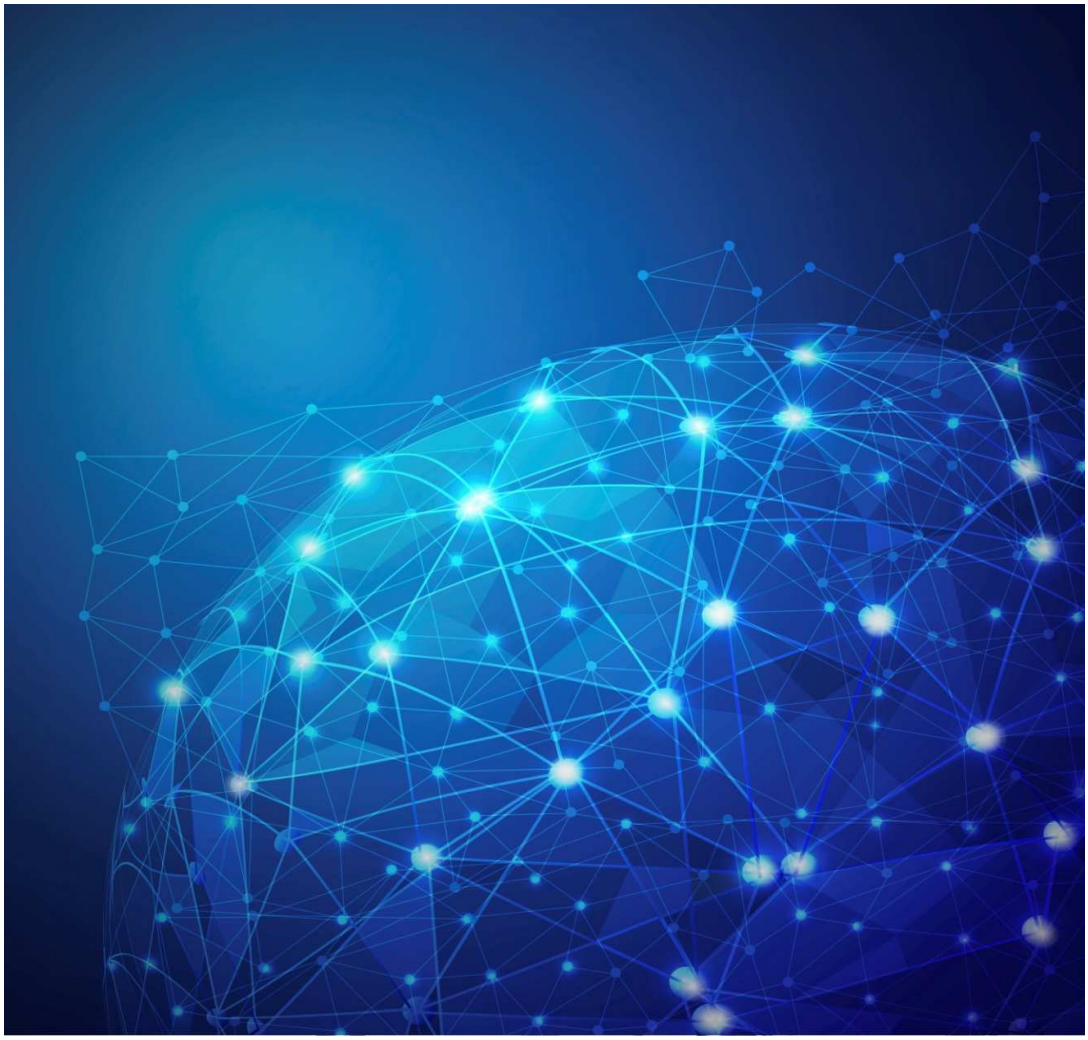
Myndigheten för samhällsskydd och beredskap

Vikten av var och när

Samhällets beroende av korrekt tids- och positionsangivelse



MSB kontakt: Verksamheten för samhällets informations- och cybersäkerhet (ICS)
Publikationsnummer MSB778 – November 2014
ISBN 978-91-7383-508-4

Innehållsförteckning

Förkortningar

DHS – Department of Homeland Security

ESA – European Space Agency

FB - Förmågebedömning

GLONASS – Globalnaja navigatsionnaja sputnikovaja Sistema

GNSS – Global Navigation Satellite System

GPS – Global Positioning System

IT – Informationsteknik

NTP – Network Time Protocol

PNT – Position, navigation och tid

PTS – Post- och telestyrelsen

RSA – Risk- och sårbarhetsanalys

SP – Sveriges Tekniska Forskningsinstitut

UTC – Temps Universel Coordonnué

Sammanfattning

Position och tid har i dag blivit kritiska faktorer för många funktioner i vårt samhälle. Vid bortfall av data eller information om någon av dessa faktorer kan många system och tjänster inte längre fungera normalt. Styrsystem för vattenrening, finansiella system, drift av nätet för elförsörjningen och diverse kommunikationssystem är exempel på system som kan drabbas av störningar i GNSS.

Global Navigation Satellite System, GNSS, är ett samlingsnamn för de olika satellitsystem som agerar som tid-, positions- och navigationsdistributörer. Position, navigation och tidsdata (PNT) är den data och komponent som många system idag bygger på och vilket denna rapport belyser som ett problematiskt beroende.

I denna rapport beskrivs tekniken bakom position och navigation samt tid- och frekvenssynkronisering. Vidare beskrivs de risker, hot och problem som omgärdar tekniken. Slutligen presenteras en rad förslag på möjliga alternativ, både generella och tekniskt orienterade, för att minska sårbarheterna i system som använder PNT, bland annat beroendet av GNSS.

Dokument belyser vikten av att veta vilka beroenden som existerar i den egna verksamheteten av att ha kontinuerlig tillgång till data om position och tid. Framför allt bör inte samhällsviktiga funktionerna, ha ett ensidigt beroende av GNSS-baserade tjänster. Främst gäller det tid- och/eller frekvenssynkronisering men även positioneringsberoendet.

