Giltig från och med: 2021-04-15

Dokumentägare: Per Ståhle

Västra Götalandsregionen

Fastighet, stöd och service

12897 v.2.0, IT, säkerhetskrav för tekniska IT-system – Tekniska krav

Gäller för bussdepå, folkhögskola, kontor, naturbruksskola, resecentrum, sjukhus, spårvagnsdepå

VÄSTRA GÖTALANDSREGIONEN

Innehållsförteckning

Versionshistorik

Version	Publicerad	Ändringsbeskrivning	Arkiverat
2	2021-04-15	antal mac adresser i vgrit switchar har ädrats	
1	2019-07-30		2021-04-15

Inledning och syfte

Tekniska krav är Fastighet, stöd och service specifika komplement till lagar, förordningar och projekteringspraxis.
Dokumentet ger uttryck för beställarens och verksamhetens krav och önskemål på utförande och utformningar och ska vara ett hjälpmedel vid projektering vid ny-, till- och ombyggnader. I dessa anvisningar anges Fastighet, stöd och service särskilda krav och önskemål, i övrigt gäller AMA.
Dokumentet ska läsas som ett stöd under projektering och användas som underlag vid framtagande av teknisk beskrivning (Utförandeentreprenad enl AB 04) och rambeskrivning (Totalentreprenad enl ABT 06).
Dokumentet ansluter till senaste utgåva av AMA Boverkets Byggregler (BBR), Plan- och Bygglagen (PBL) samt Anvisningar för fastighetsförvaltning (Aff). Hänsyn avseende fysisk tillgänglighet ska beaktas i projektering.
 denna TK gäller för samtliga fastigheter inom beställarens fastighetsbestånd.

En rekommendation är att projektledaren, eller av denne utsedd person, går igenom TK med konsult och berörd teknisk förvaltare/strateg inför uppstart av projektet,

Övriga kravställande dokument

Dokumentet läses tillsammans med gällande projekteringsdokument från Fastighet stöd och service bygg och förvaltning, Fastighet, stöd och service

Allmänt

Definitioner

Tekniska IT-system används som samlingsnamn för datorbaserade system som utför styrning, reglering och övervakning av fysiska processer i fastigheterna.

Andra namn som kan användas för denna typ av system är ”Industriella informations- och styrsystem” (ICS) eller ”Supervisory Control And Data Acquisition” (SCADA).

Exempel på tekniska IT-system är ventilation, kyla, elförsörjning, passerkontroll, kallelsesignalanläggning, brandlarm och rörpost.

DDC (Direct Digital Control) är utrustningar/enheter i systemen som är försedda med analoga/digitala in- och utgångsmoduler (I/O). Exempel på DDC är Central, Nod, DUC och PLC.

VGRNet är Västra Götalandsregionens nätverk.

IT i Västra Götalandsregionen.

Hos Västra Götalandsregionen (VGR) ansvarar VGR IT för IT-drift av den regionala IT-infrastrukturen för Tekniska IT-system. Fastighet stöd och service hos VGR ansvarar för tekniska anläggningar i fastigheten.

Molntjänst

VGR är återhållsamma med användning av internetbaserade molntjänster för tekniska system, då det ofta finns krav på att tekniska system ska fungera i beställarens miljö utan yttre påverkan. För att en molntjänst ska ha möjlighet att bli godkänd att

användas måste först aktiviteter som beskrivs i dokument ”Införande av molntjänst” genomföras. Först därefter tas beslut om molntjänst får användas.

Driftsättning av applikation för Tekniska IT-system

Avser driftsättning av applikation på server eller klientdator. Beställare (VGR) levererar och driftsätter hårdvara så som server och klientdatorer samt nätverkskommunikation. Applikationer ska driftsättas på beställarens hårdvara.

Leverantören ska delta med uppgifter för IT-driftdokument. IT-system ska använda VGRs AD för inloggning. Applikationer och installation av IT-system ska följa VGR:s detaljerade IT-krav

Nätverkskommunikation.

VGR:s nätverk heter VGRNet. Nätet används för alla typer av datakommunikation via nätverk.

IPv6 ska vara avaktiverat för att förhindra att nätverket blir tillgängligt för otillåten åtkomst.
Omvandlare från Ethernet till seriellt gränssnitt innan anslutning av DDC till nätverkskommunikation får inte användas för ny utrustning.
I VGRNet används Säker access. Det innebär att utrustning måste ha VGR giltigt certifikat enligt 802.1x eller vara registrerad med Mac adress hos beställaren för att kunna kommunicera i VGRNet.

Leverantören ska medverka vid framtagande av listor med uppgifter om utrustningen för tilldelning av IP-adresser samt för registrering av utrustning för Säker access.

Härdning av Tekniska IT-system

Leverantören ska i nätverksutrustningar och i Tekniska IT-system härda systemet såsom att stänga av tjänster och funktioner som inte ska användas i den aktuella tillämpningen.
Funktioner, parametrar och tjänster ska vara skyddade mot förändringar. Portar som inte används ska vara stängda.
Default lösenord ska ersättas med av systemansvarig anvisat lösenord.

