

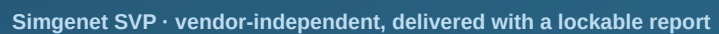


DESIGNED & ENGINEERED IN TÜRKİYE

SVP

traffic, timing, OAM, TSN, power-utility and security tests in one instrument.

1 G → 200 G





01

COMPANY

The Company That Builds the Network and Proves It

Simgenet Mühendislik is a Turkish engineering company delivering industrial networking and critical-infrastructure communication systems. The SVP software is **entirely original**, developed in house at Simgenet; it is not an adaptation of an off-the-shelf package.

2000

FOUNDED

500+

COMPLETED PROJECTS

30+

COUNTRIES SERVED

100+

PRODUCT TYPES

■ Why we built a test platform

Handing over the router, switch and timing networks we have deployed for years, "it works" was never enough. We wanted to make the measurement the standard prescribes, for the duration the standard prescribes, and document it **together with the raw data**. SVP grew out of that need and is used today both on our own deployments and as an independent test service.

■ Why our own software

- **Technological sovereignty** — no dependency on foreign tester licences and roadmaps
- **Testing to the specification** — the clause the project requires is added to the menu
- **Local engineering** — test design and reports in your language
- **Long service life** — the same measurement discipline across a 15–20 year infrastructure lifecycle

Our departments are separate. The software of Simgenet-branded products is developed by our own **manufacturing and R&D department**; transmission systems and field deployment are delivered by separate specialist teams. We measure the network we build with SVP and hand over the result with its standard reference.

Our Mission

To deliver innovative, reliable and sustainable technology for industrial networks and critical-infrastructure communications, safeguarding our customers' business continuity.

Our Vision

To become Türkiye's most trusted and innovative network-infrastructure technology partner, recognized as a global brand.



02

PLATFORM

What is Simgenet SVP?

Simgenet SVP (Simgenet Validation Platform) is an independent network test and validation platform that verifies routers, switches, time servers, NAC/AAA servers and line quality against **RFC / ITU-T / MEF / IEEE / IEC** references. It is **vendor-independent**: every manufacturer's device is measured on the same test ports with the same standard methodology. Every result is stored in the database with its parameters, raw data and PASS/FAIL verdict, and delivered as a lockable report.

■ One platform

Capabilities that require separate instruments or separate licences on commercial testers, in one box:
Ethernet traffic and bandwidth,
PTP/NTP/gPTP timing analysis,
Y.1731 OAM, TWAMP/STAMP,
TSN, IEC 61850/HSR-PRP,
NAC/AAA and OT security testing.

■ Nanosecond-class measurement

Measurements use the hardware timestamp of the network interface. Functional validation in the field, conformance in the lab and SLA activation at circuit turn-up are all done with the same instrument.

■ Transparent evidence

The report states not only the result but **what the test does and does not prove**: duration-validity tiers, measured/claimed distinction, raw-data appendix and compliance stamp.

Test Families

- Bandwidth and throughput — RFC 2544, RFC 2889, RFC 3918, RFC 6349, Y.1564
- Time and synchronization — PTP, SyncE/ESMC, NTP, gPTP, absolute 1PPS
- TSN and automotive Ethernet — Qbv/Qbu/Qav/Qci/FRER, 100/1000BASE-T1
- Industrial protocols — IEC 61850, IEC 104, DNP3, HSR/PRP, ERPS
- Service OAM / SLA — Y.1731, TWAMP, STAMP, one-way delay
- Authentication and management (AAA) — RADIUS, TACACS+, accounting
- Network access control (NAC) — 802.1X/EAP, MAB, CoA, dynamic VLAN
- VPN / encrypted tunnel — IPsec (IKEv2/ESP), WireGuard
- OT / cyber security — IEC 62351, GOOSE/R-GOOSE, time spoofing
- Network management (NMS) — SNMP accuracy, alarm chain, notification storm, scale
- Measurement integrity — port calibration (GUM), link emulation, BER
- 5G / mobile transport — GTP-U user plane, base-station timing budget

"Just plug the cable." PTP auto-discovery detects domain, profile and grandmaster automatically; DUT adapters configure the device before the test and verify it afterwards. The test engineer focuses on the measurement, not on device setup.



