DATOVÉ KONCENTRÁTORY VE SCADA - LOGICKÝ MODEL, FUNKCE, KYBERNETICKÁ BEZPEČNOST

Jindřich Zoubek, TECHSYS – HW a SW, a.s.

Příspěvek pojednává o logickém modelu datových koncentrátorů v oblasti sekundární techniky a SCADA.

Rozebrány jsou jednotlivé funkce datových koncentrátorů a význam tohoto nezávislého řešení sběru dat pro posílení robustnosti a bezpečnosti řídicího systému jako celku.

Speciální část je věnována zhodnocení významu koncentrátorů z pohledu kybernetické bezpečnosti. Rozebrány jsou otázky výhod nezávislé funkčnosti subsystému sběru dat a zabezpečení na úrovni telemetrických komunikací.

1. ÚVOD

Podnětem k sepsání tohoto článku byl fakt, že se ve společnosti TECHSYS – HW a SW, a.s., touto problematikou zabýváme již od zrodu společnosti. Různé varianty řešení datových koncentrátorů byly a jsou denním chlebem činnosti naší společnosti, troufáme si tvrdit, že naši lidé jsou odborníky na tuto problematiku. Kromě řešení z oblasti energetiky, využíváme naše zkušenosti i v dalších oborech, jako jsou průmysl, telekomunikace, doprava ale také např. vodohospodářství.

Článek rozebere témata týkající se datových koncentrátorů a to jak témata obvyklá a standardní, tak témata týkající se vývoje v této oblasti z poslední doby. Článek se bude především opírat o naše řešení SW Twister, které v řadě situací bereme jako standardní, případně o další známá řešení. Projdeme tedy postupně témata:

- Definice
- Architektura
- Funkce
- Kybernetická bezpečnost
- Příklady konkrétních řešení a jejich výhody
- Závěr
- Historická tečka

2. DEFINICE

Nejprve uveďme některé volně dohledatelné definice, které jsou k dispozici u různých výrobců.

Definice TECHSYS: *Datový koncentrátor slouží ke sběru dat z různě rozlehlých podřízených systémů, jejich archivaci a předávání do systémů nadřazených. Datový koncentrátor je typickou částí SCADA systémů, kde zajišťuje nejen sběr dat a vazbu do dalších systémů, ale i vrstvu zajišťující bezpečnostní oddělení citlivých částí.*

Definice dalších výrobců (ELVAC): *Pokud je v síti mnoho zařízení, může být efektivnější, nebo v některých případech i nutné, data zkoncentrovat v daných uzlech a poslat je společně do nadřazeného systému. Tímto způsobem je možné sbírat data z různých typů rozhraní a protokolů. Vše může být samozřejmě provedeno jako redundantní systém, který může s nadřazeným systémem komunikovat např. pomocí dvou nezávislých kanálů, nebo například lze komunikovat v rámci podřízených zařízení v kruhovém propojení. Modulární verze koncentrátorů mohou být navrženy přímo na míru konkrétní aplikace.*

Definice dalších výrobců (SUBNET): *A data concentrator is a software and hardware solution that connects a number of data channels with one destination. Data concentrators are found within substations to help manage many different data sources at one main source.*

Definice dalších výrobců (AEC): *Data Concentrator Unit (DCU) is the backbone infrastructure that helps in data acquisition, transfer of data to the central database.*

Definice toho, co je datový koncentrátor se drobně odlišuje obor od oboru, nicméně napříč obory se shoduje v tom, že se v zásadě jedná o entitu, která zajišťuje čtení a sběr dat z podřízených částí a transfer těchto dat do centrální databáze, která může být vlastní součástí koncentrátoru, jako takového.

V oblasti energetiky se také můžeme setkat s pojmem telemetrický koncentrátor.

3. TYPICKÁ ŘEŠENÍ

Jak vypadají typická řešení datového koncentrátoru napříč obory, si uveďme na následujících obrázcích se stručným komentářem.

3.1. SMART METERING A AMM

Datové koncentrátory jsou typické pro oblast Smart Meteringu, resp. AMM (Advanced Metering Management) a AMI (Advanced Metering Infrastructure), což je z pohledu dnešní doby velmi aktuální téma. Většina výrobců elektroměrů nějakým způsobem řeší i datový koncentrátor. Jeho úkolem je obvykle konsolidovat data z velkého množství podřízených elektroměrů a předat je nějakým standardním rozhraním do vyšší vrstvy zpracování, např. centrály odečtů. Speciálním případem koncentrátoru může být i samotný elektroměr, který následně zastupuje např. větší množství elektroměrů propojených dohromady (např. na sběrnici RS485).

obrázek 1 – koncentrátor AMM (zdroj: „Energetická maturita“ ČEZ)

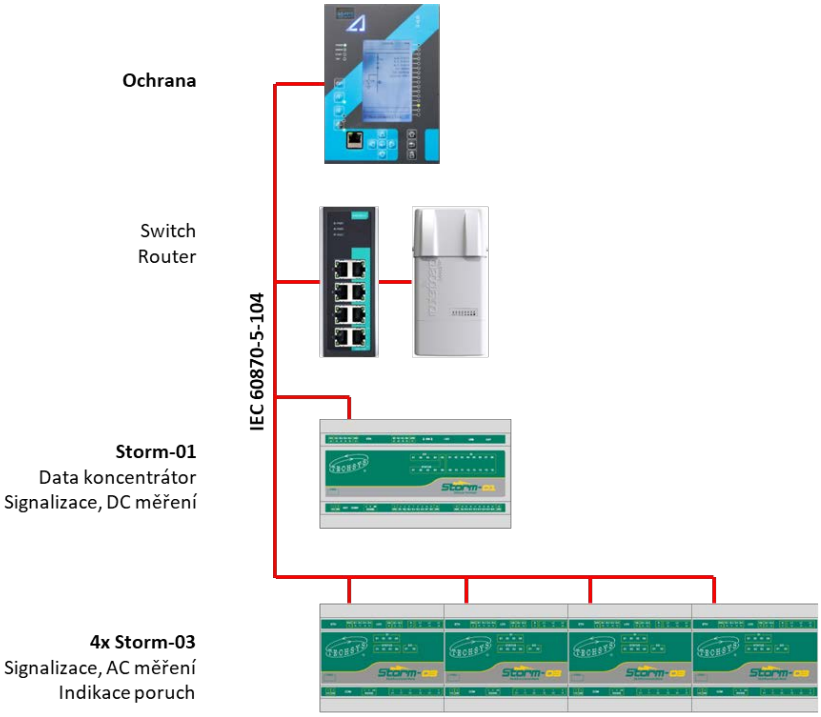
3.2. MĚŘENÍ A REGULACE, PRŮMYSL

Jinou oblastí, kde je hojně využíváno datových koncentrátorů, je oblast měření a regulace (MaR), případně obecně průmysl. Koncentrátor zde obvykle řeší sběr dat z průmyslových regulátorů, měřičů a přenos do monitorovacího systému