Operativsystem/applikationer

Nätverksutrustningar (tex HMI, OP/MP paneler, centraler eller DDC) får inte innehålla standard PC-operativsystem utan ska vara konfigurerade för användning i nätverksutrustning.

Exempel på tillåtet operativsystem är Windows IoT LTSC och Windows IoT Core.

Operativsystemet ska inte vara beroenden av regelbunden patchning eller uppdatering. Operativsystem ska vara anpassat för automation samt ska ha EOL > 5 år efter leverans. Leverantören ska installera säkerhetspatchar som släpps under garantitiden.

När DDC eller panel PC innehåller webbserverfunktion tillåts inte Java Applet. HTML5 standard ska i användas i första hand.

Utrustningar får inte innehålla applikation för fjärraccess.

HMI

HMI ska ha funktion för automatiskt viloläge med utloggning och släckt belysning.

Industriswitch

Switchar ska vara i utförande för montage på DIN skena i apparatskåp och i industriutförande.

Managerbara switchar är endast tillåtna om efterfrågad funktionalitet inte går att lösa på annat sätt. I övrigt är managerbara switchar är inte tillåtna.

Managerbara switchar ska konfigureras så att inte fjärrmanagering är möjlig. Switch får inte använda ”Spanning tree protocol”.

Programmering

Programmering av utrustning, DDC, ska utföras med öppen programvara tillgänglig för beställaren.

All projektspecifik programkod och de generella funktionsbiblioteken som använts för att programmera projektet ska ingå i leveransen.

Programkod ska överlämnarnas till beställaren.

Tekniska larm

Det ska finnas redundanta (dubblerade) larmvägar för de fastighetslarm som är kritiska för drift av fastigheten. D.v.s. larm som kräver omedelbar åtgärd för att förhindra att en skada på person eller egendom uppstår. De båda larmvägarna får inte nyttja samma kommunikationsvägar.

Operatörer

Användarbehörigheter ska vara möjliga att förändra utan omprogrammering av nätverksutrustning. Det ska vara möjligt att ta bort samt lägga till nya användare. Beställaren ska från leverantören erhålla de lösenord som krävs för att hantera och ändra funktioner eller program i utrustningen. Operatörshändelser loggas i DDC där minst de senaste 25 händelserna ska kunna avläsas. Nätverksansluten utrustning ska förses med användarnamn och lösenord som inhämtas från systemadministratören.

Trådlös kommunikation

Med trådlös kommunikation avses all kommunikation som sker trådlöst så som tex Wifi, IR, Bluetooth och andra typer av radiokommunikation.

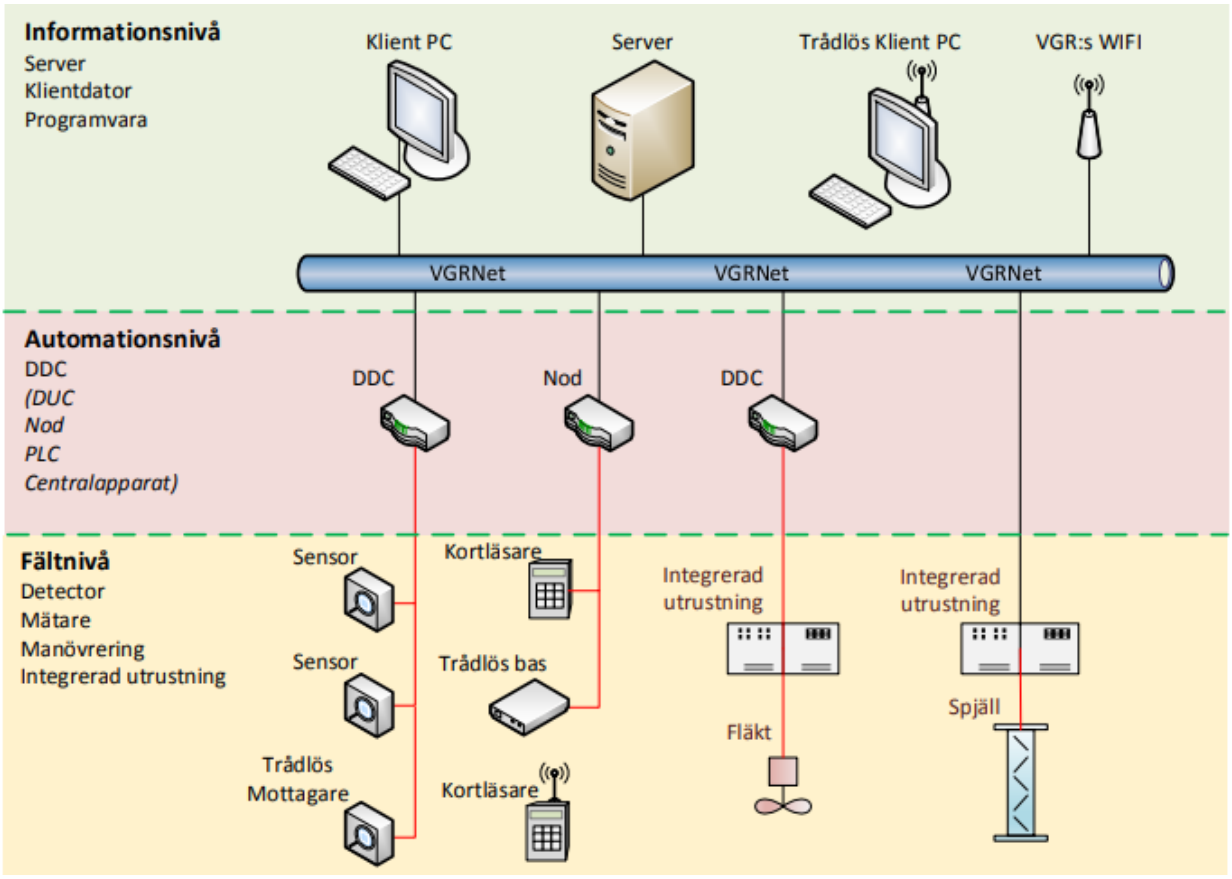
Trådlös kommunikation ska undvikas där funktionen kan lösas på annat sätt.

