BEZPEČNOST ŘÍDICÍCH SYSTÉMŮ VE VODÁRENSTVÍ

Milan Lindovský [1], Jiří Kašparec [2], Šárka Kročová [3]

ABSTRAKT
Přednáška se zabývá problematikou bezpečnosti řízení vodárenských systémů, kde existují rizika omezující plynulost zásobování obyvatelstva vodou. Vzhledem k tomu, že riziku přerušení dodávek pitné vody nelze zabránit (např. nové nebezpečí je tzv. hacker attack) je nutné vytvářet legislativní, organizační a technické podmínky pro minimalizaci těchto nebezpečí. Cílem těchto opatření by měl být systému řízení výroby a distribuce vody, který dokáže vzniklá nebezpečí a mimořádné situace bránící v plynulém zásobování vodou, předcházet a řešit.
Autoři popisují aspekty, jak předcházet nebo eliminovat nebezpečí omezení dodávek pitné vody obyvatelstvu a tím zvýšit bezpečnost provozování vodárenských systémů.

Klíčová slova: vodovod, kybernetická bezpečnost, průmyslové řídící systémy, bezpečnost provozu,

ABSTRACT
The article deals with the issues of safety management of water supply systems, where there are risks of limiting continuity supplying the population with water. Given that the risk of interruption of drinking water cannot be avoided (e.g. a new danger is called Hacker attack), it is necessary to create legislative, organizational and technical conditions to minimize these dangers. The aim of these measures should be the management system of production and distribution of water, which can create the risk of emergencies and prevent the continuous water supply, prevent and solve. The authors describe aspects of lectures on how to prevent or eliminate the danger of limiting the supply of drinking water to the population and increase the security of the operation of water supply systems.

Key words: Water supply, cyber security, industrial control systems, operation safety,

1.Milan Lindovský,Ing, PhD, MBA, Jiří Kašparec,Ing, VAE CONTROLS Group, a.s., náměstí Jurie Gagarina 233/1, 710 00 Ostrava, Česká republika; tel:+420 602 735335, email: milan.lindovsky@vaecontrols.cz
3.Šárka Kročová, doc, Ing, PhD, Fakulta bezpečnostního inženýrství, Technická univerzita Ostrava, Lumírova 13, 700 300 Ostrava, Česká republika; tel:+420 596992892, email:sarka.krocova@vsb.cz

ÚVODEM

Nedílnou součástí infrastruktury každého státu je problematika zásobování vodou obyvatelstva. Vodovody pro veřejnou potřebu v Evropské unii dodávají pitnou vodu pro 72 až 100 % obyvatel států Unie (celkem žije v Evropské unii 507,4 milionů obyvatel). V České republice, počet obyvatel je 10,5 milionů, téměř 93% obyvatel závislých na veřejných vodovodech, je nutno ročně vyrobit přes 600 mil. m^3 pitné vody. Tuto oblast zajišťuje v ČR téměř 2600 provozovatelů, z čehož je ale strategických cca. 50 provozovatelů, kteří zajišťují přes 75% vyrobené pitné vody[1]. Existuje celá řada hrozeb od přírodních vlivů (sucha, povodně, sesuvy půdy, apod.) po lidské vlivy (nedbalost, havárie, terorismus, počítačové hackerství), která mohou ovlivnit bezpečnost provozování vodovodních sítí. Vodohospodářská infrastruktura je proto součástí tzv. kritické infrastruktury státu.

Přednáška se zaměřuje na bezpečností rizika související s řídicími systémy vodárenských sítí, a to zejména s ohledem na legislativní normy v oblasti provozování vodovodů, krizového řízení a kybernetické bezpečnosti.

I když příspěvek vychází z české legislativy, jsou, vzhledem k harmonizaci evropských právních norem, jeho poznatky, návrhy a závěry analogicky použitelné ve všech státech Evropské unie a v obecné rovině platí pro všechny vodárenské systémy.

1 KYBERNETICKÁ BEZPEČNOST VODÁRENSKÝCH SÍTÍ

Kritická infrastruktura státu je podle usnesení Výboru pro civilní nouzové plánování (VCNP) České republiky (ČR) definována jako „výrobní a nevýrobní systémy a služby, jejichž nefunkčnost by měla závažný dopad na bezpečnost státu, ekonomiku, veřejnou správu a zabezpečení základních životních potřeb“. Oblastmi kritické infrastruktury ČR jsou energetika, vodní hospodářství, potravinářství a zemědělství, zdravotní péče, doprava, komunikační a informační systémy, bankovní a finanční sektor, nouzové služby a veřejná správa. Kritická infrastruktura ČR je provázána s Evropskou kritickou infrastrukturou, která je definována v tzv. Zelené knize o Evropském programu na ochranu kritické infrastruktury (2005).