obrázek 2 – koncentrátor AlfaBox+ (zdroj: http://www.alfamik.cz)

3.3. ENERGETIKA

Nyní si ukažme řešení přímo z energetiky (míněno distribuce). Naším příkladem bude řešení distribuční trafostanice (DTS) lokální distribuční soustavy (LDS). Vlastní RTU Storm-01 zde řeší nejen funkci RTU, ale rovněž funkci datového koncentrátoru pro zbylé komponenty DTS, a zajišťuje hlavní vazbu mezi komponentami DTS a dispečerským systémem (a jeho datovým koncentrátorem).

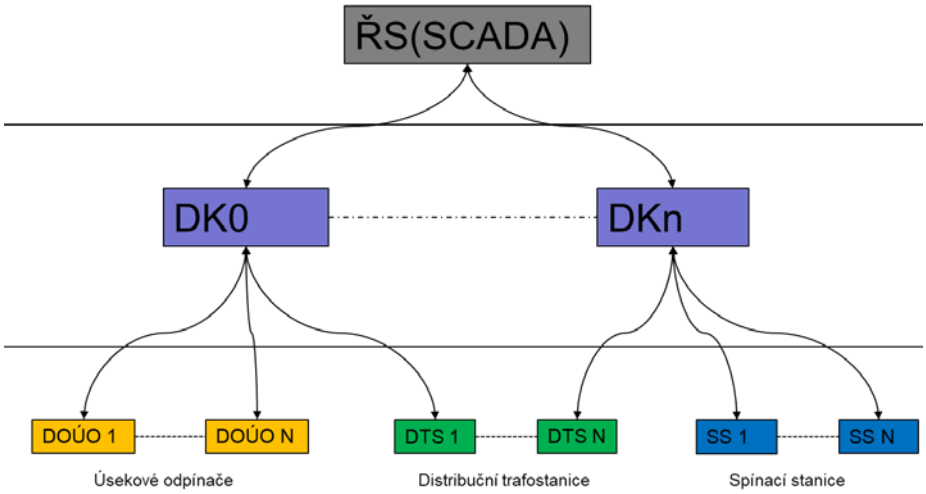


obrázek 3 – řešení DTS (zdroj: projektová dokumentace TECHSYS)

Výše jsme si ukázali některá řešení, kdy vlastní koncentrátor byl řešen hlavně pomocí specifického HW. Tento článek se dále chce zabývat především obecnějším SW řešením, které je v celé řadě případů možno integrovat i do téměř libovolného HW, resp. je na HW nezávislé.

4. LOGICKÝ MODEL V OBLASTI SEKUNDÁRNÍ TECHNIKY A SCADA

Obrázek č. 4 zachycuje umístění datových koncentrátorů (DK) ve struktuře hlavní části sekundární techniky distribuční energetické společnosti tak, jak jej obvykle řešíme.

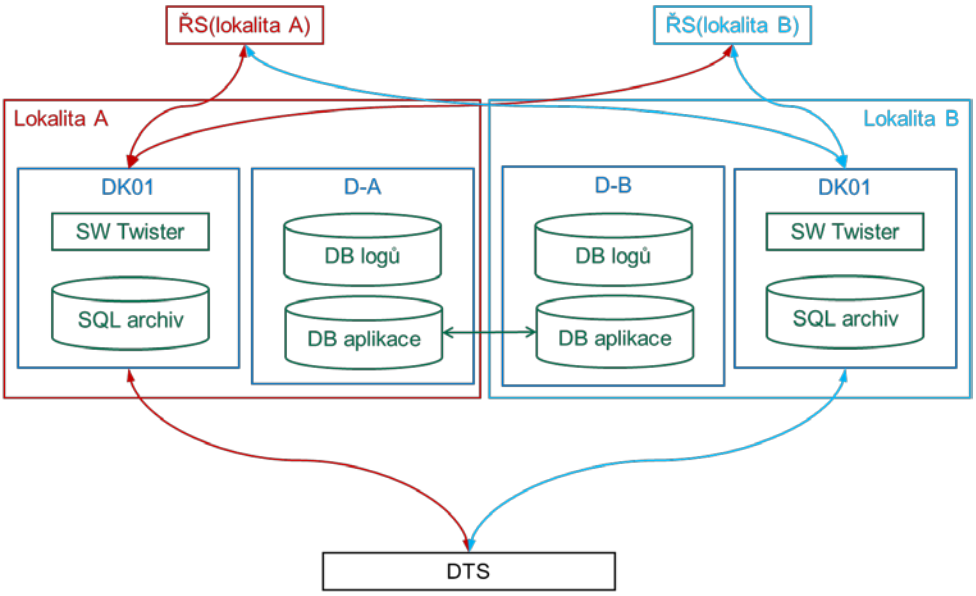


obrázek 4 – logický model DK ve SCADA (zdroj: TECHSYS)

Je zde vrstva řídicího systému (ŘS), vrstva datových koncentrátorů (DK) a vrstva technologií odkud se data sbírají (staniční ŘS, RTU, …). Nicméně je potřeba podotknout, že tento model (stromová struktura) s úspěchem funguje i v dalších oborech. V kořenech stromu se ovšem nejedná o elektrické stanice, nýbrž např. telekomunikační stojany v lokalitách ústředen nebo data-center telekomunikační společnosti pro oblast telekomunikací nebo o vodní díla vodohospodářské společnosti pro oblast vodohospodářství, případně o výrobní haly a jejich technologie v průmyslovém podniku.

