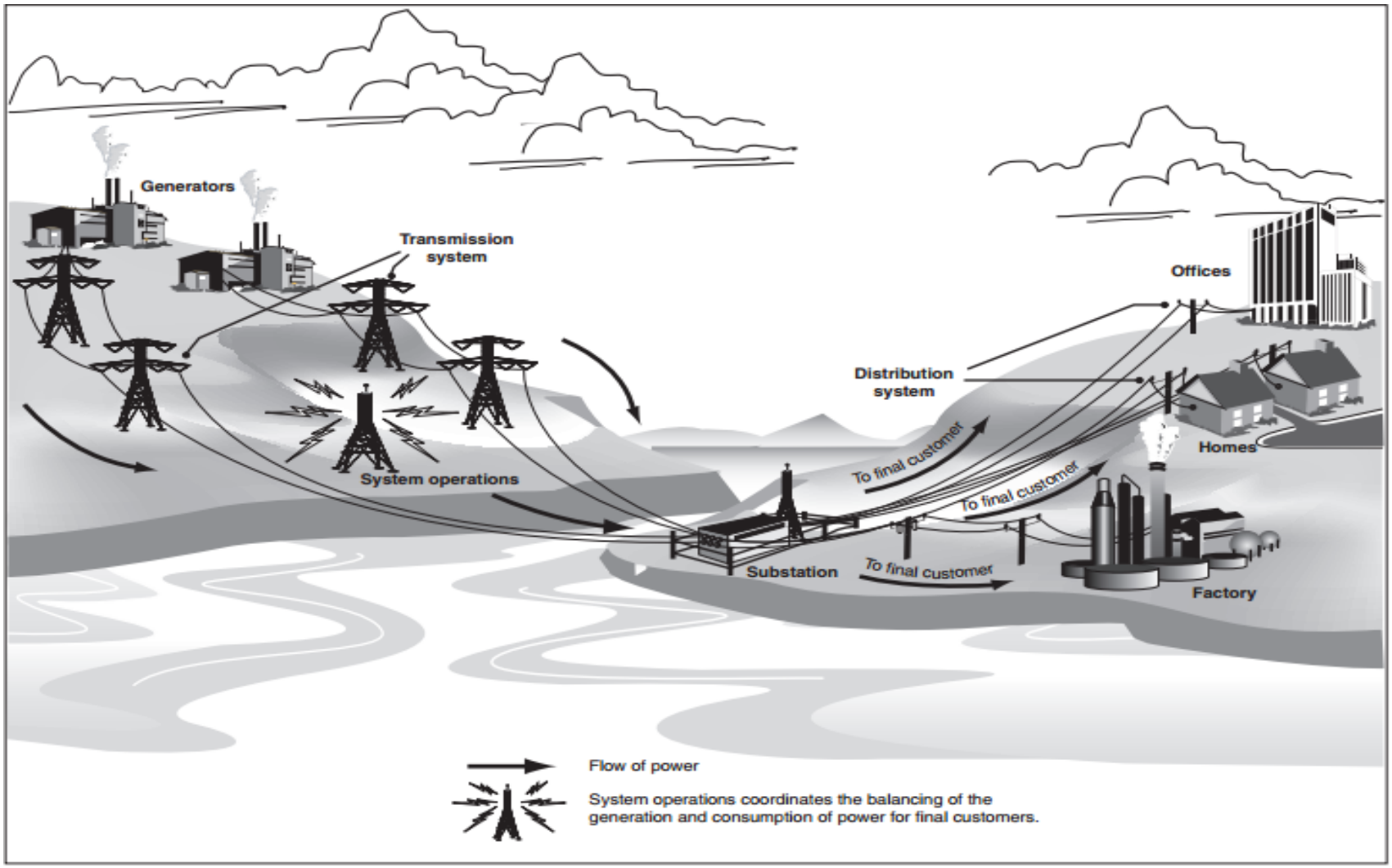
Bezpečnostné útoky na smart gridy

Bez(a)Dis

Juraj Hájek, Project Manager, Ardaco, a.s.

