به نام خدا

سند هدف امنیتی

یکسوساز جریان داده رهبان نسخه ۱.۰

RDD-1001

شرکت روناک صنعت ماندگار

بهمن-۱۴۰۲

نسخه ۱.۰

فهرست

۱ معرفی سند هدف امنیتی

۱/۱ مرجع سند هدف امنیتی و محصول

عنوان سند هدف امنیتی	یکسوساز جریان داده رهبان
نسخه	RDD-1001
تاریخ	۱۴۰۲/۱۱/۱۲
نویسندگان	امیرمحمد کتیرائی – علی اسکندری – علی غلامی – حمیدرضا زارع

نام تولید کننده	شرکت روناک صنعت ماندگار
نام محصول	یکسوساز جریان داده رهبان
نوع محصول	سخت افزار
نسخه	RDD-1001

نوع محصول

این محصول یک سخت افزار مستقل می باشد که جریان داده ورودی را به صورت یک طرفه به پورت خروجی منتقل می نماید.

نرم‌افزار/سخت‌افزار/میان‌افزار پیش نیاز محصول

- برای بررسی محصول در سمت گیرنده و فرستنده به موارد زیر نیاز است. (بدیهی است که سخت افزار، سیستم عامل و نرم افزاهای مربوطه در حوزه این آزمون قرار نمی گیرند)

کامپوننت	حداقل الزامات
پردازنده	پردازنده اینتلGHz1 یا بالاتر
حافظه	2 GB یا بالاتر
فضای آزاد دیسک	1 GB یا بالاتر
مانیتور	VGA
سیستم عامل	Windows xp یا بالاتر (۳۲ یا ۶۴ بیت)
کارت شبکه	100 Mb ethernet
نرم افزار	.net core v 3.x

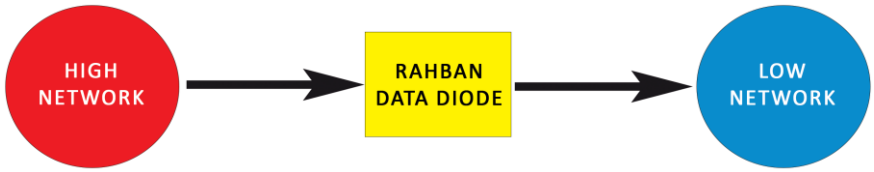
۲٫۱ شرح محصول

مخاطرات مختلفی شبکه های محلی سازمانها را تهدید می‌کنند که این موجب شده است تا سازمانها به منظور کاهش مخاطرات شبکه های ایزوله از هم داشته باشند: به عنوان مثال می‌توان به جدا بودن شبکه اینترنت از شبکه اینترانت سازمان اشاره کرد. با وجود جدا بودن این شبکه ها، نیاز به انتقال اطلاعات بین شبکه ها وجود دارد. معمولا نیازمندی اصلی انتقال اطلاعات از یک شبکه به شبکه دیگر و نه برعکس- به صورت یکطرفه- است.

اتصال شبکه های ایزوله میتواند با ابزارهای مختلفی انجام شود: یکی از این ابزارها یکسوساز جریان داده است. این محصول به صورت کاملا سخت افزاری ارتباطی یکطرفه بین دو شبکه برقرار می نماید این ارتباط از طریق کانالی سخت افزاری برقرار میشود که تمام سیگنالهای در خلاف جهت از بین میروند و سیگنال فقط از یک طرف به طرف دیگر حرکت میکند و این ارتباط کاملا به صورت سخت افزاری یک طرفه شده است. شکل ۱ نمایی از این محصول و قرارگیری آن در معماری شبکه را مشاهده می نمایید.

این پروفایل حفاظتی برای آن دسته از محصولات یکسوساز جریان داده انتشار شده است که هیچگونه کنسول مدیریتی برای پیکربندی محصول فراهم نمیکند. از این رو برای سایر محصولاتی که ارائه کننده کنسول

مدیریتی هستند باید علاوه بر الزامات مطرح شده در این پروفایل، الزامات موجود در پروفایل حفاظتی تجهیز شبکه یا دیگر الزامات تعیین شده در پروفایل های آتی نیز برآورده نمایند



شکل ۱ : معماری سطح بالا از یکسوساز جریان داده (Data Diode)