Hlavní význam kritické infrastruktury je v zajištění bezpečnosti státu, fungování ekonomiky, výrobních a nevýrobních systémů a služeb, fungování veřejné správy a zabezpečení základních životních potřeb obyvatelstva státu. Její narušení, tj. omezení činnosti, provozu, služeb by mělo negativní dopady hospodářské, politické, sociální, psychologické a ekologické na fungování státu.

Vodárenské provozovatelské společnosti sice nepatří mezi subjekty kritické informační infrastruktury, na které se zákon o kybernetické bezpečnosti, v České republice zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů“, který nabyl účinnosti 1.1.2015 [2] (dále jen „ZKB) přímo vztahuje, ale dle metodiky ZKB je možné odvodit povinnosti z něj vyplývající i na vodárenské

společnosti. Je to obdoba kritérií pro určení prvků kritické infrastruktury definovaná v Nařízení vlády č. 315/2014 [3] pro oblast vodárenství:

- zásobování vodou z jednoho nenahraditelného zdroje při počtu zásobovaných obyvatel nejméně 125 000,
- úpravna vody o výkonu nejméně 3 000 l/s
- vodní dílo o objemu zachycené vody nejméně 100 mil. m^3.

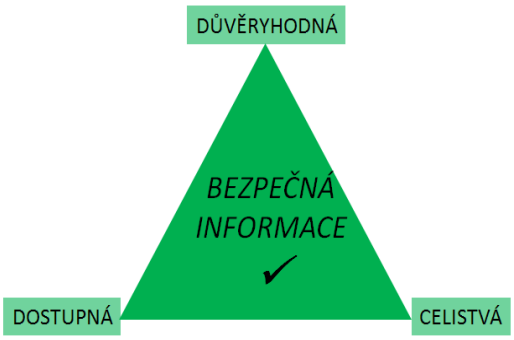
Z uvedených kritérií je zřejmé, že tyto parametry nejsou typicky orientované na standardní velikost tuzemských vodárenských společností, ale analogicky lze vyvodit, že požadavky vyplývající z tohoto nařízení vlády se dotýkají všech provozovatelů veřejných vodovodů dle zákona č. 274/2001 Sb. o vodovodech a kanalizacích[4], a proto je nutné se touto problematikou zabývat.

Jak již bylo uvedeno, ZKB je prioritně zaměřen na informační oblast kritické infrastruktury (netýká se tedy přímo vodárenského odvětví), ale dle doporučené metodiky Národního centra kybernetické bezpečnosti, které je garantem plnění tohoto zákona, vyplývá, že uvedený zákon se vztahuje i na informační systémy, které rozhodují o provozování vodárenských a kanalizačních sítí. Takto definované informační systémy jsou obecně známé jako systémy SCADA (Supervisory Control And Data Acquision) a ve vodárenské praxi využívány jako monitorovací a řídicí systémy vodárenského a kanalizačního dispečinku. Současně je nutné dodržet bezpečnostní opatření stanovená v dokumentech WHO[5], a IWA[6].

Je však neoddiskutovatelné, i kdyby výše uvedená legislativa nebyla přijata, že vodárenské informační a řídicí systémy jsou rozhodující pro řádný chod a provozování vodárenských sítí. Existuje zde reálné nebezpečí jejich vyřazení z provozu, ať již z přírodních či lidských faktorů, proto je nutno uvedené problematice věnovat mimořádnou pozornost.

1.1 KLÍČOVÉ OBLASTI VODÁRENSKÉHO ŘÍDICÍHO SYSTÉMU

ZKB definuje tzv. Kybernetický prostor jako „digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy a službami a sítěmi elektronických komunikací“. Informace, systémy, sítě a služby je zde nutné pojímat v nejširším smyslu slova, to znamená včetně průmyslových řídicích systémů a jejich dat. Bezpečností informací je definována jako „zajištění důvěrnosti, integrity a dostupnosti informací“.