De funktioner som lutar sig på positions- och navigationstjänster är ofta lätta att identifiera. Det är därför relativt enkelt att också säkerställa om man redan har en ersättningstjänst eller -funktion för positionering eller navigering. Beroenden av tid- och frekvenssynkronisering är däremot mer komplexa. Ofta finns det inte fullständig kännedom om vilket beroende ett givet system har av tid- och frekvenssynkronisering samt hur noggrann synkronisering som krävs.

De viktigaste generella åtgärderna för att säkerställa en verksamhets kontinuitet jämte dess beroende av PNT-data är att medvetandegöra, inventera och identifiera om existerande beroenden, klassificera system efter beroendegrad samt att se över upphandlingar, leverans och förvaltning av PNT-försörjande tekniker. De tekniskt orienterade åtgärder som föreslås är att undvika singulärt beroende, använda hybrida lösningar av multipla källor som erbjuder tid och att säkra befintlig utrustning mot yttre störningar.

1. Inledning

Position, navigation och tid (PNT) har i dagens samhälle blivit kritisk information för att en rad olika system och tjänster ska fungera. Vid bortfall av sådan information kan system och tjänster inte alltid fungera normalt. För att kunna åtgärda riskkällor inom detta område, som kan leda till problem med kontinuitet i en verksamhet, måste därför förmågan att kunna identifiera användande och beroende av PNT finnas.

I denna rapport beskrivs tekniken bakom position och navigation samt tid- och frekvenssynkronisering. Vidare beskrivs de risker, hot och problem som omgärdar sagda teknik. Slutligen presenteras en rad förslag på möjliga alternativ, både generella och tekniskt orienterade, för att minska sårbarheterna i system som använder PNT, bland annat beroendet av GNSS.

1.1 Problembilden

Störningar i exempelvis GNSS kan ta sig många uttryck. De flesta störningar ger direkta, och tydliga konsekvenser och uppdagas ofta omedelbart, men det kan också tillkomma problem efter hand framförallt för system eller tillämpningar som är beroende av GNSS för tid och/eller frekvens. Störningar kan uppstå i styrsystem, datanätverk, larmsystem, övervakningsnätverk och kommunikationssystem.

Problemen som kan uppstå är beroende på ur systemen är utformade och hur tid förs in i systemet.

Det kan dock många gånger vara svårt för aktörer att veta hur beroende man är av PNT. Många aktörer kan ofta ange ungefär hur beroende man är av tidssynkronisering via GNSS t.ex. i it- och kommunikationssystem, men det råder ofta större osäkerhet kring hur påverkan på externa system/tjänster som man är beroende av, exempelvis telefoni, datakommunikation och Rakel ser ut.

Vad som händer med ett system eller en tjänst som är beroende av tid- och frekvenssynkronisering vid bortfall av inkommande position-, navigation- och tidsdata, från exempelvis GNSS, är således inte alltid lätt att förutse samtidigt som konsekvenserna kan vara omfattande. Detta har också framkommit i svaren på det GNSS-scenario, som myndigheterna fick ta ställning till i risk- och sårbarhetsanalysen för 2014. Även kunskapsnivån om innehav och beroenden av tekniken varierar bland aktörerna.

Denna rapport har tagits fram för att stötta och uppmuntra samhällsviktiga aktörer eller aktörer som bedriver samhällsviktig verksamhet att initiera insatser för att arbeta bort ensidigt beroende av GNSS. I detta stöttande behöver det kommuniceras ut vilka risker som verkligen finns med att ha

samhällsviktiga funktioner som exempelvis är ensidigt beroende av GNSS-baserade tjänster.

1.2 Syfte och mål med rapporten

Detta dokument beskriver framförallt riskerna med ett beroende av tid- och frekvenssynkronisering, position (och navigation) behandlas sekundärt, i syftet att få till en medvetandehöjning kring risker och sårbarheter. Dokumentet ger även förslag till åtgärder som syftar till att stötta arbetet kring ett säkrare användande och minskat kritiskt beroende av GNSS-baserad position och navigation samt tid- och frekvenssynkronisering.

För att kunna få en bild över hur olika samhällsviktiga funktioner kan hantera ett bortfall av position, tid- och frekvenssynkronisering samt distributionstjänster såsom GNSS, bör aktörerna ha en förståelse om vilka delar av deras verksamhet som kan ha ett beroende av position, tid- och frekvenssynkronisering samt tillhörande distributionstjänster. Ansvaret för att tydliggöra detta beroende ligger på varje enskild aktör. Detta dokument syftar till att medvetandegöra och motivera ett sådant arbete hos framförallt de samhällsviktiga aktörerna i samhället.

1.3 Underlag samt avgränsningar i arbetet

Till grund för detta dokument ligger främst de svar som kommit in till MSB via 2012 års *risk- och* sårbarhetsanalyser (RSA) med det tillhörande scenariot *Störningar i GNSS* (Global Navigation Satellite System[1]), *förmågebedömningar* (FB), samt svenska och internationella studier inom området. Det har också skett dialoger med bland annat Pensionsmyndigheten, Post- och Telestyrelsen (PTS) och Sveriges Tekniska Forskningsinstitut (SP).

Rapporten syftar inte till att vara en fullödig studie, utan endast belysa exempel och möjliga åtgärder inom ett antal utvalda samhällsviktiga funktioner som bedömts kunna ha ett beroende av korrekt tidsangivelse, frekvenssynkronisering samt i viss mån position- och navigationsangivelse. De legala kraven som eventuellt finns angående spårbar tid har inte heller ingått i litteraturstudierna.

[1] Se avsnittet ”GNSS – Global Navigation Satellite System” på sidan 11

2. Position, navigation och tid

Alltsedan den första sovjetiska Sputnik-satelliten och byggandet av det amerikanska Transit-systemet så har mänskligheten med en allt ökande precision kunnat positionera och navigera sig på jordens yta.

Positioneringsteknologin bygger i grunden på att mottagaren parallellt tar emot kodade signaler från flera satelliter, oftast av ett minimum på fyra stycken. Ur signalerna kan mottagaren bestämma avståndet till satelliterna samt få information om satelliternas positioner. Med hjälp av dessa två variabler kan man bestämma sin egen position, efter latitud, longitud, altitud och tid, givet att man har signaler från minst fyra satelliter.