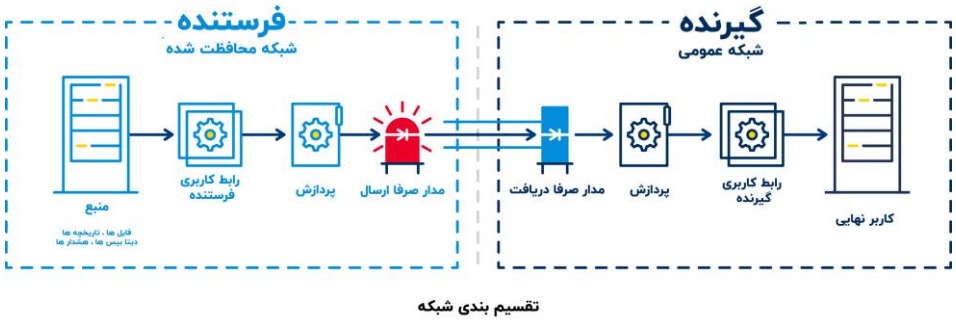
این محصول خط مشی ارسال یکطرفه داده را پیاده سازی نموده است که در زیر توصیف میشود:

- موجودیتهای فعال:
  - پورت بالا/ارسال کننده (واسط ورودی یکسوساز جریان داده)
  - پورت پایین/دریافت کننده (واسط خروجی یکسو ساز جریان داده)
- اطلاعات (سیگنال هایی که میتوانند در خروجی بالا و یا خروجی پایین ورود نمایند)
- خط مشی
  - اطلاعات فقط اجازه دارند از پورت بالا وارد شده و از پورت پایین خارج شوند.
  - اطلاعات اجازه ندارند از پورت پایین وارد شده و از پورت بالا خارج شوند.

حوزه فیزیکی

عناصر سختافزاری و نرمافزاری مورد استفاده با توجه به پیکربندی ارزیابی در جدول زیر معرفی می‌شود:

عناصر محصول	شماره مدل یا نسخه
یکسوساز	RDD-1001



شکل ۲ : قرار گیری محصول در محیط عملیاتی و پیکربندی آن

حوزه منطقی

کارکردهای امنیتی هدف ارزیابی تحت عنوان حوزه منطقی شناخته می‌شود که باید به صورت مشخص هریک از کارکردها و شرح آنها در این قسمت مطرح شود.

کارکردها	توصیف
انتقال یکسویه اطلاعات	انتقال یکسویه داده بین دو شبکه ایزوله
داده های دریافتی از پورت بالا به مدار صرفا ارسال داده ارسال شده و پس از تبدیل به پالس های نوری از کانال فیبر نوری که Tx پورت بالا را به Rx پورت پایین مدار صرفا دریافت متصل می کند در مسیر یکطرفه منتقل می شود. با توجه به عدم اتصال Tx پورت پایین به Rx پورت بالا به واسطه هیچ مدیومی (مثلا فیبر نوری، کابل یا امواج رادیویی) داده ها قابلیت عبور در مسیر بازگشت را نداشته و یکسویه بودن انتقال اطلاعات تضمین خواهد شد.	

۲ ادعای انطباق

۱/۲ انطباق با استاندارد ارزیابی امنیتی معیار مشترک

انطباق با استاندارد ارزیابی امنیتی معیار مشترک	ISO/IEC 15408, version 3.1, revision 5, April 2017
انطباق با SARها (قسمت دوم از CC)	توسعه یافته
انطباق با SARها (قسمت سوم از CC)	منطبق
نام پروفایل حفاظتی	پروفایل امنیتی یکسوکننده جریان داد ه
سطح تضمین امنیت ی	EAL1

3 تعریف مسائل امنیتی

3.1 خط مشی

خط مشی ها	توصیف
ارتبا ط یکطرفه P.ONE_WAY_FLOW	تمام ارتباطات باید از یک طرف(ارسال کننده) ارسال و از طرف دیگر (دریافت کننده) دریافت شود.

3.2 تهدیدات

تهدید	توصیف
نشت اطلاعات T.DATA_LEAK	هرکدام از سیستمهای ارسال کننده و دریافت کننده میتواند باعث نشت و درز اطلاعات شود.

۳ تعریف مسائل امنیتی

۱/۳ خط‌مشی

خط مشی‌ها	توصیف
ارتباط یکطرفه P.ONE_WAY_FLOW	تمام ارتباطات باید از یک طرف (ارسال کننده) ارسال و از طرف دیگر (دریافت کننده) دریافت شود.

۲/۳ تهدیدات

تهدید	توصیف
نشت اطلاعات T.DATA_LEAK	هرکدام از سیستمهای ارسال کننده و دریافت کننده می تواند باعث نشت و درز اطلاعات شود.

