Projekt	Infrastruktur för utveckling av LSS Mark
Projektnr	E3800903
Uppdragsgivare	FMV
FoT-område	Ledning
Exportkontroll	nej
Handläggare	Mikael Wedlin, Oscar Granfeldt

Anläggningen SAFELAB med tillhörande förmågor

1 Inledning

Inom projektet LSS MARK har det under flera år funnits ambition att genomföra tester på skyddsvärda system, och där resultaten omfattas av sekretess. En förutsättning för att detta skall kunna genomföras är att det finns tillgång till en anläggning och lokaler som är godkända för sekretessbelagd verksamhet. Under 2023 påbörjades därför arbete för att etablera en sådan anläggning. FOIs anläggning för detta har namnet SAFELAB [1] och har varit redo för skarp drift sedan 1 april 2024.

Syftet med detta MEMO är att kortfattat dokumentera implementationsfasen och etablerandet av labbet.

Huvudkravet på anläggningen är att den skall vara godkänd för verksamhet upp till och med säkerhetsskyddsklassen begränsat hemlig i enlighet med (MUST 2015). Där det, med rimlig insats, är möjligt är labbet även förberett att i framtiden uppdatera skyddsnivåerna till att hantera verksamhet upp till och med säkerhetsskyddsklassen hemlig.

Under arbetets gång har tre separata utrymmen byggts upp. Datorrummet, radionätslabbet, och operatörsrummet. Tidigare utrymme för radionätslabbet har varit arbetsmiljömässigt undermåligt. Därför har flytten till ändamålsenlig lokal även inneburit en förbättring av arbetsmiljön. Arbete som involverar samverkan mellan C2-system och radiosystem har även underlättats då utrymmena ligger i direkt anslutning till varandra.

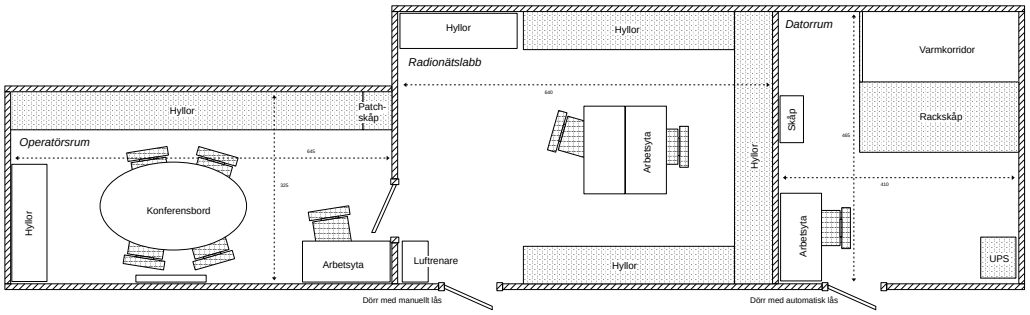
2 Lokal

SAFELAB är inrymd i tre rum: datorrummet, radionätslabbet och operatörsrummet (se figur 2.1). Rummen är uppdelade i två segment, där datorrummet ingår i ena, och övriga två rum ingår i det andra. Segmenten uppfyller skyddsnivå 2 respektive 1, i enlighet med försvarsmaktens författningssamling, FFS (MUST 2015).

2.1 Datorrum

Datorrummet är att betrakta som ett IT-utrymme i enlighet med (MUST 2015; MSB 2013; FMV 2018) och uppfyller skyddsnivå 2.

[1] Safe Amenity For Evaluation Lab



Figur 2.1: Planlösning SAFELAB

Administrationsservrar och datornoder är inrymda i tre rackskåp, där rackskåpen ingår i en inkapsling från *Enoc Systems* (Enoc System 2024). Inkapslingen är konstruerad så att systemet får en varm- och kallkorridor, vilket ger effektivare kylning än den traditionella metoden att bara kyla luften i rummet. Mellan rackskåpen sitter en kylanläggning, dimensionerad för maximalt 20 kW kyleffekt vid 35 °C ingående luft. Strömförsörjning till rummet sker via en UPS [1] med 24 kW uteffekt. UPS:en är dimensionerad att klara externt strömbortfall i minst 20 minuter.

Miljön i rackskåpen är funktionellt och fysiskt uppdelad i två separata sektioner: en öppen och en hemlig del. Dessa är åtskilda av en datadiod (se delkapitel 3.1).

