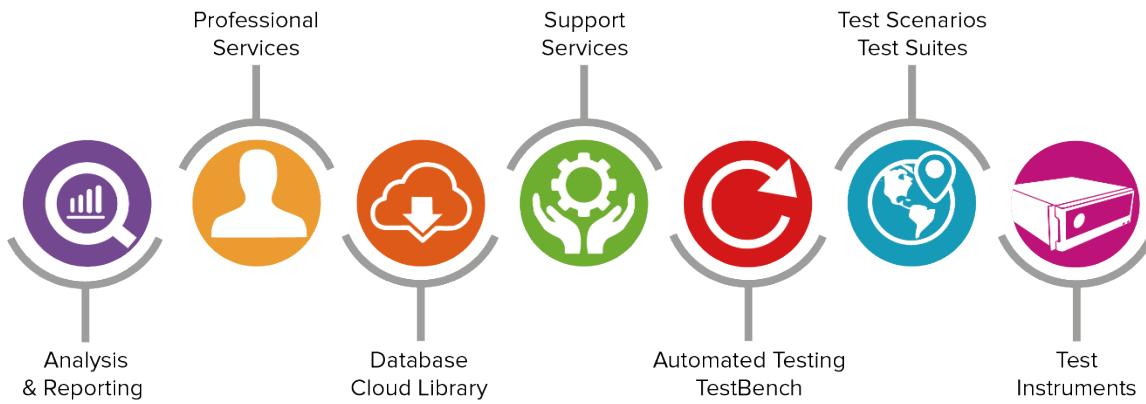


Spirent SimSAFE™

协作机构:



Spirent SimSAFE™

本文档的目的

本产品资料描述了SimSAFE™产品包的以下内容：

- 配置
- 功能
- 性能
- 可交付项

本产品资料还提供了各项技术数据和配置信息，包括订购编码等。然而，思博伦仍然建议您在订购前与您的思博伦销售代表讨论您的具体要求。

重要提示：目标用途声明

SimSAFE™的主要用于在实验室的非辐射环境中执行GPS欺骗模拟测试。

请注意：

SimSAFE™在任何情况下不得用于执行空中欺骗。

例如，对于正在研发的接收机或设备，SimSAFE™可用于在实验室中评估欺骗干扰对待测设备的影响。然而，SimSAFE™的设计目标不是为了在实验室环境之外生成欺骗信号用于干扰真实GNSS信号的接收。

思博伦只为SimSAFE™在本文档所描述的预期用途中的使用提供保证。思博伦不为将SimSAFE™挪作它用的后果承担责任，其中包括但不限于将SimSAFE™用作空中欺骗器。

专有信息

本文档内容中包含的专有信息为思博伦通信公司的财产。在未经思博伦通信公司书面特别授权的情况下，本文档的持有人应对本文档所有信息加以保密，并应像保护自己的保密信息一样，防止这些内容的全部或部分被披露和传播给任何第三方。

©思博伦通信公司版权所有2017年至2019年

本文档中所有其它注册商标的所有权归其各自所有者所有。

目录

本文档的目的.....	2
重要提示：目标用途声明	2
目录.....	3
表格清单.....	5
图表清单.....	5
简介.....	6
特性和优势.....	6
为何您会需要SimSAFE™.....	6
支持GPS L1、L2、L5和Galileo E1、GLONASS L1.....	6
LOS和多径信号上的伪距坡度生成.....	6
LOS和多径信号上的功率电平坡度生成.....	7
伪码、载波和功率电平的偏移量控制.....	7
正弦多径信号的生成.....	7
接收机和模拟器测量结果的可视化.....	7
接收机和模拟器测量结果的对比.....	7
多径信号的生成.....	7
接收机测量结果和模拟器测量结果的日志记录.....	8
SimREMOTE命令的日志记录.....	8
压制干扰的模拟 – 需要兼容的干扰生成器.....	8
天线位置的修改.....	8
通过NTP或GPS PPS在SimSAFE™真实天空信号模式下实现的时间同步	8
模拟信号模式下的轨迹控制.....	8
受支持的GNSS接收机包括:.....	8
卫星克隆 – 可用于执行模拟信号模式下的导航数据攻击.....	9
用户行动调度器.....	9
授时欺骗攻击.....	9
模拟的导入/导出	9
接收信号参数显示窗口.....	9
自动启动/停止日志记录.....	9
经改进的选星模式.....	9
对只使用参考接收机的配置提供的支持.....	10
多径创建辅助功能.....	10
模拟信号模式下的轨迹控制.....	10
SimSAFE™真实信号模式下的轨迹控制.....	10
多轨迹位置显示.....	10
欺骗攻击的生成.....	10
含平滑欺骗信号的多/单通道(粗同步).....	10
含多普勒偏移的多/单通道(粗同步)	11
多/单通道(细同步)	11
正弦欺骗信号.....	11
干扰后再欺骗.....	11
导航数据篡改.....	11
真实信号回放(假象干扰)	11

Spirent SimSAFE™

SimSAFE™概览	12
SimSAFE™的功能	12
工作原理.....	12
SimSAFE™的配置模式.....	13
SimSAFE™模拟信号模式	13
SimSAFE™真实天空信号模式	14
配置的适用范围.....	16
SimSAFE™真实信号模式配置中的时间同步.....	16
模拟信号模式配置中的轨迹控制.....	17
监视接收机性能和评价消减策略.....	18
GNSS干扰探测器 (GID)	19
NMEA监视器.....	20
性能规格.....	21
总体概览.....	21
授权.....	21
一般性限制.....	21
支持的软件.....	21
支持的硬件.....	21
性能规格.....	22
精度 - 信号生成.....	22
信号能力.....	22
精度 - 接收机测量结果监视.....	23
系统更新率.....	23
SimSAFE™真实信号模式的时间校准.....	24
订购信息.....	24
交付物.....	24
支持和保证.....	27
Septentrio PolarRx5接收机	27
u-blox EVK-M8N评价工具包.....	27
戴尔笔记本电脑.....	27
参考文档.....	27
相关产品出版物.....	28

表格清单

表1 - SimSAFE™配置对比	16
表2 - 根据所用的方法规定的真实信号模式下的时间偏移量	17
表3 - SimSAFE™真实信号模式的运行方式和典型用途	18
表4 - GID特性	19
表5 - 信号范围和分辨率	22
表6 - 信号相关性能	22
表7 - 接收机测量结果监视性能说明 (GID)	23
表8 - SimSAFE™软件功能的更新率	23
表9 - SimSAFE™真实信号模式的时间校准规格	24
表10 - SimSAFE™真实信号模式的可交付项	24
表11 - 1PPS设备同步的可交付项	26
表12 - SimSAFE™模拟信号模式的可交付项	26
表13 - SimSAFE™ 被测接收机的可交付项	26
表14 - SimSAFE™ 软件交付项	27
表15 - 参考文档	27
表16 - 相关产品出版物	28

图表清单

图1 - 典型SimSAFE™主显示窗口	12
图2 - SimSAFE™模拟信号模式配置图	14
图3 - SimSAFE™真实信号模式配置图	15
图4 - 示例接收机监视结果显示图	19
图5 - GNSS干扰探测 (GID) 窗口	20
图6 - NMEA查看界面	20

Spirent SimSAFE™

简介

SimSAFE™测试工具是一种支持与SimGEN和GNSS接收机建立接口的软件应用，目的是为在实验室中对接收机漏洞评估和信号验证策略的开发提供便利。在参考（“真实”）信号的基础上，SimSAFE支持用户对关键参数进行自定义修改，例如功率、伪距和导航消息内容等，从而生成所谓的“欺诈”信号，SimSAFE™可以帮助用户仿真出欺骗攻击，并在同时对被攻击接收机进行实时监视。