۳/۳ فرضیات

فرضیات	توصیف
فیزیکی A.PHYSICAL	محصول و پورت های ارتباطی آن به صورت فیزیکی در مقابل دسترسی غیرمجاز و هر مداخله فیزیکی، مانند مداخله های مکانیکی، الکتریکی، اپتیکی، تشعشعی محافظت می شوند.
نصاب آموزش دیده A.INTEGRATOR	فرض شده است کسی که عملیات نصب و پیکربندی محصول را انجام می دهد (نصاب) این کار را به صورت صحیح، بر طبق راهنمای کاربری انجام می دهد و به جز محصول راه ارتباطی دیگری بین دو شبکه قرار نمی دهد.

٤ اهداف امنیتی

۱/۴ اهداف امنیتی برای هدف ارزیابی

هدف امنیتی	توصیف
محرمانگی O.NO_HIGH_INFO	تمام اطلاعات سمت گیرنده باید به صورت محرمانه نسبت به طرف ارسال کننده باشد و هیچ اطلاعاتی نباید به سمت ارسال کننده از طرف گیرنده فرستاده شود.
ارسال یکطرفه O.ONE_WAY_FLOW	تمام اطلاعات از سمت ارسال کننده به سمت گیرنده ارسال می شود.

۲/۴ اهداف امنیتی برای محیط عملیاتی

هدف امنیتی	توصیف
فیزیکی OE.PHYSICAL	محصول و پورت های ارتباطی آن به صورت فیزیکی در مقابل دسترسی غیرمجاز و هر مداخله فیزیکی، مانند مداخله های مکانیکی، الکتریکی، اپتیکی، تشعشعی محافظت می شوند.
نصاب آموزش دیده OE.INETGRATOR	فرض شده است کسی که عملیات نصب و پیکربندی محصول را انجام میدهد (نصاب) این کار را به صورت صحیح، بر طبق راهنمای کاربری انجام میدهد و به جز محصول راه ارتباطی دیگری بین دو شبکه قرار نمی دهد.

۵ الزامات کارکرد امنیتی

شماره الزام	نام الزام	عنصر متناظر با الزام
۱	خط مشی کنترل جریان اطلاعات ۲	FDP_IFC.2.1
۲	خط مشی کنترل جریان اطلاعات ۳	FDP_IFC.2.2
۳	عملیات کنترل جریان اطلاعات۱	FDP_IFF.1.1
۴	عملیات کنترل جریان اطلاعات۲	FDP_IFF.1.1
۵	عملیات کنترل جریان اطلاعات۳	FDP_IFF.1.1
۶	عملیات کنترل جریان اطلاعات۴	FDP_IFF.1.1
۷	عملیات کنترل جریان اطلاعات۵	FDP_IFF.1.1

Commented [aa1]: نام الزامات تکراریست میبایست اصلاح گردد.

۱٫۵ کلاس حفاظت از داده کاربر ی

شماره	عنصر امنیتی

الزام	
۱	**خط مشی کنترل جریان اطلاعات ۲**
محصول باید خط مشی ارسال یکطرفه را روی موجودیت های فعال: پورت های بالا و پایین/اطلاعات: هر نوع سیگنال نوری که از پورت بالا یا پایین عبور کند و هر نوع عملیاتی که منجر به عبور اطلاعات از/به موجودیت های فعال تحت این خط مشی شود اعمال کند.	
۲	**خط مشی کنترل جریان اطلاعات ۳**
محصول اطمینان میدهند که همه عملیاتی که ردوبدل شدن اطلاعات در موجودیتهای فعال محصول را در بر میگیرند توسط یک خط مشی[1] پوشش داده می شود.	
۳	**عملیات کنترل جریان اطلاعات ۱**
محصول باید خط مشی ارسال یکطرفه را بر اساس این نوع مشخصه های امنیتی اطلاعات و موجودیت های فعال اعمال کند: موجودیت های فعال: پورت های بالا و پایین - اطلاعات: هر نوع سیگنال نوری که از پورت بالا یا پایین عبور کند.	
۴ . عملیات کنترل جریان اطلاعات ۲	
با توجه به قوانین زیر، محصول باید اجازه جریان یافتن اطلاعات بین یک موجودیت فعال کنترل شده و اطلاعات کنترل شده را از طریق عملیات کنترل شده بدهد: [اختصاص: برای هر عملیات، باید ارتباطی بر اساس مشخصه امنیتی بین اطلاعات و موجودیت فعال وجود داشته باشد.	
۵ . عملیات کنترل جریان اطلاعات ۳	
محصول باید انتقال یکسویه جریان داده تنها و تنها از پورت بالا به پورت پایین را اعمال نماید	
۶. عملیات کنترل جریان اطلاعات ۴	