Z obrázku je patrné, že datové koncentrátory mohou zajišťovat z pohledu celého systému:

- Logické ale i fyzické oddělení řídicího systému (ŘS) od podřízených technologií (podřízené ŘS, RTU, měřící převodníky, indikátory poruch, ochrany…).
- Sjednocení rozhraní sběru dat (různé komunikační protokoly, různí dodavatelé, historické důvody, …), často sám vrcholný ŘS nepodporuje veškerou škálu níže použitých komunikačních protokolů a rozhraní, což ani není jeho primární úkol.
- Koncentraci dat a komunikací do jednoho kanálu vůči ŘS. Tedy zastřešení obrovského množství zařízení jedním.
- Sjednocení z pohledu množství a kadence dat – „deltování“, filtrování a přenos pouze významných událostí může být klíčové. Zahlcený systém nebude dost dobře funkční.
- Typovou nebo množstevní diverzifikaci podřízených technologií (např. koncentrátor pouze pro DTS, atd.).
- Georedundanci – jednotlivé koncentrátory mohou být řešeny distribuovaně-zálohovaně do více lokalit. Zvyšuje se tím jak spolehlivost, tak dostupnost systému. Mimochodem, vlastní ŘS může být rovněž řešen jako distribuovaná entita (např. dělením mezi dvě lokality) – z pohledu datových koncentrátorů je jedinou změnou více spojení mezi koncentrátory a ŘS. Příklad takového dělení ŘS i koncentrátorů ukazuje následující obrázek č. 5.



obrázek 5 – georedundance ŘS i DK (zdroj: TECHSYS)

5. ARCHITEKTURA, VLASTNOSTI, FUNKCE

Jaké by měly být vlastnosti softwarového datového koncentrátoru, proč se jimi zabývat a proč jich využívat? Na tuto otázku odpovíme právě v této kapitole.

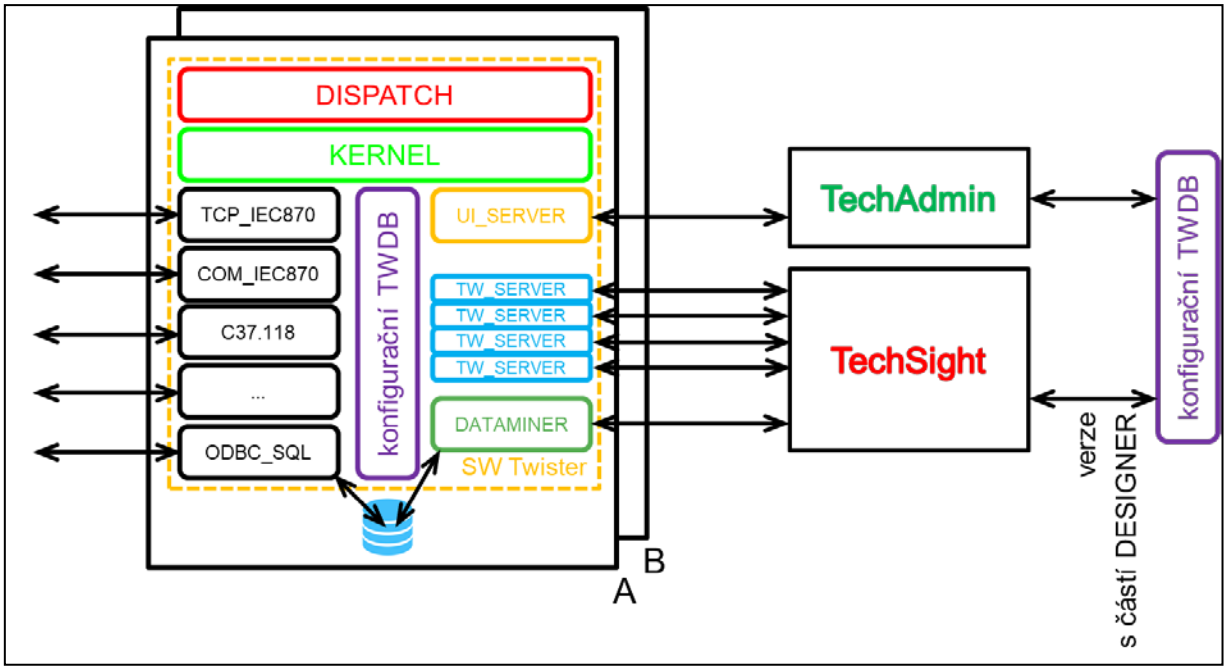
Dnešní doba je, z pohledu řešení SW nebo IT systémů, protknuta hesly jako „standardní“, „otevřený“, „přenositelný“, „bezpečný“, „univerzální“, „škálovatelný“, „modulární“, atd. Proto i naše řešení se snaží jít touto cestou a vyhovět tak potřebám doby z pohledu požadavků i možností techniky.

Podstatné je rozebrat vlastnosti (obecné vlastnosti SW) z několika dalších hledisek, jako jsou:

- struktura, resp. architektura řešení
- obecné IT vlastnosti (škálovatelnost, modularita, multiplatformnost resp. přenositelnost na jiné platformy, rozšiřitelnost, zálohování, …)
- operační systém, HW infrastruktura
- ergonomie (uživatelský komfort), obecné uživatelské vlastnosti
- analytické možnosti a nástroje
- komunikační možnosti
- bezpečnost

5.1. STRUKTURA A OBECNÉ IT VLASTNOSTI

Následující obrázek ukazuje strukturu našeho řešení SW Twister a dokresluje význam některých uvedených vlastností.



obrázek 6 – SW Twister – struktura (zdroj: TECHSYS)

Z modelu je vidět následující:

- SW se ubírá cestou standardizace – implementuje komunikační protokoly a rozhraní dle standardů a norem (např. IEC 60870-5, IEC 61850, OPC, atd.). Touto cestou podporuje rovněž otevřenost systému. Implementovaná proprietární rozhraní obsahuje pouze z důvodu zpětné kompatibility a historických souvislostí.
- SW je modulární – je to v podstatě balík SW modulů, což umožňuje jeho snadné rozšiřování a integraci dalších nových modulů.
- SW **může, ale nemusí** být zdvojen (proto část A a B) a může tak řešit zálohování způsobem MAIN-HotStandBy, pokud není využito dnes běžného zálohování na úrovni HW infrastruktury nebo OS.
- SW je škálovatelný – to je z obrázku vidět pouze částečně, každopádně pouhou změnou konfigurace systému je možno měnit velikost řešeného systému, vše ostatní záleží již jen na výkonu infrastruktury, na které systém běží.

