

Problematika eksploatacije i održavanja vezana za zaštitu kritične infrastrukture u domenu procesne industrije

Branislav Todorović¹, Darko Trifunović¹, Marina Todorović², Mina Marković²

- ¹ Institut za nacionalnu i međunarodnu bezbednost
- ² Air Serbia



Procesing '22 1–3. jun 2022, Beograd

1

Kritična infrastruktura (CI) - Koncept zaštite i otpornosti

- Zaštita kritične infrastrukture (Critical Infrastructure Protection - CIP) je koncept koji se odnosi na spremnost i reagovanje na ozbiljne incidente vezane za kritičnu infrastrukturu regiona ili nacije
- Evropski program za zaštitu kritične infrastrukture (EPCIP) se odnosi na doktrinu ili dodatne planove urađene na bazi direktive Evropske komisije EU COM(2006) 786 koja označava evropsku kritičnu infrastrukturu, a koja bi u slučaju otkazivanja, incidenta ili napada mogla uticati i na državu gde se nalazi i na najmanje jednu drugu evropsku državu članicu
- Zbog teškoće planiranja i predviđanja svih vidova pretnji, kao i sprovođenja preventivnih mera na nivou koji bi obezbedio nesmetan rad CI u svim okolnostima, pored zaštite je razvijen i koncept otpornosti kritične infrastrukture (Critical Infrastructure Resilience – CIR)



Procesing '22 1–3. jun 2022, Beograd

2

Kritična infrastruktura u domenu procesne industrije

- Neki segmenti procesne industrije su od vitalnog značaja za društvo, pa se mogu okarakterisati kao kritične infrastrukture, npr. energetska sektor, velika hemijska postrojenja, postrojenje za pripremu vode za piće, itd.
- Konkretno odluke koji segmenti i/ili pojedinačna procesna postrojenja pripadaju CI treba da donesu relevantne vlasti na državnom, regionalnom ili drugim administrativnim nivoima
- Jednom definisana, kritična infrastruktura u procesnoj industriji zahteva planove, mere i aktivnosti zaštite i razvijanja otpornosti na svim nivoima inženjerskog rada: počevši od projektovanja i izgradnje pa do svakodnevnog rada i dugoročnog planiranja



Povezanost segmenata kritične infrastrukture

- Infrastrukturne međuzavisnosti se definišu kao relacije koji postoje između više infrastrukturnih sistema zbog njihove međusobne povezanosti i međuodnosa, drugim rečima, ono što se dešava sa jednim sistemom može uticati na druge infrastrukturne sisteme
- Zbir kritičnih infrastrukture, infrastrukturnih mreža i njihovih međuzavisnosti stvara veoma složen nelinearan sistem koji je težak za razumevanje donosiocima odluka i vlasnicima/operatorima sistema, posebno tokom stanja poremećaja ili u vanrednim situacijama
- CIP problematika i principijelna podela bezbednosti i rizika kritičnih infrastrukture na deo vezan za informacione tehnologije (IT) i na fizičke pretnje/incidente takođe ima sve više preklapanja, tako da se uglavnom nije moguće nezavisno baviti cyber i fizičkom zaštitom postrojenja



Tehnički i ostali aspekti funkcionisanja postrojenja

- Uspešna primena tehnologije podleže zadovoljavanju niza uslova vezanih za različite ciljeve, tematiku i metode u odgovarajućim oblastima (npr. u automobilske industriji, tehnologiji rada elektrana, rashladnoj tehnologiji, računarskim sistemima ili građevinarstvu)
- Postoje i hibridni sistemi, na primer u energetici gde se kombinuju klasični sa obnovljivim izvorima energije u cilju smanjenja klimatskih uticaja, koji postavljaju nove izazove kod planiranja i realizacije zbog dopunskih ekonomskih, tehničkih i društvenih faktora i faktora životne sredine
- Pouzdano funkcionisanje CI i bezbednost zavisi i od ljudskog faktora, ne samo u pogledu mogućih grešaka u radu, već i u pogledu cyber rizika. Takođe, ljudi imaju tendenciju da se ponašaju drugačije tokom incidenata, stvarajući tako mogućnost za nove probleme ili kreirajući nove rizike



Zaštita kritične infrastrukture (CIP) u EU

- U cilju poboljšanja zaštite kritične infrastrukture i cyber bezbednosti, Evropska komisija je 2020 pokrenula novu strategiju EU
- Kao deo ove velike revizije, Komisija je objavila dva predloga: NIS2 Direktivu za bolje rešavanje sajber rizika i novu Direktivu o otpornosti kritičnih subjekata (Critical Entities Resilience - CER) i infrastruktura koja uzima u obzir rizike od fizičkih pretnji kao što su na pr. prirodne opasnosti, hibridne pretnje, terorizam, uticaj ljudskog faktora i unutrašnji incidenti, vanredne situacije ili nesreće u javnom zdravlju
- **Predložena CER Direktiva proširuje i obim i dubinu strategije, obuhvatajući sektore energetike, transporta, bankarstva, infrastrukture finansijskog tržišta, zdravstva, vode za piće, otpadnih voda, digitalne infrastrukture, javne uprave i svemira**