Commented [aa2]: قوانین ذکر شده در این الزام باید حذف گردد و در بخش اختصاص از کلمه "هیچ" استفاده شود

[1] SFP

محصول باید بر اساس قوانین زیر اجازه ی جریان یافتن اطلاعات را دهد: اطلاعات تنها می توانند از پورت بالا به سمت پورت پایین انتقال یابد و خلاف این امر ممکن نیست.
۷. عملیات کنترل جریان اطلاعات ۵
محصول باید بر اساس قوانین زیر مانع جریان یافتن اطلاعات شود: اطلاعات نمی تواند از پورت پایین به سمت پورت بالا جریان یابد و یکسوساز مانع این انتقال خواهد شد.

Commented [aa3]: قوانین ذکر شده در این الزام باید حذف گردد و در بخش اختصاص از کلمه "**هیچ**" استفاده شود

٦ الزامات تضمین امنیتی

الزامات عملکرد تضمین توصیف کننده چگونگی ارزیابی هدف ارزیابی است. در این بخش الزامات EAL1 آورده می‌شود که لیست الزامات آن در جدول زیر آمده است.

نام کلاس	نام الزام	توضیحات
Development	ADV_FSP.1	مشخصات کارکرد ابتدایی
Guidance Documents	AGD_OPE.1	راهنمای کاربری
	AGD_PRE.1	راهنمای آماده‌سازی
Tests	ATE_IND.1	آزمون مستقل-منطبق
Vulnerability Assessment	AVA_VAN.1	تحلیل آسیب‌پذیری
Life cycle Support	ALC_CMC.1	برچسب گذاری هدف ارزیابی
	ALC_CMS.1	پوشش پیکربندی هدف ارزیابی

داده های دریافتی از پورت بالا به مدار صرفا ارسال داده ارسال شده و پس از تبدیل به پالس های نوری از کانال فیبر نوری که Tx پورت بالا را به Rx پورت پایین مدار صرفا دریافت متصل می کند در مسیر یکطرفه منتقل می شود. با توجه به عدم اتصال Tx پورت پایین به Rx پورت بالا به واسطه هیچ مدیومی (مثلا فیبر نوری، کابل یا امواج رادیویی) داده ها قابلیت عبور در مسیر بازگشت را نداشته و یکسویه بودن انتقال اطلاعات تضمین خواهد شد.

۱.۶ کلاس توسعه

اطلاعات محصول، از طریق مستندات راهنمای کاربر و بخش مشخصات امنیتی محصول از سند هدف امنیتی در اختیار کاربر نهایی قرار میگیرد الزامی بر وجود بخش مشخصات امنیتی محصول در سند هدف امنیتی نیست اما در صورت وجود باید محتوای آن با الزامات کارکردی مرتبط بوده و مورد تائید توسعه دهندگان محصول باشد.

۲.۶ کلاس راهنمای کاربر

مستندات راهنما همراه با سند هدف امنیتی برای استفاده کاربران ارائه خواهند شد. در این دسته از مستندات شرحی از مدل مدیریتی و نحوه بررسی محیط عملیاتی توسط مدیر (تا مشخص گردد که آیا میتواند نقش خود را برای کار کرد امنیتی ایفا نماید) ارائه میشود.

برای هر محیط عملیاتی که در سند هدف امنیتی ادعای پشتیبانی از آن شده باید مستند راهنما ارائه گردد. این راهنما شامل :

دستورالعمل نصب موفقیت آمیز محصول در محیط

دستور العمل مدیریت امنیت محصول به عنوان یک محصول و به عنوان بخشی از یک محیط عملیاتی بزرگتر دستور العمل هایی که ارائه دهنده قابلیت مدیریتی محافظت شده از طریق استفاده از قابلیتهای محصول، محیط عملیاتی یا هر دو است.