I stort sett alla program som körs på en dator idag använder maskinens inbyggda klocka på något sätt. Operativsystemet använder klockan till att fördela processorns kraft mellan olika program som körs. Varje gång en fil skapas får den en tidsstämpel som måste vara mer eller mindre exakt beroende på vad filen ska användas till. Nästan alla kommunikationssätt datorer använder för att kommunicera styrs på något sätt av tid eller definierade tidsintervall. Varje gång en dator eller ett system sätts i skarp drift är det därför viktigt att ställa sig frågan om det aktuella systemet är beroende av tid på något sätt. Om svaret är ”ja” måste analysen gå vidare med att kartlägga vilka felmarginaler som kan tillåtas och säkerställa att den tidskälla som används klarar av att leverera tillräcklig noggrannhet. Och viktigast av allt – vad händer om tidskällan slutar fungera?

2.1 Absolut tid vs synkroniserad tid (sann vs korrekt tid)

Ibland är det viktigt att den *absoluta* tiden är korrekt. Vid till exempel brottsutredningar vill man kunna knyta en händelse från en övervakningskamera till en exakt tidpunkt. Ett annat exempel är biltullar där den loggade tiden för bilens passage måste stämma överens med verkligheten.

Andra gånger är det viktigare att tiden på två datorer eller system överensstämmer. Det spelar kanske inte så stor roll om det inte är absolut rätt tid så länge de båda systemen har exakt samma fel. Om två system har samma tid är systemen *synkroniserade*. Även noggrannheten i tid är viktigt liksom att tid alltid går framåt. Ett exempel är händelser som inträffar vid tidpunkter som sammanfaller mycket nära varandra. Tre stycken händelser inträffar vid tidpunkt A, B och C (i nämnd ordning). För att man ska kunna veta detta måste dels upplösningen på tiden vara större än det minsta tidsintervallet mellan händelserna och dels måste tiden hela tiden öka (så att tidsstämplar för A, B och C i ordning är vid senare tidpunkter).

I många *realtidssystem* är det just synkroniseringen som är det viktiga. Synkronisering kan vara svårt i geografiskt distribuerade system. Om två

datorer befinner sig hundratals mil från varandra är det inte helt enkelt för de att synkronisera sina klockor. En tänkbar lösning är att datorerna då och då skickar aktuellt tid till varandra. Problemet med detta är att det tar en viss tid för en sådan synkroniseringssignal att skickas över till exempel internet. Framför allt är tiden för signalens färd ofta omöjlig att beräkna eftersom det bland annat beror på hur belastat nätet är för tillfället och vilka fördröjningar som därför uppstår. Det finns system som erbjuder mer precis tidsdata över internet, exempelvis IEEE1588 (PTP) och SyncE. Ett exempel på när varken sann eller korrekt tid förekom var under mordutredningen på Anna Lindh. Vid utredningsarbetet användes 21 övervakningskameror för att följa gärningsmannen. Det var olika tid på samtliga och felet var mellan trettio minuter och tre dygn. I detta fall gick man ut till de som hade sett gärningsmannen på varuhuset och begärde att få in kvitton från kassorna, som hade en mer korrekt tid. Sedan identifierade man köparna på filmen och kunde därmed fastställa en mer korrekt tid på filmen. Allt detta bidrog till en fördröjning i utredningsarbetet. Fördröjningen hade kunnat undvikas om kamerorna hade haft någon form av synkroniserad, spårbar tid.

Förenklat kan sägas att korrekt tid innebär samma tid på alla datorer inom ett system inom en definierad tidsram för systemets verksamhetskrav.

2.2 Svensk normaltid

I Sverige föreskriver regeringen i förordningen SFS 1979:988 ”Förordning om svensk normaltid” att den för tidsangivning inom landet gällande tiden (svensk normaltid) ska vara den av Bureau International de l'Heure fastställda normaltiden Temps Universel Coordonnué (UTC) ökad med en timme. Fysiskt realiseras denna vid Sveriges Tekniska Forskningsinstitut (SP), i Borås och benämns UTC (SP).

2.3 Synkronisering

För att vissa funktioner i samhället ska kunna fungera, behövs någon form av synkronisering av tid och/eller frekvens. Där man har ett operativt perspektiv har man oftast krav på synkronisering av tid och vid till exempel drift av elnät har man behov av synkronisering av frekvens. För exempelvis. digital kommunikation behövs synkronisering av tid/fas och frekvens (tillsammans: takt). Hur exakt synkroniseringen behöver vara, bestäms av vilken tjänst eller samhällsfunktion man avser.

2.3.1 Tidsynkronisering

Persontransporter som tåg och buss har typiskt en minuts noggrannhet i sina tidtabeller. Om en passagerare kommer en minut för sent till bussen, vems klocka går egentligen rätt, bussbolagets eller passagerarens? För detta exempel krävs det kanske inte så hög tidsnoggrannhet, men tiden relativt en referenstid måste finnas. Andra exempel där det är önskvärt eller krävs en spårbarhet mot en referenstid, är där man har ett operativt perspektiv, till exempel inpasseringssystem/skalskydd, it-forensik, kassautrustning och andra finansiella funktioner (exempelvis högfrekvenshandel med aktier).

I finansiella system så krävs det betydligt noggrannare tidsynkronisering och även spårbarhet mot en referenstid, enligt finansiella sektorns riktlinjer. I USA har vissa finansiella organisationer egna atomur för att helt säkerställa att de har en sann och korrekt tid, vilket bland annat uppmärksammas i en rapport från *United States Government Accountability Office* till den amerikanska kongressen 2013.

2.3.2 Atomuret – en potent takthållare

Tekniken bakom atomur går ut på att mäta tid efter resonansfrekvensen hos atomer där dessa med hjälp av strålning laddas upp till att nå sina övergångstillstånd för att sedan laddas ur och falla tillbaka till sitt grundtillstånd. Denna pendling mellan olika tillstånd avger ett konstant energiöverskott vilket i sin tur kan avläsas som en konstant frekvens. Med denna konstanta frekvens går det således att få en ytterst hög mätsäkerhet av tid, ett exempel är atomuret ”NIST-F1” i Colorado, USA, som varken får eller tappar 1 sekund i noggrannhet på 100 miljoner år.

