Je Smart Grid bezpečný?

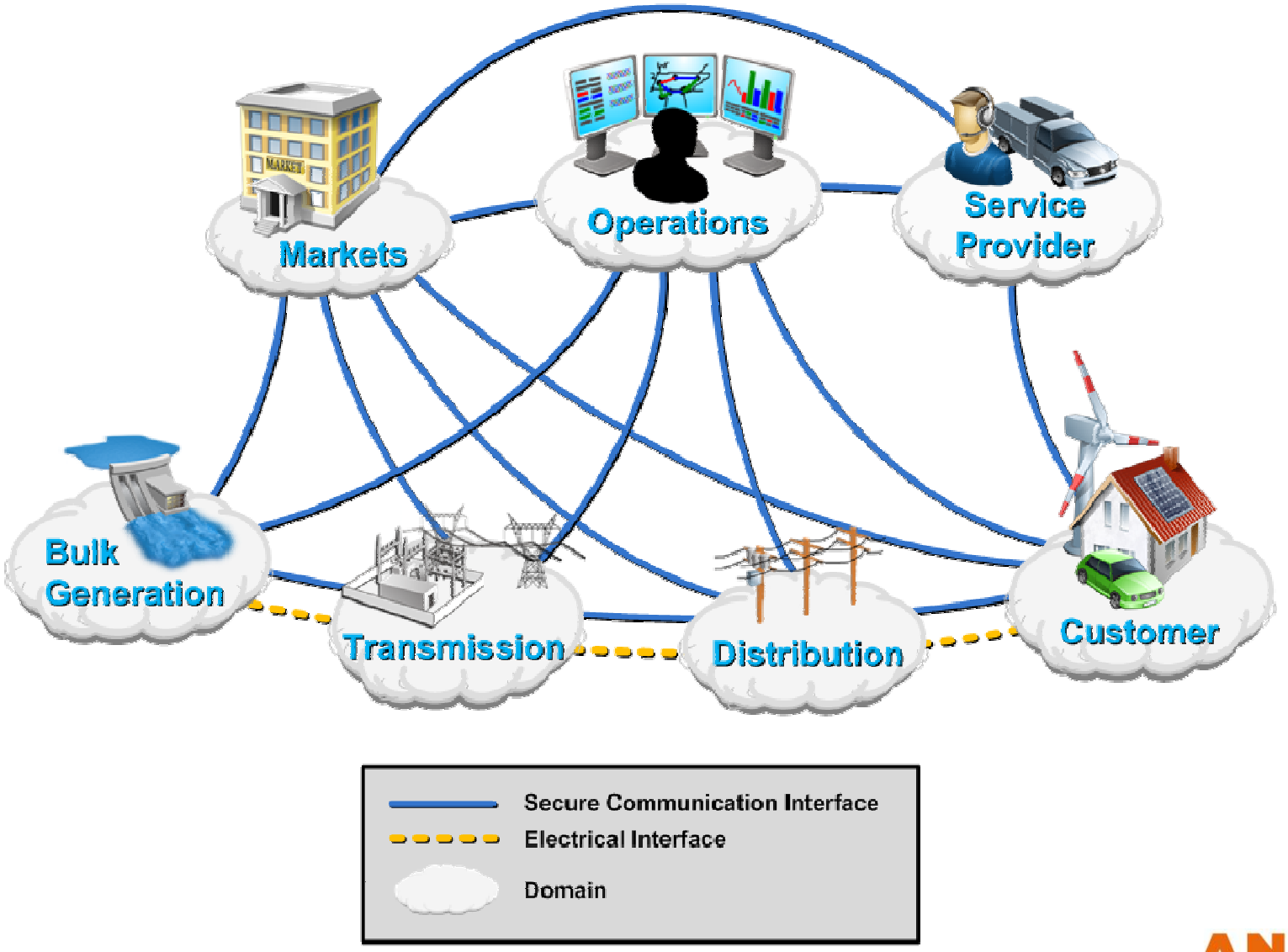
Petr Paukner
petr.paukner@anect.com **- člen představenstva**

