



Vägledning för upphandling av beredskapstjänst för mobil SCADA- kommunikation

TERACOM 
SAMHÄLLSNÄT

*Säker drift & övervakning - även vid allvarliga kriser och under höjd beredskap.
Så här upphandlar du en beredskapstjänst för mobil SCADA-kommunikation.*

KRAVBILD och KONSEKVENSER

Ett skärpt ansvar enligt försvarsbeslutet

Sveriges försvarsbeslut 2025–2030 tydliggör att samhällsviktig verksamhet ska fungera även vid allvarliga störningar, kris och krig, vilket innebär ett tydligt ansvar för verksamheter inom vatten, värme och elproduktion att säkerställa drift och styrning även under mycket påfrestande förhållanden.

Begränsningar vid kriser

När den tekniska SCADA-kommunikationen slutar att fungera innebär det stora konsekvenser för den samhällsviktiga verksamheten. Driftcentralen är ”blinda” och kan inte avgöra om allt fungerar som det är tänkt eller om något måste åtgärdas. Servicetekniker kallas ut i onödan och till fel områden, för att åtgärda fel som kanske inte finns eller som har låg prioritet. Det blir på tok för kostsamt och ineffektivt.

Skärpta regleringskrav

Sverige befinner sig i ett allvarligt och försämrat säkerhetsläge med ett förhöjt terrorhot och ökade hot från främmande makt som söker sårbarheter i ny teknik och kritisk infrastruktur. NIS2-direktivet ställer ökade krav på säkerhet och hindrar främmande makt från att utnyttja svagheter i t.ex. IoT-system, SCADA-kommunikation, fjärrstyrning eller andra OT-miljöer. En nyhet i NIS2 är att styrelse och högsta ledning blir straffrättsligt och administrativt ansvariga vid bristande cybersäkerhet.

Stöd till verksamhetsansvariga och beslutsfattare

Den tekniska kommunikationen mellan anläggningar i fält och drift- eller datacentraler (OT/SCADA) är en avgörande förutsättning för att bedriva verksamheten effektivt och ha kontroll. Samtidigt bygger många verksamheter i dag sin tekniska kommunikation på civila mobilnät som främst är dimensionerade för normaldrift och vanliga konsumenter, vilket vid kris och höjd beredskap ökar risken för trängsel, störningar och bortfall.

Fokus på robusthet och motståndskraft

Mot denna bakgrund har Teracom tagit initiativ till denna vägledning och tillhörande rådgivning. Målsättningen är att ge beslutsfattare och verksamhetsansvariga stöd i hur mobil kommunikation för teknisk SCADA-trafik kan säkras i linje med verksamhetens behov och totalförsvarets krav. Fokus ligger på att upphandla en robust och prioriterad kommunikationstjänst som är byggd för att fungera även under långvariga störningar – inte en standardlösning för normaldrift. Rätt upphandlad bidrar en sådan tjänst till minskad sårbarhet, ökad handlingsfrihet och trygghet i verksamhetens leveransförmåga även i ett allvarligt omvärldsläge.

*Säker drift & övervakning - även vid allvarliga kriser och under höjd beredskap.
Så här upphandlar du en beredskapstjänst för mobil SCADA-kommunikation.*

SÅ HÄR UPPHANDLAR DU EN BEREDSKAPSTJÄNST

1. Problembild – och vad som ska uppnås

När verksamheten har stationer och anläggningar utplacerade i stora geografiska områden är det särskilt viktigt att ha koll på sin tekniska övervakning. En robust uppkoppling och stabil täckning är avgörande för effektiv felsökning. Problem uppstår när den tekniska SCADA-kommunikationen är upphandlad eller införd utifrån en alltför låg kravbild. Teknikvalet har inte fattats i linje med verksamhetens behov och totalförsvarets krav.

- *Publika mobilnät: är byggda för konsumenttrafik med risk för trängsel, bortfall och kort batteridrift.*
- *Fiber: Mycket stabilt lokalt för primära anläggningar, men dyrt och opraktiskt över stora ytor.*
- *Licensfri radio: Begränsad räckvidd och störningskänslig.*
- *Satellit: Bra reserv, men hög latens och saknar nationell rådighet.*

Ett annat problem är att avsaknad av krav på informationssäkerhet, robust och kontrollerbar kommunikation, användandet av publika IP-adresser, trafikseparering, hantering av skyddsvärd information osv. kan öppna en väg in för obehöriga.