2.3.3 Frekvenssynkronisering

Tid och frekvens eller frekvenssynkronisering är extremt viktig i dagens samhälle. Synkroniserade nät möjliggör en högre datahastighet i kommunikationsnät, jämfört med en asynkron motsvarighet. De flesta av systemen som används för elektronisk kommunikation måste vara synkroniserade i frekvens för att fungera inom ett operatörsområde, mellan operatörer och för att kommunicera utanför landets gränser. Frekvenssynkroniseringen för de flesta större digitala kommunikationsnät (transmissionsnät) görs genom en extra kanal med en klockpuls (takt).

Frekvensnoggrannheten för dessa system är specificerad i ett antal olika standarder. Sveriges Tekniska Forskningsinstitut (SP) slår fast i sin rapport ”*Korrekt tid och säker tidsangivning*” att då noggrannheten avviker från specifikationen kommer kvaliteten på kommunikationen att successivt försämras för att till slut upphöra helt. Om frekvensen på klockpulsen i sändare respektive mottagare skiljer sig åt, så kan mottagaren inte läsa av meddelandet på ett korrekt sätt och ett så kallat bitfel uppstår. Ofta innehåller protokollen någon form av felrättande funktioner och det finns även möjlighet att sända om meddelandet. Detta sänker dock den möjliga datahastigheten på förbindelsen.

Om noggrannheten på synkroniseringen försämras kan det, beroende på hur systemet för frekvenssynkroniseringen är uppbyggt, handla om minuter upp till timmar och dygn innan kommunikationen försvinner. Det är oftast inte trivialt att få igång synkroniseringen igen. Exempelvis fungerar mobiltelefonnäten bara då basstationerna får rätt tid och frekvens från en central källa. Om källans tid och frekvens fluktuerar så kommer näten att börja tappa samtal och till sist går det inte alls att ansluta.

. För att uppnå en tillräckligt noggrann frekvenssynkronisering finns det en mängd tekniska lösningar, allt ifrån användande av olika typer av frekvensnormaler till att hämta frekvens direkt från till exempel GNSS. Att enbart förlita sig på GNSS som källa ger dock upphov till vissa risker vilket beskrivs senare i detta dokument.

3. Distribution av position-, navigation- och tidsdata – NTP och GNSS

3.1 NTP – Network time protocol

NTP eller Network Time Protocol är ett protokoll för att synkronisera tiden i ett nätverk med varierande svarstider. NTP använder Internetprotokoll (IP) med UDPsom sitt transportskikt.

NTP är uppbyggt hierarkiskt för att skapa bättre kommunikation och det systemet är benämnt ”clock strata”. Dessa strata finns i flera nivåer och för varje nivå minskar exaktheten något. 0 utgör den högsta nivån av exakthet. För NTP version 4 är den maximala strata nivån 16.

Stratumnivåer
Stratum 0 är enheter så som atomur, GPS-klockor och andra former av radiobaserade klockor. Detta är högsta nivån i hierarkin

Stratum 1 kallas även för primära NTP servrar. Stratum 1 servrar hämtar sin tid direkt från stratum 0-enheter via direktkopplingar, så som RS-232 eller radiokommunikation via GNSS.

Stratum 2 kallas även för sekundära NTP servrar. Dessa hämtar sin tid från stratum 1 servrarna, det vill säga från de primära servrarna.

Stratum 3 hämtar sin tid från stratum 2 servrar och fungerar på samma sätt som en stratum 2 server i övrigt. Andra servrar kan i sin tur hämta tid från en stratum 3 server.

För varje nivå minskar exaktheten något, dock knappt märkbart för normal användning.

3.2 GNSS – Global Navigation Satellite System

Global Navigation Satellite System, GNSS; är ett samlingsnamn för de olika satellitnavigeringssystem som använder sig av signaler från en konstellation av satelliter eller markbaserade fasta punkter (pseudosatelliter) som fungerar som stödsystem till stelliterna ovan. GNSS är, förutom position- och navigationsdistributörer, i princip atomur i rymden. Atomklockorna ombord på satelliterna synkroniseras var tolfte timme mot en referenstid och håller en noggrannhet på under 1ns. Satellitnavigeringssystemet, som består av ett stort antal satelliter, skickar via radio ut PNT-data till den allt mer växande mängden mottagare nere på jorden.

Det mest kända satellitnavigeringssystemet är GPS – Global Positioning System, som drivs av US Air Force och finansieras av det amerikanska

försvarsdepartementet, men det finns också andra, såsom ryska GLONASS, kinesiska Beidou/Compass och det EU- och European Space Agency-finansierade, Galileo. Då GNSS har en tidsangivelse som är väldigt exakt och en GNSS-mottagare kan köpas för några enstaka hundralappar, så har det blivit väldigt vanligt att många tjänster använder sig av GNSS-tid istället för att ha egna atomur eller annan tjänst för tid- eller frekvenssynkronisering.

Positionering och navigation
Med hjälp av GNSS-systemet ovan går det i dagsläget att positionera och navigera sig över i princip hela jordytan. Systemets tidsnoggrannhet gör det möjligt att med stor exakthet (~m) bestämma vid vilken position en mottagare befinner sig. För ytterligare noggrannhet (~cm) behöver man även använda de markbaserade fasta punkterna. Ett exempel på sådana fasta punkter är stationerna i Lantmäteriets system SWEPOS.

Tid och frekvens (takt)
För tidsynkronisering är det, med lämplig mottagare, möjligt att uppnå en högre noggrannhet, med ett maximalt tidsfel på ~10-20ns.

3.3 Kombinerade lösningar – där de två systemen möts

Tid kan således distribueras på flera olika sätt där de vanligaste sätten är via nätverk (NTP) eller via radio (GNSS). Men det finns även möjligheter att kombinera och integrera dessa system. Ibland används exempelvis kombinerade lösningar där en tidskälla tar emot tid från GNSS och sedan distribuerar tiden via NTP.

4. Identifiera krav och beroenden

Innan åtgärder för att säkerställa tillförlitligheten hos PNT-data implementeras eller beslut tas för val av lösning för tid- och frekvenssynkronisering måste krav och beroenden identifieras och klassificeras. Krav och beroendearbetet ska styras av resultatet utifrån en verksamhetsanalys.

