



Arta de a trăi în siguranță.



CONFERINȚA NAȚIONALĂ A A.R.T.S.

**Siguranța și securitatea cetățeanului și a comunității
Aportul tehnicii de securitate**



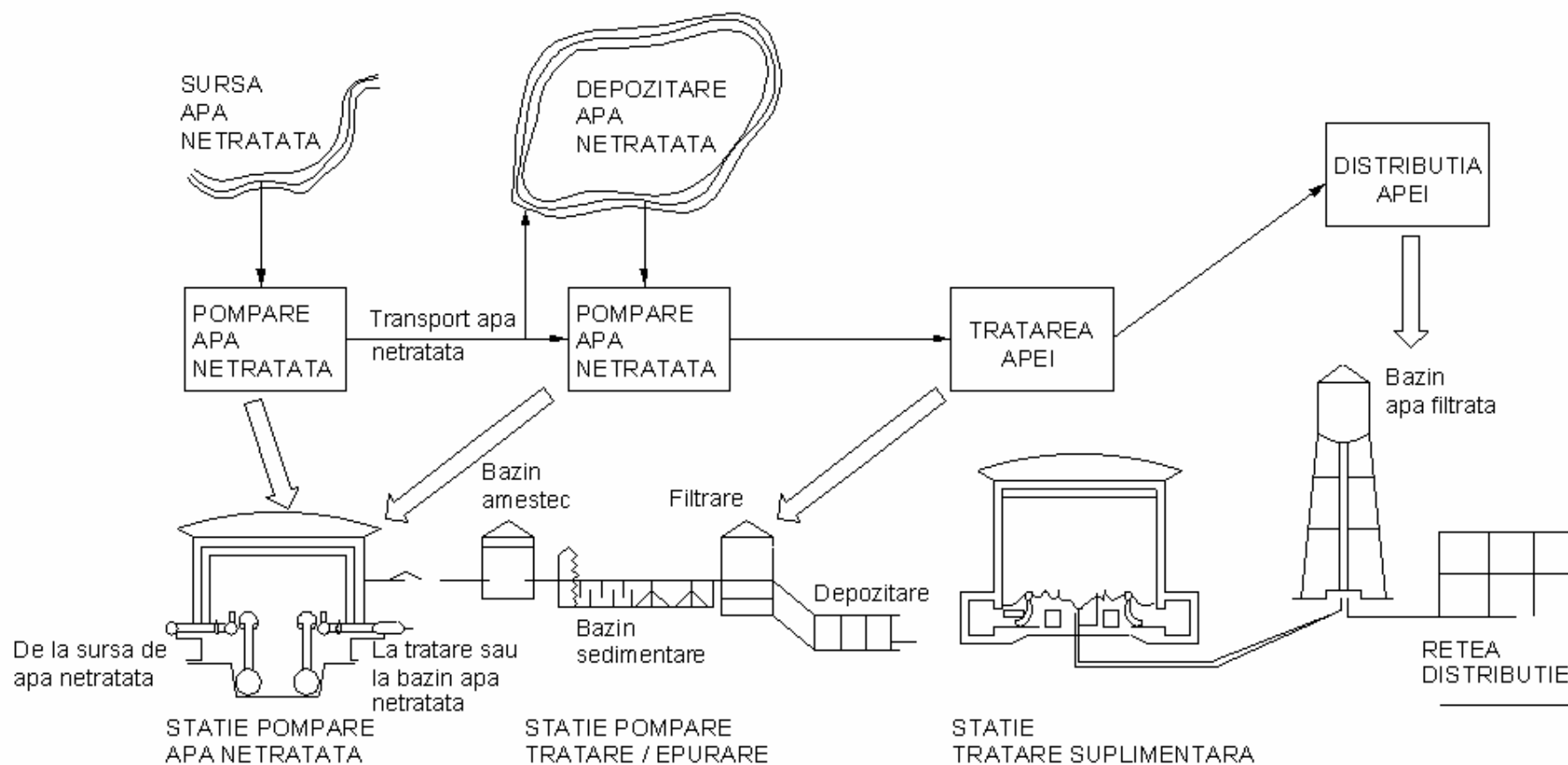
REȚELELE DE APĂ – INFRASTRUCTURI CRITICE -



- *„Infrastructura critică” este definită în „The U.S.A. Patriot Act” ca sisteme și valori fizice sau virtuale, de importanță deosebită pentru Statele Unite, astfel încât expunerea sau distrugerea acestor sisteme sau valori ar putea avea un impact negativ asupra securității, securității economice, stării de sănătate publică și siguranță.*
- *În concepția U.E. “Infrastructurile critice se referă la acele obiective, rețele, servicii, active fizice și mijloace informatice care, dacă sunt întrerupte sau distruse, vor avea un impact serios asupra sănătății, siguranței, securității sau a bunăstării economice a cetățenilor sau asupra funcționării efective a actului de guvernare din statele membre”.*

În categoria „*infrastructuri critice*” sunt incluse, de regulă, toate structurile vitale ale unei societăți, care, prin discontinuitatea lor, aduc societatea în imposibilitatea de a-și exercita funcțiunile, respectiv:

- - sistemele de electricitate (energia);
- - obiectivele și instalațiile nucleare;
- - sistemele informatice și de telecomunicații (rețelele de calculatoare, rețeaua de telefonie fixă și mobilă, Internetul);
- - sistemele de extracție, prelucrare, depozitare și transport ale petrolului, gazelor și altor resurse primare de energie;
- - deșeurile rezultate din activități economice de procesare/prelucrare a materialelor radioactive, toxice;
- - **sistemele de aprovizionare cu apă (apa);**
- - infrastructura și mijloacele de comunicații (rutiere, aeriene, feroviare și navale);
- - sistemele bancare, financiare și de asigurări;
