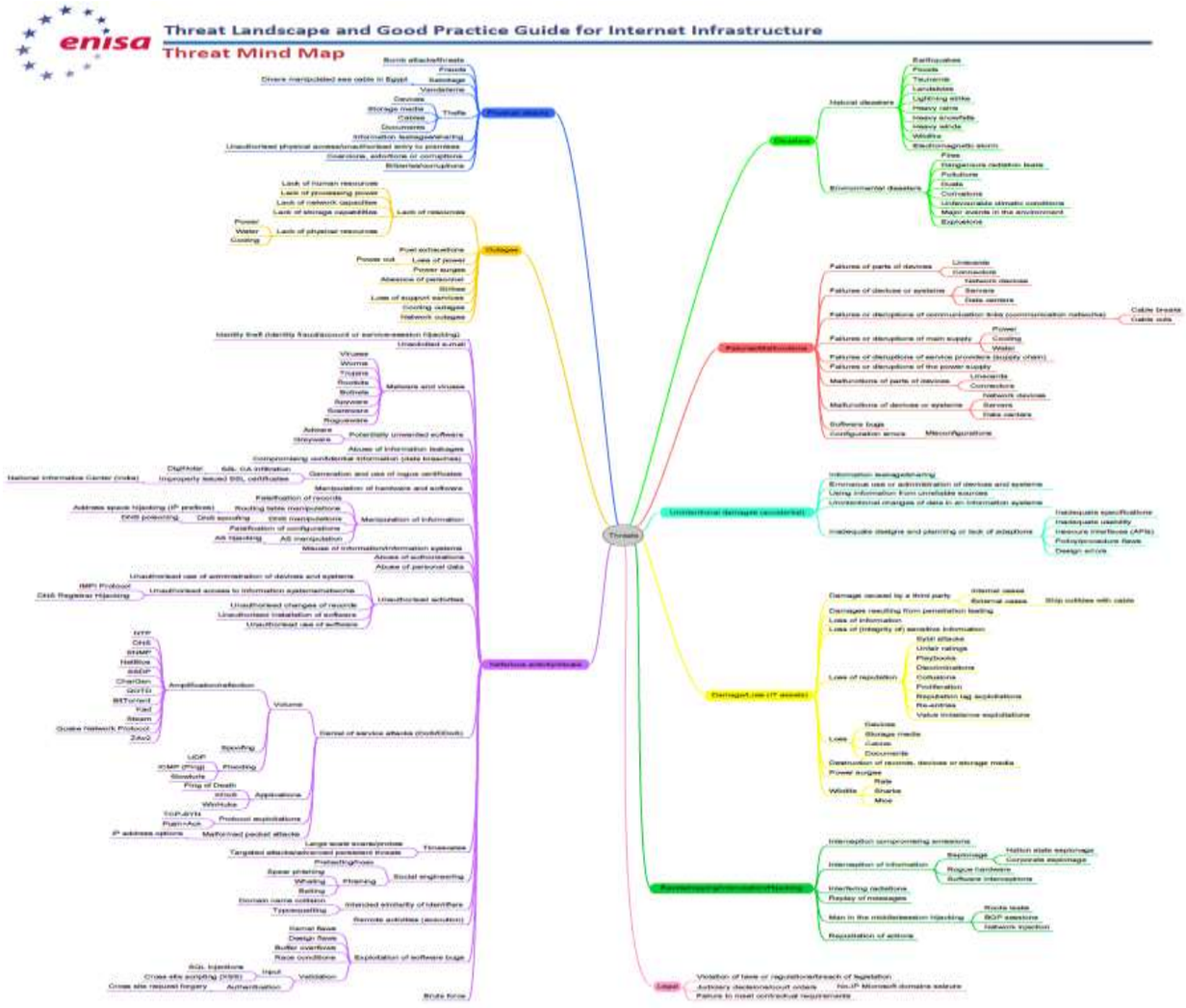
OT mitai #2

- **Hackerių nedomina OT**
  - **Hakerius labai domina OT aplinkos. Jau eilę metų tokiose konferencijose kaip Black Hat nuolat skaitomi pranešimai apie OT pažeidžiamumus. Laisvai prieinamuose įrankiuose yra įdiegtos OT testavimo priemonės (MetaSploit)**

Kas bando pakenkti?

- **Išoriniai asmenys, organizacijos**
  - valstybių remiamos grupės, konkurentai, konkurentai, piktavaliai asmenys, kriminalinio pasaulio atstovai, hacktivistai, „smalsuoliai“ ir t.t.
- **Įmonės darbuotojai**
  - piktavaliai darbuotojai, darbuotojai atliekantys kenkėjišką veiklą per neapdairumą/nežinojimą, darbuotojai, kuriais pasinaudoja treti asmenys jiems nežinant.

Grėsmių tipai



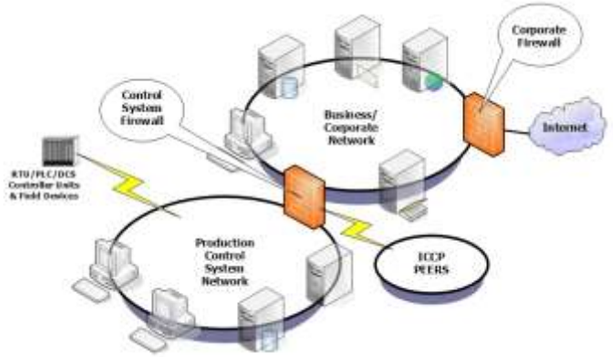
Kaip kenkėjai, kenkėjiški kodai patenka į IT/OT?