Trådlös kommunikation ska använda godkända frekvensband och ha kodad signal som skydd för obehörig åtkomst.

Trådlös kommunikation som inte används ska vara avstängd och oåtkomlig.

Tekniska IT-system indelas i tre nivåer för att beskriva förekomst av olika typer av trådlös kommunikation:

- Informationsnivå
- Automationsnivå
- Fältnivå



Informationsnivå

På informationsnivån kan man övervaka och styra de tekniska installationer som ingår i systemet. På denna nivå finns bland annat server, klientdator och programvara för att analysera och bearbeta information som samlas in.

Trådlös kommunikation får endast ske till server och klient med de tjänster som VGR erbjuder, så som tex VGR:s Wifi.

Automationsnivå

På automationsnivå sker övervakning och reglering av elektrisk och mekanisk utrustning i fastigheten. Hårdvaran på denna nivå finns normalt i teknikutrymmen och

kan bestå av DDC (tex. PLC, Nod och DUC). Trådlös kommunikation får inte användas på automationsnivå.

Fältnivå

Fältnivån omfattar utrustning för detektion (t.ex. av rök, gas, larmknapp och passerkort), mätning (t.ex. av temperatur) samt manövrering (tex via ställdon, motor och ellås). Hit räknas även integrerade utrustningar, med inbyggd övervakning och reglering.

Trådlös kommunikation till en mottagare på fältnivå får endast användas om:
- mottagare är konstruerad för ett specifik detekterings ändamål, tex att mäta temperatur.
- mottagare för den trådlösa kommunikationen endast kan kommunicera information för avsett ändamål till systemet. Exempel: för en trådlös temperaturmätare får mottagare enbart kunna skicka information om temperatur i systemet.
- Störning på den trådlösa kommunikationen (tex störsändare) inte kan leda till skada på person eller egendom. Undantag från detta kan göras om trådlös kommunikation måste användas för rörliga objekt, tex människor eller flyttbar utrustning, där det inte är möjligt att använda en fast installation.

Med fjärrkontroll avses en trådlös apparat som används för att styra utrustning på avstånd. fjärrkontroll för konfiguration av utrustningar (till exempel pumpar eller aktiva luftdon). Får enbart användas om räckvidden för fjärrkontrollen befinner sig innanför det fysiska skalskyddet (dörrar och väggar) som avgränsar en lokal, en byggnad eller en del av byggnad där utrustningen är placerad. Kan räckvidden inte begränsas med lokalens fysiska skalskydd kan ett elektroniskt skalskydd användas innanför det fysiska skalskyddet.

Dokumentation/intyg

Leverantören ska redovisa:

- System och utrustningars lösenord till systemansvarig.
- vilka frekvenser och protokoll som används för trådlös kommunikation.
- trådlösa funktioner som är avstängda i utrustningen.
- i egenprovningsprotokoll att man har härdat systemet.
- vilket OS och vilken version av detta som levereras med utrustningen.
- vilka portar som ska vara öppna samt vad de används till. - vilka portar som ska vara stängda.
- vilka tjänster som ska vara igång och för vilket syfte.
- en uppdateringspolicy och visa på hur man hanterar nytillkomna säkerhetshål/risker.
- hur man arbetar med IT-säkerhet. Det kan tex vara ISO certifiering, eller säkerhetsutbildningar samt hur man säkerställer att tillverkarens information om säkerhetsrisker tillämpas och åtgärdas med informeras till slutkund.
- Om systemet kräver åtkomst till internet och i så fall orsak samt till vilka adresser.