Většina obecných IT vlastností již byla popsána výše textem nebo obrázkem, zmiňme tedy již jen to, co zbývá, a tím je **přenositelnost** na jiné platformy.

Na počátku vývoje je potřeba si říci, zda daný SW bude vyvíjen pouze pro jednu platformu (např. MS Windows, Linux, Unix, Solaris, …) nebo bude přenositelný mezi vybranými platformami. Na základě tohoto rozhodnutí se pak řídí další postup a metodika vývoje. Možností, jak následně vést celý vývoj, jaký zvolit programovací jazyk, atd., je celá řada.

5.2. OS PLATFORMA A HW INFRASTRUKTURA

Řešení TECHSYS se snaží jít cestou přenositelnosti mezi platformami. Na jedné straně to sice vyžaduje větší investici do času a financí vlastního vývoje, nicméně výhody jsou obrovské. Dokážeme náš SW provozovat napříč vybranou skupinou operačních systémů a tím pádem uspokojit i potřeby zákazníků, kteří nehodlají investovat své finance do draze licencovaných OS, případně SQL platforem tím, že využijeme cestu Open Source s OS Linux. Cesta Open Source má i tu výhodu, že jsou dostupné zdrojové kódy od vlastního OS, což se dá v řadě případů velmi výhodně využít např. při úpravách ovladačů pro specifické potřeby.

Je-li tedy SW navržen jako přenositelný, lze jej s výhodou, v nezměněné podobě s daným portfoliem funkcí a vlastností, provozovat napříč vybranou skupinou operačních systémů a HW platforem.

Jaké jsou typické OS pro provoz datového koncentrátoru:

- OS Microsoft Windows (různé verze) – komerční, pozor dnes řada jich již bez podpory od MS.

- OS Linux – obecně svobodný a otevřený operační systém (např. Debian, Ubuntu, atd.), nicméně jsou i komerční verze jako Red Hat Enterprise (jeho volně dostupná distribuce je CentOS).
- OS UNIX – např. Solaris, BSD – komerční, řada verzí a klonů – často i speciální HW (např. SPARC pro Solaris). Solaris je dnes na „vymření“ a BSD se uplatňuje především v jiných oblastech.

Díky tomu, že naše řešení datového koncentrátoru je především SW balík pro danou skupinu operačních systémů, je mu v podstatě jedno, na jaké infrastruktuře je provozován.

Na dalším obrázku si ukažme, jaký může být typický HW pro provoz datového koncentrátoru.

obrázek 7 – příklady HW infrastruktury (zdroj: TECHSYS a WEB)

Prvním příkladem je odolný průmyslový počítač, určený pro umístění např. do rozvaděče. Jeho výhodou je, že nemá žádné pohyblivé části, má odpovídající průmyslové parametry z pohledu teplotních rozsahů a EMC a je poměrně výkonný. Je typickým příkladem možného řešení datového koncentrátoru pro distribuční trafostanici nebo menší monitorovací/řídící systém. Výhodou je rovněž nižší pořizovací cena.

Druhý „kusem“ HW je klasický server určený pro montáž do stojanu. Je využíván v případě, že je dostupné datové centrum nebo serverovna, a očekává se vysoký výpočetní nebo archivační výkon.

Posledním příkladem je v podstatě SW platforma – jedná se o virtualizaci. Ta může být provozována na předešlém „kusu“ HW, případně v datovém centru nebo dnes moderně na CLOUD. Virtualizace má obrovskou výhodu v tom, že se dá snadno škálovat i vlastní infrastruktura, tedy v případě, že již nestačí přidělený výkon, diskový prostor, paměť nebo další systémové prostředky, lze je poměrně jednoduše navýšit.

5.3. OBECNÉ UŽIVATELSKÉ VLASTNOSTI

Jak jsme si řekli výše, z našeho pohledu je datový koncentrátor SW balík, se kterým mají uživatelé pracovat, a který je nainstalován na vybrané platformě OS a HW infrastruktuře.

Aby se uživatel k tomuto SW dostal např. z důvodů parametrizace, nastavení, obsluhy, diagnostiky atd., potřebuje nějaký nástroj. Může se jednat o tlustý nebo tenký klient. V případě SW Twister se jedná o program TechAdmin (viz obrázek 6), který slouží přesně k těmto účelům.

Daný program může mít i svou konzolovou verzi, což umožňuje s výhodou využívání při dávkovém zpracování datových podkladů a hromadné parametrizaci.

Z pohledu určitých částí obsahuje tzv. „managementy“, které zajišťují požadované uživatelské funkce:

1) Accounting Management
    a. Možnost logování aktivit jednotlivých uživatelů, volba úrovně logování.
    b. Možnost logování do nezávislého systému pro centrální správu LOGů
    c. Možnost auditingu jednotlivých uživatelů z hlediska využitého systémového času a zátěže Systému
    d. Možnost jednoduchého prohlížení a vyhodnocení logů i auditních logů
2) Security Management

a. Autorizace přístupu uživatelů do systému i na dohlížené prvky
b. Přidělování vícestupňových uživatelských rolí a oprávnění
c. Jednoduché prohlížení a vyhodnocení bezpečnostních logů
d. Možnost konfigurovat pravidla pro tvorbu a vypršení hesla
e. Možnost začlenit SW Twister pod centrální správu hesel a oprávnění (Active Directory, LDAP)