Den logiska uppdelningen i olika nätverkssegment sker med hjälp av färgkodning av patchkablarna.

2.2 Radionätslabbet

Radionätslabbet uppfyller skyddsnivå 1 och utgörs till största delen av datornoder (laptops) sammankopplade med taktiska radioenheter via nätverksväxlar (switchar). Nätverksväxlarna går att sammankoppla med valfritt virtuellt nätverkssegment i den simulerade miljön, såväl som att kopplas ihop i ett fysiskt nätverk. Sammankopplingen möjliggör samspel mellan fysiska och virtuella system, som exempelvis virtuella maskiner och taktiska radioenheter, eller fysiska system och emulerade radioenheter. I radionätslabbet finns även en arbetsyta dimensionerad för 2–3 personer. Rummet är dimensionerat för att under kortare perioder kunna hantera upp till 80 radionoder.

[1] Avbrottsfri kraftförsörjning (uninterruptible power supply).

2.3 Operatörsrum

Ett viktigt skäl med separat operatörsrum är att arbetsmiljön både i datorrummet och radionätslabbet är otillfredställande, främst med avseende på ljudnivå i enlighet med (AV 2024). Vid arbete med radioutrustning finns dessutom behov av att manövrera dessa fysiskt, varpå operatörsrum och radionätslabbet valts att placeras i direkt anslutning till varandra.

Operatörsrummet innehåller även datornoder för utvärdering av C2-programvara. Utrymmet klarar i normalläget 38 enheter, men vid behov kan detta utökas på bekostnad av övrig möblering.

Det finns en arbetsyta för tekniker som arbetar mot datorrummets eller radionätslabbets olika nät. Via en skärmmatris på arbetsytan kan även daglig statusinformation avläsas, så som hårdvarurapporter och simuleringsresultat.

Operatörsrummet kan ytterligare fungera som mötesrum för mindre grupper. Utrymmet är därför utrustat med storbildsskärm, samt möjlighet för användare att koppla sig till FOI:s intranät.

Då detta utrymme hanterar nät av olika sekretessklasser så har särkild vikt lagts på riskreducerande strategier för att undvika felkoppling. Bland annat tillämpas även i detta rum färgkodning av patchkablar och tydlig märkning av uttag.

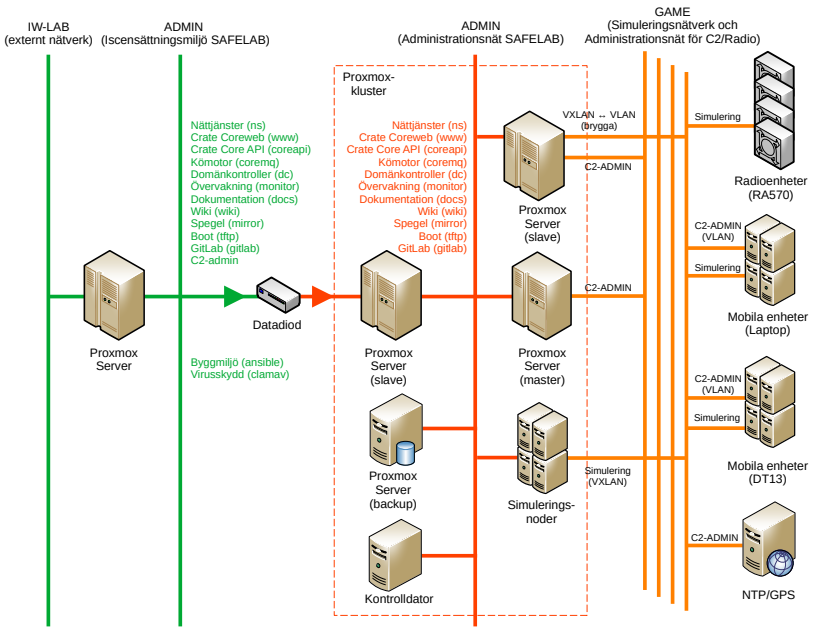
Detta utrymme uppfyller skyddsnivå 1.

3 System

I grunden utgår systemet SAFELAB från arkitekturen bakom FOI:s nationella cyberanläggning för totalförsvaret, Crate (FOI 2024). Den primära skillnaden ligger i att SAFELAB är nätverksmässigt isolerad från internet, vilket medför en minskad risk för att sekretessbelagd information exponeras på ett oönskat sätt. Nätverksisoleringen innebär dock en ökad teknisk utmatning att hålla delsystem uppdaterade, samt att införa ny förmåga. För att ändå möjliggöra goda förutsättningar för utveckling, förvaltning och utvärdering i SAFELAB har den framtagna lösningen blivit att skapa en iscensättningsmiljö (staging environment) på den öppna sidan som sedan replikeras till den isolerade miljön. Replikeringen sker i denna lösning genom en datadiod (se delkapitel 3.1).