03

BANDWIDTH AND THROUGHPUT

Ethernet Performance Testing

Line rates

Hardware-timestamped measurement at every line rate of critical infrastructure:

1 G

10 G

25 G

50 G

100 G

200 G

- 64 B to 9600 B jumbo frames; IMIX and EMIX profiles
- 802.1Q VLAN, QinQ and PCP/DEI tagged flows; IPv6
- L1-calculated pacing; 64 B full-line-rate load at 200 G

■ RFC 2544 / RFC 9004 certification

- **Throughput** — NDR binary search + sweep
- **Latency** — LIFO / FIFO / LILO; store-and-forward ↔ cut-through distinction
- **Frame loss** and **back-to-back** burst (RFC 9004)
- Comparison (A/B) runs and single-port reflector (field PoC)

■ ITU-T Y.1564 service activation (SAT)

- Service configuration test: CIR ramp 25-50-75-100 %, EIR, CBS/EBS burst, colour-aware PCP/DSCP
- Service performance test: multi-service concurrent; 15 min / 2 h / 24 h
- Policing step per the standard formula (CIR + 1.25×EIR); parametric SAC band
- Y.1563 availability: SES / unavailable-second state machine
- 200 G trunk path and 1 G EMIX path — separate menus, same report discipline

■ Switch, multicast and TCP

- **RFC 2889**: forwarding rate (§5.1), MFR (§5.6), broadcast (§5.10), congestion/HOL (§5.5), address learning and caching (§5.7–5.8), errored-frame filtering (§5.9)
- **RFC 3918**: multicast throughput, join/leave latency, group capacity
- **RFC 6349**: TCP throughput — BDP/RWND, Transfer-Time-Ratio, Efficiency %, Buffer-Delay %

■ In-house EMIX L2 measurement engine

- Own sequence numbering and monotonic timestamping — FLR / FTD / FDV / dup / reorder in one tool
- MEF 66 latency histogram; MEF 48.1 / 35.1 report compliance
- Micro-burst and latency-under-load analysis; PDV/IPDV (RFC 5481)
- PCAP export — packet-level evidence

■ Impairment and failover

- Controlled **delay / loss / jitter / reorder / dup** injection; flow filter (PTP, VLAN, MAC, port)
- Protection switching and ring failover time (ms) + loss window: SR TI-LFA, **ERPS (G.8032)**, HSR/PRP
- Long-duration stress load with resource monitoring
- Software ↔ hardware timestamp comparison runs



04

TIME AND SYNCHRONIZATION

PTP, SyncE and NTP Validation

Grandmasters, boundary clocks and NTP servers of every brand are measured with the same method. Measurement is hardware-timestamped; the verdict is given against the standard's mask, and **if the duration is insufficient the report says so explicitly**.

■ PTP — IEEE 1588-2008/2019

- Metrics: **cTE / dTE / maxTE, MTIE / TDEV**, PDV suite (Sync, Follow_Up, Delay_Req; FPP/FPC/FPR — G.8261.1)
- PASS/FAIL against standard masks: **G.8273.2** Class A/B/C · **G.8272** PRTC A/B · G.8271/G.8271.1 · IEC 61850-9-3 / IEEE C37.238 · Y.1541
- Profiles: G.8275.1 (L2 multicast) · G.8275.2 (unicast) · power profile · gPTP
- Relative measurement (between two ports) and **absolute measurement** (1PPS-referenced, Class B/C)
- Automatic path-asymmetry detection; PTP v2/v2.1 interoperability

■ Advanced PTP tests

- PTP under load — traffic + mask in a single run
- Noise tolerance and noise transfer (G.8273.2 §7.2 / §7.3)
- BMCA dual-GM failover; Delay_Req load test; 24 h+ holdover
- **PTP security**: rogue GM, time spoofing, BMCA manipulation
- GM Announce analysis: clockClass, accuracy, priority, timeSource, leap, traceability + change-event stream
- Servo state tracking: ACQUIRING → LOCKED → HOLDOVER
- **PTP/NTP client capacity** — multicast and unicast client load

■ SyncE — ITU-T G.8262 / G.8264 / G.781

- ESMC/QL message analysis and QL transition tracking
- SyncE ↔ PTP hybrid scenario validation

■ NTP — RFC 5905

- offset / RTT / stratum / root delay-dispersion / precision / leap; RMS offset, frequency drift
- NTP under load; server-pool management and preflight; management-plane SNTP compliance

Duration discipline. A short test is only a lock check; cTE needs ≥ 1000 s, field conformance $\geq 10\,000$ s, wander 24–72 h. With insufficient duration the report prints an **explicit warning** instead of a verdict — the customer is never given false confidence.