3) Configuration Management
   a. Manuální i automatizovaná změna konfigurace
   b. COMMIT nebo RESTART pro výměnu konfigurace
   c. Importy/Exporty dat a datových pokladů
   d. Výměna nových verzí SW modulů
4) Fault Management
   a. Každý SW modul generuje vlastní LOG, který lze využít pro diagnostiku
   b. Alarmy, historie alarmů, logy, servisní okna
5) Performance Management
   a. Každý SW modul poskytuje data z pohledu rezervovaných zdrojů OS
   b. Delta kritéria, agregace dat, změna hloubky archivace dat

5.4. ANALYTICKÉ MOŽNOSTI A NÁSTROJE

5.4.1. Analýza komunikačních protokolů a rozhraní

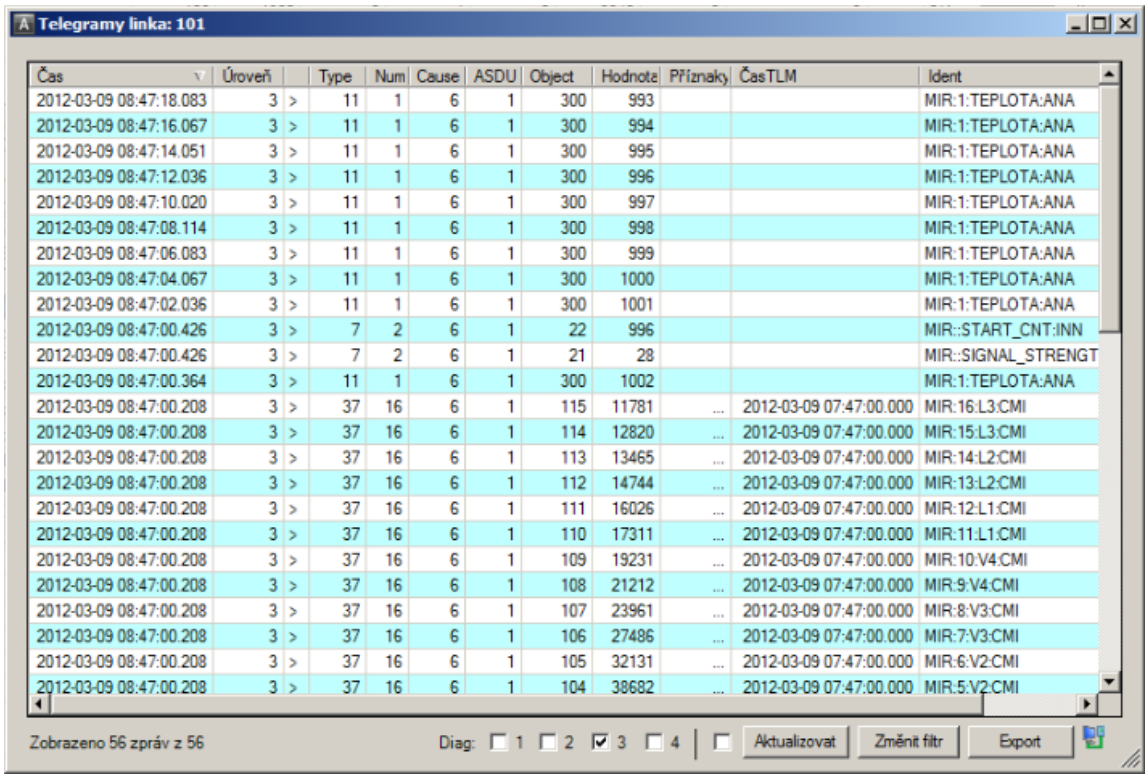
Základní funkcí je přehled (tabulka) komunikačních kanálů a rozhraní, kde jsou v přehledu vidět základní informace, jako stav komunikačního kanálu a počet změn.

Silnou stránkou řešení je možnost online analýzy komunikačních protokolů a rozhraní. Ta je, pro každý dílčí komunikační kanál, řešena na několika úrovních/vrstvách:

- Binární výpis probíhající komunikace
- Formátovaný výpis telegramů probíhající komunikace
- Výpis datových bodů probíhající komunikace dekódováním telegramů
- Výpis aktuálních hodnot datových bodů z datového obsahu daného komunikačního kanálu.

Především formátovaný výpis telegramů je velmi zajímavý, jelikož umožňuje uživateli vidět jednotlivá dekódovaná pole dle daného standardu, např. pro IEC60870-5-104 jsou to pole: Type, počet objektů, Cause ASDU, Objekt (InfNr) a dále dekódovaná hodnota, časová značka a příznaky (příklad je na obrázku 8). To má obrovskou výhodu při hledání chyb komunikace nebo nastavení, jelikož uživatel vidí přímo hand-shake komunikace, její obsah a odezvy.

Probíhající komunikaci je samozřejmě možno nahrávat a exportovat pro následnou analýzu. Jiným příkladem může být rozhraní pro SQL komunikaci, které umožňuje sledovat přímo probíhající SQL dotazy a pozorovat případnou chybu např. při správném formátování daného SQL dotazu.



obrázek 8 – výpis telegramů IEC60870-5-104

5.4.2. Log událostí SW modulů a jejich diagnostika

Základní funkcí je přehled (tabulka) komunikačních kanálů a rozhraní, kde jsou v přehledu vidět základní informace, jako stav kanálu a počet změn.

Další z analytických možností je logování událostí a zajímavých stavů každého dílčího SW modulu. Např. u SW Twister se jedná o několik úrovní a to:

- DEBUG – ladící hlášky pro vývojáře, autory modulů
- WARNING – varovní hlášky
- ERROR – chybové hlášky
- INFO – informativní hlášky, podstatné události

Úrovně hlášek umožňují uživateli soustředit se pouze na to podstatné, co jej zajímá. Běžného uživatele určitě pro jeho obvyklou práci nebude zajímat DEBUG úroveň, ale přesto je schopen předat dodavateli systému případný vyexportovaný záznam pro analýzu. Uživatel naopak určitě využije úroveň INFO, kde je možno sledovat např. náběhy a výpadky komunikačních kanálů, úspěšný/neúspěšný COMMIT, případně změnu parametrů atd.