SimSAFE™支持两种测试配置模式(架构)：

- **SimSAFE™模拟信号模式** – 合法的真实GNSS信号和欺骗信号均由模拟产生。
- **SimSAFE™真实信号模式** – 作为环境空间信号(SIS)的GNSS信号在被天线接收后会被用作真实GNSS信号，“真实信号”和“伪造欺骗信号”经合路通过同轴电缆输出到被测接收机。SimSAFE™可以避免因测试的目的而将“欺骗”的信号广播出去。

特性和优势

为何您会需要SimSAFE™

SimSAFE™支持用户对欺骗攻击(虚假或复制GNSS信号)对GNSS接收机造成的影响进行评估。它还可以帮助用户模拟一系列不同的攻击向量，从使用简易装备发起的简单攻击，到使用带坡度功率水平，并在欺骗前利用干扰强迫接收机进入重新捕获模式，甚至篡改广播消息中导航数据的精密攻击。

SimSAFE™还可以实现对高水平的接收机监视，帮助您理解接收机在面对真实和伪造信号时的不同反应。

SimSAFE™的主要应用领域包括：

1. 评价GNSS欺骗攻击对用户系统或GNSS接收机造成的影响。SimSAFE™能够模拟多种可能的欺骗攻击向量，是执行GNSS系统漏洞风险评估时的必备工具。
2. 干扰消减技术或信号验证策略的开发。虽然我们支持用户选择的任意GNSS接收机来执行这项工作，但如果被测接收机支持Septentrio二进制文件(SBF)，SimSAFE™将提供一系列接收机监视工具，更好地满足用户测试需求。为此，本解决方案的标准配置中也附带了一台合适的Septentrio接收机。

SimSAFE™具备一系列全球领先的特性，使您能够在欺骗模拟中拥有前所未有的控制水平：

支持GPS L1、L2、L5和Galileo E1、GLONASS L1

SimSAFE™支持L1频段的GPS、Galileo和GLONASS信号，以及GPSL2和L5的频段信号。

LOS和多径信号的伪距坡度生成

当接收机的相关器锁定欺骗信号时，伪距坡度可用于改变目标GNSS接收机的位置。欺骗攻击的目的就是让目标接收机报告不正确的位置

(或时间) – 一旦接收机锁定了欺骗信号, 伪距坡度会逐渐改变卫星的测距信息, 使目标接收机看起来似乎漂移到了一个全新的位置。这一特性使用户可以非常有效地控制测距信息, 适合在需要修改不同高度的多卫星测距信息的导航解决方案中使用。

LOS和多径信号的功率水平坡度生成

当模拟启动后, 这种特性可以对欺骗信号的功率水平持续进行持续调节 – 该功率水平可能在模拟开始时低于实际信号, 但可以逐步爬坡上升, 并找出目标接收机会在怎样的功率水平下易受到欺骗信号的危害, 而且它还可以使该功率逐渐下降, 确定接收机会在何时停止跟踪该欺骗信号。该特性可以提供对功率水平的完整控制, 并允许在模拟的全过程中对功率水平加以控制。

伪码、载波和功率水平的偏移量控制

SimSAFE™允许在模拟时对伪码、载波和功率水平的偏移量进行设置。伪码和载波偏移量可在以模拟信号回放攻击时使用, 而功率水平偏移则可以实现对功率水平的校准 – 这对于任何欺骗模拟而言都十分重要, 因此该特性已成为任何GNSS欺骗模拟器的一项必备功能。

正弦多径信号的生成

正弦信号是一种可以协助设置“智能”型干扰机模拟的特性。正弦波形可用于同时攻击多台接收机 – 它不仅是一种可能的攻击向量, 而且在模拟中使用这种波形类型开展实验的能力将使用户具备一种非常先进的特性。

接收机和模拟器测量结果的可视化

接收机测量结果在查看时既可以使用Septentrio接收机, 也可以使用带NMEA格式输出的标准GNSS接收机。前者可以实现一些扩展查看功能, 因为SimSAFE™支持其专有接口, 而后者的查看功能则相对有限一些。模拟器测量结果也可以在SimSAFE™中或通过SimGEN查看。当我们需要了解欺骗信号对目标接收机造成的影响时, 查看接收机测量结果的能力便具有至关重要的意义, 而将所有模拟器设置实时可视化的能力也同样不可或缺。这两方面的能力可以让用户对仿真过程和结果有更深层次的认知。

具备查看欺骗信号对目标接收机造成影响的能力是非常重要的, 因为它可以帮助开发者更好地弄清楚接收机中最有效的欺骗信号监测机制。C/N0和PR率的变化值是GNSS接收机中最值得监视的两项参数 – SimSAFE™可实现对模拟过程中所有阶段的接收机和模拟重要参数的实时监视。

接收机和模拟器测量结果的对比

SimSAFE™具备支持用户实时查看测试结果的特性 – 这就使用户可以对模拟器和接收机测量结果进行对比, 并对多种实验性数据加以捕捉。

多径信号的生成

SimSAFE™将其生成的欺骗信号称为“回声(Echo)”, 这样可以很方便地区别在模拟设置过程中以及模拟信号模式期间的真实和欺骗信号。当SimSAFE™与单台思博伦GNSS模拟器结合使用时, SimSAFE™可以将模拟器的多径信道用作欺骗信号的传输通道。

Spirent SimSAFE™

接收机测量结果和模拟器测量结果的日志记录

从模拟中捕捉数据并供日后详细分析的能力有时比模拟数据的实时监视更加重要。SimSAFE™的独特设计可同时支持这两种能力，能够以实时方式将数据可视化，并以日志方式将数据记录下来，以便日后对其加以分析。

SimREMOTE命令的日志记录

SimREMOTE是适用于思博伦全系列GNSS模拟器的实时外部远程控制和运动数据接口。SimSAFE™允许用UCD格式将所有SimREMOTE命令记录到日志中。

压制干扰的模拟 – 需要兼容的干扰生成器

欺骗目标接收机的最简单方法之一就是，当目标接收机处于捕获模式时，以高于真实GNSS卫星的功率水平广播伪造信号 – 这样可以使目标接收机更容易锁定这些欺骗信号。而强迫GNSS接收机进入捕获模式的方法之一就是首先对其进行干扰，即使用足够的功率来阻止它跟踪真实的GNSS卫星信号。SimSAFE™也可以实现与外部信号生成器的协作运行，从而利用SimSAFE™接口来模拟和控制“先干扰后再欺骗”的攻击向量。目前，SimSAFE™已可兼容思博伦GSS7765干扰生成器。

天线位置的修改

在模拟的过程中，用户可以将天线偏移施加在模拟出来的天线位置上。这在需要改变天线位置的静态场景中是一项非常有用的特性。利用该特性，天线在X、Y和Z轴的模拟位置均可以移动500米。

通过NTP或GPS PPS在SimSAFE™真实天空信号模式下实现的时间同步

要在欺骗模拟中将真实天空GNSS信号与模拟出来的GNSS信号结合在一起往往回遇到很大的问题，主要是因为真实天空信号与模拟信号之间的时间同步问题。幸运的是，SimSAFE™可以完成以上所说的所有工作。根据具体的实验需求，用户可以从SimSAFE提供的两种同步技术中自行选择。在有Internet连接的情况下，您可以使用NTP版本，通过精确的网络时间来实现同步。而在没有Internet连接的地方（这种情况在封闭的实验室中很常见），SimSAFE™还可使用GPS接收机的1PPS输出来提供所需的同步水平。