Time reference inside the instrument. The Timing package includes a GNSS-disciplined **rubidium reference** with a magnetic-mount antenna: disciplined before going on site, measuring in holdover where no antenna is possible. It also works from external 1PPS / 10 MHz inputs and is offered as a package with the Simgenet GNSS Server.



05

DETERMINISTIC NETWORKS

TSN and Automotive Ethernet

All six time-sensitive networking mechanisms are tested from a single menu: SVP both **generates scheduled traffic** and **analyses and judges** the bridge's behaviour at nanosecond class. Designed for automotive, aerospace, rail and industrial-automation networks.

■ 802.1AS — gPTP

Time-sync validation; loop self-test and DUT slave mode.
Nanosecond-class offset and path delay.

■ 802.1Qbv — TAS

Time-aware shaper: gate latency, bounded latency and determinism measurement (gPTP-synchronized).

■ 802.1Qbu / 802.3br

Frame preemption:
preemptable/express traffic separation and observation of preemption behaviour.

■ 802.1Qav — CBS

Credit-based shaper: class A/B bandwidth and reservation behaviour.

■ 802.1CB — FRER

Frame replication and elimination: zero-loss validation over redundant paths.

■ 802.1Qci — PSFP

Per-stream filtering and policing: validation of gate and meter behaviour.

■ Automotive Ethernet — 100BASE-T1 / 1000BASE-T1

- Validation of in-vehicle network harnesses and production-line connections
- PTP/gPTP and traffic testing over T1 — single twisted pair
- Ethernet performance and TSN menus used unchanged on T1 ports

■ TSN traffic generation

- Launch-time triggered frame generation, up to 4 ports
- Priority-class (PCP) and VLAN-tagged flow templates
- Targeted ↔ observed arrival-window report against the gate schedule

Sector use. Vehicle harness acceptance on the automotive production line, deterministic signalling-network validation in rail, TSN bridge selection in industrial automation — all documented in the same report format.



06

INDUSTRIAL PROTOCOLS

Power Utility Automation and SCADA

A substation network is measured not by bandwidth alone but by **whether the protection message arrives on time and without loss**. SVP generates, captures and analyses GOOSE/SV and proves that the redundant topology is truly seamless.

■ IEC 61850 — GOOSE / SV / SCL

- GOOSE (8-1) and Sampled Values (9-2) generation + analysis + capture
- **SCL import (IEC 61850-6)**: automatic test scenarios from the project files
- **QoS-61850 (IEC TR 61850-90-4)**: GOOSE latency/loss criteria under background saturation
- Power-profile PTP masks — IEC 61850-9-3 / IEEE C37.238 ($\leq 1 \mu\text{s}$)

■ R-GOOSE / R-SV — IEC 61850-90-5

- Routable GOOSE/SV over WAN/5G — UDP SPDU envelope, HMAC
- Generation and analysis for wide-area protection and virtual-substation scenarios
- Replay / spoofing / unsigned-frame injection (see security page)

■ Redundancy — HSR / PRP / ERPS

- **IEC 62439-3** HSR/PRP RedBox seamless failover measurement — break the ring, prove zero loss
- **ITU-T G.8032 ERPS** ring failover time (ms) and loss window
- SR TI-LFA protection switching time

■ SCADA — IEC 60870-5-104 / DNP3

- IEC 104 master ↔ outstation test over the real network
- DNP3 (IEEE 1815) master ↔ outstation test
- SCADA session continuity under load and impairment

■ L2 switch protocol validation

- LLDP neighbourship and TLV correctness; RSTP/MSTP topology convergence
- LACP aggregation, port security and IGMP snooping behaviour
- VLAN / QinQ / IPv6 isolation test

■ GNSS receiver and grandmaster test programme

- Grandmaster acceptance: lock, holdover, clockClass degradation, Announce fields
- 1PPS-referenced absolute time error; PRTC metrics
- The same programme for every GM brand, including the Simgenet GNSS Server

Substation acceptance in one report. GOOSE latency, power-profile PTP, HSR/PRP seamlessness and OT security resilience are measured in the same run set; a single standard-referenced report goes into the commissioning file.