راهنمای کاربری ۱,۲,۷

مؤلفه های اقدامات توسعه دهنده	
نام خانواده	عنصر امنیتی
راهنمای کاربردی (AGD_OPE)	نام عنصر راهنمای کاربردی ۱ شماره مؤلفه AGD_OPE.1.1D شرح مؤلفه: توسعه دهنده باید راهنمای کاربردی ارائه نماید

مؤلفه های محتوایی	مؤلفه های محتوایی
نام خانواده	عنصر امنیتی
راهنمای کاربردی AGD_OPE	نام عنصر راهنمای کاربردی ۱ شماره مؤلفه AGD_OPE.1.IC شرح مؤلفه : سند راهنمای کاربردی باید برای هر نقش کاربری کارکردها و مجوزهای دسترسی را که باید در یک محیط پردازشی امن کنترل شوند توصیف نماید همانند هشدارهای مناسب.
	نام عنصر راهنمای کاربردی ۱ شماره مؤلفه AGD_OPE.1.2C شرح مؤلفه: سند راهنمای کاربردی باید برای هر نقش کاربری توصیف نماید که چگونه از واسط های در دسترس ارائه شده توسط محصول به صورت امن استفاده می گردد.
	نام عنصر راهنمای کاربردی ۱ شماره مؤلفه AGD_OPE.1.30 شرح مؤلفه : سند راهنمای کاربردی باید برای هر نقش کاربری کارکردها و واسطهای در دسترس به خصوص تمام پارامترهای امنیتی تحت کنترل کاربر را توصیف نموده و مقادیر امن را به صورت مناسبی تعیین نماید.
	نام عنصر راهنمای کاربردی ۱

مؤلفه های محتوایی	
نام خانواده	عنصر امنیتی
	شماره مؤلفه AGD_OPE.1.4C شرح مؤلفه : سند راهنمای کاربردی باید برای هر نقش کاربری هر نوع رویدادهای مربوط به امنیت را به کارکردهای در دسترس کاربر که نیاز است انجام داده شوند مرتبط نماید، همانند تغییر مشخصات امنیتی موجودیتهای تحت کنترل توابع امنیتی محصول.
	نام عنصر راهنمای کاربردی ۱ شماره مؤلفه AGD_OPE.1.5 شرح مؤلفه : سند راهنمای کاربردی باید تمام مدهای عملیاتی محصول مدهایی شامل شکست عملیات یا خطای عملیات آثار آنها و مستلزم بودنشان برای حفظ عملیات در حالت امن را مشخص نمایند.
	نام عنصر راهنمای کاربردی ۱ شماره مؤلفه (AGD_OPE.1.6C) شرح مؤلفه : سند راهنمای کاربردی باید برای هر نقش کاربری معیارهای امنیتی را که توسط کاربر تبعیت میشوند توصیف نماید تا .اهداف امنیتی محیط عملیاتی که در سند هدف امنیتی شرح داده شده اند، کاملا اجرا گردند.
	نام عنصر راهنمای کاربردی ۱ شماره مؤلفه AGD_OPE.1.7C شرح مؤلفه سند راهنمای کاربردی باید واضح و قابل فهم باشد.

مؤلفه های اقدامات ارزیاب	
نام خانواده	عنصر امنیتی
راهنمای کاربردی	نام عنصر راهنمای کاربردی ۱
مؤلفه های اقدامات ارزیاب	

نام خانواده	عنصر امنیتی
AGD_OPE	شماره مؤلفه: AGD_OPE.1.1E شرح مؤلفه: ارزیاب باید تائید نماید که اطلاعات ارائه شده در سند راهنمای کاربردی تمام مؤلفه های محتوایی را برآورده می نماید.

راهنمای آماده سازی

مؤلفه های اقدامات توسعه دهنده	
نام خانواده	عنصر امنیتی
راهنمای آماده سازی (AGD_PRE)	نام عنصر راهنمای آماده سازی ۱ شماره مؤلفه AGD_PRE.1.ID شرح مؤلفه : توسعه دهنده باید محصول را همراه با سند آماده سازی ارائه نماید.

مؤلفه های اقدامات محتوایی	
نام خانواده	عنصر امنیتی
راهنمای آماده سازی (AGD PRE)	نام عنصر راهنمای آماده سازی ۱ شماره مؤلفه AGD_PRE.1.1C شرح مؤلفه : مستندات آماده سازی باید تمام مراحل لازم برای پذیرش امن محصول توسط مشتری را مطابق با رویه های تحویل توسعه دهنده شرح دهند.
	نام عنصر : راهنمای آماده سازی ۱ شماره مؤلفه AGD_PRE.1.2 شرح مؤلفه :

مؤلفه های اقدامات محتوایی	
نام خانواده	عنصر امنیتی
	مستندات آماده سازی باید تمام مراحل لازم برای نصب امن محصول و آماده سازی امن محیط عملیاتی را مطابق با اهداف امنیتی محیط عملیاتی ذکر شده در سند هدف امنیتی، شرح دهند.