模拟信号模式下的轨迹控制

SimSAFE™支持创建动态（非静态）的欺骗攻击场景 – 也就是说，欺骗信号的伪距可以与用户在场景开始时所设置的轨迹完全匹配，也可以在场景运行期间由用户调节。也就是说，利用该能力可对有车辆参与的欺骗场景进行设置和评价。轨迹功能则可以设置出最大3000米的偏移值范围。

受支持的GNSS接收机包括：

- Septentrio PolaRx4 PRO
- Septentrio PolaRx5
- 普通NMEA 接收机

卫星克隆 – 可用于执行模拟信号模式下的导航数据攻击

这是一种可以让用户对信号源文件进行修改的工具。克隆出来的卫星拥有与另一颗卫星相同的PRN、轨道和导航电文信息，但ID有所不同。也就是说，用户可以设置和配置一颗克隆卫星，然后对克隆卫星的伪码和载波偏移量进行设置，甚至可以对克隆卫星发送的导航电文信息进行修改，因此当SimSAFE™和单台模拟器组成系统运行时，通过修改导航电文实施欺骗干扰便成为了可能。

用户行动调度器

SimSAFE™可以提供一种可对信号修改命令、多径创建命令和功率切换命令进行调度的全新设置窗口。在模拟启动前，用户可以对欺骗攻击的执行方式加以定义，并利用相同配置使该次模拟进行一次或多次。

授时欺骗攻击

SimSAFE™可以提供一种模拟时间欺骗攻击的简单方法。用户行动调度器可以利用对af0(时钟偏差)、af1(时钟漂移)和af2(时钟漂移率)这几项参数来定义欺骗攻击。SimSAFE™通过修改以上参数对欺骗信号的范围进行修改。

模拟的导入/导出

UCD文件可在SimSAFE™场景运行过程中生成(即在运行时以日志方式记录所用的信号修改命令)，也可以(利用可配置的更新率)导出命令调度器窗口中创建的命令并对其加以预处理。

如果UCD文件在模拟运行时创建，而SimSAFE™拥有可见卫星的信息，因此它将只为这些视野范围内的卫星创建UCD命令(在轨迹欺骗场景中尤其推荐使用该方法)。

接收信号窗口

接收信号窗口的设计可以为模拟器和接收机的测试数据提供清晰的可视化。该窗口由一个表格构成，每一行均对应一个独立的信号。用户可以选择一行或多行，并将其拖放至调度器中，以便定义需对哪些信号进行修改。

自动启动/停止日志记录

用户可以自行决定是否允许日志记录在模拟执行时自动启动和停止。

经改进的选星模式

待模拟卫星的选择方式有3种定义机制：

场景启动时的可见卫星：如果该选项被选中，则只有在模拟开始时可见的卫星才会被启用，而在模拟过程中才变得可见的卫星将被禁用(它们将不会在模拟过程中出现)。

所有卫星：如果该选项被选中，在模拟过程中变得可见的卫星将不会被禁用(选择过程由SimGEN负责处理)。

手动选择：如果该选项被选中，用户可以手动选择要模拟哪些卫星。

Spirent SimSAFE™

对只使用参考接收机的配置提供的支持

SimSAFE™还支持一种只在真实天空信号配置中可用的全新配置选项，即使用单台具备SBF能力的接收机作为参考。利用该配置可执行模拟时，参考接收机被用于提供导航消息的复本、日志记录，以及参考测量结果（在GID模块中的）可视化功能。

多径创建辅助

在用户行动调度器的多径开/关选项卡中，SimSAFE™可以提供图形控制能力，以便计算出用作回声的最佳信号集。最佳集的计算时要选择可优化下列参数之一的卫星：GDOP、PDOP、HDOP、VDOP和TDOP。此外，通过选择那些范围最小的卫星，也可以完成最佳集的计算。

模拟信号模式下的轨迹控制

SimSAFE™引入了不同类型的模拟欺骗轨迹攻击：“难”、“中”和“易”。这一难度概念指的是真实场景中攻击的复杂程度。在“难”欺骗难度下，欺骗信号发射器的位置和轨迹被假定与被攻击接收机相同，或者欺骗方能够完美地补偿其（与受攻击对象的）相对动态。在“中”难度下，欺骗方和被攻击接收机并不处于相同的位置，但欺骗方会估计被攻击接收机的位置（但会在估计中产生一些误差）。SimSAFE™引擎会充分考虑欺骗方造成的估计误差。在“易”欺骗难度下，欺骗方和被攻击接收机被假定处于不同的位置，而且欺骗方不会对被攻击接收机的位置进行估计，因此也不会为相对动态提供补偿。

SimSAFE™真实天空信号模式下的轨迹控制

SimSAFE™可在真实天空信号模式的配置中提供轨迹控制能力。在这种情况下，欺骗信号以GNSS RF模拟器生成的LOS信号的形式出现，而真实的信号通过使用天线从真实的卫星直接接收。在真实天空信号模式的配置下，可选择的欺骗难度只有“难”，而且真实轨迹都应是静态的。

多轨迹位置显示

在SimSAFE™中，被攻击接收机计算出的位置、真实轨迹、欺骗性轨迹和欺骗方轨迹都会在一个专用窗口中以图形方式显示。

欺骗攻击的生成

SimSAFE™能够模拟多种真实的欺骗攻击类型：

含平滑欺骗信号的多/单通道（粗同步）

- 攻击者会创建一个或多个欺骗信号，其最初的偏移介于500米至600米之间，衰减为10 dB。
- 伪距坡度可以减少码延迟（在确定伪距坡度的变化速度时，您必须将接收机PLL的带宽也考虑在内）。当编码延迟接近零时，可以提高欺骗信号的强度，强迫接收机相关器锁定新的伪造信号。

含多普勒偏移的多/单通道（粗同步）

- 这种攻击与之前的相同，但欺骗信号并不改变其多普勒特性。编码/载波延迟（相对于视线信号）改变时的步进为5至10米，也可以使用某个伪距坡度。

多/单信道（细同步）

- 欺骗信号在生成时已经具备一个初始大小为数米的码延迟（相对于视线信号）。欺骗信号的强度会缓慢增加，其初始衰减为5-10dB。接下来，欺骗信号会从视线缓慢移开，不仅会导致位置偏移，还会避免锁定丢失。

正弦欺骗信号

- 通过利用正弦模式改变伪码和信号强度，欺骗信号会尝试攻击特定区域内的多台接收机。

干扰后再欺骗

- 为避免根据信号强度和跟踪功能来探测攻击信号，并迫使接收机转变为捕获状态，您可以在欺骗攻击之前施加一次干扰攻击（例如，信号记录与回放、信号模拟和粗略同步欺骗），并导致码锁定丢失。

导航数据篡改

- 欺骗信号会篡改位置计算所用的导航消息中的内容，导致接收机计算出位置发生的精度发生恶化。

真实信号回放攻击（假象干扰）

- 通过回放来自空间的真实卫星数据，可生成欺骗信号，从而欺骗任何基于卫星数据真实性验证机制。

Spirent SimSAFE™

SimSAFE™概览

SimSAFE™的功能

工作原理

SimSAFE™测试工具是一种与SimGEN和GNSS接收机建立接口的软件应用，目的是故意伪造出GNSS信号，加快实验室中对接收机漏洞评估进程，并对欺骗信号的探测和消减策略的有效性进行验证。