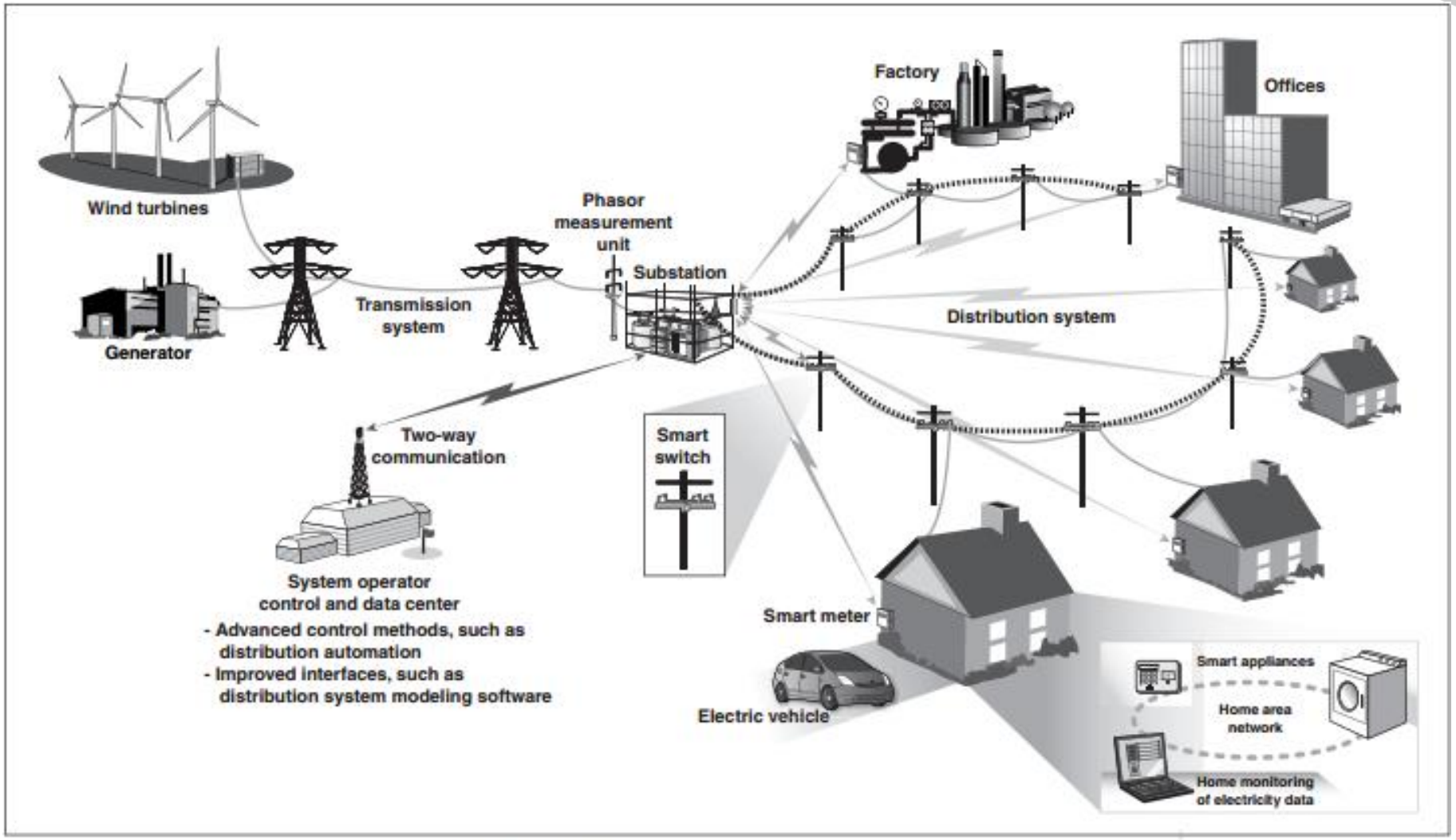
Košice, 5.12.2012

Tradičná sieť



Source: GAO analysis.

Komponenty smart gridu



Source: GAO analysis.

Dodatočné riziká

- Vyššia komplexita
  - Vyššie vystavenie možným útočníkom
  - Viac zraniteľných bodov a nové cesty útoku
- Splývanie s IT infraštruktúrou
  - Škodlivé kódy
  - DoS útoky
- Možné narušenie súkromia

Northeast blackout 2003

- Príklad ako netreba ani kyberterorizmus ☺
- SW chyba -> kaskádovitý výpadok siete
- Dopad na 55.000.000 obyvateľov (USA, Kanada)
- Druhý najväčší výpadok v histórii

Jadrová elektráreň Brown's Ferry (USA)

- Incident 2006: Odstavenie Bloku 3
- Zlyhanie dvoch púmp na cirkuláciu vody
- Príčina – zahltenie riadiacej siete
- Firemná sieť s pripojením na internet prepojená s riadiacou (!!!)