De huvudsakliga systemkomponenterna som utgör SAFELAB är ett Proxmox-kluster [1] som innehåller programvara för Crate, samt ett antal datornoder som innehåller den virtuella miljö där prov och försök sker. En grov systemöversikt

[1] Proxmox är en virtualiseringsmiljö byggd huvudsakligen på öppen källkod.



Figur 3.1: Systemöversiktav SAFELAB

av SAFELAB kan ses i figur 3.1. Utöver den generella utvärderingsmiljö som Crate erhåller har specialanpassningar gjorts för att hantera den specifika miljön som utgör SAFELAB.

3.1 Datadiod

För att reducera risken att sekretessbelagd information exponeras används en diodlösning. Administrativa delsystem, samt uppdateringar och föränderlig information, kan konstrueras/hämtas i en öppen miljö och regelbundet synkroniseras genom dioden till SAFELAB. Nuvarande diodlösningen har en överföringskapacitet upp till 1Gbit/s, men i praktiken antas kapaciteten vara något lägre. Diodens in- och utgång är galvanisk separerade med en fiberoptisk länk vilket ger ett pålitligt skydd mot försök att skicka data i fel riktning [2].

FOI har utvecklat särskild programvara för synkroniseringen mellan den öppna och den hemliga miljön. Denna bygger på verktyget *rsync*, med en omslutande specialanpassning skrivet i programspråket *Python*.

[2] Ex. https://www.fibersystem.com/data-diodes/

All data som synkroniseras över dioden genomgår granskning med hjälp av ett virusskydd. Valet av virurskydd är ClamAV från *Cisco Talos*.

3.2 Delsystem

De delsystem som utgör basplattan för SAFELAB utgår från specifikationen för cyberanläggningen Crate, samt de ytterligare behov som ställs för administration av radio- och C2-system. Programvara för delsystemen utgår primärt från FOI-utvecklad programkod, samt öppen källkod. För delsystem med sluten källkod finns licensavtal kopplad till hårdvara, FOI-centrala avtal eller i några få fall separata avtal.

För att hålla gemensam korrekt tid på den hemliga sidan används en GPS/GNSS-ansluten NTP-server, vars tidsuppfattning distribueras över hela SAFELAB. Denna finns placerad i datorrummet med en antennkabel till GNSS-labbet, varifrån man kan välja att distribuera en antennsignal från taket eller någon specialkomponerad GNSS-signal.

En backup-server finns tillgänglig inuti den hemliga miljön för att vid behov återstarta havererad IT-tjänst.

En översikt av fysiska servrar och tjänster som ingår i SAFELAB finns i tabellerna 3.1 och 3.2.

Tabell 3.1: Fysiska servrar i SAFELAB

Namn	Värdnamn	Beskrivning
Adminserver 1	pve1	Proxmox Virtual Environment no.1 (staging)
Adminserver 2	pve2	Proxmox Virtual Environment no.2 (slave)
Adminserver 3	pve3	Proxmox Virtual Environment no.3 (master)
Adminserver 4	pve4	Proxmox Virtual Environment no.4 (slave)
Backupserver 2	pbs2	Proxmox Backup Server no.2
Kontrolldator 1	ctl1	Kontrolldator för övervakning av kluster.
NTP	ntp.c2	GPS/GNSS-mottagare för tid, LANTIME M200.

4 Hårdvara

Delsystemen i SAFELAB utgår huvudsakligen från COTS-produkter, i form av rackmonterade administrationsservrar, samt bladmonterade [1] noder för

[1] Mindre enhet där strömförsörjning och/eller utrymme är begränsat.