通过允许通过用户自定义的方式实现对关键参数篡改，例如功率、伪距和导航电文内容，在参考（“真实”）信号的基础上形成一个（“欺诈”）信号，SimSAFE™可以帮助用户仿真出GNSS欺骗攻击，并同时对被攻击接收机进行监测。

SimSAFE™支持两种测试配置（架构）：SimSAFE™真实天空信号模式和SimSAFE™模拟信号模式。

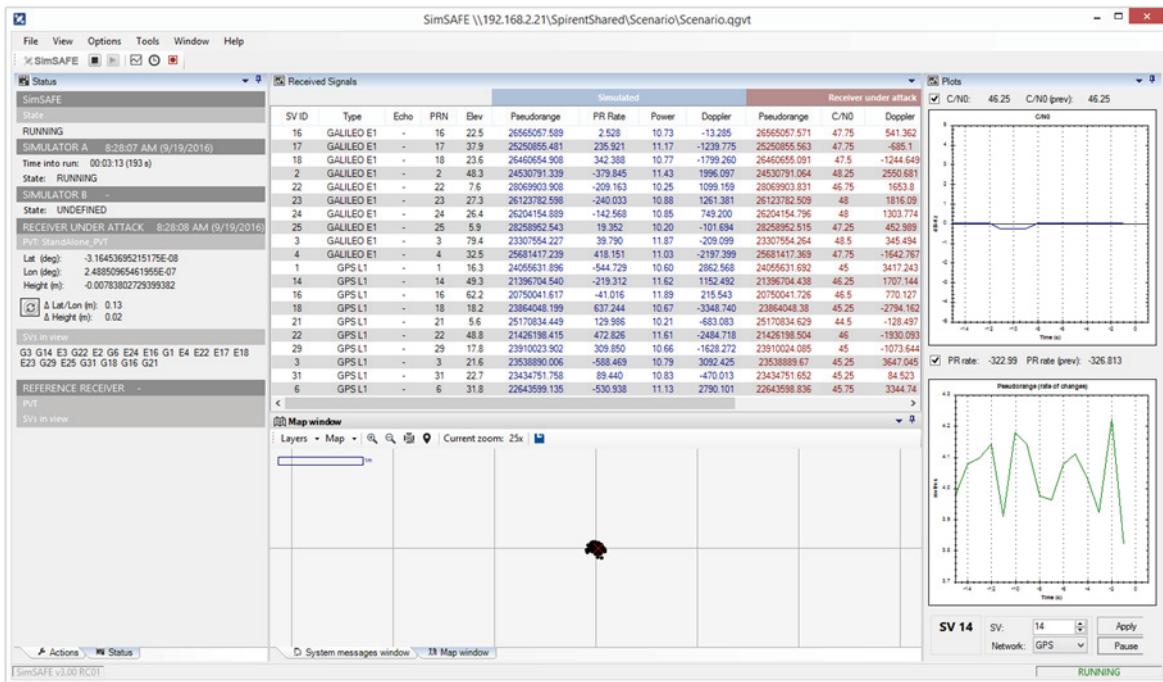


图1 - 典型SimSAFE™主显示窗口

SimSAFE™运行在自己的控制器上，与运行SimGEN的控制器完全独立。SimSAFE™可通过向SimGEN发送的远程命令来控制模拟器。这样便可以让软件来选择和编辑各类场景，并将所有的各类必要参数传递给SimGEN来仿真出欺骗攻击。

尽管欺骗信号都是模拟产生的，但通过真实天空信号或模拟器也可以提供（用于测试用途的）真正的信号，分别以SimSAFE™真实天空信号模式或SimSAFE™模拟信号模式的配置形式来实现。

需要注意的是，如果真实天空信号的GNSS信号被用作真正的信号，那么就需要使用一台Septentrio监视接收机。然而，如果模拟器既能提供真正的GNSS信号，也能提供欺骗GNSS信号，则无需使用监视接收机。

SimSAFE™还可以提供监视功能，用于监视被测设备的性能，并可对可能的消减策略的效性进行评价，支持NMEA消息类型的普通接收机也具备监视能力。

SimSAFE™的配置模式

SimSAFE v3.02支持两种配置：

- SimSAFE™模拟信号模式
- SimSAFE™真实天空信号模式

每项配置所用的GNSS信号模拟器类型是完全不同的，因此所得的执行欺骗模拟的系统能力也不尽相同。

每项配置都提供使用或不使用GNSS接收机的选项：

- 两台接收机：如果使用了两台接收机（只在SimSAFE™ Live中可用），其中一台（参考接收机）会被用于提供参考测量结果，以便与第二台接收机（被测接收机）的测量结果进行对比。该配置选项在SimSAFE™ Live和SimSAFE™ Dual Box中可用。
- 一台接收机（被攻击接收机）。该接收机为被测接收机（可以是支持SBF协议的Septentrio接收机，也可以是支持NMEA协议的其它接收机）。
- 一台收机（参考接收机）。该接收机为参考接收机（应当是支持SBF协议的Septentrio接收机，也可以是支持NMEA协议的其它接收机）。该选项只在SimSAFE™真实天空信号模式的配置中可用。
- 一台接收机。该接收机为被测接收机（可以是支持SBF协议的Septentrio接收机，也可以是支持NMEA协议的其它接收机）。
- 无接收机。SimSAFE™不与被测接收机建立接口。该选项假定对接收机测量结果的监视由第三方软件来执行。

参考接收机必须是一台支持SBF（Septentrio二进制文件）的Septentrio接收机。被测接收机可以是一台SBF接收机或支持NMEA协议的普通GNSS接收机。在第二个选项中，SimSAFE™监视能力会受到标准NMEA 0183协议可交换的信息量的限制。

SimSAFE™模拟信号模式

该配置使用单台GNSS信号模拟器来生成真实卫星模拟信号和欺骗信号。该配置不需要使用真实空间卫星信号，并具有在“受控程度更高”的环境中实现攻击测试的优势。例如，它可以控制干扰信号相对于真实信号的相位（因具备毫米级的精度而无需担心载波/编码的偏移）。模拟信号模式下的信号配置还可以用于测试动态场景（无需使用第二台模拟器）。利用视线（LOS）和欺骗，真实卫星模拟信号利用模拟器的LOS功能生成，而欺骗信号则使用模拟器的多径能力模拟产生。