07

SECURITY AND ACCESS

OT Security, AAA, NAC and VPN Testing

SVP is not a penetration-testing tool or a passive IDS: **it generates the attack itself and measures the response of the device and the security system**. The same platform validates authentication servers, network access control and encrypted tunnels under load and malformed traffic.

■ OT / cyber security — IEC 62351

- GOOSE security: poisoning (stNum/sqNum), replay, flooding/DoS
- R-GOOSE: replay, spoofing, unsigned-frame injection
- **IEC 62351-6 conformance**: forged-HMAC / invalid-signature rejection
- PTP / GNSS time spoofing: offset injection and slow-pull
- **IEC 62443** switch-hardening arbitration: port security, DAI, IP Source Guard, DHCP snooping, CoPP
- Policy, RBAC, signature, log and SBOM audit; BER-fuzz

■ Authentication and management (AAA)

- **RADIUS (RFC 2865/5607)**: device-admin login, privilege level, accounting (Start/Interim/Stop), security (BlastRADIUS, malformed corpus R1–R7, replay, mandatory Message-Authenticator)
- **TACACS+ (RFC 8907)**: authentication, authorization, command authorization; concurrent load + malformed/replay flood; ramp/watchdog KPI (degradation curve, auto-stop at red threshold)
- Local fallback when the server is unreachable, DAS/CoA session teardown, web session revocation, TOTP; management NTP compliance; secrets are never typed into the UI

■ Network access control (NAC) — IEEE 802.1X

- Supplicant emulation: EAP-TLS / PEAP authentication success and time, re-authentication, EAPOL-Logoff
- Certificate lifecycle: enrolment via SCEP/EST, OCSP, rejection of revoked certificates
- MAB, dynamic VLAN (RFC 3580), CoA / Disconnect (RFC 5176) — protocol ACK and data plane verified separately
- Capacity and HA: 100 → 5000 client load, takeover/failback time, split-brain, accounting loss
- Rejection of non-inventoried devices (IEC 62443 SR 1.2); SNMPv3 MIB verification

■ VPN / encrypted tunnel

- **IPsec (IKEv2/ESP)** and **WireGuard** — SVP acts as the tunnel peer
- Classification: cipher suite, rekeying, MTU/fragmentation behaviour
- Chain capacity: number of tunnels and throughput under load

Is the software right, or the tester? Every run includes a known-PASS and a known-FAIL control vector; on FAIL the tester audits itself first. A "device is faulty" verdict is thereby separated from a tester error.



08

SERVICE AND MEASUREMENT

OAM, NMS, 5G and Measurement Integrity

■ Ethernet OAM — ITU-T Y.1731 / G.8013

- ETH-CC continuity and LOC detection
- ETH-DM / DMM delay (FD / FDV)
- ETH-LM / LMM frame loss; ETH-SLM/SLR synthetic loss (MEF 35.1)
- Self-test (internal loop) and real-DUT (peer MEP) modes; in-service measurement

■ TWAMP / STAMP / OWAMP

- **TWAMP (RFC 5357)**: always-on reflector + stateful session; forward/reverse loss separation; TWAMP-Light
- **STAMP (RFC 8762)**: sender + reflector; TWAMP ↔ STAMP reflection auto-detection
- **True one-way delay (OWD)**: PTP-synchronized — not a round-trip estimate

■ Network management (NMS) test family

- **NMS-1** SNMP accuracy and access (v2c/v3)
- **NMS-2** alarm-chain latency — from event to NMS screen
- **NMS-3** notification reliability and trap storm
- **NMS-4** scale load — virtual device fleet

■ 5G / mobile transport

- **GTP-U (N3/N6)** encapsulated user-plane generation and analysis — mobile backhaul / private 5G
- Base-station timing validation: G.8271.1 time-error budget and PRTC metrics

■ Measurement integrity and physical layer

- **Port calibration (ISO/IEC 17025 practice)**: loopback calibration event record (as-found / as-left), calibration due-date tracking
- **GUM measurement uncertainty (k=2)** and guard-band decision rule — a borderline result is flagged "borderline"
- Link diagnostics and **BER**: PRBS-based error rate; G.826 ES/SES/BBE/UAS
- **Layer diagnostics**: L1–L4 fault localization — is the problem in the cable, port, routing or transport layer
- Link emulation: delay / loss / jitter / reorder / duplicate