- - serviciile de sănătate (publică și privată) și de intervenție în cazuri deosebite (incendii, calamități, dezastre, avarii).
- - valorile și utilitățile publice de interes strategic;
- - autorități publice (președinție, parlament, guvern, structurile informative etc.).



SISTEM DE DISTRIBUTIE A APEI

Un sistem municipal tipic de distribuție a apei (infrastructură critică) este compus, în principal, din trei entități majore:

- stații de pompare;
- depozit(e) de distribuție;
- rețea(rețele) de conducte pentru distribuție.

Acestea sunt active critice (elemente ale unei infrastructuri critice). Nu au fost incluse aici sursele de apă, stațiile de tratare, depozitele de sedimentare etc.







AMENINȚĂRI LA ADRESA REȚELELOR DE APĂ

Amenințarea se referă la existența unei intenții și la capacitatea cuiva (sau ceva) de a provoca consecințe dezastruoase. Amenințările sunt caracterizate atât prin mijloacele prin care se produc cât și prin probabilitatea apariției lor.

Un sistem de distribuție format din conducte, țevi, pompe, rezervoare de depozitare și din anexe/accesorii/dependințe ca: diferite tipuri de valve, aparate de măsură și control etc. oferă oportunități pentru acte de terorism deoarece sistemul este:

- extensiv;
- relativ neprotejat și accesibil;
- izolat (de multe ori).





TIPURI DE AMENINTARI

❖ Amenințări fizice:

- Distrugerea fizică a bunurilor sistemului sau întreruperea alimentării cu apă. Un singur terorist sau un grup mic de teroriști ar putea ușor să paralizeze un oraș întreg prin distrugerea echipamentului potrivit;
- Pierderea presiunii apei care compromite capacitatea de luptă cu focul (a pompierilor) sau poate facilita formări de bacterii în sistem;
- Presiune mare care produce un *efect de ciocan de apă* prin deschiderea și închiderea unor valve de control major sau deschiderea/închiderea prea rapidă a pompelor, provocând rupturi, spurgeri în rețea.