مؤلفه های اقدامات ارزیاب	
راهنمای آماده سازی (AGD_PRE)	نام عنصر راهنمای آماده سازی ۱ شماره مؤلفه AGD_PRE.1.1E شرح مؤلفه : ارزیاب باید تائید نماید که اطلاعات ارائه شده تمام مؤلفه های محتوایی را برآورده می نماید.
	نام عنصر راهنمای آماده سازی ۱ شماره مؤلفه AGD_PRE.1.2E شرح مؤلفه : ارزیاب باید رویه های آماده سازی شرح داده شده در سند را بکار ببرد تا تائید نماید، محصول می تواند به صورت امن برای عمل نمودن آماده شود.

۳.۶ کلاس آزمون

آزمون محصول برای بررسی بخشهای کارکردی سیستم و همچنین بخشهایی که طراحی و پیاده سازی آنها برای سیستم دارای آسیبهای امنیتی است در نظر گرفته میشود آزمون بخشهای کارکردی سیستم از طریق خانواده ATE_IND و آزمون بخشهایی که طراحی و پیاده سازی آسیبزایی دارند از طریق خانواده AVA_VAN صورت میگیرد. در این سطح از ارزیابی سطح (EAL1) آزمون بر اساس کارکردی که برای محصول در نظر گرفته شده و واسطهایی که بر اساس اطلاعات طراحی در اختیار ارزیاب قرار میگیرد انجام می گردد. نتایج آزمون و تحلیل آسیب پذیری باید در گزارش آزمون لحاظ شوند این مسئله در الزامات زیر در نظر گرفته شده است.

۱٫۳٫۷ آزمون مستقل

آزمون مستقل برای تائید کارکرد محصول که در بخش مشخصات امنیتی محصول از سند هدف امنیتی و مستندات راهنمای مدیر ارائه شده صورت میگیرند هدف اصلی آزمون اطمینان از برآورده شدن الزامات کارکردی مشخص شده در سند هدف امنیتی است. ارزیاب باید در سند گزارش آزمون طرح آزمون و نتایج آن را مستند نماید.

مؤلفه های اقدامات توسعه دهنده	
نام خانواده	عنصر امنیتی
آزمون مستقل (ATE_IND)	نام عنصر آزمون مستقل ۱ شماره مؤلفه ATE_IND.L.ID شرح مؤلفه : توسعه دهنده باید برای آزمودن محصول را ارائه نماید .

مؤلفه های اقدامات محتوایی	
نام خانواده	عنصر امنیتی
آزمون مستقل (ATE_IND)	نام عنصر آزمون مستقل ۱ شماره مؤلفه (ATE_IND.1.1C) شرح مؤلفه : محصول باید مناسب آزمودن باشد.

مؤلفه های اقدامات ارزیاب	
آزمون مستقل نام عنصر آزمون مستقل ۱ ATE_IND	آزمون مستقل نام عنصر آزمون مستقل ۱ شماره مؤلفه: ATE_IND.1.1E شرح مؤلفه: ارزیاب باید تائید نماید که اطلاعات ارائه شده مؤلفه های محتوایی را برآورده می نماید.
	نام عنصر آزمون مستقل ۱ شماره مولفه : (ATE_IND.1.2E) شرح مؤلفه : ارزیاب باید زیر مجموعه ای از توابع امنیتی محصول را آزمون نماید تا تائید نماید که توابع امنیتی محصول به صورت مشخص شده عمل نماید.

کلاس آسیب پذیری ۴.۶

۱,۴,۷ تحلیل آسیب پذیری

مؤلفه های اقدامات توسعه دهنده	
نام خانواده	عنصر امنیتی
آسیب پذیری (AVA VAN)	نام عنصر آسیب پذیری ۱ شماره مؤلفه AVA_VAN.L.ID شرح مؤلفه : توسعه دهنده باید برای آزمودن محصول را ارائه نماید.

مؤلفه های اقدامات محتوایی	
نام خانواده	عنصر امنیتی
آسیب پذیری AVA_VAN	نام عنصر آسیب پذیری ۱ شماره مؤلفه: AVA_VAN.1.1C شرح مؤلفه : محصول باید مناسب آزمودن باشد.

