ویکی‌پدیا
دانشنامهٔ آزاد

امنیت سیستم نرم‌افزار

از ویکی‌پدیا، دانشنامهٔ آزاد

در مهندسی نرم‌افزار، **امنیت سیستم نرم‌افزار،** ایمنی سیستم را در طراحی، توسعه، استفاده و نگهداری سیستم‌های نرم‌افزاری و ادغام آنها با سیستم‌های سخت‌افزاری ایمن در محیط عملیاتی بهینه می‌کند.

بررسی اجمالی

ایمنی سیستم نرم‌افزار زیر مجموعه ای از امنیت سیستم و مهندسی سیستم و مترادف با جنبه‌های امنیت عملیاتی مهندسی نرم‌افزار است. به عنوان بخشی از کل برنامه ایمنی و توسعه نرم‌افزار، نرم‌افزار نمی‌تواند به‌طور مستقل عمل کند. سیستم‌های چندگانه ساده و بسیار یکپارچه هردو در حال رشد فوق‌العاده ای در استفاده از کامپیوترها و نرم‌افزار برای نظارت یا کنترل زیر سیستم‌ها یا عملکردهای ایمنی-بحرانی هستند. خطای مشخصات نرم‌افزار، نقص طراحی یا فقدان الزامات ایمنی-بحرانی عمومی می‌تواند موجب خرابی سیستم یا تصمیم اشتباه انسانی شود. برای دستیابی به سطح قابل قبول ایمنی برای نرم‌افزار مورد استفاده در برنامه‌های مهم، در ابتدا مهندسی ایمنی سیستم نرم‌افزار باید در تعریف نیاز و فرایند طراحی مفهومی سیستم مورد توجه قرار گیرد. سپس نرم‌افزار ایمنی-بحرانی باید مدام مورد توجه مدیریت و تجزیه و تحلیل مهندسی در طول توسعه و چرخه عملیاتی سیستم قرار گیرد.

در ابتدا تجزیه و تحلیل خطرهای عملکردی (FHA) اغلب به موازات یا به عنوان بخشی از تجزیه و تحلیل عملکرد مهندسی سیستم (برای تعیین توابع ایمنی-بحرانی (SCF) سیستم برای تجزیه و تحلیل بیشتر و بازبینی) به کار برده شدند. ایمنی سیستم نرم‌افزار به‌طور مستقیم به جنبه‌های مهم طراحی و ویژگی‌های ایمنی در نرم‌افزار و قابلیت سیستم ارتباط دارد، در حالیکه ویژگی‌های کیفی نرم‌افزار از لحاظ ذاتی متفاوت هستند و نیازمند بررسی دقیق استاندارد و دقت توسعه است. سطح اطمینان توسعه (DAL) و سطح دقت مرتبط (LOR) یک رویکرد درجه‌بندی شده به کیفیت نرم‌افزار و تضمین طراحی نرم‌افزار به عنوان پیش نیاز است که یک فرایند مناسب نرم‌افزار برای اطمینان بوسیله آن دنبال می‌شود. مفاهیم LOR و استانداردهایی مانند DO-178C جایگزین ایمنی نرم‌افزار نمی‌شوند. ایمنی نرم‌افزار هر IEEE STD-1228 و MIL-STD-882E بر الزامات ایمنی صریح و حتمی متمرکز شده و با استفاده از رویکردهای عملکردی از تجزیه و تحلیل الزامات ایمنی و دیدگاه تست تأیید می‌شود. تجزیه و تحلیل خطر ایمنی نرم‌افزار مورد نیاز برای سیستم‌های پیچیده تر که در آن نرم‌افزار توابع بحرانی را به‌طور کلی کنترل می‌کند در دسته‌های ترتیبی زیر هستند و در مرحله ای به عنوان بخشی از ایمنی سیستم یا فرایند مهندسی ایمنی انجام می‌شود: تجزیه و تحلیل الزامات ایمنی نرم‌افزار؛ تجزیه و تحلیل طراحی ایمنی نرم‌افزار (سطح بالا، طراحی دقیق و در سطح کد)؛ تجزیه و تحلیل آزمون ایمنی نرم‌افزار و تجزیه و تحلیل تغییر ایمنی نرم‌افزار. هنگامی که این تجزیه و تحلیل عملکردی ایمنی نرم‌افزار تکمیل می‌شود، تیم مهندسی نرم‌افزار می‌داند در هنگام طراحی در ویژگی‌های ایمنی نرم‌افزار برای اطمینان از عملکرد صحیح و شناسایی خطاها، خرابی‌ها، کاستی‌ها و پیاده‌سازی تعدادی از استراتژی‌های کاهش ریسک برای کنترل خطرات، کجا بر ایمنی تأکید کند و بر چه موضوعات عملکردی، مسیرهای عملکردی، دامنه‌ها و مرزهایی تمرکز کند. فناوری‌های امنیت نرم‌افزار و فناوری‌های مختلف محافظت از نرم‌افزار شبیه به ویژگی‌های ایمنی نرم‌افزار در طراحی برای کاهش انواع آسیب‌پذیری‌ها و خطرات تهدید است. نرم‌افزار تعیین‌کننده در طراحی بوسیلهٔ بررسی رفتار درست و قابل پیش‌بینی در سطح سیستم، مطلوب است.

