




	<p>سند هدف امنیتی نرم افزار اسکادای فرینه فناور</p>	
<p>صفحه ۱ از ۵</p>	<p>ارزیابی امنیتی نرم افزار اسکادای فرینه فناور</p>	<p>نام پروژه:</p>
<p>Rev No: A1</p>	<p>FF-ITRC-SCADA-INF-v1.0</p>	<p>نام فایل الکترونیکی:</p>

فرم مشخصات محصول			
نام محصول	FarinehSCADA	نسخه محصول	v.26.6.0.38 شماره سریال - نام شرکت فرینه فناور
نوع محصول	SCADA System		
نام سند هدف امنیتی	FF-ITRC-SCADA-ST-v1.0	نام پرو فایل حفاظتی	پرو فایل حفاظتی سامانه اسکادا - نسخه ۱،۰ - مرکز مدیریت راهبردی افتا
نسخه نرم افزاری محصول مورد ارزیابی	FarinehSCADA v. 26.6.0.38		
محدوده فیزیکی	این محصول از اجزاء سخت افزاری و نرم افزاری به شرح مدل ارائه شده (به مدرک FF-ITRC-SCADA-ST-v1.0 بند ۵-۱ مراجعه شود) در آیتم بعد جهت انجام فرایندهای خود استفاده می کند.		
تجهیزات مورد ارزیابی	<ol style="list-style-type: none"> 1. SCADA Server (DIS) 2. Engineering (HPI Design) 3. Operation (HPI Run) 4. OPCUA Server (FEP) 		
شرح محصول			
<p>محصول اسکادای فرینه فناور، راهکاری شامل مولفه های نرم افزاری است که در کاربردهای کنترل صنعتی از طریق اتصال به سرورهای OPC امکان دریافت، پردازش، مصورسازی، ارسال فرامین و ذخیره سازی داده های تجهیزات فیزیکی جهت پایش و کنترل زیرساخت های تولیدی، پالایش و انتقال انرژی و موارد مشابه را دارد.</p> <p>الف- ساخت افزار و ب- سیستم عامل، محیط و زیرساخت اجرای محصول اسکادا را به عنوان لایه های سیستمی ایجاد می کنند. محصول اسکادای فرینه فناور در سیستم های مبتنی بر Microsoft Windows و لینوکس اجرا می شود. سلسله اقدامات تنظیم پارامترهای سطح سیستم های عامل، امن سازی، نصب و کاربرد محصولات ثالث مورد نیاز جهت عملکرد مطلوب و امن اسکادای فرینه فناور با عنوان تنظیمات سیستمی بیان می شود.</p> <p>هدف ارزیابی محصول اسکادای فرینه فناور بخش ج- سرور، کلاینت و ایستگاه کاربری مهندسی اسکادا در مدل ارائه شده در Error! Reference source not found. است. محصول اسکادای فرینه فناور با انجام تنظیمات و مهندسی داده و پروژه در مولفه HPI Design، و اجرا در مولفه های سرور DIS و FEP و کلاینت اسکادا HPI Run عملیاتی می شود. تنظیمات و مهندسی نوعی جهت تعریف و اجرای یک پروژه اسکادا به شرح زیر است.</p> <ul style="list-style-type: none"> • برای سطح سرور اسکادا: نوع و آدرس سرور OPC، لیست سیگنال های دریافت شده از سرور OPC، تنظیمات محاسبات و پردازش داده ها، معرفی کلاینت های اسکادا، تنظیمات آلارم ها، فرمول ها و اسکریپت ها، تنظیمات امنیتی و تعریف کاربران و دسترسی های کلاینت ها • برای سطح کلاینت اسکادا: تعریف و کنترل اشکال و سمبل ها، تعریف صفحات، تنظیمات انیمیشن ها، تعریف المان های استاندارد HMI شامل متن ها، دکمه ها، تنظیمات نمودارها و ترندها و غیره 			
***برای توضیحات تکمیلی به مدرک FF-ITRC-SCADA-ST-v1.0 مراجعه شود.			

