iAcuity
Telco

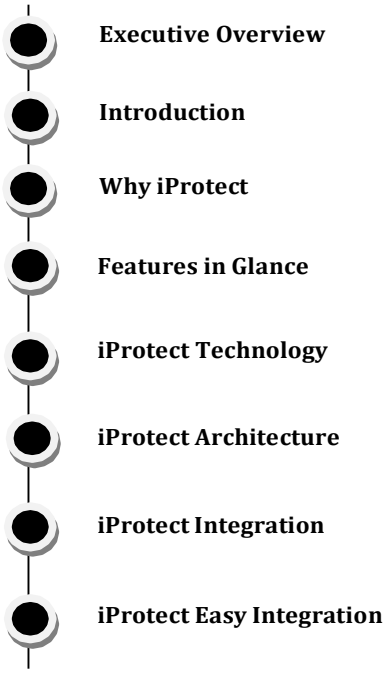
iProtect

DATASHEET

TELECOM FRAUD SOLUTION

Advantages and Implementation of iAcuity

Telco SolutionFraud Management Solution



Executive Overview

Service Providers success has never been so fragile. Technology breakthroughs, regulatory upheavals, geopolitical shocks, and then malicious activities induced—these are just a few of the forces undermining today's business models. With the world growing increasingly turbulent, perennially successful companies are failing. Service Providers earnings are whipsawing. Performance slumps are proliferating. Today Service Providers can no longer count on the flywheel of momentum and incumbency to sustain performance. Instead, they need **strategic resilience**: the ability to dynamically reinvent business models and strategies as circumstances change, to continuously anticipate and adjust to changes that threaten their core earning power—and to change *before* the need becomes desperately obvious. The quest for resilience starts with these bold aspirations: a strategy that's forever morphing in response to emerging opportunities and trends; an operator that's constantly remaking its future rather than defending its past; a company where revolutionary change comes in lightning quick, evolutionary steps—with no calamitous surprises, indiscriminate layoffs, or colossal write offs.

What is Telecommunications Fraud?

There are as many definitions of telecom fraud as there are fraud managers employed in the industry. However, there does seem to be a general consensus that telecom fraud, as the term is generally applied, involves the theft of services or deliberate abuse of voice and data networks. Furthermore, it is accepted that in these cases the perpetrator's intention is to completely avoid or at least reduce the charges that would legitimately have been charged for the services used. On occasion, this avoidance of call charges will be achieved through the use of deception in order to fool billing and customer care systems into invoicing the wrong party.

Telecommunications fraud has been identified as the single biggest cause of revenue loss for telecommunications providers, with figures averaging between 3 and 5 percent of an operator's annual revenue. Current statistics point to a global loss of USD 55 billion per year, making telecommunications fraud a bigger business than international drug trafficking. IDC estimates that more than 200 variants of telecom fraud exist and that this number is growing with the advent of new services such as 3G and VoIP. Telecom fraud attacks are becoming increasingly sophisticated and are tapping into the arrival of these new telecommunication technologies.

What is IProtect?

iProtect is iAcuity Telco Solution's real-time telecom fraud management solution. IProtect is a well-defined and technically advanced fraud management product. IProtect provides multiple features enabling the operator to target fraud and abnormal behavior on the network and realize revenues. It is tightly integrated with the iAcuity Telco Solution VisionNG Framework for Revenue Assurance, Rating and Other BSS Applications.

- **Flexibility** Address Fraud for any telecom network in real-time. The engine is based on per transaction and network anomalies are detected at real-time fashion. The system can draw data from any data source and produce real-time and authentic Alarms and Reports.

- **Scalability** IProtect is highly scalable. Means as you grow, as the engine is based on real time transaction mechanism and not on primitive ETL (Extraction, Transformation and Loading) methods.

- **Tech Agnostic** The system is highly convergent in nature and has ready to use off-the-shelf adapters to work with any network be it Fixed, Wireless or IP and importantly the system is designed to have the easy adaptability to any 3rd. party OSS/BSS software application.

Introduction

iAcuity Telco Solution Fraud Management solution, IProtect are highly acclaimed by number of telecom operators in Europe, South America and India. The solution is robust, highly flexible and is proven to have handled over 3 billion CDR per month, with unmatched accuracy.