Följande scenarior kan ge exempel på vilka krav som kan anges på tid- och frekvenssynkronisering och ge en referensram för hur tidsberoende olika typer av it-system är:

Scenario 1: tid- och frekvenssynkronisering med noggrannhet på c:a 1 sekund (s) till 1 minut
Vissa it-system som använder speciella autentiseringsfunktioner eller ramverk har tidskrav på att servrar och klienter måste arbeta inom vissa tidsramar för att systemen ska kunna kommunicera. I exempelvis en klassisk, distribuerad datormiljö av typen DCE (Distributed Computing Environment) ligger tidskravet på mellan 1 – 10 sekunders tidsdifferens. Är det för stor differens mellan två kommunicerande noder får en part inte ansluta. Generellt kan det sägas att ju högre känslighetsgrad på informationen desto kortare tidsdifferens mellan klient och server kan accepteras.

Scenario 2: tid- och frekvenssynkronisering med noggrannhet på c:a 100 ms till 1 s
Inom detta intervall ligger bland annat krav på loggservrar för it-system och vissa finansiella transaktioner.

Scenario 3: tid- och frekvenssynkronisering med noggrannhet på c:a 1 ms till 100 ms
I den dominerande standarden för kommunikation i kraftanläggningar, IEC 61850, föreskrives att i princip samtliga kraft- och kommunikationskomponenter ska vara synkroniserade med krav på exempelvis under 4ms noggrannhet för relän/brytare och 1µs noggrannhet för mätning av spänningskarakteristik. Det senare exemplet faller utanför scenario 3.

Scenario 4: tid- och frekvenssynkronisering med noggrannhet på c:a 1 ms och lägre
I detta segment ligger bland annat tidsynkroniseringskrav på frekvenssynkronisering i eldistributionsutrustningar, tidssynkroniseringskrav mellan basstationer i mobila datanätverk och mellan basstationer och terminal samt synkron datakommunikation.

5. Riskkällor och metoder för att störa ut korrekt position-, navigation- och tidsdata

5.1 Uppkomsten av störd eller felaktig PNT-data

Att ha system och tjänster som bygger på tillförlitlig PNT-data är att förlita sig på en kedja av olika tekniker där var och en har en uppsättning risker och sårbarheter. Vissa risker är knutna till naturfenomen och dess inverkan på hårdvara medan andra uppkommer från ett antagonistiskt hot med tillgång till störningsteknik. Nedan följer en uppdelning mellan de två olika distributionssystemen, som gicks igenom i tidigare avsnitt, och deras respektive risker och sårbarheter.

5.2 NTP

NTP är framförallt känsligt för ”man in the middle” attacker om inte datapaketen som innehåller NTP-data är kryptografiskt signerade. Denna funktion finns i version 4 av NTP men tyvärr är denna signering rätt processorkrävande och kan vara opraktiskt på vissa tidsservrar som fördelar tid till många mottagare.

5.3 GNSS

Generellt kan det sägas att satellitkommunikation, såsom den som sänds ut från satelliterna i GNSS, har väldigt låga signalnivåer. Det medför att mottagarna måste vara väldigt känsliga och även ha relativt fri siktlinje mot satelliterna. Man kan säkerställa att antennen har fri siktlinje mot tillräckligt många satelliter i fasta installationer men för mobila enheter kan skymmande föremål göra att man inte kan ta emot signaler från tillräckligt många satelliter. Ett resultat av detta är svårigheten att ha tillförlitlig position i stadsmiljöer då höga hus blockerar kommunikationen.

Då signalnivåerna är låga, så kan även störningar från andra signalkällor vara ett problem. Vid en militärövning i bukten utanför San Diego 2007 råkade den amerikanska flottan störa GPS-signalerna för ett stort antal användare i stadens hamn. Kombinationen av generellt sett svaga GPS-signaler och flottans oavsiktliga störningssignaler fick därför en omfattande inverkan på hamnområdet i staden.

Risker – oavsiktliga

Naturliga risker
Förutom fysiskt skymmande föremål så är det främst solstormar som kan påverka GNSS. Solstormar är samlingsnamnet för de kraftiga utbrott av strålning och plasma som kastas ut från solen och kan påverka jordens

magnetfält och jonosfär. Detta kan i sin tur påverka den rymdbaserade infrastrukturen och samhällsviktig verksamhet på jorden.

Jonosfären
Det övre lagret av jordens atmosfär joniseras av strålningen från solen och rymden och kallas jonosfären. Då solstormar uppkommer kan jonosfären bli så pass joniserad att satellitsignaler som måste passera genom atmosfären störs ut, beroende på signalfrekvens. När intensiva solstormar har träffat jorden har man t.ex. noterat total förlust av GNSS-signaler.

Utslagna satelliter – påverkan av rymdvädret/solstormar
Solstormar kan även skada själva satelliten på flera olika sätt och förkorta satellitens livslängd eller i värsta fall slå ut den permanent. Laddade partiklar kan skada satelliter både utvändigt och invändigt, vilket kan leda till störning i data, falska kommandon och komponentskador. Det kan även skada satelliters solpaneler. Vidare, kan en kraftig solstorm orsaka att jordens atmosfär expanderar, vilket kan störa omloppsbanan för främst LEO-satelliter (low earth orbit) samt leda till försämrad kontakt med satelliter och därmed övervakningen av deras position. Även om effekterna från en kraftigare solstorm skulle kunna få svåra konsekvenser så ska det poängteras att sådana stormar uppskattas uppkomma ungefär en gång på 100 år, risken är relativt sett mycket låg.

Risker – avsiktliga
Det krävs inte speciellt höga sändareffekter för att kunna överrösta GNSS-signaler. De avsiktliga riskerna kan delas in i två huvudgrupper:

- **Störning**, överrösta alla GNSS-signaler med en stark brussignal så mottagaren tappar kontakten och position och tidsinformation kan då inte bestämmas.

- **Spoofning** (förfalskade signaler), samla in och modifiera GNSS-signaler som sedan sänds ut med aningen högre signalstyrka än original GNSS-signalerna, mottagaren tror då automatiskt att dessa signaler är korrekta och kommer då att acceptera dessa signaler som äkta.