 <p>فرینه فناور</p>	<p>سند هدف امنیتی نرم افزار اسکادای فرینه فناور</p>	 <p>وزارت ارتباطات و فناوری اطلاعات پژوهشگاه ارتباطات و فناوری اطلاعات</p>
<p>صفحه ۲ از ۵</p>	<p>ارزیابی امنیتی نرم افزار اسکادای فرینه فناور</p>	<p>نام پروژه:</p>
<p>Rev No: A1</p>	<p>FF-ITRC-SCADA-INF-v1.0</p>	<p>نام فایل الکترونیکی:</p>

پیکربندی مورد ارزیابی

	<p>سند هدف امنیتی نرم افزار اسکادای فرینه فناوری</p>	
<p>صفحه ۳ از ۵</p>	<p>ارزیابی امنیتی نرم افزار اسکادای فرینه فناوری</p>	<p>نام پروژه:</p>
<p>Rev No: A1</p>	<p>FF-ITRC-SCADA-INF-v1.0</p>	<p>نام فایل الکترونیکی:</p>

۱- توصیف عملکرد توابع محصول



هدف ارزیابی شامل بخش های زیر است.



۱-۱- اجزاء عملکردی سرور

- **اكتساب داده های سطح فیلد و ارسال فرامین:** ToE شامل توابع ارتباطی است که امکان تبادل اطلاعات شامل دریافت داده از/ارسال فرامین به تجهیزات سطح فیلد نظیر PLC, DCS, RTU, IGW و دیگر کنترلرهای صنعتی از طریق پروتکل های OPC-DA, OPC-UA, و F3IM (سیستم کنترل فرینه فناوری) را فراهم می سازد. با توجه به سطح ارزیابی مورد درخواست، صرفاً پشتیبانی سرور DIS از پروتکل OPC-UA به عنوان کلاینت OPC-UA در محدوده ToE است.
- **تبادل داده:** ToE امکان ارسال و دریافت جریان های اطلاعاتی با استفاده از رابطها و پروتکل های استاندارد نظیر OPC-UA و Syslog با سرورهای OPC ثالث و محصولات مدیریت رویدادهای امنیتی را دارد. همچنین ToE امکان ارسال ایمیل و SMS در صورت فراهم بودن زیرساخت های ارتباطی لازم را دارد. ارسال ایمیل و SMS خارج از محدوده ارزیابی ToE است.
- **مدیریت آلامها:** ToE امکان تشخیص بروز شرایط آلام با استفاده از اطلاعات دریافت شده از تجهیزات سطح فیلد یا داده های سطح سرور و پردازش، انتقال و ثبت اطلاعات آن را دارد.
- **توابع آرشیو:** ToE توابعی برای آرشیو و بازیابی داده های پردازش شده ارائه می کند. ذخیره آرشیو سیگنال های مشخص شده در دو سطح به شرح زیر ارائه می شود.
 - آرشیو در قالب فایل های باینری مختص نرم افزار به شکل محلی روی ماشینی که داده در آن پردازش می شود.
 - آرشیو روی یک ماشین راه دور با استفاده از سرویس (Historical Data Warehouse) HDW در قالب های مرسوم پایگاه داده نظیر MS-SQL یا فایل های باینری (سرویس HDW خارج از محدوده ارزیابی است).
- **توابع افزونگی:** با هدف اطمینان از عملکرد سامانه اسکادا با دسترس پذیری بالا^۱ سرور اسکادا از افزونگی پشتیبانی می کند.