Veškeré události mohou být dále poskytnuty k centrálnímu zpracování LOGů, např. v SIEM (Security Information and Event Management) předávané pomocí protokolů SYSLOG.

Kromě LOGu je k dispozici i přehledová tabulka jednotlivých SW modulů, jejich stav a údaje z pohledu zdrojů OS (zátěž CPU, spotřeba paměti, atd.).

5.4.3. Log událostí datového koncentrátoru

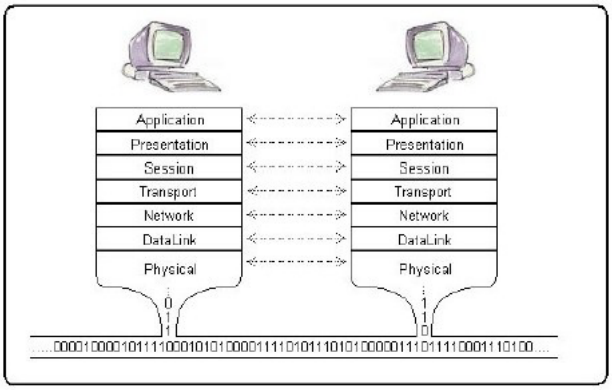
Centrální LOG událostí zachycuje především administrativní události. Těmi mohou být např. přihlášení uživatele, změna nastavení koncentrátoru, výměna dílčího SW modulu za novou verzi, atd. I zde je možno využít centrálního logování do SIEM.

5.5. KOMUNIKAČNÍ MOŽNOSTI

Jednou z velkých výhod řešení datového koncentrátoru by mělo být především široké portfolio komunikačních protokolů a rozhraní. Např. pro koncentrátor SW Twister, který je navržen modulárně, jak již bylo patrno z předešlých schémat, znamená následné doplňování nových komunikačních protokolů pouze vývoj dílčího protokolu a celá bohatá funkčnost zbytku SW balíku je stále k dispozici a lze ji využívat tak, jak je uživatel zvyklý.

Nyní vyjmenujme komunikační protokoly a rozhraní, se kterými se můžeme v oblasti energetiky (a nejen jí) setkat:

- Jednoduché: Modbus RTU, Modbus TCP
- Standardní: IEC 60870-5-101, 104, DNP3.0, IEEE C37.118, SNMP, OPC, SOAP
- Objektové: IEC 61850-8-1, IEC 60870-6 TASE2, IEC 62056 DLMS/COSEM
- Starší: RP570, TG809, SSI, COMLI
- Bezpečnostní nadstavba dle IEC 62351
  - Nadstavba pro rodiny IEC 60870 (101, 104), MODBUS, atd.
  - TLS (šifrování + certifikáty)
  - Autorizace povelování



obrázek 9 – ISO/OSI model

5.6. ARCHIVACE DAT

Další, již méně typickou funkcí datového koncentrátoru, může být požadavek na archivaci dat. Důvodů k archivaci dat může být několik:

- Uložiště pro návaznou vizualizační část pro zobrazení historie dat v grafu nebo tabulce.
- Poskytování dat pro jiné systémy, případně předávání dat do těchto systémů.
- Určitá záloha dat s odpovídající hloubkou.

Vlastní archiv je pak typicky řešen nějakou SQL platformou, např. MS SQL, ORACLE, PostgreSQL, atd. Stejně jako pro OS lze využít Open Source řešení a ušetřit tak náklady za licenční poplatky.

Struktura archivu může být naprosto jednoduchá, řešená jednou tabulkou, ale obvyklejší řešení je strukturovaný archiv, kde jsou data rozdělena po určitém období, a vazba na identifikátory daných veličin je oddělena v samostatné části.

5.7. DALŠÍ FUNKCE – APLIKAČNÍ

Kromě základních funkcí a vlastností, které jsme uvedly výše, mohou mít datové koncentrátory ještě další funkce, již aplikační. Uveďme si je stručně dále:

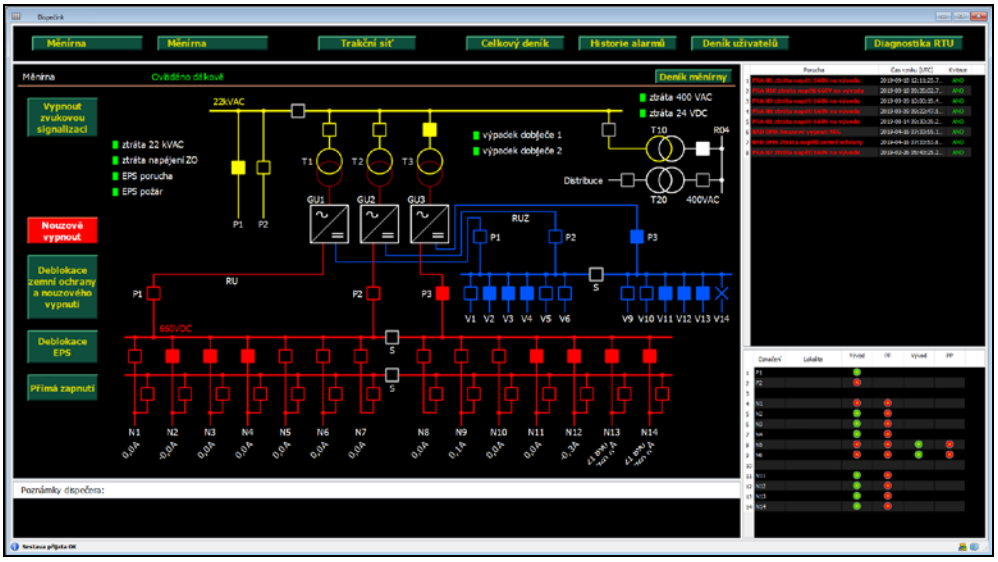
1) Poskytování dat do dalších systémů – typickým konzumentem dat je ŘS (SCADA), ale takovýchto systémů dat může být více a dokonce jiného typu:

a. Monitorovací systém určité technologie nebo infrastruktury
b. SAP
c. Systém evidence a inventarizace zařízení
d. Business inteligence systém