■ External reference reader

- Reference-clock and GNSS-receiver status over RS-232 / SCPI (lock, holdover duration, estimated error) enters the report as a line
- Vendor-independent device profiles; port, baud rate and profile selected from the UI
- Temperature and hardware sensors recorded at ± 1 K resolution

Measurement hides no problem. If the counters of the port in use are missing the result is INCOMPLETE; an interrupted run is INCONCLUSIVE; rate is always counter / recorded window. The report writes what could not be measured as "not measured".



09

REPORTING AND INTEGRATION

Reporting, DUT Automation and Management

Y1564-SAT-1G Raporu

Rapor No:	SVP-2026-07-01-001	Test No:	Y1564-SAT-1G-001
Tarih:	2026/07/01 10:00:00	Sıra:	15438
Müşteri:	-	Proje:	-
Çihaz (SVP):	Y1564-SAT-1G	Operatör:	AKB

Test Sonucu — Anahtar Göstergeler

SONUÇ:	PASS	Not:	N/A
--------	------	------	-----

Y1564-SAT Kademeli Servis Testi (ITU-T Y.1564) — 1G 1000 (eth8 - eth16, RD-21)
 Cihaz: Y1564-SAT-1G (1000 Mbps) | Servis: Y1564-SAT-1G (1000 Mbps) | Cihaz ID: Y1564-SAT-1G-001 | Servis ID: Y1564-SAT-1G-001

Test Adı	Oran	Y1564-SAT-1G (1000 Mbps)	Y1564-SAT-1G (1000 Mbps)	Kayıp	Y1564-SAT-1G (1000 Mbps)	Y1564-SAT-1G (1000 Mbps)	Y1564-SAT-1G (1000 Mbps)	Y1564-SAT-1G (1000 Mbps)	Y1564-SAT-1G (1000 Mbps)
25.0	cardium (1000)	24.000	24.000	0.000	100	100	100	100	100
50.0	cardium (1000)	49.000	49.000	0.000	100	100	100	100	100
75.0	cardium (1000)	73.000	73.000	0.000	100	100	100	100	100
100.0	cardium (1000)	98.000	98.000	0.000	100	100	100	100	100
125.0	cardium (1000)	123.000	123.000	0.000	100	100	100	100	100
150.0	cardium (1000)	147.000	147.000	0.000	100	100	100	100	100
175.0	cardium (1000)	171.000	171.000	0.000	100	100	100	100	100
200.0	cardium (1000)	195.000	195.000	0.000	100	100	100	100	100

Lockable report with evidence attached

Report number (SVP-YYYY-MM-DD-nnn), test number, customer/project/device identity and operator; raw data as Appendix A; compliance stamp and report digest (hash) for integrity. A locked report cannot be modified; engineer-notes field and witnessed review.

Test Geçmişi

Rapor No	Test No	Tip	Test Sonucu	Çihaz	Müşteri	Proje	Başlangıç	Sonuç	Notlar
SVP-2026-07-01-001	Y1564-SAT-1G-001	Y1564-SAT-1G	PASS	Y1564-SAT-1G	-	-	2026/07/01 10:00:00	100	100
SVP-2026-07-01-002	Y1564-SAT-1G-002	Y1564-SAT-1G	PASS	Y1564-SAT-1G	-	-	2026/07/01 10:05:00	100	100
SVP-2026-07-01-003	Y1564-SAT-1G-003	Y1564-SAT-1G	PASS	Y1564-SAT-1G	-	-	2026/07/01 10:10:00	100	100
SVP-2026-07-01-004	Y1564-SAT-1G-004	Y1564-SAT-1G	PASS	Y1564-SAT-1G	-	-	2026/07/01 10:15:00	100	100
SVP-2026-07-01-005	Y1564-SAT-1G-005	Y1564-SAT-1G	PASS	Y1564-SAT-1G	-	-	2026/07/01 10:20:00	100	100

Database-first record

Every run with its parameters and raw data in PostgreSQL. Comparison view (two runs side by side, common-scale charts), archive, re-run, single-file diagnostic bundle; event log (X.733 alarm classes) and audit trail. Reports in EN/TR, PDF / CSV / HTML; standards-basis table and three-state verdict (PASS / FAIL / NOT MEASURED); calibration certificate.