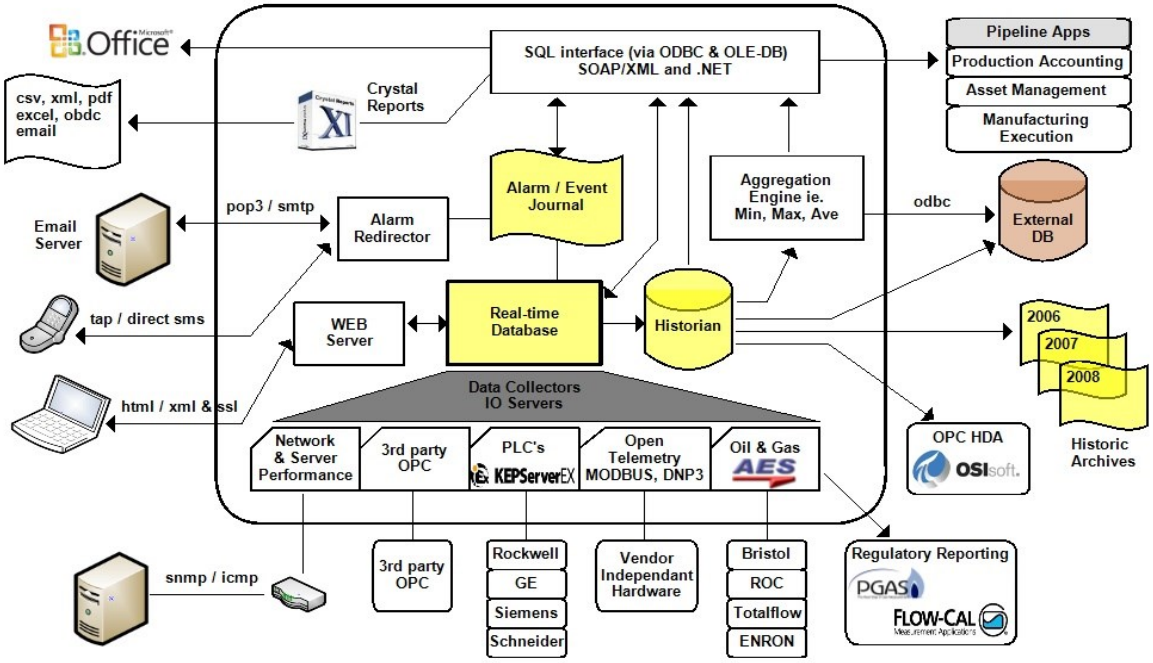
Obr. 1 Bezpečná informace - definice

Dnešní kybernetický prostor se dá (při určité míře zjednodušení) rozdělit na 2 základní části [7] :

- IT (Informační Technologie) – zajišťují fungování „kancelářských“ systémů, zahrnují servery, sítě a jejich prvky, klientské stanice (osobní počítače), telekomunikační sítě atd.
- ICS (Industrial Control Systems) – zajišťují fungování technologií, zahrnují vše od zařízení MaR přes provozní technologie (ASŘ) až po SCADA a MES systémy.

Tato oblast zahrnuje i veškeré řídicí systémy instalované ve vodárenských společnostech.

Obě části byly ještě v nedávné době považovány za zcela samostatné a do značné míry byly i funkčně a fyzicky odděleny. Dnes se v mnohém prolínají – společné sítě, servery, stejný správce, stejní uživatelé. Prostřednictvím IT se dá najít cesta k napadení ICS a naopak.



Obr. 2 Příklad prolínání IT a ICS [8]

ICS se stávají stále častěji terčem cílených kybernetických útoků. Historicky první kybernetický útok na ICS se odehrál již v r. 1982 v tehdejším SSSR prostřednictvím ukradeného systému pro řízení plynovodu. Asi nejznámějším případem je tzv. červ Stuxnet, zaznamenaný především v Iránu v roce 2010. Prostřednictvím počítačů s nainstalovaným systémem pro programování PLC Siemens, které se nacházely v „IT“ síti se podařilo skrytě přeprogramovat tato PLC a vyřadit z provozu frekvenční měniče pohonů na jaderných zařízeních pro obohacování uranu.

Každá ze zmíněných částí je také charakteristická dosud zcela odlišným přístupem k jejímu zabezpečení. IT systémy zaznamenaly v posledních 10 – 15 letech mohutný rozvoj bezpečnostních prvků a opatření – firewally, antiviry, šifrování, unikátní uživatelé a hesla. Rovněž existuje obecné povědomí o hrozbách a s tím související relativní připravenost správců i uživatelů systémů. V současné době se hovoří o etapě průmyslového rozvoje jako o tzv. Průmyslu 4.0, tedy o tzv. čtvrté průmyslové generaci v dějinách lidstva, tj. o propojení digitálního a fyzického světa. Hoří se o tzv. Internetu věcí (IoT). Přitom ale SW a HW nástroje používané v těchto sítích nemají implementovanou bezpečnost a používaná PLC (lokální automaty pro řízení technologie) nemají implementovaná potřebná hesla a další bezpečností prvky bránící jejich napadení prostřednictvím internetových sítí.