Vodná elektráreň Itaipu (Brazília/Paraguaj)

- 2009: Reportáž o hacku v r. 2005 a 2007 (výpadky)
- Vláda informácie poprela
- Do 24h po popretí systém opäť zhodený
- Rozpor vládne vyšetrovanie vs. wikileaks

Leningradská jadrová elektráreň (Rusko)

- 2008: Útok na web stránky
- Publikovanie falošných informácií o úrovni radiácie

Ďalšie a ďalšie incidenty

- 2009: USA deklarovalo napadnutie energetických zariadení špiónmi z Ruska a Číny
- 2009: Austrálska spoločnosť Integral energy – 1.000 infikovaných počítačov

Niekoľko záverov

- Nejde o teoretické riziká
- Vlastníci a operátori majú odpor k hláseniu incidentov
- Nedostatočne investujú do zabezpečenia

Veľké dopady

- Všeobecná rozšírenosť elektrickej siete
- Systémy sú kritické a 24x7
- Závažné závislosti
  - Výroba/distribúcia/spotreba energie
  - Zásobovanie vodou
  - Doprava
  - Komunikácia

Motivácia útočníka

- Získanie pozornosti
- Dokázanie si schopností
- Pocit sily
- Finančný prospech
- Politická agenda
- Pomsta
- Nenávisť
- Špionáž
- ...

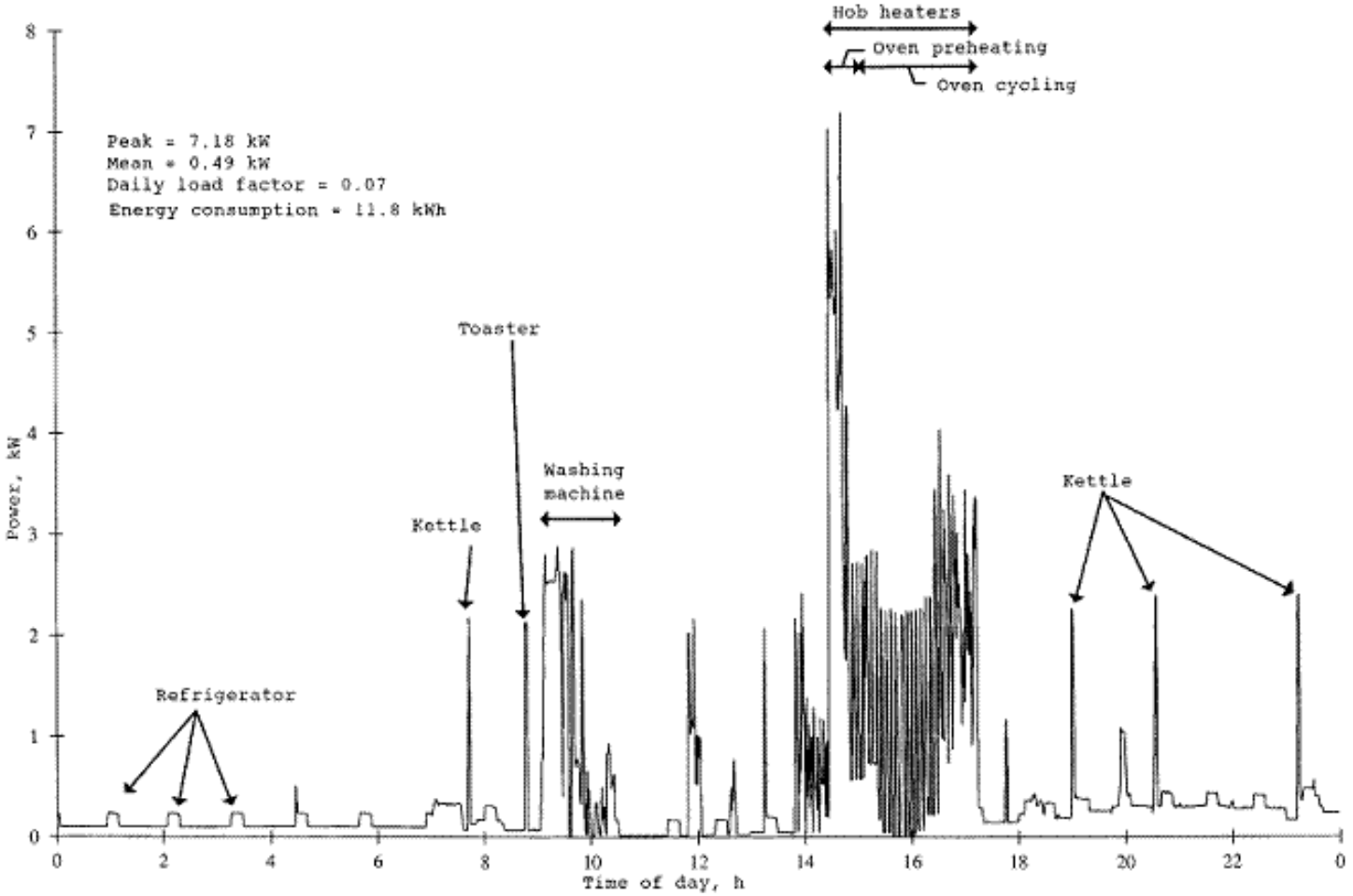
Požiadavky na bezpečnosť

- Kľúčové vlastnosti - CIA
  - **C**onfidentiality - dôvernosť
  - **I**ntegrity - integrita
  - **A**vailability - dostupnosť
- Stratégia
  - Prevencia
  - Detekcia
  - Reakcia
  - Zotavenie