Kontext

Moderní Smart Grids potřebují zajistit:

- **Aktivní participaci producentů i konzumentů energií, při zachování ochrany jejich dat**
- **Anticipaci a reakci na narušení systémů**
- **Poskytování kvalitních služeb pro digitální ekonomiku**
- **Umožnit vytváření nových produktů, služeb a celých trhů**
- **Podporovat alternativy při generování a uchovávání elektrické energie**
- **Zajistit odolnost proti útokům a přírodním katastrofám**
- **Optimalizovat využívání zdrojů, majetku**

Koncepční pohled na Smart Grids



Hlavní témata zabezpečení Smart Grids

Stabilizace distribučních a přenosových systémů

- **Spolehlivost SG**
  - Komunikační infrastruktura
  - Řízení a kontrola provozu (businessu) v logickém kontextu
- **Ochrana proti zneužití řídící soustavy**
  - Zajištění komunikační infrastruktury
  - Zabezpečení řídících systémů
  - Bezpečná a efektivní autentizace pro uživatele SG a provozní pracovníky

Operation

- **Funkce monitorování, řízení a automatizace**
  - Řízení a kontrola provozu (businessu) v logickém kontextu
  - Kontrola procesů
  - Snížení rizik
  - Efektivita sítě

E-mobility – součást SG

- **Systém autentizace vozidel, nebo řidičů**

Hlavní témata zabezpečení Smart Grids

Stabilizace distribučních a přenosových systémů

- **Spolehlivost SG**
  - Komunikační infrastruktura
  - Řízení a kontrola provozu (businessu) v logickém kontextu
- **Ochrana proti zneužití řídící soustavy**
  - Zajištění komunikační infrastruktury
  - Zabezpečení řídících systémů
  - Bezpečná a efektivní autentizace pro uživatele SG a provozní pracovníky

Operation

- **Funkce monitorování, řízení a automatizace**
  - Řízení a kontrola provozu (businessu) v logickém kontextu
  - Kontrola procesů
  - Snížení rizik
  - Efektivita sítě

E-mobility – součást SG

- **Systém autentizace vozidel, nebo řidičů**

Základní otázky

Jak chceme zajistit:

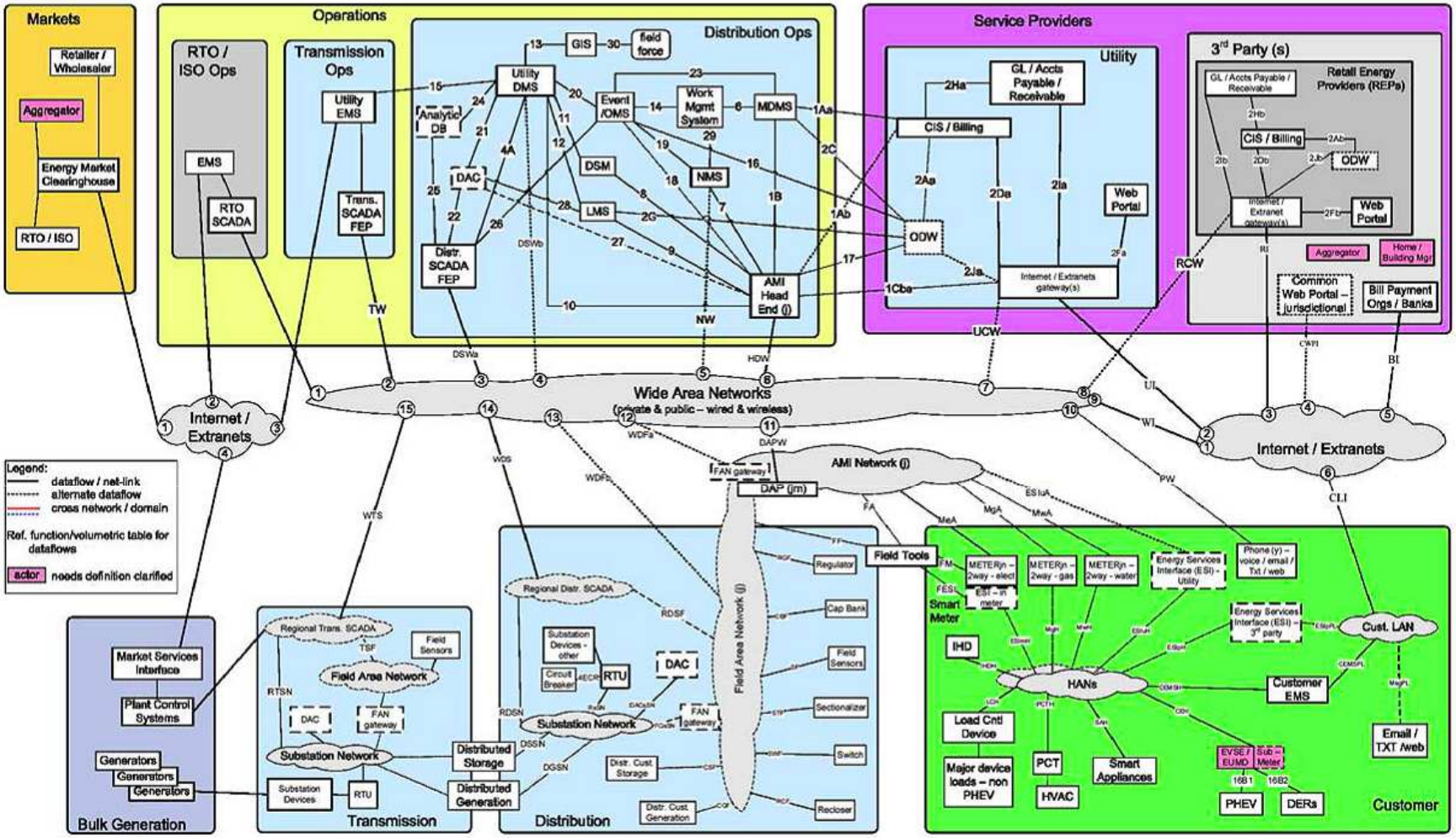
- **Upozornění na nestandardní, neobvyklé a nepředvídatelné chování v síti?**
- **Monitorování, ochranu a kontrolu komunikačních nástrojů a síťových aplikací?**
- **Sledování toho co se opravdu děje v síti právě teď?**
- **Hledání neznámých škodlivých aplikací, které se mohou v různé formě vyskytovat v síti?**
- **Odhalení a analýzu podezřelých událostí a možných hrozeb?**
- **Analýzu a odhalování podezřelého chování uživatelů?**
- **Prevenci úniku, nebo zničení citlivých informací?**

ANECT

Smart Grid Conceptual Actors / Data Flow Diagram – Cross Domain Network Focused – OpenSG / SG-Network TF

