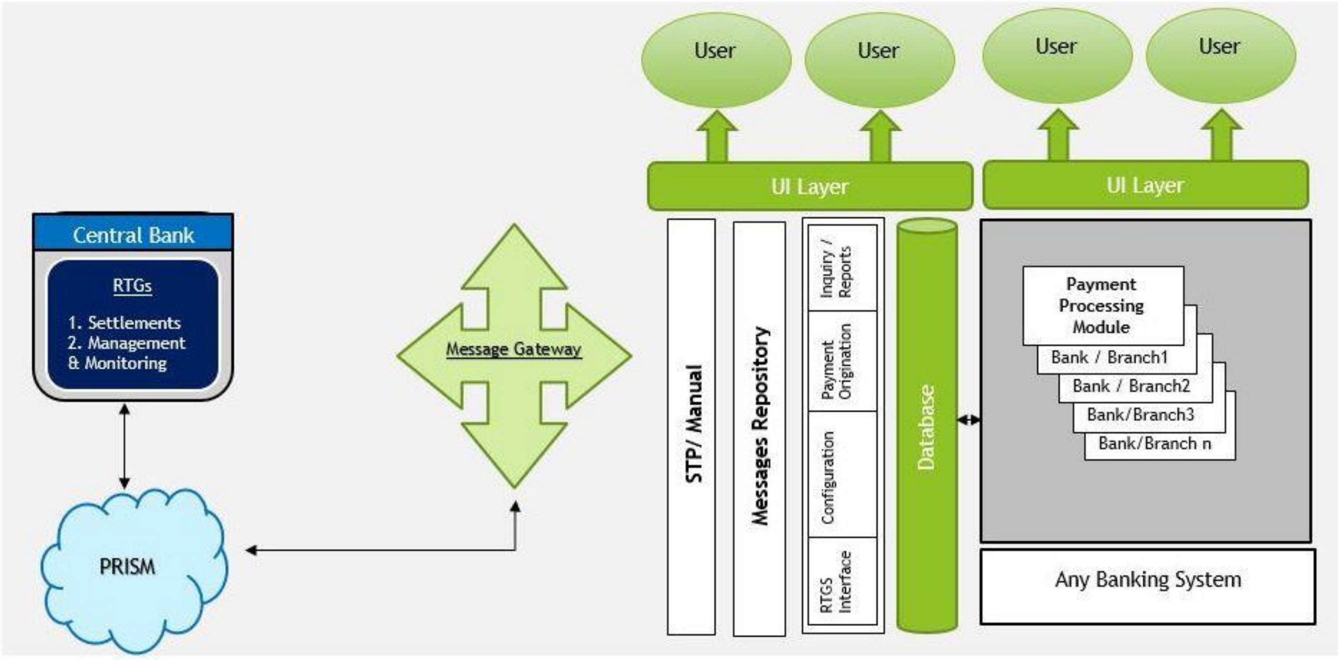
Detail Functionality of AutoRTGS – RTGS Straight Through Processing Utility

Real-time Gross Settlement STP Utility is a real-time application interface for processing of large value interbank remittance/branch transactions in real-time as per the policies and procedures of Central Bank. The transactions are processed on Gross basis and can be linked with the Central Bank RTGS system; this minimizes the systemic risks that are inherent in large-value net settlement systems.

AutoSoft's RTGS STP Utility can be interfaced with the Central Bank RTGS system via the Message Gateway. Any banking system can easily link with the STP utility for processing of messages.

The architecture diagram of the RTGS STP utility is given below:



Salient features of the RTGS STP Utility:

- RTGS transaction processing and posting for following remittance transactions:
- MT – 102
- MT – 103
- MT – 199
- MT – 202

Processing of data from external channels for (STP / Non-STP) - RTGS messages.

- Provision to hold outgoing RTGS messages (on manual processing / Non-STP)
- Provision for RTGS messages monitoring (Messages queues dashboard)
- Straight through Processing
- Centralized audit log monitoring

Benefits of AutoSoft's STP Host - It will be beneficial to:

- Reduce operational risk by eliminating manual intervention.
- Greater visibility of financial / non-financial transactions.
- Quicker Transaction Processing Times.
- Improve accuracy, reliability, and data availability.
- Increases efficiencies by standardizing and streamlining the processes and procedure

Advanced Security Mechanisms – The system puts a high emphasis on security, incorporating the following security controls:

- Application level security refers to those security services pertaining to users of the application including password security (password length, expiry, history encryption, etc.), user level security (user roles, authorization and transaction limits, menu, interface and tab level rights, etc.)

- Database level security refers to the system, processes, and procedures that protect the database from unintended activity. Including access control, auditing and data encryption.

Auditing Controls – The system facilitates enabling/blocking of users based upon their IP addresses. All activities can be tracked and monitored through the session ID and complete audit trails and logs are available which enable the bank to carry out following tasks:

- ***Audit log monitoring*** – Generation of automatic logs for errors and notification, logs for event occurrence and financial/non-financial transactions, setting logs or notification priorities with log archival support.

- ***Centralized auditing*** allows for maintenance and viewing of all logs on the central server with the ability to run queries on them for accurate reporting.