Tabell 3.2: Tjänster i SAFELAB

Namn	Värdnamn	Värdserver	Beskrivning
Diodsändare	diode	pve1	Tjänst för datadiod, öppen sida.
Diodmottagare	diode	pve2	Tjänst för datadiod, sluten sida.
Nättjänster	ns1	pve3	DHCP, DNS
Crate Coreweb	www	pve3	Webbgränssnitt för Crate.
Crate Core API	coreapi	pve3	Crate Backend Server.
Kömotor	coremq	pve3	RabbitMQ för intern kommunikation.
Domänkontroller	dc	pve3	Användarhanterare.
Dokumentation (1)	wiki	pve3	Dokumentationstjänst.
Dokumentation (2)	docs	pve3	Crate-dokumentation (API).
Rapportverktyg	overleaf	pve3	Webbverktyg (Overleaf) för rapportskrivning.
Spegel	mirror	pve3	HTTP(S)-spegel för extern data.
Boot	tftp	pve3	Boot-server för ny-/ominstallation av noder.
GitLab	gitlab	pve3	Versionshanteringssystem för intern utveckling.
NTP	ntp	pve3	Tjänst för hantering av tid.
VXLAN ↔ VLAN	-	pve4	Nätverksbrygga för VXLAN till VLAN.
C2-ADMIN	-	pve4	Administrationstjänster för radio- och C2-system.
Övervakning	monitor	ctl1	Prometheus och Grafana.
Integritet	-	ctl1	Tjänster för systemintegritetskontroll.

virtualisering. Av synergiskäl är merparten av systemen av samma fabrikat som valts för huvudanläggningen Crate. Vanligaste valet för servers är fabrikatet Supermicro och vanligaste fabrikatet av switchar är HP. Installationerna är dock tillräckligt generiska för att utan orimligt stora anpassningar kunna bytas ut mot andra fabrikat i framtiden om detta skulle visa sig lämpligt.

FOIs nuvarande uppskattningen är, i enlighet med rekommendationer från tillverkare av hårdvaran, att delar av hårdvaran omsätts över tiden 2–5 år (Supermicro 2024; Western Digital 2024).

I tabell 4.1 listas exempel på hårdvara som installerats i SAFELAB. Hårdvaran har, där det varit möjligt, dimensionerats med god kapacitetsmarginal (som RAM, CPU, nätverk) för att även klara kortare perioder av extrem belastning.

Tabell 4.1: Hårdvara i SAFELAB

Namn	Antal	Beskrivning
SuperStorage 2028R-E1CR24N, 24 multitrådade kärnor, 512GB RAM, 2x1TB NVMe	5	Administration, Backup
SuperServer SYS-530MT-H8TNR, 8 delsystem à 8 multi-trådade kärnor, 128GB RAM, 1TB NVMe	10	Simulering
Western Digital 2TB GREEN SSD 2.5”	32	Lagring
HP Procurve 3500YL-48G-PoE+ Layer 3 Switch (J9311A)	6	Nätverk
Fibersystem, Data Diode 1Gbit MM Secure Tempest	1	Datadiod
Meinberg, LANTIME M200	1	NTP/GPS
Broadcom, BCM57412 NetXtreme-E 10Gb	3	Nätverkskort
Aruba 10G SFP+ DAC 3M	4	10Gbe-kabel
Patchkablar, Cat6e, röda	90	Adminnät
Patchkablar, Cat6e, oranga	90	Simuleringsnät

Litteratur

AV (2024). *Krav vid olika bullernivåer*. Besökt 2024-04-10. URL: https://www.av.se/halsa-och-sakerhet/buller/krav-vid-olika-bullernivaer/.

Enoc System (2024). *Effektiv inkapsling av datacenter*. Besökt 2024-04-10. URL: https://enocsystem.com/produktkategori/datacenter/inkapsling/.

FMV (2018). *Beskrivning: Utformning av lokaler*. Diarenummer 15FMV10927-43:1. Försvarets materielverk.

FOI (2024). *Crate - Sveriges nationella cyberanläggning för totalförsvaret*. Besökt 2024-04-03. URL: https://www.foi.se/forskning/informationssakerhet/crate---sveriges-nationella-cyberanlaggning-for-totalforsvaret.html.

MSB (2013). *Vägledning för fysisk informationssäkerhet i it-utrymmen*. Myndigheten för samhällsskydd och beredskap (MSB) och Riksarkivet. ISBN: 978-91-7383-401-8.

MUST (2015). *Försvarets Författningssamling, FFS*. Försvarsmakten, MUST.

Supermicro (2024). *Warranty | Supermicro*. Besökt 2024-04-05. URL: https://www.supermicro.com/en/support/warranty.

Western Digital (2024). *Warranty | Western Digital*. Besökt 2024-04-05. URL: https://www.westerndigital.com/en-se/support/store/warranty-policy.