Illustrative

DRAFT 25Oct10
Base – file SG-NET-diagram-r0.6g.vsd
page size: ANSI-D



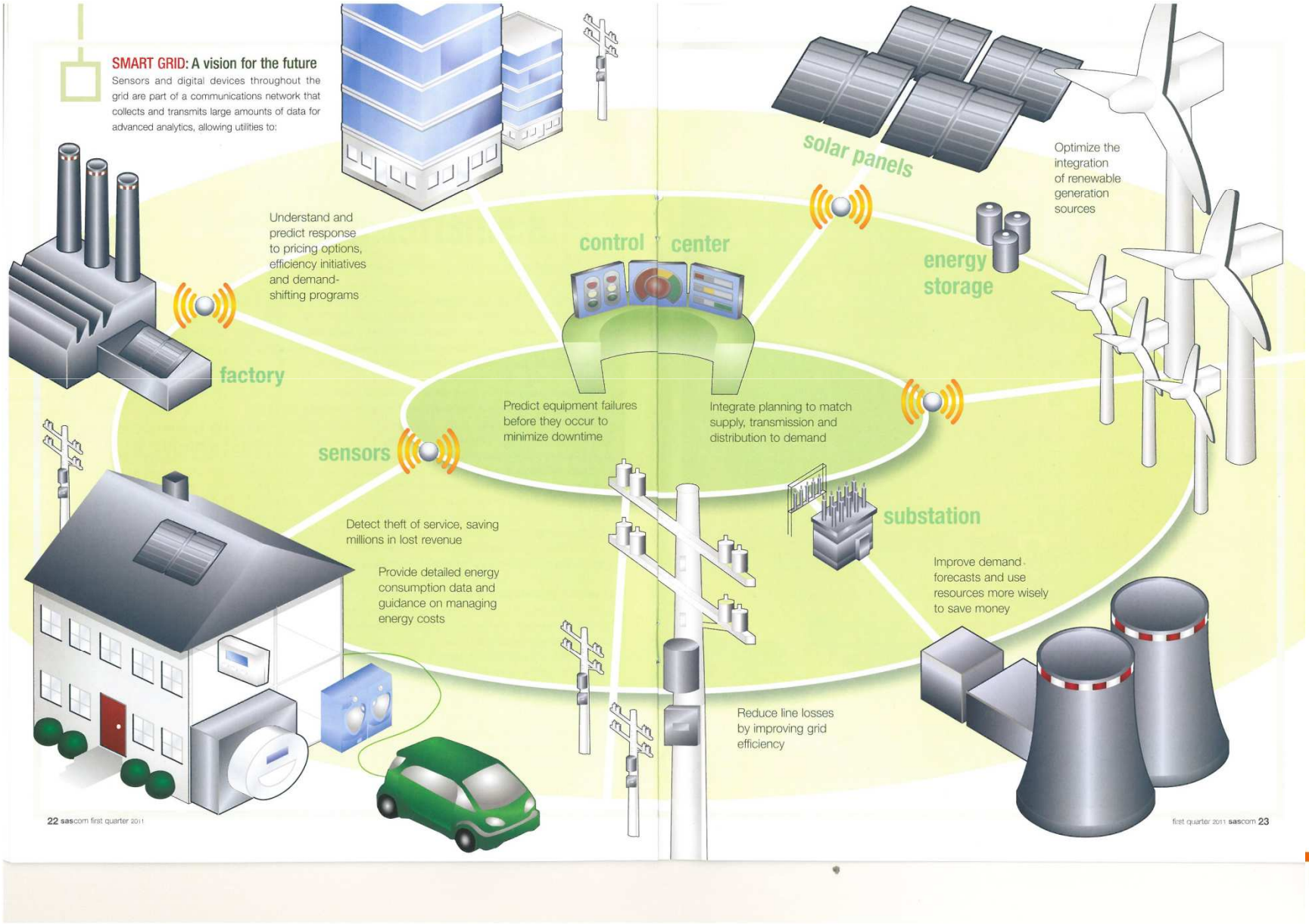
ANECT

Rozšířený koncept bezpečnosti

Komplexní, flexibilní kontrola a ochrana před hrozbami, zviditelnění, prevence a zamezení úniku dat – v reálném čase:

- **Aktivní průběžná kontrola**
- **Ochrana obsahu**
- **Omezení hrozeb**
- **Kontrola toku dat**
- **Monitorování a omezení podezřelého chování uživatelů**

Kdo je kdo – autentizace v komplexním prostředí



Systém autentizace ALUCID

Moderní systém autentizace a ochrany

- **ALUCID je patentovaná ochrana nového systému pro autentizaci a řízení identit**
- **Systém dokonale odstiňuje IT problematiku od uživatelského pohodlí**
- **Jednoduchost a intuitivnost použití (koncept plug & charge)**
- **Zabraňuje špehování**
- **Systém splňuje dosud nejvyšší známé prvky ochrany**
- **Systém je otevřený pro další rozvoj a flexibilní implementace dosud neznámých kryptografických metod, přičemž se změny nedotknou uživatele**