DUT management and automated testing

- Multi-vendor DUT adapters: common router/switch vendors, SMGOS and generic server systems — automatic configuration, verification and factory reset; new vendors plug in modularly
- Device inventory: SSH/CLI access, port discovery, wiring map, ping/preflight
- Running-config snapshot, suggested test configuration, post-test cleanup and backup; configuration via **NETCONF / RESTCONF client** (RFC 6241/6242, NACM)
- On-device correlation:** on FAIL the DUT's event window is fetched automatically and attached to the report — whether the problem is on the wire or in the device is separated in one report
- Auto-Test sessions: select DUT → combination preview → unattended multi-test → best-config recommendation

Management, monitoring and integration

- HTTPS web interface: test triggering, live run banner, history, device/customer/project; roles admin / operator / viewer; EN and TR
- REST API (OpenAPI) — all tests and management; CI/automation integration
- SNMP: SIMGENET-SVP-MIB (test-FAIL and hardware-signal traps); integration with common NMS systems
- Periodic conformance rounds (sentinel mode), watchdog, reboot-persistent services
- Backup (with manifest) and factory reset; branding (customer/integrator logo)
- Remote support: time-limited, admin-approved, per-device keyed and audited outbound tunnel
- Certificate infrastructure: SCEP/EST client, OSCP, TLS 1.3

Sentinel mode. SVP stays permanently attached to the installation: periodic conformance rounds, GM Announce change tracking and SNMP/NMS alarms reveal faults the moment they occur — the commissioning instrument becomes the monitoring instrument in operation.



10

APPLICATIONS

Use Cases and Sectors

■ Telecom / ISP

Circuit turn-up and SLA activation (Y.1564 / RFC 2544), OAM, 1 G → 200 G performance, SyncE + PTP telecom profiles; **independent Class B/C claim verification** in operator tenders.

■ Power / substation

IEC 61850 GOOSE/SV, power-profile PTP, QoS-61850, R-GOOSE, HSR/PRP, SCADA 104/DNP3 and OT security — **combined OT + timing acceptance** in one report.

■ Automotive / aerospace / rail

100/1000BASE-T1 in-vehicle harness acceptance, the six TSN mechanisms, gPTP; deterministic signalling-network validation and HSR/PRP redundant topologies.

■ Government / defence / enterprise

NAC/AAA capacity and conformance acceptance (802.1X, RADIUS, TACACS+, 5000-client load), VPN tunnel classification, NMS alarm-chain and scale testing.

■ 5G / mobile

GTP-U user-plane testing, base-station synchronization budget (G.8271.1), fronthaul/backhaul timing validation.

■ Laboratory / R&D / metrology

Automated router/switch regression matrix before every release; GUM-uncertainty measurement; **independent reference arbiter** in multi-vendor environments.

Typical Positioning

Commissioning

Acceptance test, SLA activation, locked report hand-over

Laboratory

200 G full-line load, regression matrix, reference arbiter

Operation

Sentinel mode — periodic conformance round, NMS alarm, GM monitoring

Evidence-based hand-over. We measure the network we build with our own test platform and document the result with its standard reference — instead of an "it works" statement, a measured and lockable report is delivered.



11

SCOPE

Test Coverage and Configuration

One software, hardware configured per project. The only difference is the **installed cards and licences**: TSN, T1 or the Timing package can be added later to the same instrument.

■ Hardware configuration

- Compact field enclosure or 19" rack chassis; expansion slots per project
- Test ports 1 / 10 / 25 G (SFP28) · 100 G (QSFP28) · 200 G (QSFP56); modules included
- TSN generation card and 100/1000BASE-T1 card optional
- **Timing package**: GNSS-disciplined rubidium reference + magnetic-mount antenna; 1PPS and GNSS SMA inputs; external 1PPS / 10 MHz input
- 1+1 redundant power and carrying case optional

■ Licensing and growth

- Rate-class licence: 1 G / 10 G / 25 G / 100 G / 200 G
- Test families individually or as packages: Ethernet Performance · OAM · Timing · TSN/T1 · Power · OT Security · NAC/AAA · NMS · 5G
- The same instrument grows later with cards + licences; no second unit needed
- Timing package with the Simgenet GNSS Server