2) Zpracování dat – rozdělme na dvě části:
   a. Běžná funkce koncentrátoru při zpracování dat
      i. Konverze dat – příklady:
         1. přepočet na fyzikální hodnoty,
         2. lineární konverze,
         3. BCD konverze,
         4. konverze signalizací – invertování.
      ii. Deltování – slouží k „naředění“ dat tekoucích dále, aby nedošlo k zahlcení nadřazeného systému nebo zbytečnému přísunu nepotřebných dat. Deltování může být různého typu:
         1. Prostá změna dat.
         2. Integrální nebo obyčejné delta kritérium.
         3. Časové delta.
         4. Atd.
      iii. Filtrace dat – procházejí pouze data vyhovující určitým kritérium.
   b. Speciální výpočty – SW moduly datového koncentrátoru mohou zajišťovat vybrané specializované funkce:
      i. Bilancování energií – energetický management
      ii. PLC funkce
      iii. Stárnutí technologie dle standardu IEC
      iv. Zatěžování vedení
      v. Atd.

3) SCADA funkce
   a. Kombinací s vizualizačním klientem může vzniknout SCADA systém se základními funkcemi, případně i funkcemi vyššími, jsou-li k dispozici.
   b. Řešení SW Twister v kombinaci s klientem TechSight toto poskytuje. Datový koncentrátor je v tomto případě „srdcem“ SCADA systému, jelikož zajišťuje komunikaci s řízenými a monitorovanými technologiemi a zároveň zajišťuje data a interpretaci povelů pro vrstvu vizualizační. Struktura viz. obrázek 6 a příklad SCADA dopravního podniku na obrázku 10 níže.

4) Inventory a profilaxe
   a. Datový koncentrátor doplněný o archivaci dat je možno využít rovněž jako systém pro evidenci zařízení (inventář) a profylaxi.
   b. Online evidence technologických IT zařízení:
      i. RTU, vývodové terminály s ochranou, měřící převodníky, …
      ii. verze SW, HW a firmware – aktuálnost verzí
      iii. sledování sériových čísel HW, identifikační údaje
   c. Možnost online profylaxe
   d. Diagnostika poruchovosti linek – tlak na dodavatele (např. operátoři GSM/GPRS) ohledně kvality a dodržování pohotovosti
   e. Typická rozhraní pro sběr takovýchto dat jsou: SNMP, IEC 61850, ICMP, TCP



obrázek 10 – příklad SCADA dopravního podniku

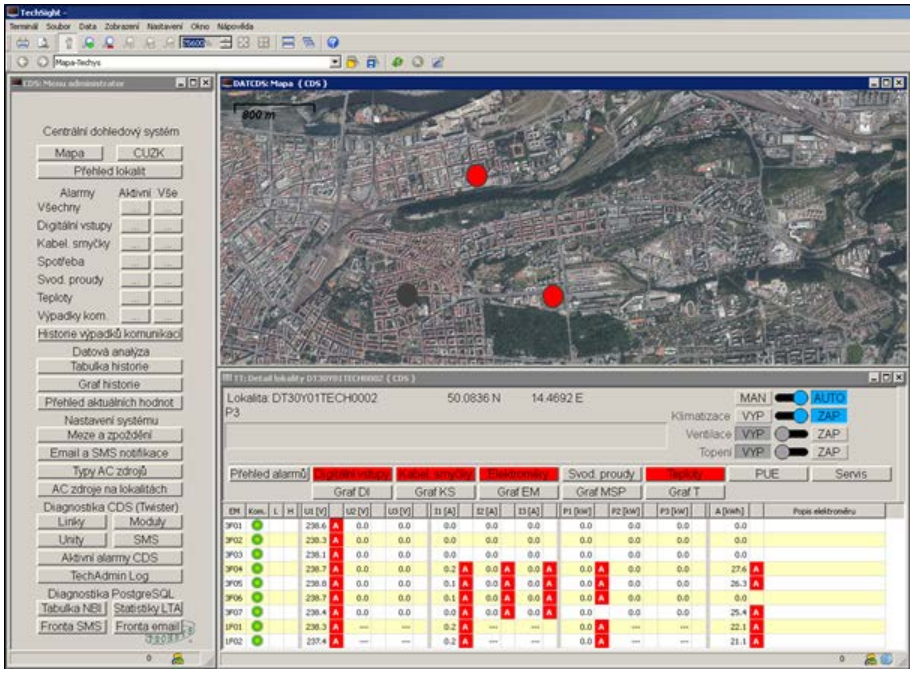
5) Monitoring – monitorovací systémy, resp. odbočení dat do dalších systémů

   a. Datový koncentrátor, jako „srdce“ systému, lze s výhodou použít i pro různá odbočení dat pro ne-SCADA využití, především pro účely monitorovacích systémů.

   b. Z pohledu bezpečnosti, se jedná o prvek, který zajišťuje možnost odbočení dat mimo privilegovanou zónu z pohledu kritické infrastruktury. Bezpečné tak zpřístupní důležitá provozní data pro údržbu a servis i neprivilegovaným uživatelům.

   c. Příkladem takového monitorovacího systému může být centrální dohledový systém pro **monitoring distribuované infrastruktury** a to, jak v energetice, např. různé tzv. dohledové agendy technologií jako jsou DTS, ale např. také v telekomunikacích pro dohled technologií telekomunikačních ústředen nebo datových center.

   d. Při velkém množství sledovaných prvků, se velmi často pro vizualizaci využívá **spolupráce s mapovými servery**, kdy má uživatel k dispozici nejen vlastní monitorovaná data ale rovněž koordináty, či půdorysy a schémata technologie a může, v případně potřeby přímo z centrálního dispečinku, vést zásah servisního týmu.



obrázek 11 – centrální dohledový systém s mapovými podklady

6. KYBERNETICKÁ BEZPEČNOST

Kybernetická bezpečnost je určitě téma, které je v dnešní době aktuální pro systémy, jako jsou datové koncentrátory. Málokdo chce, aby byla získávaná data zpochybňována, měněna nebo zneužívána pro jiné účely než je zamýšleno.