以下列表定义了使用SimSAFE™模拟信号模式的配置测试GNSS接收机的必需和可选（斜体组件）：

- SimSAFE™ 软件
- SimGEN软件
- 1台GSS6700、GSS7000或GSS9000模拟器
- 1台被测接收机（具备SBF或NMEA能力）

Spirent SimSAFE™

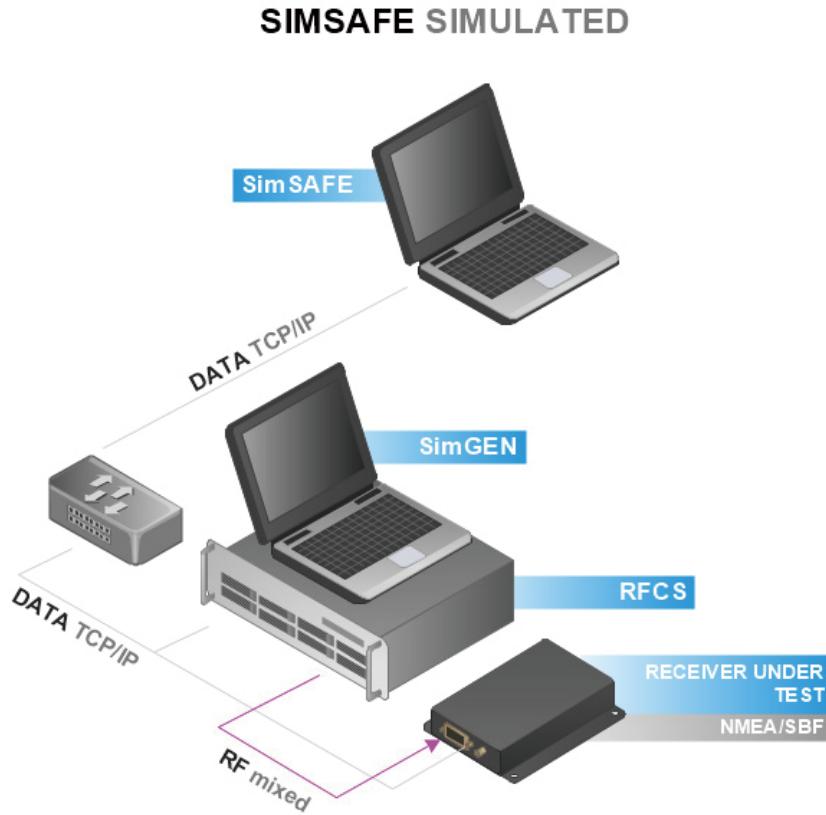


图2 - SimSAFE™模拟信号模式的配置

即使没有具备SBF能力的接收机,这项SimSAFE™模拟信号模式的配置也可使用。在本案例中,SimSAFE™可以在不显示任何接收机信号和测量结果的情况下实现对信号的控制。需要强调的是,在使用SimSAFE™模拟模式的配置时,欺骗和真正信号之间的延迟是已知的(因为它们都由相同的模拟器时钟生成,并且都受SimSAFE™的控制)。

SimSAFE™真实天空信号模式

该配置适用于使用真实天空信号的欺骗场景模拟。当在该配置中运行时,SimSAFE™会对要与GNSS时间同步的模拟执行进行调度。这样便可能使模拟出的信号与真实天空等真正的信号实现最初的同步。

可用的两种时间同步选择包括:

- NTP:该配置需要使用网络时间协议(NTP)客户端来实现SimSAFE主机与UTC时间的同步。该配置能够在不使用额外设备的情况下完成时间同步,但需要用到一台NTP服务器或Internet接入。
- 1PPS:使用一个u-blox评价工具包和思博伦提供的一个USB适配器来同步模拟的起始时间。该选项可以提供更高的精度,而且不需要Internet连接。

以下列表定义了使用SimSAFE™真实天空信号模式的配置来测试GNSS接收机的必需和可选(斜体)组件:

- SimSAFE™软件。
- SimGEN软件。

- 1台思博伦GSS6700、GSS7000或GSS9000模拟器。
- 1条辅助输出端口线(仅用于GSS6700且由思博伦提供)。
- 1套u-blox EVK-M8N,含思博伦提供的适配器(仅用于1PPS套装同步选项)。
- 1台GNSS参考接收机,含1PPS和10MHz输出(或1台Septentrio PolaRx4 Pro或PolaRx5接收机)。
- 1台被测接收机。

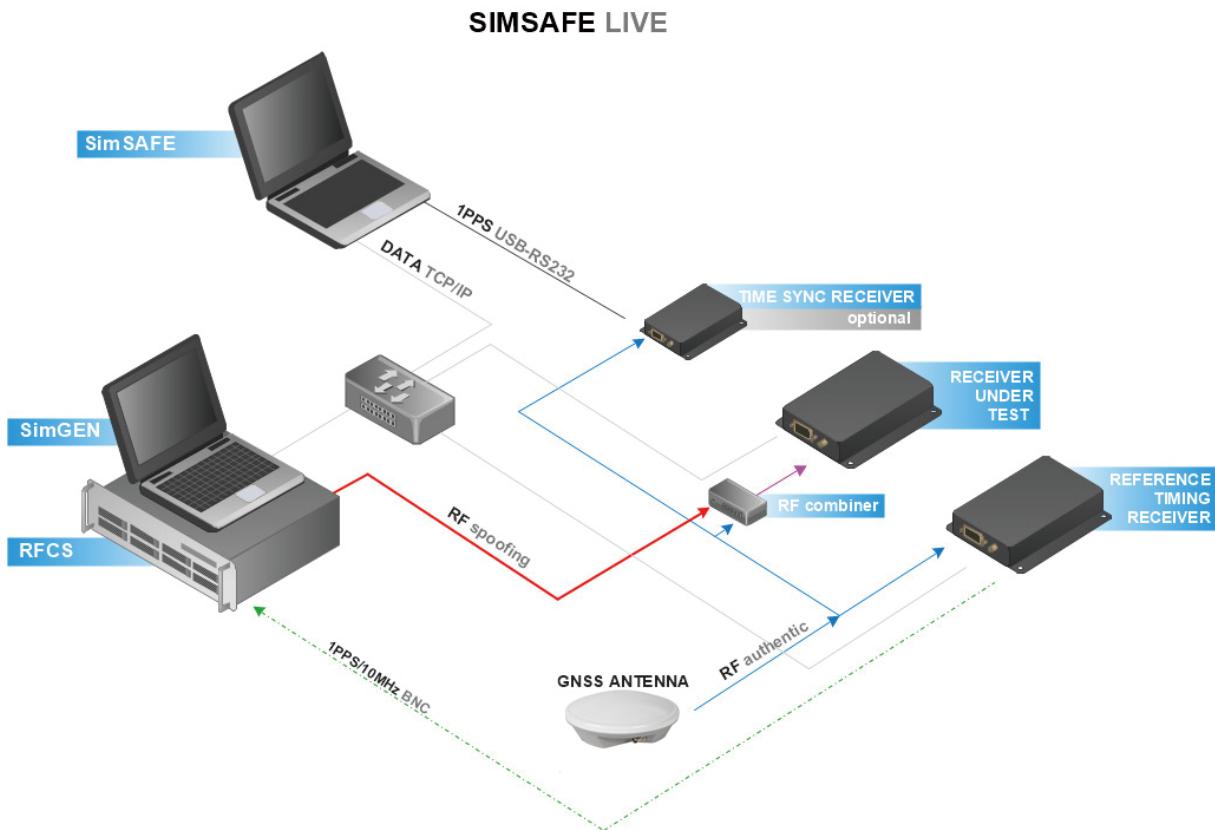


图3 - SimSAFE™真实天空信号模式配置示意图

由于包含了作为该配置中具备SBF能力的可选被测接收机的第二台Septentrio PolaRx4 Pro或PolaRx5接收机,SimSAFE™可以将被测接收机的测量结果与参考接收机的测量结果进行对比。此外,它可以提供以下功能(在本例中不需要有联网的被攻击接收机):

- 在模拟器模拟出的信号上复制出真实信号正在广播的导航消息内容。
- 真实的信号观测量日志记录。
- 为GNSS RF模拟器提供时间和频率参考。

如果该配置中未出现一台具备SBF能力的参考接收机,参考接收机仍然必须用于向GNSS信号模拟器提供10MHz和1PPS输出。

Spirent SimSAFE™

配置的适用范围

表1显示的是SimSAFE™的两种可用配置所具备的功能差异。配置的选择实际上取决于所要执行的测试类型 – SimSAFE™模拟信号模式可提供全面的纯模拟能力 – 它可以完美地实现信号同步，并在任何需要的情形下建立“实际”星座。在另一方面，SimSAFE™真实天空模式虽然不能提供对实际信号的任何控制，但可以用于更精确地演示欺骗攻击中可能出现的实际困难。