Tzn., že v oblasti ICS byla bezpečnost zatím seriozně řešena jen u vysoce kritických aplikací (energetika, vojenství). Časté jsou případy sdílených hesel pro několik uživatelů, strategie „nesahat na to, co funguje“. Funguje princip dobré víry, neočekává se útok, banalizují se potenciální následky a cíleně se přesunuje odpovědnost na pracovníky IT.

V okamžiku, kdy se „hrozba“ dostane na dosah průmyslového řídicího systému, zejména k jeho spodním úrovním, je obvykle tento systém (na rozdíl od IT) naprosto otevřený a bezbranný.

1.2 HROZBY U PRŮMYSLOVÝCH ŘÍDICÍCH SYSTÉMŮ

V České republice bylo dosud zaznamenáno jen nepatrné množství cílených elektronických útoků na průmyslové řídicí systémy a žádný s rozsáhlými následky. Přesto potenciálních hrozeb je celá řada. Mezi nejdůležitější patří:

- cílený průnik zvenčí – útok hackera s cílem způsobit škodu. Obvykle je podpořen znalostí místních poměrů, topologie sítě, otevřených portů, využití nástrojů sociálního inženýrství apod.,
- cílený průnik zevnitř – útok proveden nebo podpořen zaměstnanci společnosti s cílem poškodit firmu, pomstít se,
- poškození způsobené omylem – typicky při pracích na systému dodavatelskou firmou,
- zneužití „zapomenutých“ konfiguračních nástrojů, backdoors apod. Typickým příkladem je červ Stuxnet popsaný výše.

Dále můžeme vyjmenovat alespoň několik oblastí, které se dnes jeví jako nejrizikovější z hlediska možného napadení. Běžně se používají právě i v průmyslových řídicích systémech aniž by byly mimořádně chráněny.

- chytrá zařízení, internet věcí, jde o prudce se rozvíjející oblast nejen v komerční, ale i v průmyslové oblasti navíc s velkým potenciálem růstu v následujících letech,
- webové a mobilní aplikace, řešení „cloud“, další skupina velmi populárních služeb. Řešení typu „nechte vše na nás“ je pro provozovatele reálnou hrozbou, neboť má svá data zcela mimo kontrolu.

V této části se jedná zejména, některými provozovateli preferována řešení monitoringu vodárenských a kanalizačních sítí, o řešení, kdy veškerá data z těchto sítí jsou vodárenské společnosti poskytovány prostřednictvím „cizího dodavatelského serveru“ a WEB přístupem k datům (např. systém Fiedler).

- cizí média – USB paměti (i nové), CD, DVD. Každé takové zařízení může obsahovat škodlivý kód, který se většinou zcela bez vědomí uživatele může dostat do systému,

Riziko využívání těchto nástrojů nespočívá v nich samotných, ale v tom, že otevírají dveře k dalším důležitým a klíčovým systémům provozovatele, pokud nejsou dostatečně zabezpečené, případně oddělené od kritických struktur.

1.3 OCHRANA ICS

Je zcela mimo jakoukoliv pochybnost, že je nutné systémy ICS chránit ať už spadají po působnost ZKB nebo ne. Nehledě na to, že legislativa prochází neustálým vývojem a co dnes není zahrnuto do kritické infrastruktury, napřesrok už může být. Postup při řešení kybernetické bezpečnosti se příliš neliší od postupu při zajišťování provozní bezpečnosti, v podstatě jde jen o její podmnožinu. Celý proces by tedy měl probíhat v cyklu, počínaje identifikací rizik přes jejich zhodnocení, provedení nápravných opatření a jejich verifikaci[9]. Stručně by se daly tyto aktivity shrnout do následujících bodů:

- bezpečností audit ICS – je možno jej provést v první fázi jako interní, tedy vlastními silami, následovat by měl ale externí, provedený firmou se zkušenostmi v oboru. Pokud má mít trvalý smysl, musí audit probíhat v pravidelných intervalech, neboť vše prochází neustálým vývojem,
- úprava procesů – je zcela klíčová, organizačně může být poměrně náročná, na druhou stranu nepřináší investiční náklady. Beze změny procesů ztrácejí jakákoliv technická opatření smysl,
- doplnění o technické prvky, např. firewally, „safety boxes“ atd.