Mere za otpornost kritične infrastrukture

- Savet Evrope je 20.12. 2021. odobrio opšti pristup nacrtu direktive o otpornosti kritičnih subjekata, sa ciljem za smanjenje ranjivosti i jačanje otpornosti
- Brojne krize poslednjih godina, uključujući terorističke napade, COVID-19 i ekstremne vremenske uslove, dovele su u pitanje spremnost sistema i infrastrukture i pokazali da treba više da uradimo da bismo bili kolektivno spremni za buduće krize, bez obzira na njihovu prirodu
- Zemlje članice EU će morati da imaju strategiju za poboljšanje otpornosti kritičnih sistema i da sprovode procenu rizika najmanje svake 4 godine
- CI i drugi kritični subjekti će morati da identifikuju relevantne rizike koji mogu značajno da poremete rad, da preduzmu odgovarajuće mere da obezbede otpornost i obaveste nadležne organe o incidentima



Situacija u Republici Srbiji

- Republika Srbija je 2018. donela Zakon o kritičnoj infrastrukturi ("Sl. glasnik RS", br. 87/2018)
- Ovim zakonom uređuje se nacionalna i evropska kritična infrastruktura, identifikacija i određivanje kritične infrastrukture Republike Srbije, zaštita CI, nadležnost i odgovornost organa i organizacija u oblasti kritične infrastrukture i informacije, izveštavanje, pružanje podrške odlučivanju, zaštita podataka, upravljanje i nadzor u oblasti CI (Član 1)
- Nažalost, Zakonu i dalje nedostaju podzakonski akti za praktičnu primenu pa se Srbija i dalje mora oslanjati na prethodne planove i dokumente
- Republika Srbija je dobro organizovana da reaguje na elementarne nepogode, što je potvrđeno u više slučajeva tokom prethodnih decenija, ali to treba proširiti i na oblast zaštite kritične infrastrukture



Najnovije pretnje i mogući razvoj situacije

- Nakon početka rata u Ukrajini mnoge institucije u Srbiji dobile su pretnje bombom, počevši sa letovima Air Serbia iz Beograda za Moskvu
- Do sada su pretnje dolazile bolnicama, školama, aerodromima, tržnim centrima, beogradskom zoološkom vrtu, na ulicama, itd., uglavnom preko mejla. Objekti su evakuisani iz predostrožnosti, rad je onemogućen mada nijedna pretnja nije bila istinita
- Iako se često pretpostavlja da je u pitanju lažna uzbuna, sve mere moraju biti preduzete dok se ne dokaže da nema pretnje
- Nakon mnogih obmana u vrlo kratkom vremenskom periodu ljudi postaju manje pažljivi, čime se povećavaju rizici i kod kritične infrastrukture
- Takođe se učinak pojedinca smanjuje bilo da je direktno (bezbednosna služba, obaveštajna služba...) ili indirektno uključen u ovu situaciju



Jačanje CIP procesa - primer

- Kao primer složene kritične infrastrukture za analizu u domenu procesne industrije može se uzeti sistem elektrana povezan elektroenergetskom mrežom, mreža magistralnog gasovoda sa mernim i kompresorskim stanicama ili postrojenje za pripremu vode za piće sa distributivnom mrežom cevovoda
- Svaki od navedenih primera uključuje više postrojenja, zgrada, resursa i drugih objekata raspoređenih na većoj površini. Zbog veličine i složenosti sistema, organizovano upravljanje takvim sistemom može predstavljati ključni izazov zaštite kritične infrastrukture.
- Za pouzdan rad važno je da se preko jače sistemske integracije centralizuju operacije CI i pojača opreznost u vezi sa fizičkim i virtualnim pretnjama, gde je uloga procesnog inženjera nezamenljiva kod analize i definisanja rizika i kritičnih tačaka vezanih za njegovu oblast



Jačanje CIP procesa - primer

- U slučaju pomenutih složenih sistema, svaka sigurnosna pretnja može imati katastrofalne posledice, zbog čega se menadžeri odlučuju za korišćenje **višeslojnih sistema zaštite perimetra**, kao jedne od mera
- Arhitektura ovih postrojenja podrazumeva inicijalni pojas volumetrijskih senzora (visine od 4–6 metara) sa izraženom mogućnošću detekcije, uzbunjivanja i ograde za usporavanje napadača
- Iza tog pojasa obično dolazi pregledan prazan prostor širine i do deset metara radi verifikacije pomoću kamera ili drugog pojasa detekcije, poput mikrovalnih senzora, podzemnih volumetrijskih kablova ili infracrvenih detektora. Mogućnost je i dodatna ograda sa inteligentnim sensorima.
- Ključno je adekvatno integrisati videonadzor sa sistemima za detekciju neovlašćenih upada, koji automatski šalje obaveštenje komandnom centru sa odgovarajućim snimkom kamere na konkretnoj lokaciji kako bi operateri i služba obezbedjenja bili u mogućnosti da reaguju.