مؤلفه های اقدامات ارزیاب	
نام خانواده	عنصر امنیتی
آسیب پذیری (AVA_VAN)	نام عنصر آسیب پذیری ۱ شماره مؤلفه AVA_VAN.I.IE شرح مؤلفه : ارزیاب باید تایید نماید که اطلاعات ارائه شده تمام مولفه های محتوایی را براورده مینماید.
	نام عنصر آسیب پذیری ۱ شماره مؤلفه AVA_VAN.1.2E شرح مؤلفه : ارزیاب باید برای شناسایی آسیب پذیریهای بالقوه در محصول در منابع عمومی جستجویی را انجام دهد
	نام عنصر آسیب پذیری ۱ شماره مؤلفه (AVA_VAN.1.3E) شرح مؤلفه : ارزیاب باید بر اساس آسیب پذیریهای بالقوه شناسایی شده آزمون نفوذ انجام دهد تا مقاومت محصول را در برابر حملات با توان پایه که توسط مهاجمان صورت می گیرند مشخص نماید.

۵.۶ کلاس پشتیبانی از چرخه حیات

در سطح اطمینانی که این پروفایل حفاظتی ارائه شده است (EAL1) کلاس پشتیبانی از چرخه حیات به ویژگی هایی از چرخه حیات محدود میگردد که توسط کاربر نهایی قابل مشاهده باشد. این به معنی نیست که سبک و سیاق توسعه دهنده نقش کمرنگی در قابل اعتماد بودن محصول دارد بلکه در این سطح اطمینان (EAL1) تنها به این اطلاعات نیاز است.

۱.۵.۷ قابلیت های پیکربندی

این مؤلفه جهت معرفی محصول به صورت مجزا از دیگر محصولات یا نسخه ای که توسط فروشنده ارائه شده است. بدین معنی که جدا از برچسب گذاری محصول محصول که ممکن است بخشی از یک محصول باشد به تنهایی بر چسب گذاری شود نام محصول نسخه آن و غیره بدین ترتیب کاربر نهایی میتواند محصول که توسط مرکز گواهی تائید شده است را به آسانی تشخیص دهد.

مؤلفه های اقدامات توسعه دهنده	
نام خانواده	عنصر امنیتی
قابلیت های پیکربندی ALC_CMC	نام عنصر برچسب گذاری محصول ۱ شماره مؤلفه ALC_CMC.I.ID شرح مؤلفه: توسعه دهنده باید محصول و مرجع محصول را ارائه نماید.

مؤلفه های اقدامات محتوایی	
نام خانواده	عنصر امنیتی
قابلیت های پیکربندی ALC_CMC	نام عنصر برچسب گذاری محصول ۱ شماره مؤلفه ALC_CMC.1.1C شرح مؤلفه : محصول باید با یک مرجع یکتا برچسب زده شود.

مؤلفه های اقدامات ارزیاب	
نام خانواده	عنصر امنیتی
قابلیت های پیکربندی (ALC_CMC)	نام عنصر برچسب گذاری محصول ۱ شماره مؤلفهALC_CMC.1.1E شرح مؤلفه : ارزیاب باید تائید نماید که اطلاعات ارائه شده تمام مؤلفه های محتوایی را برآورده می نماید.

۲.۵.۷ حوزه پیکربندی

مؤلفه های اقدامات توسعه دهنده	
نام خانواده	عنصر امنیتی
قابلیت های پیکربندی (ALC_CMS)	نام عنصرپوشش پیکربندی محصول ۱ شماره مؤلفهALC_CMS.1.1D شرح مؤلفه : ارزیاب باید لیست پیکربندی محصول را ارائه نماید.

مؤلفه های اقدامات محتوایی	
نام خانواده	عنصر امنیتی
حوزه پیکربندی (ALC_CMS)	نام عنصر پوشش پیکربندی محصول ۱ شماره مؤلفه ALC_CMS.1.1C شرح مؤلفه : لیست پیکربندی باید شامل خود محصول و مدارک مورد نیاز توسط الزامات تضمین امنیتی باشد.
	نام عنصر پوشش پیکربندی محصول ۱ شماره مؤلفه ALC_CMS.1.1C شرح مؤلفه : لیست پیکربندی باید موارد بیکربندی را به صورت یکتا معرفی نماید.

مؤلفه های اقدامات ارزیاب	
نام خانواده	عنصر امنیتی
حوزه پیکربندی (ALC_CMS)	نام عنصر پوشش پیکربندی محصول ۱ شماره مؤلفه ALC_CMS.1.1E شرح مؤلفه : ارزیاب باید تائید نماید که اطلاعات ارائه شده تمام مؤلفه های محتوایی را برآورده می نماید.