Velmi populárním termínem jsou dnes tzv. penetrační testy. Jejich podstatou je simulace pokusu o proniknutí do systému jak zvenčí, tak i zevnitř. Mohou zahrnovat testování jak technických, tak i organizačních opatření. Nabízí je řada firem a zdánlivě nabízejí všelék pro zabezpečení systémů. Je nutno podotknout, že tomu tak není.

Penetrační test je pouze jedním z nástrojů, který za určitých okolností může odhalit slabá místa, díry v systému. Jeho výsledky nelze považovat za komplexní analýzu zabezpečení systému. Při jeho použití navíc existuje riziko přetížení a zhroucení testovaného systému. To může být do jisté míry akceptovatelné pro IT síť, ale pro běžící řídicí systém je to vysoce rizikové.

Zásadní rizika kompromitace průmyslových sítí totiž neplynou ani tak ze snahy ukrást data o výrobních cyklech a zneužít je, ale spíše z možnosti narušení kapacity či kvality výroby.

2 PROVOZNÍ BEZPEČNOST VODÁRENSKÝCH SÍTÍ

Vodárenské společnosti musí být, a to nejenom z pohledu citovaného zákona o kybernetické bezpečnosti, ale i ze zákona č. 240/2000Sb. o krizovém řízení, připraveny na řešení možných mimořádných a krizových situací, které mohou nastat vlivem přírodních, technických či lidských podmínek[10]. (povodně, havárie, poruchy, terorismus). Podrobná analýza možných rizik je např. uvedena v publikaci[11].

Podmínkou efektivní řešení mimořádných situací vzniklých na vodárenském systému je přitom existence jednotného systému řízení vodárenské společnosti. Pro zavedení tohoto jednotného systému je nutné, v rámci vodárenské provozní společnosti, vytvořit organizační a řídicí strukturu tvořenou[12]:

- určeným managementem, tj. krizovým štábem (např. vedoucí provozu, technolog, zástupce užšího vedení společnosti, ekonom, vedoucím dispečinku) řešící danou mimořádnou událost, organizační a pracovní vztahy, styk s majiteli, krizovým štábem obcí a měst, Hasičským záchranným sborem,
- technickým vybavením (měřící, přenosová, výpočetní a ovládací technika) tvořící telemetrický dispečerský systém v navrženém rozsahu,
- podnikovým informačním systémem (ERP), geografickým systémem (GIS), SCADA systémem dispečinku,
- informační a datovou podporou (manipulační řády, plány krizové připravenosti, projektovou dokumentací, programovým vybavením pro podporu rozhodování, tj. manažerským krizovým informačním systémem.

Takto navržený systém organizace řízení, jehož součástí bude výše uvedený návrh organizačně-technických preventivních opatření pro omezení rizik vzniku, případně účinného řízení mimořádných situací, by měl garantovat zvýšení[13]:

- fyzické bezpečnosti objektů,
- informační bezpečnosti podnikových sítí,
- personální bezpečnosti vodárenských provozů,
- organizační bezpečnosti vodárenské společnosti,
- kvality operativního řízení provozu,
- účinnosti monitoringu,
- unifikace a adaptability informačního systému,
- efektivní zvládání řešení vzniklých mimořádných situací.

Fyzická bezpečnost objektů

Tato část návrhu organizace stanovuje požadavky na jednotlivé části systému fyzické ochrany jako prostředku zajištění fyzické bezpečnosti vodárenských objektů. Jedná se zejména o následující oblasti[14]:

- poplachový zabezpečovací systém,
- kamerový systém,
- systém kontroly vstupu,
- mechanické zábranné prostředky,
- případně fyzická ostraha a kontrola.

Fyzickou zábranou, tj. oplocením jednotlivých vodárenských objektů a jímacího území a využitím informací poplachového a kamerového systému při přenosu na dispečerské pracoviště lze omezit případné násilné poškození vodárenské technologie.

Informační bezpečnost

Informační bezpečnost je rozhodujícím pilířem ochrany systému informací spravovaných uvnitř databází a informačních systémů a procesů, které nad těmito daty pomocí aplikačního vybavení probíhají, proti hackerským útokům. Mezi základní parametry systému řízení informační bezpečnosti patří[14]:

- identifikace a autentizace přístupu k SW aplikaci pomocí osobního hesla,
- řízení logického přístupu k systému pomocí časových limitů práce, blokace k vybraným databázím, automatickým vypnutím nečinných uživatelských přístupů,
- integrita programového vybavení pomocí aktualizace operačních systémů a síťových komponent od výrobce,
- zálohování a skartace dat,
- odolnost počítačových sítí pomocí redundance síťových zařízení, šifrovacích spojení, oddělovačů firewall, komunikačních protokolů, antivirových ochran.
- využití privátních komunikačních sítí, šifrovacích protokolů.