Konsekvensen vid SCADA-bortfall eller intrång blir en driftcentral som är 'blind' – felaktiga larm, onödiga utskick, ökade kostnader – och i allra värsta fall stor antagonistisk påverkan på försörjningen av el- och vatten.

2. Så upphandlar du en lösning på problemen – och skyddar din verksamhet

Om er kravbild motsvarar den där samhällsviktig verksamhet ska fungera även vid större störningar, elavbrott, kris, höjd beredskap och krig är rekommendationen att ni upphandlar ”**en beredskapstjänst för mobil SCADA-kommunikation**” – dvs en kraftsäkrad, tillgänglig och säker mobil kommunikation för teknisk SCADA-kommunikation.

Två viktiga principer:

- Upphandla en funktion – inte bara “SIM-kort” eller “abonnemang
- Undvik “stor upphandling av allt” - där SCADA-SIM hamnar i samma paket som telefoni/mobila tjänster för kontorsbruk.

*Säker drift & övervakning - även vid allvarliga kriser och under höjd beredskap.
Så här upphandlar du en beredskapstjänst för mobil SCADA-kommunikation.*

3. Hur man upphandlar – praktisk vägledning i 6 steg

Steg 1: Avgränsa behovet

- Definiera verksamhetens uppgift i kris, under höjd beredskap och krig
- Definiera dimensionerande händelser ("krislägena"): för vilka typer av händelser ska driften kunna fortgå (elbortfall, översvämningar, skogsbrand, stormar, cyberattacker, sabotage) och hur många simultana attacker ska ni klara av
- Definiera driftkrav för krislägena: minsta acceptabla tillgänglighet, ledtider, återställningstid, uthållighet vid elbortfall, försörjningstrygghet tex på drivmedel, externa beroenden som måste fungera tex transporter.

Steg 2: Kravställ utifrån resultatkrav (se Steg 4 och Punkt 4 nedan)

- Definiera mätbara nivåer
- Definiera ska-krav för normaldrift och för krislägena
- Använd utvärderingsfrågor som tvingar fram bevis: referenser, dokumenterade övningar, beskrivna scenarier, vilka mätbara nivåer används

Steg 3: Säkerhets- och jurisdiktionskrav som "hygienfaktor"

- Krav på efterlevnad av säkerhetsskydd, NIS2, GDPR och möjlighet till SUA/säkerhetsskyddsavtal.
- Krav på datahantering: data tillhör Beställaren, behandling/lagring inom Sverige eller EU/EES efter godkännande, ingen tredjelandsöverföring.
- Krav på ISO 27001 eller motsvarande

Steg 4: Utvärdera med viktning som styr mot rätt förmåga

Den leverantör vinner avtalet som uppvisar bästa samlade förmåga att skapa rätt resultat inom:

- Robusthet – tålighet och uthållighet
- Redundans – alternativa vägar/resurser
- Resiliens – återställningsförmåga
- Rådighet – faktisk kontroll över resurser och lågt tredjepartsberoende

Rekommenderad modell:

- Robusthet, Resiliens, Redundans, Rådighet och Intervju viktas med 20% var
- Ska-poäng för skriftliga svar: 0/5/10 för var och en av R-områdena ovan
- 10p = tydlig och trovärdig beskrivning med bevisad lösning/erfarenhet
- 5p = tydlig lösning men saknar bevis i avgörande delar
- 0p = inget/otydligt/motsägelsefullt svar

*Säker drift & övervakning - även vid allvarliga kriser och under höjd beredskap.
Så här upphandlar du en beredskapstjänst för mobil SCADA-kommunikation.*

Steg 5: Genomför Intervju med anbudsgivare

Intervjun ska verifiera fakta – inte vara en "säljpitch". Fokusera på att:

- Verifiera kritiska delar av skriftliga svar (har vi förstått detta rätt?)
- Testa agerande i olika scenarion (hur hanterar ni sabotage, överbelastning?)
- Utlovad förmåga finns i praktiken (har ni bemanning, kedjor, mandat, rutiner?)