۱-۲- اجزاء عملکردی کلاینت

- **واسط انسان-ماشین:** در سطح کلاینت، ToE شامل توابع برقرارکننده رابطه میان اپراتور و سرور اسکادا به شرح زیر است:
 - **مدیریت دیگرام های شبیه سازی شده:** اپراتور نمای فرایند در حال کنترل را با استفاده از نمادهای گرافیکی و صفحات طراحی شده است، مشاهده و مدیریت می کند.
 - **آلامها:** نمایش وضعیت ها، تاریخچه آلامها و اعمال فرامین نظیر Acknowledge، فعال یا غیرفعال سازی، تنظیم ورودی گزارش ها و دیگر موارد
 - **ترندها:** نمایش، تحلیل و مدیریت ترندها
 - **شناسایی اپراتورها:** هویت اپراتور با استفاده از اطلاعات نام کاربری و کلمه عبور و توکن متعلق به وی از طریق کلاینت اسکادا به سرور اسکادا شناسایی می شود.
 - **تعامل افزونگی:** کلاینت اسکادا در سطح ToE به شکل خودکار سرور اسکادای فعال را انتخاب می کند.

 <p>فرینه فناور</p>	<p>سند هدف امنیتی نرم افزار اسکادای فرینه فناور</p>	 <p>وزارت ارتباطات و فناوری اطلاعات پژوهشگاه ارتباطات و فناوری اطلاعات</p>
<p>صفحه ۴ از ۵</p>	<p>ارزیابی امنیتی نرم افزار اسکادای فرینه فناور</p>	<p>نام پروژه:</p>
<p>Rev No: A1</p>	<p>FF-ITRC-SCADA-INF-v1.0</p>	<p>نام فایل الکترونیکی:</p>

	<p>سند هدف امنیتی نرم‌افزار اسکادای فرینه فناور</p>	
<p>صفحه ۵ از ۵</p>	<p>ارزیابی امنیتی نرم‌افزار اسکادای فرینه فناور</p>	<p>نام پروژه:</p>
<p>Rev No: A1</p>	<p>FF-ITRC-SCADA-INF-v1.0</p>	<p>نام فایل الکترونیکی:</p>

۳-۱- مشترکات

- اجرای توابع سرور به شکل نهفته در کلاینت اسکادا HPI Run وجود دارد.
- پردازش داده‌ها و اجرای اسکریپت‌ها: توابع پردازشی مشترکی نظیر انجام محاسبات و اجرای اسکریپت‌ها در ToE پشتیبانی می‌شود.
- دسترسی به داده‌های ذخیره‌شده: بنا به اهداف عملکردی، دسترسی به داده‌های ذخیره‌شده در سطح کلاینت و سرور اسکادا در سطح ToE امکان‌پذیر است.
- دسترسی به توابع مدیریتی: برخی کنترل‌ها و تعاریف مدیریتی نظیر مدیریت دسترسی‌ها، مدیریت تنظیمات، پایش نودها و بررسی وضعیت خطاهای سیستمی و مهندسی (Events logs)، پس از تعریف در HPI Design در سطوح سرور و کلاینت اسکادا در ToE در دسترس است.
- توابع استقرار تنظیمات^۲: پس از طراحی و مهندسی صفحات و ارتباطات و تنظیمات استقرار در HPI Design، این توابع در قالب فایل‌های پروژه در سطح سرور و کلاینت اسکادا توسط واسط‌های مرتبط اجرا می‌شوند.

توابع و محصولات ثالث مورد استفاده به شرح زیر خارج از محدوده ToE است.

- Kiwi Syslog: سرور دریافت logها در قالب syslog
- Padvish Endpoint Security: راهکار ضدبدافزار و امنیت نقاط انتهایی
- Farineh OPCUA Server: سرور FEP
- HDW: سرور مدیریت ذخیره‌سازی داده‌های آرشیو
- HPI Licensing: راهکار مدیریت لایسنس نرم‌افزار HPI
- EaseUs Backup: راهکار پشتیبان‌گیری از داده‌های نرم‌افزار
- Windows Backup: راهکار پشتیبان‌گیری از سیستم‌عامل
- Windows Active Directory Group Policy: راهکار اعمال سیاست‌های امنیتی
- Hardware Security Tokens: توکن‌های سخت‌افزاری مورد استفاده

***برای توضیحات تکمیلی به مدرک FF-ITRC-SCADA-ST-v1.0 مراجعه شود.

^۲ Embedded DIS server

^۳ Configuration Deployment