表1 - 可用SimSAFE™配置对比

	SimSAFE™ 真实天空信号模式	SimSAFE™ 模拟信号模式
主要目的	利用天空真实信号开展静态场景开展测试。	在完全模拟出来的信号环境中开展动态场景的欺骗测试。
是否使用空间信号	是	否。天空信号由模拟产生，而欺骗信号是由模拟产生的多径信号。
信号同步精度	若干纳秒，具体数字取决于接收机的1PPS精度、思博伦校准和所用的星历数据精度。	信号可以实现完美校准(0纳秒)，完全控制载波相位和码延迟。 无需与GNSS系统时间同步。
对导航电文内容的控制	可与模拟信号中广播数据的内容实现比特级的匹配。可用于修改某些数据字段的内容。	可用于修改某些数据字段的内容(使用卫星克隆工具)。
是否支持静态场景的模拟	是	是
是否支持动态场景模拟	否	是
每个PRN的欺骗信号数	1	4
是否支持被攻击接收机的反馈回路(用于同步)	是，当接收机通过TCP/IP支持SBF时。	是，当接收机通过TCP/IP支持SBF时。 当所用的为一台SDR或NMEA接收机，且信号延迟已知时，不需要为欺骗信号的同步提供反馈回路。

SimSAFE™真实信号模式配置中的时间同步

SimSAFE™在真实天空信号配置中支持两种时间同步方法：

- NTP：该配置需要用到网络时间协议(NTP)客户端，以便实现SimSAFE主机与UTC时间的同步。该配置能够在不使用额外设备的情况下完成时间同步，但需要用到一台NTP服务器或Internet接入。
- SW1PPS：使用一个u-blox接收机和思博伦提供的一个USB适配器来同步模拟的起始时间。该选项可以提供更高的精度，而且不需要Internet连接。此外，以下的额外项目也必不可少：

- u-blox EVK-M8N接收机
- USB电缆 (Type B公头至Type A公头, 包含在u-blox评价工具包中), 用于为接收机供电。
- 串行RS232电缆和串行RS232至USB转换器, 用于获取SimSAFE™中的1PPS信息。
- SMA RF 3向分流器和SMA电缆: 用于分离真实天空信号并将其连接至u-blox接收机的RF输入。

表2 - 不同方法下真实天空信号模式配置中规定的时间偏移

方法	值	说明
NTP服务器	最大200毫秒	NTP客户端将提供一份可用NTP服务器列表。需确保所用的NTP服务器时间偏移低于规定的值。
u-blox至串行RS232	最大0.25微秒	
使用USB 1.1适配器的u-blox至串行RS232连接	最大1毫秒	
使用USB 2.0适配器的u-blox至串行RS232连接	最大100微秒	

模拟信号模式配置中的轨迹控制

SimSAFE™目前支持对动态场景的模拟, 其中回声/多径信号的范围与用户定义的轨迹一致。该功能仅在(模拟模式)单GNSS模拟器配置中可用。通过了解真实的轨迹、欺骗性轨迹和卫星的位置, SimSAFE™能够(在模拟时)计算出要施加在用户启用的欺骗/回声信号上的伪距偏移。SimGEN中生成的多径信号的范围, 都与真实的车辆轨迹一致, 而且SimSAFE™会计算这些伪距和欺骗轨迹所计算出的伪距之间的差异。这些差异被用作(用户选定的)多径信号伪码和载波延迟的偏移。因此, 模拟出的LOS信号与SimGEN定义出的轨迹相一致, 而多径信号与SimSAFE™定义出的轨迹相一致(即认定欺骗者的发射位置与车辆的位置恰巧重合)。

SimSAFE™真实天空信号模式可在不同的硬件设置或运行模式下运行, 这些设置和模式在进行欺骗信号测试时均具备不同的功能和能力。

Spirent SimSAFE™

本表描述的是SimSAFE™真实天空信号模式的硬件(或运行模式)和典型用途：

表3 - SimSAFE™真实天空信号模式的运行模式和典型用途

SimSAFE™ Live 硬件	用途
模拟器 + 参考接收机(SBF) + 被测接收机(SBF)	两台接收机均接收真实卫星信号。 SimSAFE™真实天空模式会对来自参考接收机与被测接收机的数据进行对比，并复制广播导航数据消息的内容。 除动态场景外的所有系统的功能均为可用。
模拟器 + 被测接收机(SBF) + 通用接收机	不使用参考接收机，只使用一台可选的通用GNSS接收机，向模拟器提供1PPS和10MHz输入。 如果您不需要复制导航电文时可以使用该模式。
模拟器 + 被测接收机 (SDR或通用NMEA)	当被测接收机为软件定义的接收机时，或不支持与SimSAFE™的通信，或只支持NMEA时，可使用该模型。 该模式不允许从被测接收机获得同步信息(多普勒、伪距、时钟偏移)。 说明：必须提供1PPS和10MHz的源，以便利用真实天空信号对模拟器信号进行校准。

监视接收机性能和评价消减策略

用户可以选择使用SimSAFE™来监视被测设备(DUT)的性能，也可以选择使用自己的接收机监视和日志记录工具。

需要注意的是，SimSAFE™在运行时不需要监视接收机，因此信号生成和被测设备监视均可独立执行。

SimSAFE™提供两种类型的接收机监视：

1. GNSS干扰探测器(GID)
2. NMEA监视器

接收机也可以由用户自己的工具来负责监视，因为SimSAFE™不需要从接收机获得任何信息便可生成欺骗场景。

GNSS干扰探测器 (GID)

支持SBF(Septentrio二进制文件)的接收机还可获得更多监视工具的支持。为此,适用的接收机都会随SimSAFE™附带该工具。

下面的表4对GID的关键特性进行了归纳。

表4 - GID特性

探测方法	可用特性
	伪步进探测
利用接收机输出数据进行探测	C/N0步进探测 RAIM 信道锁定丢失
	导航电文监视
利用与基准接收机的数据对比进行探测	PVT解决方案