اهداف

- ایمنی عملکرد از طریق توسعه مهندسی به دست می‌آید تا اطمینان حاصل شود که اجرای صحیح و رفتار توابع نرم‌افزار به صورت پیش فرض است
- ایمنی سازگار با الزامات مأموریت، در نرم‌افزار به شیوه ای به موقع و مقرون به صرفه طراحی شده‌است.
- در سیستم‌های پیچیده که شامل بسیاری از تعاملات می‌شوند، عملکرد ایمنی-بحرانی باید شناسایی و قبل از بروز خطرات و حفاظت از طراحی برای مقابله با آن، کاملاً بررسی شود.

- لیست‌های عملکردهای ایمن و لیست‌های خطرات مقدماتی باید فعالانه تعیین شوند و بر الزاماتی که در نرم‌افزار اجرا می‌شود، تأثیر بگذارند.
- عوامل مشارکت کننده و علل ریشه ای اشتباهات و خطرات ناشی از آن در ارتباط با سیستم و نرم‌افزار آن، شناسایی، ارزیابی و حذف می‌شود یا خطر تا سطح قابل قبولی، در طول چرخه کاهش می‌یابد.
- تکیه بر فرایندهای اجرایی برای کنترل خطر به حداقل می‌رسد.
- تعداد و پیچیدگی رابط‌های مهم ایمنی به حداقل می‌رسد.
- تعداد و پیچیدگی اجزای مهم ایمنی نرم‌افزار کامپیوتر به حداقل می‌رسد.
- اصول مهندسی صدا برای طراحی رابط کاربری-نرم‌افزاری، احتمال خطای انسانی را به حداقل می‌رساند.
- حالت‌های شکست، سخت‌افزار ضمیمه شده، نرم‌افزار، انسان و سیستم، در طراحی نرم‌افزار مشخص می‌شوند.
- عملیات و مستندات مهندسی نرم‌افزار صدا در توسعه نرم‌افزار مورد استفاده قرار می‌گیرد.
- مسائل ایمنی و ویژگی‌های ایمنی به عنوان بخشی از تلاش تست نرم‌افزار در تمام سطوح مطرح می‌شود.
- نرم‌افزار طراحی شده برای رابط کاربری انسان و ماشین، نگهداری و اصلاح یا ارتقاء را سهولت می‌بخشد.
- نرم‌افزار با قابلیت ایمنی-بحرانی باید با تجزیه و تحلیل عینی و ترجیحاً تست شواهدی مبنی بر تمام الزامات ایمنی بر اساس معیارهای مشخص شده مورد تأیید قرار گیرد.

این مقاله شامل مواد دامنه عمومی از ادبیات دولت ایالات متحده *مشترک سیستم ایمنی نرم‌افزار سیستم کمیته* نرم‌افزار سیستم مدیریت ایمنی *یک روش فنی و مدیریت تیمی* این سند در اصل از سمت وب به دست آمده "link|date=May 2018 |bot=InternetArchiveBot |fix-attempted=yes}} sys_service /% 5B% 5D (http://www.monm / ایمنی / http://www.monmouth.army.mil/cecom (outh.army.mil/cecom/safety/sys_service/%7B%7Bdead ". که این پایگاه در سال ۲۰۱۱ بسته شده‌است. یک PDF از این سند در https://web.archive.org/web/20171013125128/http://www.system-safety.org/Documents/Software_System_Safety_Handbook.pdf موجود است 2.15 مگابایت (ht tps://web.archive.org/web/20171013125128/http://www.system-safety.org/Documents/S oftware_System_Safety_Handbook.pdf)

جستارهای وابسته

- بیمه نرم‌افزار
- IEC 61508 ایمنی کاربردی

IEEE STD-1228 http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=467427&url=http%3A%2F%2Fieeexplore.ieee.org%2Fiel1/3257/9808/00467427 (http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=467427&url=http://ieeexplore.ieee.org/iel1/3257/9808/00467427)

- سیاست محرمانگی
- دربارهٔ ویکی‌پدیا
- تکذیب‌نامه‌ها
-
- توسعه‌دهندگان
- آمار
- اظهارنامهٔ کوکی