Steg 6: Säkra att kontraktet går att följa upp

Planera redan i upphandlingen hur ni ska följa upp t.ex.:

- Årlig beredskapsövning/test, rapportering av incidenter och åtgärdstider
- Revision av säkerhetsarbete, loggning och åtkomstkontroller
- Uppföljning av reservkraftsuthållighet och faktisk täckning i driftlägen

4. Vad som är viktigast för säker kommunikation (prioriteringslista)

Inom varje område kan ni ta fram en prioriteringslista för utvärderingen t.ex.:

- Robusthet:
 - Kraftsäkring/uthållighet -hur många timmar/dygn och hur stor andel av ytan?
 - Hur hanteras separering och prioritering av trafiken?
 - Hur hanteras skydd mot privatkundsbelastning?
 - Hur hanteras logisk separation och APN/VPN/VRF?
- Redundans:
 - Finns diversitet på teknik/organisation
 - Finns diversitet på externa leverantörsberoenden?
 - Finns geografisk diversitet?
- Resiliens:
 - Finns NOC/SOC 24/7, med incidenthantering, återställningsplan?
 - Hur säkerställs snabb återetablering vid större bortfall?
 - Finns beredskapslager, reservdelar, egen reparationsförmåga?
 - Finns kontinuitetsplan, övningar och dokumenterade erfarenheter?
- Rådighet och nationell kontroll:
 - finns låg beroendekedja, försörjningstrygghet tex på drivmedel?
 - finns äganderätt för radiospektrum som används, hur länge?
 - hur skyddas infrastrukturen som används för att leverera tjänsten?,
 - hur säkerställs nyckelkompetens såsom radioplanering, installation, drift och service helt i egen regi och med krigsplacerad personal?

Tumregel för utvärderingen:

- Premiera leverantören som kan visa bevis på förmåga (referenser, driftdata, övningsresultat, dokumenterade processer) – inte den som skriver "rätt ord"
- Verifiera hur uppställda krav på SLA efterlevs - tex att tjänsten som upphandlas kan fortsätta levereras även under höjd beredskap

5. Kompetenser som ska ingå i utvärderingsgruppen

För att utvärdera samhällskritisk mobil SCADA-kommunikation krävs en utvärderingsgrupp som täcker både teknik, drift och beredskap.

Rekommenderad minimibemanning:

- Verksamhetsansvarig (anläggningschef/drift-/servicechef) – prioriteringar, acceptabla tider, operativa konsekvenser.
- OT/SCADA-ansvarig (drift/automation) – vad som är verksamhetskritiskt, krav på latens/tillgänglighet, beroenden i anläggningen.
- Säkerhetsskydd/beredskap (säkerhetsskyddschef/beredskapssamordnare) – skyddsvärden, SUA-förmåga, kontinuitet och SLA under höjd beredskap.
- Upphandlingsansvarig / inköpare (LUF) – process, likabehandling, spårbarhet.

Starka tillägg i bemanningen (ger bättre träffsäkerhet i poängsättningen)

- Informationssäkerhet (CISO/SOC-kompetens) – incident, åtkomst, NIS2, hot-bild.
- IT-infrastruktur/nätverk – IP-nät, VPN, segmentering, driftintegration
- Fält/underhåll/elkraft – reservkraft, uthållighet, praktisk återställning på plats.
- Juridik/avtalsförvaltning – uppföljning, revision, sanktioner, säkerhetsvillkor.
- Säkerhetschef – signalskydd, informationssäkerhet, skydd, kontinuitet, SUA

6. Rekommenderad arbetsform (för att undvika vanliga fel)

- Säkerställ att verksamheten (OT/SCADA/drift) äger kraven – inte enbart IT/inköp
- Involvera säkerhetschef och beredskapssamordnare
- Kräv max 4 A4 per område och utvärdera hårt på "bevis" enligt 0/5/10-skalan.
- Använd intervju enbart för att verifiera risk – inte för att ersätta skriftliga svar.

7. Hur tar du nästa konkreta steg?

Denna vägledning är till för dig som behöver robust, pålitlig och vidsträckt trådlös kommunikation för kritiska funktioner, särskilt där civila mobilnät inte räcker till.

Den visar hur din verksamhet kan säkerställa prioriterad kommunikation mellan dina anläggningar ute i fält och dina centralt placerade driftcentraler och ger en övergripande förståelse för varför säker mobil SCADA-kommunikation är en strategisk ledningsfråga och vilka principer som bör styra en sådan upphandling.

För verksamheter som efter denna inledande vägledning vill gå vidare finns möjlighet till en fortsatt rådgivande dialog med Teracom om hur den egna situationen kan analyseras och hanteras. Kontakta oss gärna: kontakt@teracom.se