- IProtect works with all the services provided by a telecom operator, viz.,
- Prepaid mobile – CDR & prepaid events like charging
- Postpaid mobile
- Fixed line
- Calling cards
- GPRS, MMSC, SMSC
- Roaming
- 3G / UMTS

IProtect is capable of identifying all the existing major telecom frauds, in both prepaid and postpaid services and is capable of scaling to future requirements. Some of the key areas include

- Subscription fraud
- Call conferencing & call forwarding frauds
- PBX hacking
- Premium number fraud
- SIM cloning
- IN and voucher management system fraud
- Internal technical fraud through system tampering
- Hot list & black list detection and many more

IProtect provides solution to monitor call transactions & network usage and identify potential fraud cases. The system generates alerts to fraud monitoring agents and tracks the status of the fraud cases till closure. IProtect provides highly scalable and extensible architecture. Easy Configuration option allows any new frauds to be easily configured in the system.

iAcuity Telco Solution has substantial experience in implementing real time based fraud detection by tapping CCS7 signaling links through SS7 probes.

IProtect provides a common case management and issue resolution module for Revenue Assurance, Fraud Management and Business Intelligence solutions.

This is a standalone web services module that can be used to automate a services provider's chosen case management workflow, starting from case compilation to case assignment and resolution. The frontend of the Case Manager is powered by a single web based Graphical User Interface (GUI) that presents suspected fraud cases and facilitates analysis, investigation and subsequent actions.

Why iProtect

When selecting the most appropriate fraud management solution, consider the following:

- IProtect can generate fast fraud alarm reports, allowing the operator to establish threshold levels for each subscriber.
- IProtect caters to various forms of fraud and allows operators to change and modify rules to cater for evolving methods of fraud.
- IProtect is highly effective as the engine is tightly integrated to Mediation System to interface anytime between the network and fraud system.
- IProtect is scalable enough to cater for operator growth and allow for budgetary constraints.
- IProtect enables easy and correct configuration and decision making
- User friendliness to cater for various skills levels.
- Reasonable hardware and licensing costs in relation to functionality and features

Loss of revenue is something no company can afford. Through planning and the implementation of IProtect fraud management solution, operators will be able to substantially reduce revenue leakage, thus reducing debt and increasing revenue.

IProtect Features at a Glance

IProtect has a range of features with complete business focus ensuring operators to target various fraud types. Resolve cases with quick efficiency. Increase operators Return of Investment for the solution. The highlights of the solution are:

Capability to Address any Fraud in any Environment

- **Prepaid**: Abnormal balances, frequent recharges, Prepaid balance not decrementing, and multiple unsuccessful recharge attempts. Call selling, internal fraud and many more.
- **Postpaid**: Subscription fraud, Ghost subscribers, calls selling, internal fraud, services fraud and many more.
- **IP, 3G**: Subscription fraud, Ghost subscribers, content fraud, internal fraud, services fraud and many more.

Data from Any Sources

- IProtect captures data and correlates from numerous sources. This becomes even more critical aspect in the multi service operations like 3G and IP with content servers, providers, convergent mediation and recreating capability of billing systems from multi sources.
- IProtect captures raw or parsed data directly from the real-time network which is based on state of the Art technology. The IProtect architecture uses adaptor technology for handling inputs, outputs and rule engine integration for maximum flexibility. At design time the user has drag and drop GUI based access to configuration of parsing logic, transformation and alarm rules. The powerful run time engine allows concurrent processing across multiple processors and computing grids. This allows the Alarm rules to be executed during and after record processing providing near real time fraud detection.

Most Comprehensive Fraud Detection System

- **Condition Builder:** IProtect presents user configurable and definable condition builders to detect different types of fraud. User can thus define the type of fraud to check for, define parameters based on which the check can be conducted. New and existing subscriber gets monitored stringently, preventing fraud. Subscribers with some or long history on the network can be monitored with other conditions ensuring fraud like balance, bill manipulation; call selling, content misuse and others are instantly identified.
- **Workflow and Alarms**: The IProtect inbuilt alarm engine supports defining alarm configuration at all data extraction levels, analyses levels and runtime levels. Thresholds can be based on event as well as the type of alarm.System level alarms are performance and task completion alerts while process alarms are results based. Alarms have multiple levels and multiple actions, with escalation.

State of the Art Analysis Tool:

- **Record Analysis:** All call and usage data is captured in the readable and enriched formats for valuable decision facilitating information to the system users. System user can now query and perform required investigative functions.

- **Finger Printing:** **C**omputes and captures finger prints of all frauds detected on the system ensuring any repeat entry of the fraudster on the network is instantly recognized.