Jačanje CIP procesa - primer

- Važno je naglasiti da se sigurnosni sistemi poput videonadzora, kontrole pristupa i zaštite perimetra mogu jednostavno povezati s drugim važnim sistemima preko centralne integrisane platforme za upravljanje
- Ovi sistemi uključuju IT, sisteme za detekciju dima i vatre, protivpožarnu zaštitu, telefonsku i radio komunikaciju i automatizaciju zgrada
- Platforma za potpunu integraciju može omogućiti operaterima kritične infrastrukture da upravljaju svim sistemima unutar lokacije kada dođe do prirodnih katastrofa, incidenata ili napada
- Kod procesnih postrojenja vrlo je važno imati definisane procedure za takve slučajeve (uključujući i incidente potpuno nepoznate prirode), koje obuhvataju i potpuno isključenje po hitnom postupku, kako bi se smanjio negativan uticaj i u što većoj meri zaštitio integritet sistema



Uticaj na troškove kod projektovanja, rada i održavanja postrojenja

- Aktivnosti vezane za zaštitu i otpornost kritične infrastrukture u velikom broju slučajeva povećavaju troškove kod postrojenja, što mora da se uzme u obzir kod ekonomskih analiza u oblasti procesnog inženjerstva
- Primena zaštite kritične infrastrukture u delu projektovanja i konstruisanja direktno utiče na investicione troškove, na pr. na povećanje investicionih troškova infrastrukture kod postrojenja zbog dodatnih bezbednosnih sistema i pratećih troškova inženjeringa
- Poboljšanje otpornosti kritične infrastrukture može da traži ojačavanje delova opreme, povećanje kapaciteta određenih segmenata, uvođenje paralelnih sistema i sl. kako bi se smanjio uticaj nekog incidenta ili omogućilo brže vraćanje u radno stanje. I pored pažljivog planiranja i dopunskih analiza kod projektovanja, time se direktno uvećavaju investicioni troškovi postrojenja bez povećavanja proizvodnog kapaciteta



SET
SAMIT ENERGETIKE TRERINJE

Procesing '22 1–3. jun 2022, Beograd

13

Uticaj na troškove kod projektovanja, rada i održavanja postrojenja

- Izmene i dopune u cilju zaštite i otpornosti kritične infrastrukture u sistemima procesne industrije se očitavaju i kod operativnih troškova. Mada to direktno zavisi od tipa postrojenja, može se proceniti sledeće:
 - Fiksni operativni troškovi, koji ne zavise od obima proizvodnje, se direktno uvećavaju u određenom procentu zavisno od primenjenih CIP i CIR mera (pored dodatnih troškova IT sektora, tu su i dodatni troškovi nadzora i održavanja procesne opreme koja služi poboljšanju otpornosti, kao na pr. dodatni moduli)
 - Promenljivi operativni troškovi, koji direktno zavise od trenutnog obima proizvodnje, su manje podložni uvećanju kod procesnih sistema sa optimizovanim CIR merama
- Važno je naglasiti da ni u okviru EU nije definisano ko snosi troškove CIP i CIR mera, tako da kod ekonomske analize investiranja u domenu procesne industrije o tome treba voditi računa i eventualno posebno prikazati te neprofitabilne elemente investicionog ulaganja



SET
SAMIT ENERGETIKE TRERINJE

Procesing '22 1–3. jun 2022, Beograd

14

Zaključak

- Uzimajući u obzir mogućnost da neka od pretnji bombom postane stvarna, kao i potrebu prilagodjavanja projektovanja i rada u cilju zaštite kritične infrastrukture u domenu procesne industrije u bliskoj budućosti, važno je da se procesni inženjeri upoznaju sa planovima, strategijama i merama u toj oblasti i da aktivno učestvuju u CIP procesu
- Treba razmotriti uključivanje CIP i CIR u analize i upravljanje rizicima u procesnoj industriji u cilju povećanja bezbednosti i pouzdanosti u radu postrojenja, kako bi se stručno pokrili budući zahtevi iz Zakona - *“Bezbednosni plan operatora za upravljanje rizikom je dokument kojim se utvrđuju mere smanjenja rizika, definišu odgovornosti i određuju dužnosti, te uspostavlja okvir za postupanje u cilju otklanjanja, odnosno smanjenja posledica bezbednosnih pretnji definisanih u analizi rizika, koja je sastavni deo plana” (Zakon o kritičnoj infrastrukturi , Član 8)*



SET
SAMIT ENERGETIKE TREBINJE

Processing '22 1–3. jun 2022, Beograd

15

Hvala na pažnji!



SET
SAMIT ENERGETIKE TREBINJE

Processing '22 1–3. jun 2022, Beograd

16