Klíčové vlastnosti

- **Jednoduchost**
- **Bezpečnost**
- **Otevřenost pro budoucí vývoj**

Systém autentizace ALUCID - použití

E-mobility

- **Umožňuje identifikovat jednotlivá vozidla (uživatele) při ochraně soukromí**
- **Zabraňuje špehování**
- **Umožňuje zcela bezpečnou identifikaci vozidla (řidiče) u nejrůznějších poskytovatelů (provozovatelů el. terminálů)**

Smart Grid

- **Ochrana sítě proti zneužití, zabránění neautorizovaným přístupům**
- **Bezpečná komunikace**

Klíčové vlastnosti ALUCID - souhrn

Jednoduchost

- IT problematiku (kryptování, nastavení PC, ..) řeší poskytovatel služby, ne uživatel
- Rolí uživatele je ochraňovat klíč (PEIG), na to je uživatel přirozeně zvyklý
- PEIG ALUCID je univerzální osobní klíč - “Single sign-on” by design

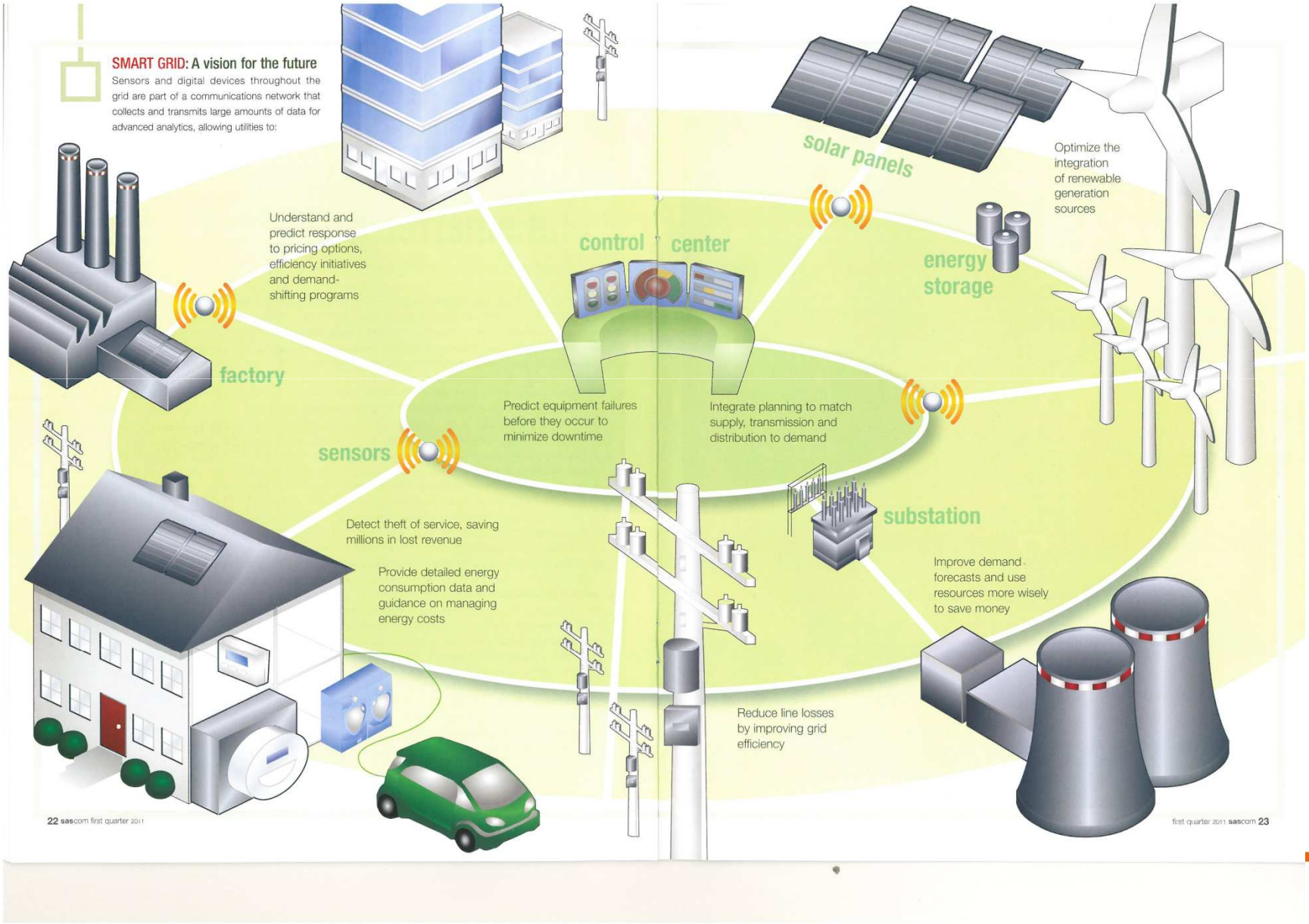
- **Bezpečnost**
- Žádné loginy a hesla = nemůžete je zapomenout, eliminace phishing atd.
- Eliminace vyzrazení osobních dat, hesel při zřizování identity
- Ochrana zneužití identity na síti (dnes certifikáty běhají po síti)
- Žádné instituce pro zřizování identity
- Identita v podobě BIO dat nechodí po síti, nelze ji kopírovat a zneužít