Dôvera spotrebiteľov

- Výskum z preferenciách zákazníkov (Accenture, apríl 2010)
  - Viaz než 9.000 zákazníkov
  - 17 krajín
  - Približne 1/3 tvrdila, že by ich odradili programy pre riadenie spotreby, ak by mal distribútor detailnejšie informácie o ich spotrebe
- **Dôvera** je kľúčová pre získanie zákaníkov
- Majú vlastnú hierarchiu potrieb, na základe ktorej sa rozhodujú

Súkromie - graf spotreby energie



- Zdroj: NISTIR 7628 Guidelines for Smart Grid Cyber Security v1.0

Súkromie

- Rôzne kategórie:
  - Osobné informácie
  - Osoba (napr. zdravotnícke pomôcky)
  - Správanie
  - Osobná komunikácia
- Kto vlastní dáta so smart gridu?

Protesty proti smart metrom

Šírenie škodlivých kódov

- Prezentácia realizovateľnosti:
  - Godspeed 2007
  - IOActive 2009
- Až 15.000 domácností/24h

Obmedzenia – kryptografia v smart devices

- Všeobecné výzvy
  - Výpočtové obmedzenia (CPU, cryptoporcessor, RAM)
  - Šírka komunikačného kanála
    - Šifrovanie – negatívne ovplyvňuje kompresné algoritmy
    - Ochrana integrity - komunikačný overhead
  - Konektivita
    - Prístup k PKI infraštruktúre
- Ďalšie faktory
  - Zdroj entropie
  - Cipher Suite (štandardizácia, zrelosť, licencovanie)
  - Key Management (vrátane dĺžky platnosti certifikátov)

Problémy implementácie

- Chýbajúca kontrola a obsluha chybových stavov (obmedzenia na veľkosť programu)
- Buffer/Integer overflows
- Malý zásobník – napr. max. hĺbka 7
- Programátorské chyby v stavových strojoch (protokoly, autentizačné schémy)
- ...

TI MSP430 - predpoklady na útok

- Používa ho viacero výrobcov smart metrov
- Cena cca $0.25 za 100.000 kusov
- LaunchPad development kit for $4.30 (including compilers, debuggers)
- Obmedzená pamäť pre kód 0.5-2 KB
- Žiadna ochrana pamäte
- Malý priestor na stacku
- Zdroj entropie nie je chránený

Zhrnutie

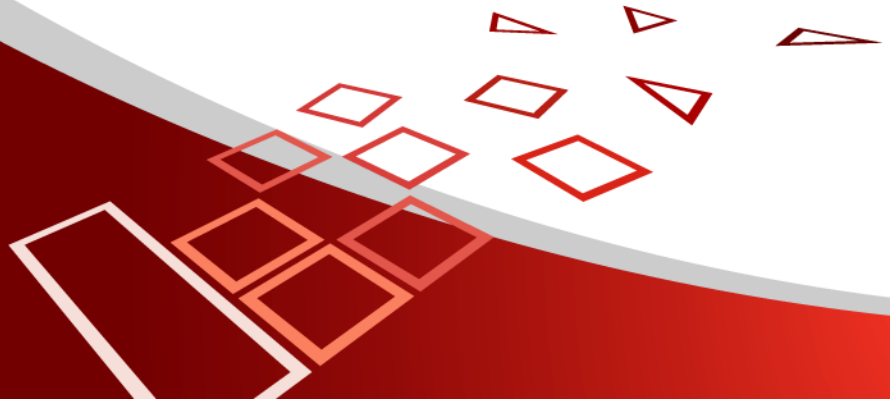
- Smart gridy predstavujú nový, inteligentnejší spôsob distribúcie energie
- Koncoví používatelia majú aktívnu úlohu
- Dochádza k splývaniu s IT infraštruktúrou
- Vznikajú nové hrozby pre bezpečnosť a súkromie
- Situáciu treba riešiť na viacerých úrovniach

Ďakujem za pozornosť

- Otázky?

ARDACO, a. s.
Polianky 5
841 01 Bratislava
Slovakia

Tel.: +421 (2) 3221 2311
Fax: +421 (2) 32212 312
info@ardaco.com



www.ardaco.com