V případě zájmu čtenáře o širší popis principů týkajících se požadavků na produkty z pohledu bezpečnosti, je možno se odkázat na článek „IMPLEMENTACE ZÁSAD KYBERNETICKÉ BEZ-PEČNOSTI DO FUNGOVÁNÍ FIRMY DODÁVAJÍCÍ SW A HW“ z konference CIRED2018. Zde proveďme pouze výtah nejpodstatnějšího.

6.1. POŽADAVKY NA PRODUKTY

Obecné požadavky na SW produkty vycházejí z obecných standardů kybernetické bezpečnosti, metodiky bezpečného vývoje a specifických bezpečnostních požadavků daného produktu, aplikace a koncového zákazníka.

Uveďme ty nejpodstatnější požadavky kladené na produkty:

1. Vývoj a testování dle přijatých standardů.
    a) Dodržování metodiky bezpečného vývoje.
    b) Prokazatelné otestování na nezávislém testovacím prostředí.
2. Logování činnosti administrátorů a uživatelů.
    a) Auditní LOG.
    b) Spolupráce se SIEM (Security Information and Event Management, tj. management bezpečnostních informací a událostí). SIEM v reálném čase umožňuje analýzu bezpečnostních alertů, které generují síťová zařízení a aplikace. SIEM řešení zpravidla je postaveno na bázi aplikace, služeb a potřebného zařízení – tento základ konzumuje záznamy bezpečnostních dat (logy) a generuje reporty.
3. Správa uživatelů navázána na AD/LDAP (Active Directory/ Lightweight Directory Access Protocol)
    a) Přidělování uživatelských rolí a oprávnění.
    b) Single Sign On (SSO). SSO centralizuje autentizační proces uživatele do jednoho místa nazývaného také poskytovatel identity. Poskytovatel identity dělá autentizaci uživatele a tyto údaje pak poskytuje ostatním aplikacím (nazývaným též poskytovatelé služeb), které uživatel běžně používá.
4. Konkrétní technické požadavky na provoz
    a) Zabezpečení síťových komunikací.
    b) Ochrana proti vnějším útokům.
    c) Šifrování.
    d) Zabezpečení telemetrických komunikací (IEC 62351).

6.2. VÝVOJ A PROVOZ

Z pohledu vývoje a vlastní následného provozu aplikace je důležité také jasné oddělení vývoje, testu a provozu, konkrétně tedy:

- Vývojové, integrační, testovací a provozní prostředí musí být zcela oddělena v sítích a musí být podporována oddělenými stroji.
- Provozní servery nesmí obsahovat překladače a systémové utility, které nejsou nezbytné pro jejich správu nebo provoz.
- Testování a vývoj nových verzí Produktů se nesmí provádět v provozním prostředí.

Implementace zásad bezpečnosti do procesu vývoj stanovuje rovněž rizika podle jejich stupně (Nízké, Střední, Vysoké). Stupeň rizika se stanovuje dle požadavků zákazníka. Stupeň vysoké se uplatňuje především u těch prvků, jež jsou vystaveny přímo na veřejném internetu.

6.3. BEZPEČNOST KOMUNIKACÍ

Ze strany komunikací, protokolů a komunikačních rozhraní má pohled na bezpečnost několik úrovní a skupin, jež požadavky kladou. Mohou to být jak skupiny přímo z oblasti telemetrií nebo řídicích systémů, ale obvykle to jsou hlavně skupiny z oblasti čistého IT, kteří mají na starosti vlastní síťovou i serverovou infrastrukturu.

V dnešní době jsou pro telemetrické komunikace obvyklá zabezpečení na úrovní šifrování, autorizace, autentizace, certifikátů a dalších hesel. Např. standard IEC 62351 popisuje rozšíření obvyklých komunikací jako IEC 60870-5, IEC 60870-6 nebo IEC 61850 o bezpečnostní nadstavbu (šifrování, certifikáty, atd.).

Jinou možností je zabezpečení na úrovni infrastruktury, tedy odděleně, nebo chcete-li transparentně od telemetrií. Pak je možno využít standardních zabezpečení formou IPSec, VPN, VLAN, nebo různých firewallů atd. Tato forma je bližší čistému IT řešení a obvykle s vlastními telemetriemi nemusí mít vůbec nic společného.

7. PŘÍKLADY KONKRÉTNÍCH ŘEŠENÍ A VÝZNAM

Nyní uveďme několik konkrétních příkladů řešení se SW Twister, kde se datových koncentrátorů a jejich funkcí hojně využívá.

1. Centrální datové koncentrátory pro SCADA distribuční společnosti
2. Monitorovací systém technologií energetické společnosti
3. SCADA systém dopravního podniku
4. Centrální dohledový systém telekomunikační společnosti
5. SCADA systém vodohospodářské společnosti
6. Datové koncentrátory DTS

8. ZÁVĚR

Datové koncentrátory mají řadu podob souvisejících s oblastí použití, jak bylo naznačeno na úvod článku. Podstatou tohoto článku ale bylo ukázat, jak se řeší nebo může řešit daná problematika čistě pomocí SW, jaká témata s tím souvisí a jaké funkční výhody z něj plynou. Pokusili jsme se upozornit na některé významné body metodiky při návrhu architektury a na požadavky ze strany bezpečnosti.

9. LITERATURA

[1] Projektová dokumentace TECHSYS.

[2] Uživatelská dokumentace TECHSYS.

[3] „Energetická maturita“ ČEZ.

[4] http://www.alfamik.cz

Ing. Jindřich Zoubek, MBA

V r. 2005 ukončil studium na ČVUT, elektrotechnické fakultě v Praze, obor Výpočetní technika, se zaměřením na systémové programování, operační systémy a sítě.

Od r. 2001 pracuje ve společnosti **TECHSYS – HW a SW, a.s.**, www.techsys.cz, kde prošel různými pozicemi v oddělení vývoje. Rovněž vedl nebo byl členem realizace těch nejvýznamnějších projektů.

Od r. 2015 je členem managementu, vrcholného vedení společnosti a představenstva, se zodpovědností za obchodní a marketingovou činnost.

Kontakt: Tel.: +420 222 541 896, e-mail: zoubek@techsys.cz