Personální bezpečnost[14]

Personální bezpečnosti se rozumí vytvoření systému školení, kvalifikací a prověrek výběru pracovníků, jejich přístupu k informačním sítím vodárenské společnosti, k řízení jednotlivých provozů, ověření jejich znalostí, psychické odolnosti a morální spolehlivosti. Součásti je zpracování systému vzdělávání a rozvoje osobních schopností a vědomostí pracovníků s cílem minimalizace ekonomických a technologických následků dopadu případných lidských chyb při řízení mimořádných situací. Každá vodárenská společnost by měla mít zpracován interní systém vzdělávání pracovníků pro zvládání mimořádných situací s nácvikem řešení modelových situací.

Organizační bezpečnost[14]

Organizační bezpečnost představuje systém organizačních norem a řídících norem pro oblast řešení mimořádných situací. Jedná se zejména o následující podnikové normy:

- organizační řád s uvedeným funkčním popisem jednotlivých pracovních funkcí pro oblast řešení mimořádných situací,
- plán krizové připravenosti,

- havarijní plány a manipulační řády.

Součástí tohoto systému musí být i zpracování metodického předpisu způsobu aktualizace jednotlivých organizačních a řídících norem.

Operativní organizace řízení provozu[14]

Operativní organizace řízení provozu je soubor opatření vedoucích k vytvoření organizačně provozních prostředků umožňující rychlé a pružné řízení vzniklých situací při provozování vodárenského systému. Jedná se zejména o soubor následujících opatření uvedených v plánech krizového opatření:

- popis jednotlivých částí kanalizačních sítí, tj. vytvoření „provozního listu“ zařízení s uvedením technického popisu jednotlivých zařízení, výrobce, četnosti údržby, rok pořízení zařízení, typy možných oprav, rozsah doby opravy, seznam náhradních dílů, odhad doručení objednaného dílu, možnosti náhrady dílů,
- rozdělení poruch dle závažnosti na odkanalizování, popis možného vzniku, způsobu odstranění.

Při tomto zpracování je vhodné, v co nejvyšší míře, využít prostředků podnikového informačního systému a digitalizovanou formou jednotlivé opatření zavést jako součást podnikového informačního systému.

Jednotnost informačního řízení[14]

Jednotný podnikový informační systém je páteří celého navrženého systému řízení mimořádných situací. Na úrovni vodárenské společnosti se jedná o vytvoření vzájemně datové propojeného systému tvořeného:

- stávajícím podnikovým informačním systémem typu ERP,
- geografickým informačním systémem GIS doplněným o navržený „provozní list“,
- telemetrickým systémem a systémem krizového řízení, např. MISMI.

Informace z takto pojatého informačního systému budou k dispozici managementu společnosti, jako podpora pro rozhodování a způsob komunikace s nadřazeným integrovaným záchranným systémem regionu, města, státu. Současně bude umožňovat, s využitím technických prostředků dispečerského systému, operativní řízení vodárenské sítě v režimu mimořádné situace.

Monitoring vodárenského systému[14]