#	TEST
1	RFC 2544 throughput / latency / back-to-back / frame loss
2	RFC 2889 forwarding (single-egress + multi-port)
3	Y.1564 service activation (EMIX)
4	RFC 6349 TCP throughput
5	VLAN / QinQ / IPv6 isolation
6	Impairment (delay / loss / jitter)
7	VPN / IPsec classification
8	PTP relative cTE/dTE, MTIE/TDEV (G.8273.2)
9	PTP absolute time (1PPS-referenced, Class B/C)
10	802.1AS / gPTP
11	PTP security (rogue GM, spoofing, BMCA)
12	SyncE / ESMC observation
13	TSN Qbv / Qav / Qbu / Qci observation + FRER
14	TSN traffic generation (launch-time, 4 ports)
15	100/1000BASE-T1 + PTP
16	IEC 61850 GOOSE / SV / R-GOOSE security + BER-fuzz
17	HSR / PRP redundancy (IEC 62439-3)
18	ERPS ring failover (G.8032)
19	OT security: attack resilience, policy, RBAC / signature / log / SBOM
20	NAC 802.1X / MAB / CoA + 100 → 5000 client load + SNMPv3
21	SCADA DNP3 / IEC 104
22	Capacity / HA / failure under load
23	GNSS receiver / grandmaster test programme
24	1 / 10 / 25 G rate tiers
25	100 G single card (1518 B / SLA class)
26	200 G / 64 B full line rate / DUO / heavy load — in the 200 G-port configuration

12

TECHNICAL SPECIFICATIONS

Simgenet SVP — Simgenet Validation Platform

FEATURE	SIMGENET SVP
Positioning	Independent, vendor-independent network test and validation platform; software developed entirely in house at Simgenet
Test ports	1 G · 10 G · 25 G · 50 G · 100 G · 200 G (SFP / SFP28 / QSFP28 / QSFP56); 100/1000BASE-T1 optional; modular card architecture
Timestamping	Network-interface hardware timestamp (PHY/PTP), nanosecond class; per-port PHC
Time reference	Embedded GNSS-disciplined rubidium (Timing package) + 1PPS/GNSS SMA inputs · external 1PPS / 10 MHz input · RS-232/SCPI external reference reader
Traffic engine	High-performance line-rate generator (64 B full line rate at 200 G) + in-house EMIX L2 measurement engine (FLR/FTD/FDV, dup/reorder, own seq + timestamp)
Ethernet performance	RFC 2544 / 9004 · Y.1564 / Y.1563 · RFC 6349 · RFC 2889 · RFC 3918 · MEF 35.1 / 48.1 / 66 · RFC 5481 PDV · impairment injection · failover (TI-LFA, ERPS, HSR/PRP)
Time synchronization	IEEE 1588-2008/2019 · G.8275.1 / G.8275.2 / gPTP / power profile · masks G.8273.2 A/B/C, G.8272 PRTC A/B, G.8271/.1, 61850-9-3 / C37.238, Y.1541 · SyncE G.8262/G.8264/G.781 · NTP RFC 5905 · client capacity
TSN / automotive	802.1AS · Qbv · Qbu/802.3br · Qav · Qci · 802.1CB FRER · launch-time generation on 4 ports · 100/1000BASE-T1
Industrial	IEC 61850-8-1 / 9-2 / 6 (SCL) · 90-4 QoS · 90-5 R-GOOSE/R-SV · IEC 62439-3 HSR/PRP · G.8032 ERPS · IEC 60870-5-104 · DNP3 (IEEE 1815) · LLDP / RSTP-MSTP / LACP / port security / IGMP
Security and access	IEC 62351(-6) OT resilience · PTP/GNSS spoofing · RADIUS (RFC 2865/2866/5607, BlastRADIUS) · TACACS+ (RFC 8907) · 802.1X EAP-TLS/PEAP / MAB / CoA (RFC 5176) / RFC 3580 · SCEP/EST/OCSP · IPsec IKEv2/ESP · WireGuard · IEC 62443 (port security, DAI, IPSG, DHCP snooping, CoPP)
Service OAM / SLA	Y.1731 / G.8013 ETH-CC/DM/LM/SLM · TWAMP RFC 5357 · STAMP RFC 8762 · OWAMP RFC 4656 · PTP-synchronized OWD
NMS / 5G	NMS-1...4 (SNMP accuracy, alarm chain, notification storm, scale) · GTP-U N3/N6 · G.8271.1 RAN timing budget

Continued on the next page: measurement integrity, reporting, DUT automation, management, configuration, licence packages and reference standards.