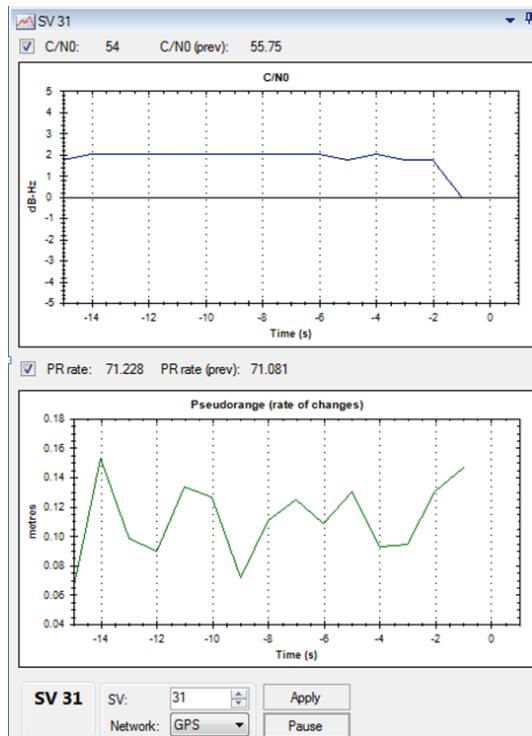


图4 - 示例接收机监视屏幕

Spirent SimSAFE™

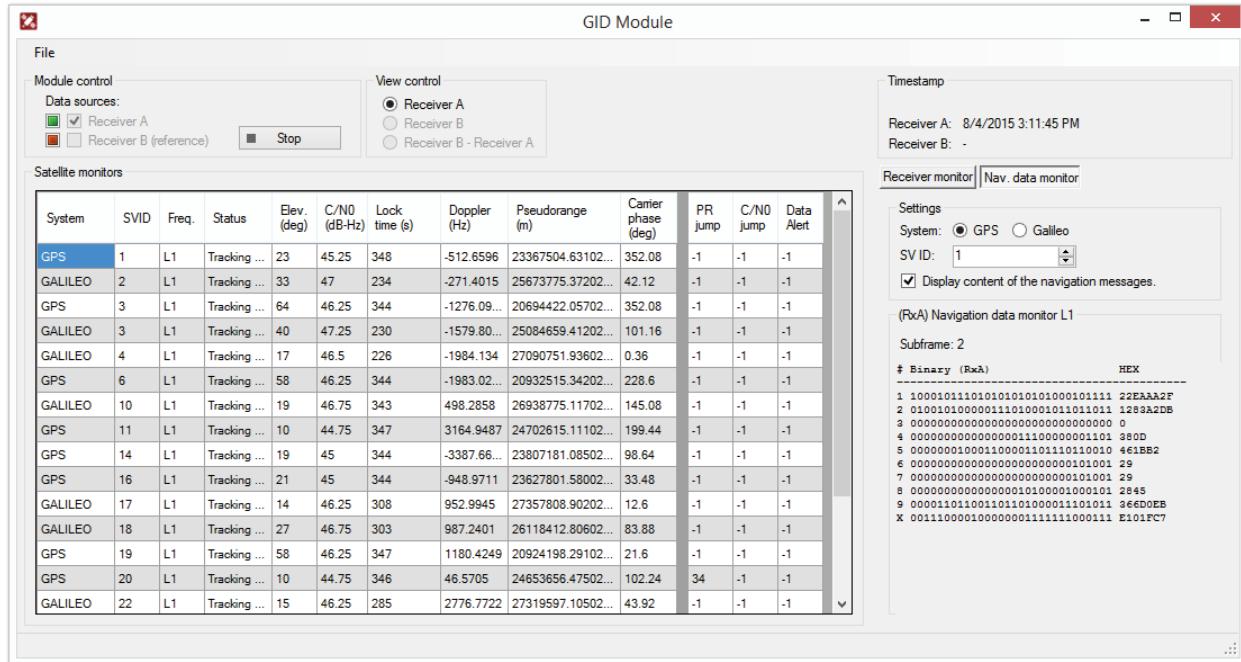


图5 - GNSS干扰探测(GID)窗口

NMEA查看器

支持NMEA 0183协议的接收机会附带提供一种简单而又方便的监视工具。

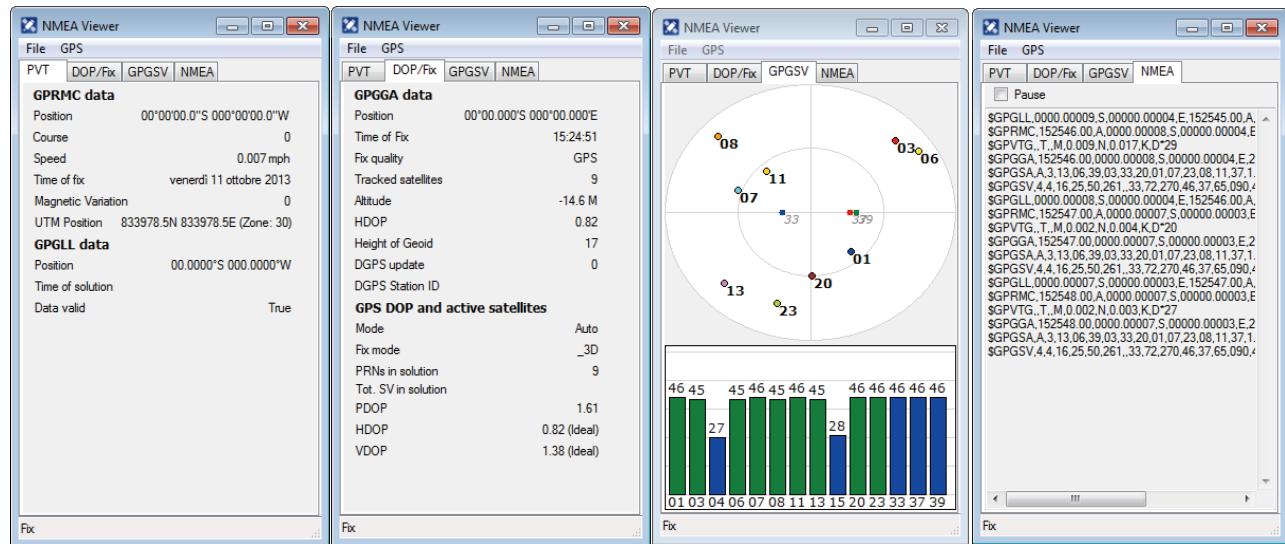


图6 - NMEA查看器屏幕

性能规格

总体概览

SimSAFE™软件是针对Microsoft .NET框架(4.0版)开发和实施的。该系统可在安装了64位Microsoft Windows操作系统的物理机(非虚拟机)上运行。

授权

该安装包内包含一个定义用户可用软件特性的授权文件。SimSAFE™只能在使用正确的激活码激活后方可执行(需要与主机计算机一对绑定)。

SimSAFE™目前可支持基于软件所安装计算机硬件ID的专有授权方案。

一般性限制

SimSAFE™的运行需要性能良好的个人计算机(例如2.26GHz P8400双核CPU或更高、4 GB内存和20 GB可用硬盘空间)。虽然不需要使用专用的计算机,但必须确保在SimSAFE™运行模拟,计算机上不能执行其它消耗资源的应用(例如反病毒或磁盘扫瞄软件)。需要注意的是,客户购买的SimSAFE™将包含适用的计算机。

支持的软件

SimSAFE™可兼容的软件:

- SimGEN v6.01和v6.05软件
- Microsoft Windows 10(64位),含Microsoft .NET Framework 4.0(也支持Microsoft Windows 7和8.1)。

支持的硬件

SimSAFE™可兼容的硬件:

- GSS9000、GSS7000或GSS6700多GNSS星座模拟器
- Septentrio PolaRx4 Pro
- Septentrio PolaRx5
- 通用NMEA接收机
- 在使用真实天空信号配置时可使用NTP客户端或1PPS设备来实现时间同步。

Spirent SimSAFE™

性能规格

精度 - 信号生成

模拟信号在生成和控制过程中的精度/性能取决于多GNSS星座模拟器的能力。详情请见参考[1]。

SimSAFE™允许用户输入下表5中所定义的分辨率范围内的数值。

表5 - 信号生成中规定的范围和分辨率

参数	范围或分辨率值	说明
卫星信号水平偏移	0.01 dB分辨率 最大+40 dB 最小-99 dB	
卫星信号水平坡度	0.1秒更新率 0.001 dB分辨率 10 dB/秒最大速度	
码相位和载波偏移	0.0001米分辨率 ± 3000米最小/最大	
码相位和载波偏移坡度	0.1秒更新率 0.00001米/秒分辨率 ± 100米/秒最大速度	
正弦信号	功率电平分辨率0.01 dB 伪距变化分辨率0.01米/秒 PWR功率电平偏移± 10 dB 伪距偏移± 1000米	