ALUCID® v evropském kontextu

- Patentová ochrana ALUCID ® - mezinárodní i národní patentová ochrana - částečně ze zdrojů ESF.
- Pilotní nasazení ALUCID ® je spolufinancováno z rámcového Programu Inovace.
- ANECT je členem mezinárodního konsorcia, jehož projekt PASSIVE, (Policy-Assessed system-level Security of Sensitive Information processing in Virtualised Environments) Cíl je uplatnění řešení ALUCID ® ve standardizačním procesu metod interoperability nástrojů elektronické identity v rámci evropského prostoru
- ANECT je platným členem evropské tematické sítě Universal eID podporované Evropskou komisí.

ANECT

Kontext v komplexním prostředí



Důležitý je kontext

Existuje řada dashboardů, které nabízejí pohledy na sítě, technologie, bezpečnostní a požární systémy, dohledové systémy apod.

- O tyto systémy se stará více dodavatelů (pod SLA) a přesto:
- Existují ztráty, výpadky, rizika provozu

Důvodem je chybějící KONTEXT

- Dejme data ze systémů do logických vazeb, které známe (nebo ještě neznáme)
- Vstupy do systému – z existujících dashboardů, systémů

abychom si odpověděli na otázky:

- Které situace jsou pro nás kritické?
- Jak je můžeme omezit v reálném čase?

ANECT

Systém ALTWORX – principy

Smart Metering – zachycuje, počítá a měří data

ALTWORX přebírá vstupy ze Smart Meteringu a dalších technologických zdrojů (zabezpečovací systémy, kamery, infrastuktury,..)

A kombinuje je s:

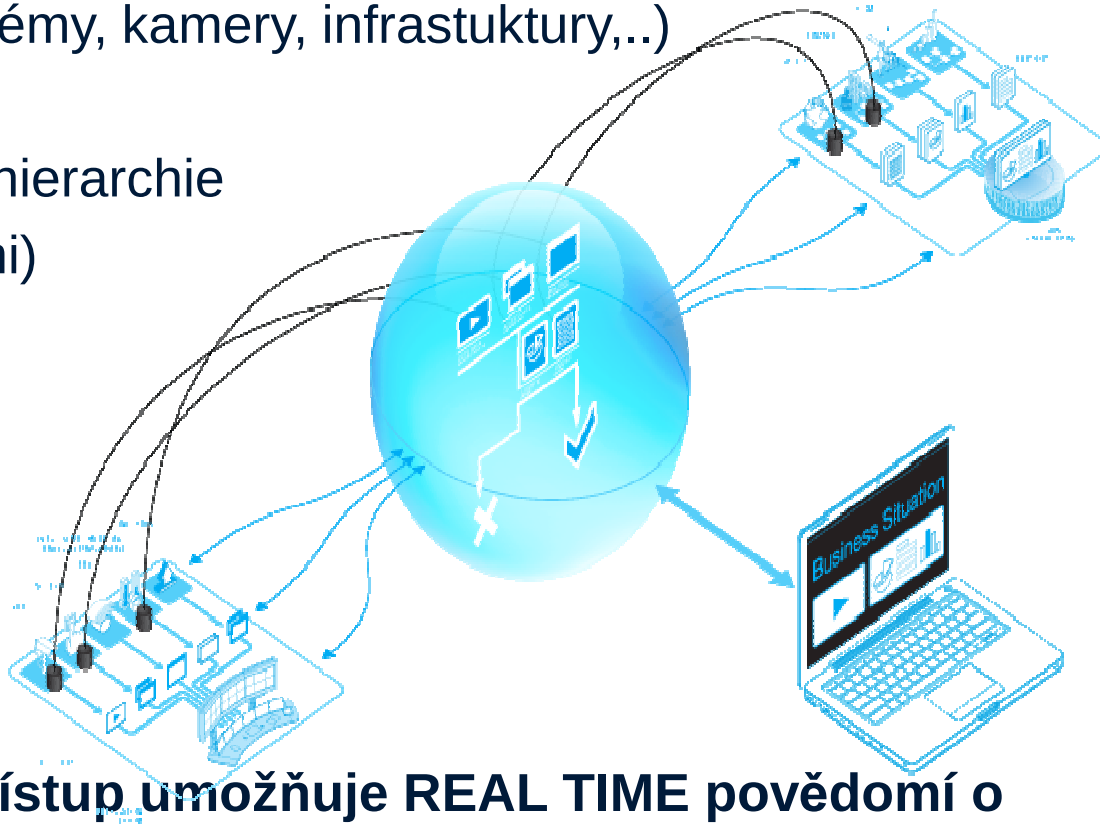
Logikou pro jednotlivé stupně hierarchie

Business požadavky (prioritami)

Předpisy a procesy

Bezpečnostními požadavky

Aspekty prostředí (teplota,….)



Nedestruktivní a kreativní přístup umožňuje REAL TIME povědomí o situaci v distribuční síti, kterou nelze vidět analýzou dat.

Systém ALTWORX – řešení

ALTWORX jednoduše využívá situační scénáře pro každou úroveň v hierarchii

- Např. v rozvodně hlídá nejen stav technologií a odběry, ale i vstupy, kamerový systém, teplotu, čas, ….
- Situační scénáře ukazují známé povolené a zakázané kombinace, například pracovní postupy, bezpečnostní předpisy apod.
- Tyto vstupy dává do kontextu a eskaluje je na vyšší úroveň.

A SOUČASNĚ

ALTWORX umožňuje pracovníkům najít příčinu poruchy, nebo neefektivity při analýze shora dolů.

Je Smart Grid bezpečný?

Ano, pokud se v něm uplatňují principy a prostředky komplexní ochrany a zabezpečení:

- **Aktivní průběžná kontrola**
- **Ochrana obsahu**
- **Omezení hrozeb**
- **Kontrola toku dat**
- **Monitorování a omezení podezřelého chování uživatelů**

Služby firmy ANECT

ANECT nabízí dvě unikátní technická řešení

- **Patent ALUCID – autentizace a bezpečné komunikace**
- **Ve spolupráci s firmou Salford systém ALTWORX – řešení pro kritické infrastruktury**

Řešení spolehlivosti, bezpečnosti a provozu kritické infrastruktury

a navíc služby a know how v oblastech

- **provozování a výstavby komunikační infrastruktury**
- **IP telefonie – řešení pro IP v6 (téma SG)**
- **služby dohledu bezpečnosti, komunikačních sítí a infrastruktury**
- **projektový management**

ANECT

Závěr

Děkuji Vám za pozornost.