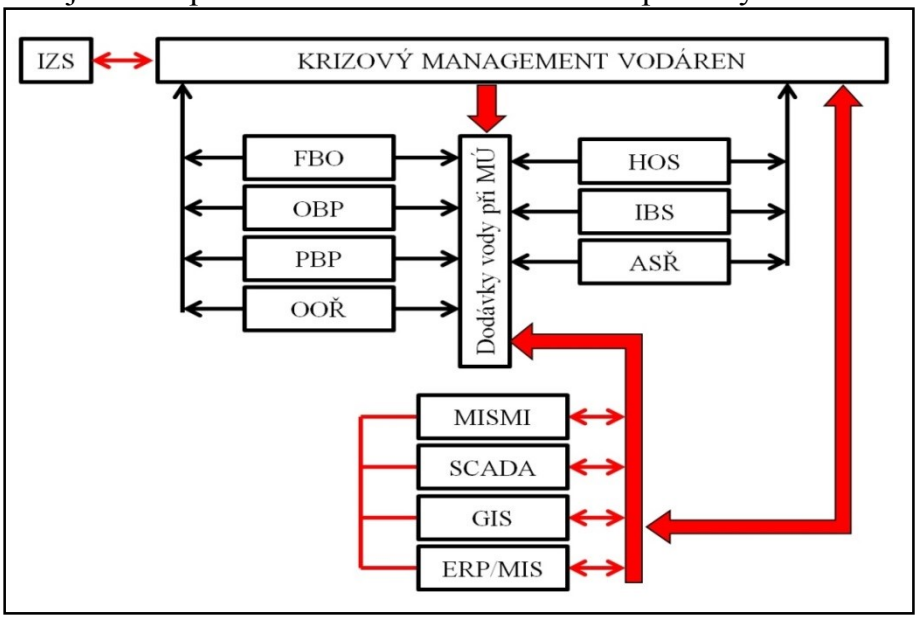
Vodárenské organizace ve většině případů využívají dispečerský systém pro operativní řízení provozu vodárenské a kanalizační sítě. Při vzniku mimořádné situace se požadavky na informační rozsah a možnosti řízení sítě násobí. Bez možností vzdáleného ovládání jednotlivých vodárenských technologií, není reálné zvládat řešení mimořádných situací. V zásadě se bude jednat o sledování a vyhodnocování základních a vypočtených informací z telemetrického dispečerského systému. Jedná se zde zejména o sledování závažných alarmů, poruch jednotlivých technických zařízení, technologií a kanalizačních sítí.

Hydraulická odolnost vodárenského systému[14]

Při nedostatku vod ve zdrojích nebo déle trvajících haváriích na přívodních vodovodních řadech má pro dodávky vody základní vliv hydraulická účinnost distribučního systému pitné a požární vody. Pro možnost měření hydraulických poměrů ve vodovodní síti je nutno tuto síť rozdělit do jednotlivých sektorů na základě matematického modelování ve fázi projektu nebo tzv. statické situaci off line způsobu výpočtu, geografického členění terénu s přihlédnutím k potřebám provozovatele, na hydraulicky uzavření nebo kaskádovitě členěné celky jednoho sektoru vodárenské sítě[15]. Délka jednotlivých, takto stanovených, částí by se měla pohybovat, na základě provozních zkušeností, mezi 10 až 15km. Tyto části je nutno hydraulicky oddělit od sebe navzájem pomocí sekčních armatur. Na vstupech a výstupech sektorů je instalován měřič s přenosem údajů na centrální dispečink. Na základě prováděných měření lze analýzou měřených hodnot stanovit potřebné tlaky a z toho odpovídající množství vody pro standardní odběr a následně řešit tlakové poměry při nouzových dodávkách vody. Za optimální tlakovou hladinu lze považovat tlak 0,3 až 0,45 MPa[16], která vyhovuje převážnému množství stavebních objektů a strojních zařízení jednotlivých odběratelů.

Současně lze, v závislosti na dlouhodobých odběrných diagramech pro různou denní a noční dobu, regulovat tyto tlakové poměry a tím snižovat možné ztráty vody vinou skrytých úniků, nezatěžovat jednotlivé technologické zařízení vodárenské sítě zvýšeným tlakem než je tlak provozní a tím i zlepšovat ekonomiku provozování a technickou životnost zařízení.

V rámci zvyšování hydraulické odolnosti vodárenské sítě je vhodné využít některé z metod snižování skrytých ztrát vody, např. operativním systémem sledování „nočních průtoků vody“. Při zjištěných zvýšených průtocích v daném sektoru vodovodní sítě je nutno provést následnou detekci místa poruchy a tuto odstranit.



Legenda: FBO-fyzická bezpečnost objektů, OBP-organizační bezpečnost provozu, PBP-personální bezpečnost provozu, OOŘ-operativní organizace řízení, HOS-hydraulická odolnost vodárenského systému, IBS-informační bezpečnost, ASŘ – úroveň telemetrického systému, MISMI – modul manažerského informačního systému pro řízení mimořádných situací, SCADA – dispečerský systém, GIS – geografický informační systém, ERP/MIS-podnikový informační systém, IZS-integrovaný záchranný systém.

Obr. 3 Návrh organizace řízení [14]

Při zjištěné a předem definované odchylce proti běžnému provoznímu stavu musí systém generovat alarmní hlášení pro určený management vodárenské společnosti, že hrozí vznik mimořádné situace.