信号能力

表6 - 信号生成中规定的性能

参数	值	说明
星座/信号	GPS L1、L2、L5 Galileo E1 GLONASS L1	
最大通道数	40	
每颗卫星最大多径 ¹ 信号数	4	多径信号创建时使用的是MP_SWITCH命令 (而非嵌入式多径)
真实天空信号通道数	40	

¹多径信号所代表的欺骗可以通过SimSAFE™来添加，并且可以实现功率和授时控制。这些信号均在SimSAFE™中使用 - 由带多径功能的单台模拟器机箱模拟产生并用于代表欺骗方。

参数	值	说明
最大欺骗信号数	任意“实际”信号数量低于40	受已经安装模拟器通道数量的限制或40个，由数量最小的条件决定。
最大模拟时长	不同轨迹欺骗场景下为12小时或4小时	

精度 - 接收机测量结果监视

表7 - 接收机测量结果监视中规定的性能(GID)

参数	值	说明
PR步进探测	分辨率0.1米 最大100米 最小0.5米	
C/N0步进探测	分辨率1 dB-Hz 最大10 dB-Hz 最小1 dB-Hz	
Δ 时钟偏差	分辨率0.01纳秒 最大10000纳秒 最小0.01纳秒	
Δ 高度	分辨率0.0001米 最大10000米 最小0.0001米	使用两台(Septentrio) SBF接收机时该功能可用。
Δ 位置	分辨率0.0001米 最大10000米 最小0.0001米	使用两台(Septentrio) SBF接收机时该功能可用。
Δ 速度(水平)	分辨率0.01米/秒 最大1000米/秒 最小0.01米/秒	使用两台(Septentrio) SBF接收机时该功能可用。
Δ 速度(垂直)	分辨率0.01米/秒 最大1000米/秒 最小0.01米/秒	使用两台(Septentrio) SBF接收机时该功能可用。
导航电文监视	分辨率1位	使用两台(Septentrio) SBF接收机时该功能可用。

系统迭代率

表8 - SimSAFE™功能的迭代率

参数	值	定义
GID 迭代率	1 Hz	

Spirent SimSAFE™

参数	值	定义
日志记录速率	10 Hz	
GUI 刷新率	1 Hz	
MOD命令更新率	10 Hz	
支持的SimGEN 迭代率(SIR)	100 毫秒(10 Hz)	

SimSAFE™真实天空信号模式的时间校准

表9 - SimSAFE™真实天空模式的时间校准规格

参数	值	定义
时间校准精度(最糟糕情况)	100纳秒	对PolarRx5和PolarRx4Pro有效。该表中提供的值适用于情况最糟糕的场景。

订购信息

如欲了解订购和流程方面的信息,请您联系当地的思博伦销售代表。

交付物

下面的几个表格显示的是每种配置和选项下的SimSAFE™可交付项。

- 模拟信号和真实天空信号配置必须与SimGEN 控制器和思博伦信号生成器关联购买。
- 每项配置均可与一台用作被测接收机的Septentrio PolarRx5接收机一同购买。
- 表10包含SimSAFE™真实天空信号模式下1PPS设备同步选项的详情。
- 如果需要将被测接收机与SimSAFE™组合使用,其选项详情可参阅表12

表10 - SimSAFE™真实天空信号模式配置的可交付项

设备	数量	注释
SimSAFE™控制器	x1	Win10 64位
SimSAFE™仅软件	x1	
Septentrio PolarRx5接收机	x1	
以太网交换机	x1	五端口
以太网线	x3	

设备	数量	注释
N-Type公头至SMA母头适配器	x1	
TNC公头至SMA母头适配器	x1	
SMA母头-公头直流隔断器	x2	
BNC公头-BNC公头电缆	x4	
SMA公头-SMA公头电缆	x5	
SMA RF合路器/分流器	x2	

Spirent SimSAFE™

表11 - 1PPS设备同步的可交付项

设备	数量	注释
u-blox EVK-M8N评价工具包	x1	
SMA公头-SMA公头电缆	x1	
SMA母头-公头直流隔断器	x1	
SMA RF 3路分流器	x1	
DB9公头/母头电缆	x1	
RS232至USB转换器	x1	

表12 - SimSAFE™模拟信号模式的可交付项

设备	数量	注释
SimSAFE™控制器PC	x1	
SimSAFE™仅软件	x1	
以太网交换机	x1	五端口
以太网线	x3	
N-Type公头至SMA母头适配器	x1	
SMA母头-公头直流隔断器	x1	
BNC公头-BNC公头电缆	x1	
SMA公头-SMA公头电缆	x1	

表13 - SimSAFE™被测接收机的可交付项

设备	数量	注释
Septentrio PolarRx5接收机	x1	
TNC公头至SMA母头适配器	x1	

表14 - SimSAFE™仅软件可交付项

设备	数量	注释
SimSAFE™应用软件	x1	
SimSAFE™授权密钥	x1	
SimSAFE™快速启动指南	x1	
SimSAFE™用户手册	x1	

支持和保证

Septentrio PolarRx5接收机

思博伦为Septentrio Polar RX4或RX5接收机提供为期4年的OEM保证。

u-blox EVK-M8N评价工具包

思博伦为u-blox EVK-M8N评价工具包提供为期1年的OEM保证。

戴尔笔记本电脑

思博伦为戴尔笔记本电脑提供为期3年的OEM保证。

参考文档

如欲了解更多信息，欢迎索取本出版物所引用的下列任意文档：

表15 - 参考文档

参考	文档编号	标题	版本
[1]	MS7000	MS7000 GSS7000系列GNSS星座模拟器产品资料及规格	最新
[2]	DGP01321AAA	SimSAFE™用户手册	最新
[3]	DGP01322AAA	SimSAFE™配置指南	最新
[4]	MS3055	GSS7765干扰模拟系统	最新

Spirent SimSAFE™

相关产品出版物

表16 - 相关产品文档

参数	描述	文档	参考
GSS9000	GNSS模拟器	产品规格说明书	MS9000
GSS7000	GNSS模拟器	产品规格说明书	MS7000
SimGEN	GNSS应用软件套装	产品规格说明书 用户手册	MS3008 DGP00686AAA
SimSENSOR	MEMS传感器仿真器	产品规格说明书	MS3086
GSS7765	干扰信号生成器解决方案	产品规格说明书	MS3055

联系我们

欲了解更多信息，请致电思博伦销售代表或访问我们的网站www.spirent.cn/ContactSpirent。

北京代表处

地址：北京市东长安街1号东方广场东方经贸城W1座8层804-805A室
邮编：100738
电话：(86 10)8518 2539
传真：(86 10)8518 2540

思博伦通信（亚洲）有限公司

地址：香港北角英皇道243-255号国都广场19楼1905-07室
电话：(852)2511-3822
传真：(852)2511-3880

上海代表处

地址：上海市淮海中路283号香港广场3402室
邮编：200021
电话：(86 21)6390 7233 / 6070
传真：(86 21)6390 7096

技术支持热线：400-810-9529

[中文网站：](http://www.spirent.cn)[全球网站：](http://www.spirent.com)www.spirent.com

广州代表处

地址：广州市环市东路403号广州国际电子大厦2002室
邮编：510095
电话：(86 20)8732 4026 / 4308
传真：(86 20)8732 4120

技术支持网站：support.spirentcom.com

[全球服务网站：](http://www.spirent.com/GS)[思博伦网络测试学院：](http://www.spirentcampus.cn)www.spirentcampus.cn

思博伦通信科技（北京）有限公司

地址：北京市海淀区学院路35号世宁大厦13层
邮编：100191
电话：(86 10)8233 0055
传真：(86 10)8233 0022