Störning är enkelt att åstadkomma men är också enkelt att detektera då signalen skiljers sig från en normal GNSS-signal. Spoofning är svårare att åstadkomma men är mycket svårt att detektera då signalerna ser ut som riktiga GNSS-signaler men är falska och har en aning högre styrka än de riktiga.

Störningar
Störning utmärker sig som den enklare varianten av de två avsiktliga riskerna med GNSS. Detta tar sig till utryck i bland annat dagens lättillgänglighet av teknisk störutrusning av GNSS-signaler. I skrivande stund kan man i Sverige köpa mobil störutrustning för GPS för ca 800 sek och från andra EU-länder för ca 400 sek. Dessa exemplar är effektiva inom 10-500m radie, beroende på omgivningen. Det finns även ritningar tillgängliga på internet, där man själv kan montera in förstärkare med lämplig effekt beroende på hur stort område man vill störa.

I november 2009 upptäckte den amerikanska luftfartstyrelsen FAA återkommande, GPS-relaterade störningar i anslutning till Newarks flygplats i New Jersey (nära New York City). Det tog runt 18 månader och en omfattande arbetsinsats för att lokalisera störningarna till en billig, liten störsändare i cigarrettändaruttaget hos ett lastfordon som regelbundet passerade på en motorled utanför flygplatsen. Föraren använde störsändaren för att blockera arbetsgivarens positioneringssystem. I USA tycks dessa utrustningar (PPD, personal privacy device) ha blivit vanliga i takt med att fler och fler åkerier och andra företag skaffat spårningsutrustning för att hålla kontroll över sina fordonsflottor (och anställda) och förbättra sina logistikflöden. Detta kan tjäna som ett exempel på en allvarlig kaskadeffekt av att avsiktligt försöka störa ut GNSS-signaler.

Sedan incidenten på Newark har amerikanska Department of Homeland Security (DHS), via programmet Patriot Watch med syfte att identifiera, analysera, lokalisera och hantera GPS-störningar, utplacerad sensorutrustning i anslutning till flygplatsen. Men det förändrar inte det faktum att det fortfarande är mycket enkelt att störa GPS-mottagning genom billig och lättillgänglig teknik.

DHS uppgav på en konferens i USA i oktober 2013 att en enda välplacerad GPS-utrustning för störning eller spoofing skulle kunna slå ut GPS-signaler i en hel region i USA, samtidigt som landet fortfarande inte har någon förmåga att snabbt upptäcka och lokalisera sådana störsändare. En företrädare för ett branschföretag uppskattade i anslutning till samma konferens att det skulle räcka med en uteffekt på 1 watt för att skapa problem i en medelstor stad.

Det finns även exempel på störningar i GPS-beroende system som har rent tekniska orsaker. En av de mest välkända incidenterna i Sverige av detta slag är störningen i Minicall-nätet i slutet av 2006 och början av 2007. Ett tekniskt problem relaterat till mottagningen av satellitsignaler ledde till att lokalt utplacerade GPS-mottagare fick bytas ut över hela sändarnätet för Minicall. Arbetet tog närmare en månad att genomföra, eftersom många sändare satt otillgängligt till i anslutning till sändarmaster och vinterklimatet i stora delar av Sverige gjorde utbytet svårt.

Spoofing –förfalskade signaler

Spoofing/förfalskade signaler är måhända ett mer avancerat alternativ än ”vanliga” störningar av GNSS-signaler men genererar i sin tur större möjligheter för den potentielle antagonisten.

Mjukvarubaserad radio är ett exempel på en teknik som kan användas för såväl störning som spoofing/förfalskade signaler. Tekniken går ut på att den logiska delen av en radio definieras och kontrolleras i mjukvara, i likhet med en vanlig dator. Hårdvarudelen kan vara ett externt kort, som ofta kopplas via USB till datorn. Begränsningen på frekvensomfång som dessa radiosystem kan hantera är endast begränsat till den externa hårdvaran. I dagsläget kan ett sändtagare-kort inköpas för c:a 3000 sek med ett frekvensomfång från 50 MHz till 6GHz. Dyrare så kallade USRP (Universal Software Radio Peripheral) klarar ett mycket bredare frekvensomfång. USRP finns även som ethernetanslutna enheter som styrs via ett nätverk. Då den logiska delen definieras och styrs i

mjukvara kan dessa radiosystem användas för nästan alla tänkbara radiosystem inklusive GNSS-mottagare och sändare.

Ett exempel där spoofing använts är den 8 december 2011 då iranska medier publicerade bilder på en erövrad US RQ-170 Sentinel-drönare. Drönaren, vars användningsområde är övervakning, hade inte skjutits ned utan med hjälp av spoofing tvingats landa hos iranierna. Genom att först störa ut GPS-navigeringssystemet ska man ha tvingat drönaren att växla till autopilot. Väl i autopilot-läge tog iranierna till spoofing för att ”lura” drönaren som i sitt sökande efter sin hemmabas istället kom att landa någon helt annanstans. Istället för att försöka ta sig in i själva kontrollsystemet av drönaren kunde man med spoofing ange precis altitud- samt longitud- och lattuttiddata för att ge drönaren sin nya landningsposition. Drönarens beroende av positionsangivelse från GNSS-teknik visade sig således vara en avgörande svaghet.

6. Möjliga åtgärder

Framförallt störningsområdet kännetecknas således av en asymmetrisk hotbild, billig och lättillgänglig utrustning samt att det går att operera med relativt liten risk för upptäckt. Men det finns tekniker för att upptäcka störningsförsök som tas fram och undersöks.

FOI (Totalförsvarets forskningsinstitut) har exempelvis utvärderat olika sätt att detektera störsignaler i de frekvensband som används inom GNSS, där själva störsignalen är okänd. I en kombination av att mäta mottagen energi och avsändarens *carrier-to-noise ratio* kan många olika typer av störsignaler upptäckas.

Ytterligare exempel på initiativ för att säkra infrastruktur i beroende av GNSS är SENTINEL-projektet. Projektet ska med hjälp av IDM-sensorer (Interference, Detection & Mitigation) upptäcka störningar kring infrastruktur och utrustning som använder GNSS för att på sikt åstadkomma en större trygghet för aktörer som förlitar sig på systemet. Utöver dessa initiativ finns det både generella och tekniska åtgärder som kan vitas redan nu för att för att säkra användandet av PNT-data och beroendet av exempelvis GNSS.