- **Naršymas internete**
  - Užkrėstos svetainės, nesaugios svetainės, neatnaujintos naršyklės, failų atsisiuntimas, programėlių padirbtos versijos, ir pan.
- **Elektroniniai laiškai**

  - Kenkėjiški laiškų priedai, nuorodos, socialinė inžinerija, Phishing
- **Laikmenos**

  - Laikmenose perduodamos bylos
- **„Peer 2 peer“ tinklai**

- **Nuotoliniu būdų pasiekiami pažeidžiami tinklo resursai**
  - Prižiūrimos sistemos, svetainės, paslaugų portalai ir pan.
- **Nekontroliuojama prieiga prie IT/OT tinklo iš vidaus**
  - Nesankcionuotas įrenginių pajungimas



Ar tikrai kažkas vyksta?

2009 Sayano–Shushenskaya Hidro elektinė

- **Prieš įvykį**

- **Po įvykio**

Ar tikrai kažkas vyksta?

Ar tikrai kažkas vyksta?

14 metų jaunuolis įsilaužė į Lodzės tramvajų valdymo sistemą (2008m)

Motyvas – pokštas

12 žmonių sužeista

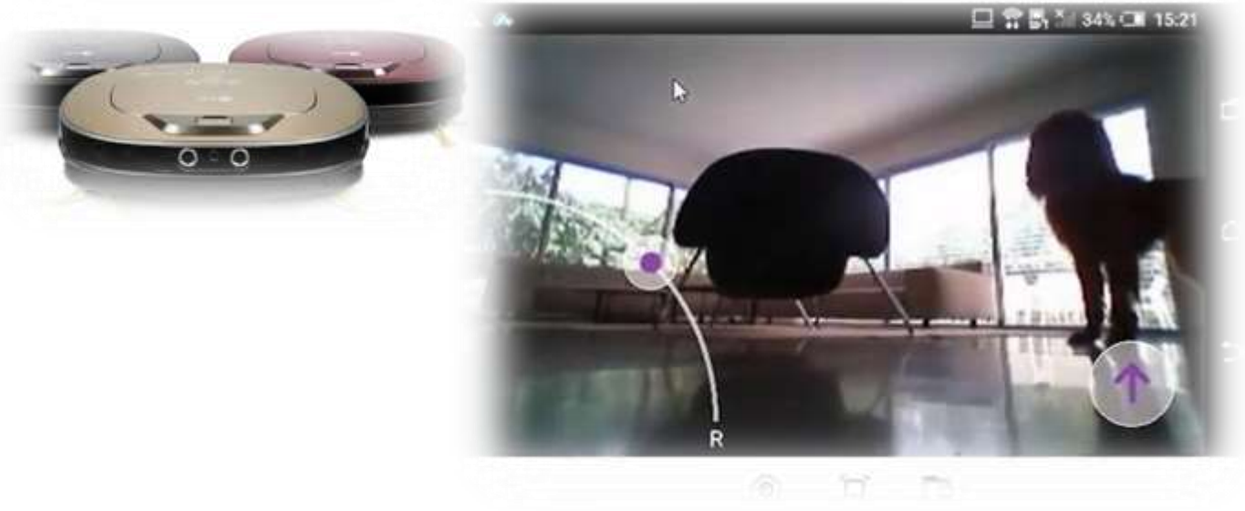
Ar tikrai kažkas vyksta?

2015m. Ukrainos elektros tinklas

Atjungta 30 pastočių
1-6 val. be elektros liko 230 tūks. žmonių

Ar tikrai kažkas vyksta?

- 2017m. įsilaužta į LG HOT-BOT siurblį



- 2017m. įsilaužta į PDQ LaserWash mašinų plovyklą Vašingtono valstijoje

Kodėl nuvertinama saugumo svarba?

- Nesukuria tiesioginės vertės
- Silpnas reguliavimas
- Menkos baudos
- „Maži“ finansiniai nuostoliai
- Trūksta metodinės paramos
- Trūksta IT saugumo profesionalų

Ko neįvertiname?

- Įvykus saugumo įvykiui nuostoliai gali būti milžiniški:
  - Prarastos gyvybės
  - Sustojusi gamyba
  - Neuždirbtos pajamos
  - Parasta intelektinė nuosavybė
  - Atskleistos komercinės paslapys
  - Klientų praradimas
  - Išlaidos krizinės situacijos valdymui
  - Veiklos sutrikdymas
  - Draudimo išlaidų padidėjimas
  - Prarasti kontraktai
  - Sužlugdytas verslas
  - Klientų informavimo išlaidos
  - Reguliuojančių institucijų skiriamos baudos
  - Advokato mokesčiai ir bylinėjimosi išlaidos
  - Reputacijos praradimas

Iššūkiai

- IT ir OT skirtingi organizaciniai vienetai
- Skirtingos IT ir OT kultūros
- Skirtingas IT ir OT saugumo brandos lygis
- Išlaidos saugumui – pelnas vs. praradimų prevencija
- Senos sistemos
- Personalo trūkumas
- IOT produktų ir sprendimų pirkimas

Ačiū
Pasirūpinkite savo ir kitų saugumu!

“*All* organizations should now assume they are in a *state of continuous compromise*” (Gartner)