13

TECHNICAL SPECIFICATIONS

Measurement, Reporting, Management and Licensing

FEATURE	SIMGENET SVP
Measurement integrity	ISO/IEC 17025-practice port calibration (as-found / as-left, due date) · GUM uncertainty k=2 · guard band · BER PRBS, G.826 · duration-validity tiers · MEASURED / CLAIMED / NOT MEASURED labelling
Reporting	PostgreSQL database-first record · report no + test no + identity · PDF / CSV / HTML · raw-data appendix · compliance stamp · report lock and hash · on-device correlation · event log + audit trail
DUT automation	multi-vendor adapters (SMGOS, generic server systems and common router/switch vendors) · NETCONF / RESTCONF client · inventory, port discovery, wiring map · auto-test sessions · best-config recommendation
Management	HTTPS web (EN/TR, role-based admin/operator/viewer) · REST API (OpenAPI) · SNMP trap SIMGENET-SVP-MIB · NMS integration · sentinel mode · backup/restore · branding · remote support
Configuration	Compact field enclosure or 19" rack chassis; expansion cards (test ports, TSN, T1, time reference) and licences per project; 1+1 redundant power option
Licence packages	Rate class 1 G / 10 G / 25 G / 100 G / 200 G · Ethernet Performance · OAM · Timing · TSN/T1 · Power · OT Security · NAC/AAA · NMS · 5G — tests individually or as packages

Reference Standards

RFC 2544 · RFC 9004 · RFC 6349 · RFC 2889 · RFC 3918 · RFC 5357 (TWAMP) · RFC 4656 (OWAMP) · RFC 8762 (STAMP) · RFC 5481 (PDV) · RFC 5905 (NTP) · RFC 2865 / 2866 / 5607 / 5080 (RADIUS) · RFC 8907 (TACACS+) · RFC 5176 (CoA) · RFC 3580 · IEEE 802.1X · RFC 6241 / 6242 (NETCONF) · ITU-T Y.1564 · Y.1563 · Y.1541 · G.8013 / Y.1731 · G.8032 · G.8261.1 · G.8262 / G.8264 · G.781 · G.8271 / G.8271.1 · G.8272 · G.8273.2 · G.8275.1 / G.8275.2 · MEF 35.1 · MEF 48.1 · MEF 66 · IEEE 1588-2008 / 2019 · IEEE 802.1AS / Qbv / Qbu / Qav / Qci / CB · IEEE 802.3br · IEC 61850-6 / 8-1 / 9-2 / 9-3 · IEC TR 61850-90-4 · IEC 61850-90-5 · IEEE C37.238 · IEC 62439-3 (HSR/PRP) · IEC 62351-6 · IEC 62443 · IEC 60870-5-104 · IEEE 1815 (DNP3) · ISO/IEC 17025 · JCGM 100 (GUM) · G.826 · 3GPP GTP-U

Grows with the specification. Because the software is developed entirely in house, the clause the project requires is added to the test menu; new vendor adapters and new test families are delivered under the existing report discipline.



Why Simgenet SVP

One platform, twelve test families

Traffic, timing, OAM, TSN, power utility, SCADA, security, AAA/NAC, VPN, NMS, 5G and measurement integrity — one box instead of separate instruments and licences.

Vendor-independent arbiter

Every manufacturer's device on the same ports with the same standard method; an independent reference measurement in multi-vendor environments.

Delivered with evidence

Raw data, duration validity, measured/claimed distinction, compliance stamp and locked report — a document that cannot be disputed afterwards.

Original and supported

The software is developed entirely in house at Simgenet; specification clauses are added to the menu, with no foreign licence lock-in.

GET IN TOUCH

Address

Kartal / İstanbul, Türkiye

Phone

+90 555 600 4506

E-mail · Web

info@simgenet.net · simgenet.net

Simgenet Mühendislik Enerji San. ve Tic. Ltd. Şti.

Product Brochure · SMG-UB-SVP-EN · Rev. 2 · © 2026

Engineered in Türkiye