6.1 Förslag på generella åtgärder

Med fokus på tidsberoendet så är ett första steg att analysera huruvida verksamheten har, och då om den verkligen behöver ha, tid- eller frekvenssynkronisering. Målet bör vara att inte använda tid- eller frekvenssynkronisering om det inte behövs. För att säkerställa korrekt synkronisering, när detta väl behövs, bör minst en alternativ källa existera, källan bör även vara spårbar, för tid och/eller takt. Nedan följer några generella förslag på åtgärder för att åstadkomma större säkerhet kring användandetav PNT-data och GNSS-teknik.

Medvetandegör
Skapa medvetande inom organisationen om GNSS-beroende och vilka möjliga problem detta kan innebära.

Inventering och identifiering
Inventera alla system och tjänster och identifiera vilka av dessa system och tjänster som har ett tid- eller taktberoende oavsett om det är direkt eller indirekt beroende.

Klassificering
Klassificera systemen eller tjänsterna utifrån de krav på hur noggrann tid och takt de behöver för att kunna fungera och leverera enligt kravspecifikationen.

Upphandling
Säkerställ att vid upphandling av system och tjänster att hänsyn tages till tid- och frekvenssynkronisering i upphandlingsdokumentationen. Vilken

synkroniseringsnoggrannhet som systemen eller tjänsterna har eller behöver måste framgå i dokumentationen.

Leverans
Säkerställ att vid leverans av system eller tjänster ska kraven på tid- eller taktsynkronisering efterlevas och/eller uppfyllas.

Förvaltning
Säkerställ att kraven på tid- och taktsynkronisering för systemet eller tjänsten efterlevs under hela livstiden. Detta görs lämpligen genom att föra in verifikationskrav i verksamhetens processer.

6.2 Förslag på tekniska åtgärder

Undvik singulärt beroende
Att förlita ett kritiskt tids- eller positionsberoende på endast en informationskälla är inte att rekommendera. Använd minst 2 oberoende informationskällor och säkerställ att det finns processer/rutiner/funktioner för att verifiera informationen mot varandra. Ett annat alternativ är att inhämta referenstid från en extern källa via fiberoptisk kanal.

Exempel:
I vissa it-system som är avskilda från externa tidskällor så används flera tidsservar, minst tre stycken, den systemtid som sedan nyttjas i it-systemet röstas fram genom att en funktion på dessa tidsservrar flera gånger i timmen kontrollerar tider och ett medelvärde mellan de tidsservrar som har minst tidsdifferens accepteras och synkroniseras framåt i tiden. Om en tidskälla ligger utanför ett accepterat tidsintervall kopplas denna bort ur röstningsförfarandet och en manuell åtgärd måste genomföras av en administratör för att hantera detta.

Att ha ett antal egna atomklockor, som synkroniserar mot till exempel UTC (SP) är också ett alternativ som ytterligare ökar robustheten. Kostnaderna för atomklockor är relativt höga jämfört med GNSS och referenstid från extern tidkälla via fiberoptisk kanal och är därmed rimligen förbehållet större aktörer som har väldigt höga krav.

Hybridlösning av multipla tidkällor
Ofta är en hybrid lösning med multipla tidskällor att rekommendera, exempelvis GNSS-baserad tjänst verifierad av en eller flera oberoende NTP-källor.

Lösning vid endast GNSS-tidkälla
I vissa fall är GNSS-baserade tjänster det enda alternativet (exempelvis långt ut i ödemarken och/eller med en begränsad budget)och ett atomur kan inte komma på fråga.. GNSS-lösningen måste designas och implementeras så robust som möjligt, med exempelvis flera diversifierade antenner och differensanalys av GNSS-signaler från dessa antenner och mottagare. Detta för att försvåra insändning av störsignal eller spoofnings signal med riktad mottagarantenn. Det existerar redan kommersiella lösningar för detta.

Tjänster och stöd i Sverige

För den nationella tidskalan i Sverige ansvarar som tidigare nämnt SP Sveriges Tekniska Forskningsinstitut.. Den nationella skalan betecknas UTC (SP) och SP tillhandahåller flera olika typer av tjänster för att man ska kunna synkronisera mot UTC (SP). Exempelvis har man öppet tillgängliga tidsservrar utplacerade vid vissa svenska internet-knutpunkter. Redan idag är tjänsterna robusta, men i samarbete med Netnod och PTS pågår arbete för att vidareutveckla systemet. Vidareutvecklingen beräknas vara klar under 2015. De tid- och frekvenstjänster som tillhandahålls av SP i samarbete med PTS och Netnod är i dagsläget troligen de mest robusta som finns i Sverige. Användning av dessa tjänster bör övervägas för samtliga samhällsviktiga verksamheter och de tjänster verksamheterna har ett beroende av.

Lantmäteriet tillhandahåller en tjänst, jonosfärsmonitorn, som visar vilken störningspåverkan jonosfären har på GNSS-signaler för fyra olika delar av Sverige. Denna kan vara ett stöd främst vid felsökning.

7. Framtiden

Vad framtiden håller för möjligheter och risker är som alltid svårt att säga någonting om men som detta dokument pekat på så är användningen av och beroendet till GNSS inte utan risker. Som alla beroenden medför GNSS-tekniken en potentiell risk mot det moderna samhället. Allt tyder på att beroendet av GNSS kommer att öka i samhället framöver.

Även om den framtida utvecklingen är viktig att ta med i beräkningen, så framstår ändå det största problemet att vi redan idag har stora beroenden som måste identifieras och eventuellt åtgärdas. Elsektorn är en sektor som redan nu beröras av denna problematik när den lutar sig allt mer på tid- och frekvenssynkronisering, men där Svenska Kraftnät arbetar aktivt för att begränsa beroendet.
Elsektorn är på väg att implementera en ny typ av elnät, som ska vara smartare och kunna utnyttja det befintliga elnätet på ett effektivare sätt. I dagsläget finns redan så kallade smarta elmätare som regelbundet meddelar såväl kundens aktuella energiförbrukning till elnätsägaren som aktuell kostnad till kunden - allt för att inblandade parter skall kunna planera sin produktion, distribution och konsumtion på ett så optimalt sätt som möjligt.. Mätarna är bara första steget mot ett ännu mer automatiserat elnät, som i princip kommer ha ett kommunikationsnät parallellt med elnätet. Kommunikationsnätet används tillexempel för att läsa av mätdata och styra komponenter.