Následně, na základě rozhodnutí managementu musí umožňovat provést operativní řídicí zásahy do technologie jímání a úpravy vody a navazujícího distribučního systému tak, aby dle stanovených priorit v dodávkách pitné vody a technických a kapacitních možností, byly jednotlivé technické subjekty zásobovány.

Konkrétním zpracováním uvedených návrhů opatření dle místních podmínek a jejich uvedením do vodárenské praxe se omezí riziko vzniku mimořádné situace, případně se vytvoří podmínky pro efektivní řízení mimořádných situací s cílem minimalizovat sociální a ekonomické škody z nich vyplývající.

ZÁVĚREM

„Systém je bezpečný tak, jak bezpečný je jeho nejslabší článek. Nejslabším článkem jsou lidé.“ *Bruce Schneider, americký kryptograf a specialista na kybernetickou bezpečnost.*

Řídit vodárenská zařízení vodovodů a vodárenských systémů již zdaleka není jen záležitosti předpokladu dostatečné provozní intuice a lidské praxe, jak tomu bylo v minulých desetiletích. V současné době se plošně na velkých územních celcích projevuje nedostatek pitné vody, počet obyvatel závislých na centrálních zdrojích a distribuci vody narůstá. Současně roste i energetická náročnost na výrobu a distribuci vody. V těchto situacích se management vodárenských společností neobejde bez preventivní projektové přípravy řízení vodárenských systémů a objevuje se zde zvýšená potřeba aplikace monitorovacích a telemetrických systémů, jako technického základu prevence a řízení mimořádných situací. Úloha telemetrických systémů a vodárenských dispečinků, při snižování provozních nákladů výroby a distribuci vody a při provozování vodárenského systému při mimořádných situacích, jako jsou např. při povodních, dlouhodobém suchu nebo nebezpečí teroristických útoků, je nezastupitelná.

Přednáška naznačuje, jak k dané problematice přistupovat a jakým způsobem se lze v každé vodárenské společnosti připravit na řešení mimořádných událostí mající dopad do jejího bezpečného provozování a ekonomické účinnosti provozu.

LITERATURA

[1] Statistická ročenka SOVAK, Praha, Silvia, 2015,
[2] Sbírka zákonů ČR: Zákon č. 181/2014 Sb. „Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů“

[3] Sbírka zákonů ČR: Nařízení vlády č. 315/2014 Sb. ze dne 8. prosince 2014, kterým se mění nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury
[4] Sbírka zákonů ČR: Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon)
[5] WHO. *Guidelines for Drinng Water Quality.* Vol.1. Recommendation.3rd edition. Geneva: WHO,2004, Chapter 4: Water safety plans,
[6] IWA (Internationa Water Association). trans. 2005, *The Bonn Charter for Save DrinkingWater,* September 2004. SOVAK,2005, č.7-8,
[7] ISO/IEC 16085. *Systems and software engineerin, Life cycle processes, Risk management*,2006, [on line] http://www.iso.org/iso/catalogue_detail,
[8] Technical Review for ClearSCADA Management Software, (2010), Scheider Electric Document,
[9] Kašparec J., Lindovský M., Feikus M. *Centrální dispečink jako nástroj na zvýšení provozní bezpečnosti kanalizačních sítí*, 2013, sborník semináře Nové metody a postupy při provozování čistíren odpadních vod, 2013, ISBN 978-80-86020-76-1.
[10] Krocova, S., 2014. *Rizika provozování vodárenských a kanalizačních systémů,* Spektrum, 2014, ISBN 978-80-7385-147-7,
[11] Tuhovcak, L. a kol., 2010. *WaterRisk Analýza veřejných vodovodů,* CERM, Brno 2010, ISBN 978-80-7204-676-8,
[12] Lindovsky, M., 2014. *Anylysis of Crisis Management Water Supply System*, Journal Inzynieria mineralna, NR 2(34), PL ISSN 1640-4902,
[13] AF-CityPlan, *Metodika posuzování bezpečnosti kritické struktury – pitná voda,* VF20102014009, 14.10.2014, materiál AF-CityPlan
[14] Lindovsky,M., 2016. *Řízení vodárenského systému při mimořádných podmínkách, P.h.D. thesis, VŠB -Technická univerzita Ostrava,*
[15] Krocova, S., 2014. The Water Protection Trends in the Industrial Landscape. *Inžynieria Mineralna*, roč. XV, č. 2,
[16] Don D. Ratnayaka, Malcolm J. Brandt, *Water Supply,* 2009*,* London, IWA Publishing, Edition 6th, ISBN 13: 978-0750668439,