❖ Amenințări cibernetice:

- Întreruperea fizică a unei rețele SCADA (*Supervisory Control And Data Acquisition*);
- Atacuri la sistemul central de comenzi pentru crearea unor avarii simultane;
- Atacuri electronice folosind viruși;
- Supraîncărcare trafic în rețea;
- Gâtuire trafic;
- Utilizare software neautorizat;
- Utilizare software malițios (ex.: modificarea datelor pentru a împiedica folosirea clorului sau a altui dezinfectant, având ca efect înmulțirea microbilor).

❖ Amenințări biologice

Există patogeni și biotoxine care sunt potențial rezistente la dezinfectarea prin clorurare și sunt stabile în apă pe perioade relativ lungi.

- Patogeni: *clostridium perfringens*, *ciuma* și altele;
- Biotoxine: *botulinum*, *alfatoxin*, *ricin* și altele.

Chiar dacă apa are potențial de diluare, o particulă plutitoare sau microcapsule pot dispersa patogeni în rețelele de apă potabilă. Eficacitatea unui atac biologic față de efectele de diluare poate fi mărită prin introducerea unei *arme biologice* în apropierea robinetului.

Sistemele de depozitare și distribuție a apei sunt vulnerabile la introducerea de substanțe toxice pentru un număr foarte mare de oameni sau utilizarea unei doze cu nivel scăzut, cu efecte pe o durată mai lungă și cu praguri de detecție mai scăzute.

❖ Amenințări chimice

Există substanțe chimice de război și otrăvuri chimice industriale. Sunt cinci tipuri de agenți chimici de război, funcție de efectul produs:

- care atacă sistemul nervos;
- care provoacă boli de piele;
- care provoacă sufocarea;
- care contaminează sângele;
- halucinogeni.

VULNERABILITĂȚILE REȚELELOR DE APĂ

Vulnerabilitatea este o slăbiciune care conduce (sau care poate fi folosită pentru a conduce) la consecințe dezastruoase.

Elementele esențiale pentru evaluarea vulnerabilității sunt:

1. Caracteristicile sistemului/rețelei de apă, incluzând misiunea și obiectivele sale;
2. Identificarea consecințelor (și clasificarea acestora funcție de priorități) ce trebuie evitate;
3. Determinarea bunurilor critice care pot fi obiect al actelor răuvoitoare care ar genera consecințe grave;
4. Evaluarea posibilității (probabilitate calitativă) unor acte răuvoitoare din partea adversarilor;
5. Evaluarea măsurilor de contraacțiune existente;
6. Analizarea riscurilor curente și dezvoltarea unui plan pentru reducerea riscurilor funcție de nivelul acestora (întocmirea unor liste de priorități).

EVALUAREA RISCURILOR

Pentru evaluarea riscurilor se pot utiliza metode calitative și/sau cantitative.

- **Metodele calitative** se bazează pe evaluări ale valorilor parametrilor și încadrarea acestora conform unor scale prestabilite, evidențiind situațiile de pericol și condițiile în care acestea se pot produce. Pe această bază, se stabilesc măsurile de contracarare sau de diminuare a riscurilor.
- **Metodele cantitative**, apreciate pentru calitatea de a furniza valori numerice determinate prin calcul, sunt mai greu de utilizat datorită dificultății de a identifica sau estima valori unanim acceptate pentru probabilități și consecințe. Aceste metode pot fi utilizate, însă, pentru analize parțiale sau pentru analize cost-efect.

In cazul **metodelor cantitative**, pentru evaluarea riscului de securitate asociat unui activ critic, se poate utiliza formula de estimare (calcul):

$$R=PA*(1-PE)*C$$

unde:

- **R** = riscul asociat cu atacul asupra activului critic;
- **PA** = probabilitatea de producere a atacului;
- **PE** = probabilitatea ca sistemul de protecție să respingă atacul;
- **C** = consecințele unui atac reușit.