I scenario 3 (se ovan avsnitt) av identifierade krav och beroenden, beskrevs standarden för kommunikation i kraftanläggningar, IEC 61850, där det är höga tidssynkroniseringskrav. För att säkerställa funktionen, måste elnätet ha en tid- och frekvenssynkronisering som inte är ensidigt beroende av GNSS. Skulle det vara ett ensidigt beroende av GNSS så riskerar man att, vid ett bortfall av GNSS, tappa kommunikationen med komponenterna och därmed styrningen av elnätet. Detta kan i sin tur leda till förstörda komponenter samt stora avbrott, med konsekvenser både i tid som vad avser geografisk spridning.

Utöver detta måste systemen som kontrollerar elnäten även vara säkrade mot obehörig åtkomst.

8. Slutsatser

Givet de olika avsiktliga eller oavsiktliga störningsmöjligheter som existerar, så bör framför allt samhällsviktiga funktionerna, inte ha ett ensidigt beroende av GNSS-baserade tjänster. Främst gäller det tid- och/eller frekvenssynkronisering men även positioneringsberoendet bör beaktas. Detta gäller framför allt de egna tjänster och funktioner man använder sig av och tillhandahåller, men även för de tjänster och funktioner som annan part levererar.

Med avseende på tid- och frekvenssynkronisering är ofta en kombinationslösning med multipla tidskällor att rekommendera, exempelvis en GNSS-baserad tjänst verifierad av en eller flera oberoende NTP-källor.

Det finns ytterligare exempel på höjandet av robusthet och säkerhet vid ett beroende av tidsdata. Vissa sektorer har till exempel valt att inte använda GNSS primärt: I USA har vissa finansiella funktioner primärt börjat nyttja egna atomur, med intern tidssynkronisering för de egna tidsberoende tjänsterna. GNSS-tjänster används i dessa fall endast sekundärt.

I slutändan är det ändå det förebyggande arbetet som har störst chans att säkra en verksamhets kontinuitet när det kommer till användandet och beroendet av PNT-data med de tillhörande givande och distribuerande systemen.

Underlag:

40th Annual Precise Time and Time Interval (PTTI) Meeting: "*Global Positioning System Timing Criticality Assessment– Preliminary Performance Results"* -Av James Carroll och Kirk Montgomery

"Extreme Space Weather—A Report Published by the UK Royal Academy of Engineering." *Space Weather* 11.4 (2013): 138-139 Av: Cannon, Paul S.

"Fortsatta störningar på Minical" Publicerad på Säkerhet, Tech World *16-01-2007*:
http://sakerhet.idg.se/2.1070/1.91915 Hämtad: 2014-09-12

"*GNSS interference detection*". rapport från FOI, av Erik Axell, 2014

"*GNSS och störningstålighet*" – Presentation av Chalmers/ SP (Sveriges Tekniska Forskningsinstitut)

"GPS Jammers Could Knock Out Signals in a Medium-Sized City" Publicerad på Nextgov 19-09-2013:
http://www.nextgov.com/defense/2013/09/gps-jammers-could-knock-out-signals-medium-sized-city/70582/ Hämtad: 2014-09-12

"*Homeland Security Studies Risks to GPS, Prompts Spoof-Proof Receiver Proposal*" Publicerad på InsideGNSS 10-11-2011:
http://www.insidegnss.com/node/2824 Hämtad: 2014-09-16

"*NIST-F1 Cesium Fountain Atomic Clock: The Primary Time and Frequency Standard for the United States",* National Institute of Standards and Technology:
http://www.nist.gov/pml/div688/grp50/primary-frequency-standards.cfm
Hämtad: 2014-11-05

Rapport 2005:12 *"Korrekt tid och säker tidsangivning "* Av SP (Sveriges Tekniska Forskningsinstitut)

Report to Congressional Requesters: "*GPS Disruptions Efforts to Assess Risks to Critical Infrastructure and Coordinate Agency Actions Should Be Enhanced",* United States Government Accountability Office, November 2013

"Risk- och sårbarhetsanalys för sektorn elektronisk kommunikation 2013" Av Post- och telestyrelsen

"Risker och förmågor 2013, nationell risk- och förmågebedömning" Av MSB

"Spårbar tid och frekvens - Perfekt tajmat", bilaga 5 i SOU 2007:97 - "Vissa metrologifrågor".
The Christian Science Monitor 15-12-11: "Exclusive: Iran hijacked US drone, says Iranian engineer": http://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer-Video Hämtad: 2014-09-11

"*Time and Frequency Transfer using Passive Techniques in Active Fiber Optic Networks*" – Avhandling av Sven-Christian Ebenhag

"*Vad händer med tiden*?" Av Jörgen Städje, publicerad på Sweclockers.com: http://www.sweclockers.com/artikel/18531-helglasning-vad-hander-med-tiden Hämtad: 2014-09-12

Som ytterligare underlag till detta dokument ligger 2013 års resultat från 2012 års risk- och sårbarhetsanalyser med tillhörande "*störningar i GNSS*"-scenario.

Vidare läsning

"Global Navigation Space Systems: reliance and vulnerabilities" Av The Royal Academy of Engineering, Mars 2011

"NSTAC report to the President on Commercial Communications Reliance on the Global Positioning System (GPS)" Av NSTAC 28-02-2008

"SP passar tiden", K. Jaldehag och P.O. Hedekvist, Elektroniktidningen nr 6 2014, sid 22-24

MSB vill rikta ett särskilt tack till Post- och telestyrelsen, SP Sveriges Tekniska Forskningsinstitut och Netnod för värdefullt stöd.

Myndigheten för samhällsskydd och beredskap
651 81 Karlstad Tel 0771-240 240 www.msb.se
Publ.nr MSB778 – November 2014 ISBN 978-91-7383-508-4