۷ شرح خلاصه‌ای از محصول

یکسوساز جریان داده رهبان امکان اتصال شبکه های ایزوله به نحوی که جهت جریان صرفا از شبکه فرستنده به سمت شبکه گیرنده باشد را فراهم می آورد. این فرایند به صورت کاملا فیزیکی و در لایه سخت افزاری اتفاق می افتد و محصول فاقد هرگونه نرم افزار و سیستم عاملی می باشد.این سامانه توانایی انتقال فایل بصورت یکطرفه و با توان عملیاتی 1 Gbps را دارد. بر مبنای این قابلیت اصلی سرویس های مختلف از جمله موارد زیر قابل ارائه می باشد:

File transfer
Screen sharing
Unidirectional API call
Secure Update
Data base replication
Industrial USG
...

روش پیاده سازی الزامات به شرح زیر می باشد:

الزام شماره ۱:
خط مشی کنترل جریان اطلاعات ۲ :

داده های دریافتی از پورت بالا به مدار صرفا ارسال داده ارسال شده و پس از تبدیل به پالس های نوری از کانال فیبر نوری که Tx پورت بالا را به Rx پورت پایین مدار صرفا دریافت متصل می کند در مسیر یکطرفه منتقل می شود. با توجه به عدم اتصال Tx پورت پایین به Rx پورت بالا به واسطه هیچ مدیومی (مثلا فیبر

نوری، کابل یا امواج رادیویی) داده ها قابلیت عبور در مسیر بازگشت را نداشته و یکسویه بودن انتقال اطلاعات تضمین خواهد شد.

الزام شماره ۲:

خط مشی کنترل جریان اطلاعات ۳ :

با توجه به عدم اتصال Tx پورت پایین به Rx پورت بالا به واسطه هیچ مدیومی (مثلا فیبر نوری، کابل یا امواج رادیویی) داده ها قابلیت عبور در مسیر بازگشت را نداشته و یکسویه بودن انتقال اطلاعات تضمین خواهد شد.

الزام شماره ۳:

عملیات کنترل جریان اطلاعات ۱ :

داده های دریافتی از پورت بالا به مدار صرفا ارسال داده ارسال شده و پس از تبدیل به پالس های نوری از کانال فیبر نوری که Tx پورت بالا را به Rx پورت پایین مدار صرفا دریافت متصل می کند در مسیر یکطرفه منتقل می شود. با توجه به عدم اتصال Tx پورت پایین به Rx پورت بالا به واسطه هیچ مدیومی (مثلا فیبر نوری، کابل یا امواج رادیویی) داده ها قابلیت عبور در مسیر بازگشت را نداشته و یکسویه بودن انتقال اطلاعات تضمین خواهد شد.

الزام شماره ۴ :

عملیات کنترل جریان اطلاعات ۲ :

با توجه به عدم اتصال Tx پورت پایین به Rx پورت بالا به واسطه هیچ مدیومی (مثلا فیبر نوری، کابل یا امواج رادیویی) داده ها قابلیت عبور در مسیر بازگشت را نداشته و یکسویه بودن انتقال اطلاعات تضمین خواهد شد.

الزام شماره ۵ :

عملیات کنترل جریان اطلاعات ۳ :

داده های دریافتی از پورت بالا به مدار صرفا ارسال داده ارسال شده و پس از تبدیل به پالس های نوری از کانال فیبر نوری که Tx پورت بالا را به Rx پورت پایین مدار صرفا دریافت متصل می کند در مسیر یکطرفه منتقل می شود.

الزام شماره ۶ :

عملیات کنترل جریان اطلاعات ۴ :

با توجه به عدم اتصال Tx پورت پایین به Rx پورت بالا به واسطه هیچ مدیومی (مثلا فیبر نوری، کابل یا امواج رادیویی) داده ها قابلیت عبور در مسیر بازگشت را نداشته و یکسویه بودن انتقال اطلاعات تضمین خواهد شد.

الزام شماره ۷ :

عملیات کنترل جریان اطلاعات ۵ :

داده های دریافتی از پورت بالا به مدار صرفا ارسال داده ارسال شده و پس از تبدیل به پالس های نوری از کانال فیبر نوری که Tx پورت بالا را به Rx پورت پایین مدار صرفا دریافت متصل می کند در مسیر یکطرفه منتقل می شود. با توجه به عدم اتصال Tx پورت پایین به Rx پورت بالا به واسطه هیچ مدیومی (مثلا فیبر نوری، کابل یا امواج رادیویی) داده ها قابلیت عبور در مسیر بازگشت را نداشته و یکسویه بودن انتقال اطلاعات تضمین خواهد شد.