- **Link Analysis:** IProtect link analysis allows operators systems analysts to identify and understand the causes for the links and resolves multiple fraud cases or threads rather than single case resolution. The system identifies fraud rings, thus weeding out multiple fraudsters.

- **GUI Reporting:** The reporting system allows automated monitoring for Usage, Profile and None usage, which show different types of fraud risk. Well-defined metrics, based on easy configurable parameters such as variation in any attribute of interest like call types, duration and other parameters. IProtect allows personalized reporting by individual users and allows viewing of alerts and issues at all levels for the same or multiple users, trend analysis, various computations, and root cause analysis.

Administration

IProtect administration system provides the system administrator to perform role based management, database administration at any level and centralized data repository management for further or future processing at any time. The system allows the monitoring of the analysis efficiency, track the actions and prepare better workflows.

Empowers Faster Decision Making Process

False or Unnecessary Alarms can create issues and generate workflows with the provision to auto close issues. IProtect notification mechanism can integrate with email systems, various messaging systems, middleware systems, third party monitoring and alarm tools. IProtect has the capability to generate critical alarms over mobile reporting system by using the existing SMSC gateways and also has the unique power of delivering automated graphical reports to critical users by using any existing MMSC gateways in regular or easy configured intervals.

IProtect

Section 1.01 Fraud detection and Analysis Methodology

A reliable and flexible mechanism for the identification and control of these "Traffic Anomalies" would offer two major advantages:

- It would allow the service provider to reduce direct economic costs by identifying and interrupting an incorrect use of the service (before this can come to represent a significant cost);
- It would implement an efficient mechanism for customer retention allowing the service provider to "protect" authorized end users from unwitting use of services, limiting subsequent economic impacts.

Section 1.02 Network Coverage

Various network elements and systems are to be covered to detect the frauds viz.,

- Radio Access Network (BSS/RAN)
- Mobile Switching Center (MSC/NSS)
- Home Location Register (HLR/VLR)
- Intelligent Network (IN)
- Messaging (SMSC, MMSC, USSD, VMS)
- Packet data (GPRS, EDGE, 3G/UMTS)
- Network Management (NMS, OMC, OSS)
- Mediation, Billing, Customer Care, and the OSS

Section 1.03 Fraud Cases

Some of the significant frauds that can be monitored and fixed using IProtect are

(a) NSS Frauds

- Creation of ghost numbering trees
- Forwarding loops
- Modification of roaming profiles
- Creation of ghost subscriptions on HLR
- Special CDR (Charging Data Record) generation rules
- DoS / Harassment / Pranks
- Injected SS7 protocol messages

(b) IN Frauds

- Modification of Prepaid account DB
- Creation of ghost 800 numbers
- Tracing of subscriber activity
- Fake trigger in SSP & fake service in SCP
- CDR generation special rules
- Modification of charging tables
- Unauthorized forwarding
- Unauthorized supplementary services

(c) Messaging level Frauds

- Interception of messages on SMSC
- Injection of messages (Spam)
- Modified MS can craft evil messages
- SS7 and IP connectivity
- VMS hacks (e.g. callout)
- Special USSD sequences

(d) Mediation & Billing Frauds

- Raw database edit, by conveniently deletes selected records containing billing data
- Modification of the charging tables in the billing system
- Patching of the rating engine application to eliminate certain CDR e.g. belonging to a given MSISDN
- Backdoors in mediation gateways to remove CDR data
- Confidential information on subscriber activities (numbers called, received, SMS, data, etc.)
- Modification of CDR processing rules
- Modification of “Test Numbers” white list
- Live patching of CDR data while in mediation queue
- Patching of mediation application (e.g. loading scripts)
- GPRS packet aggregation rules modification

(e) Transmission level Frauds

- Theft of service, interception of calling cards numbers, privacy concerns
- Introduce harmful packets into the national and global SS7 networks
- Get control of call processing, get control of accounting reports
- Obtain credit card numbers, non-listed numbers, etc.
- Messages can be read, altered, injected or deleted
- Denial of service, security triplet replay to compromise authentication
- Annoyance calls, free calls, disruption of emergency services
- Capture of gateways, rerouting of call traffic
- Disruption of service to large parts of the network
- Call processing exposed through Signaling Control Protocol
- Announcement service exposed to IP through RTP
- Disclosure of bearer channel traffic

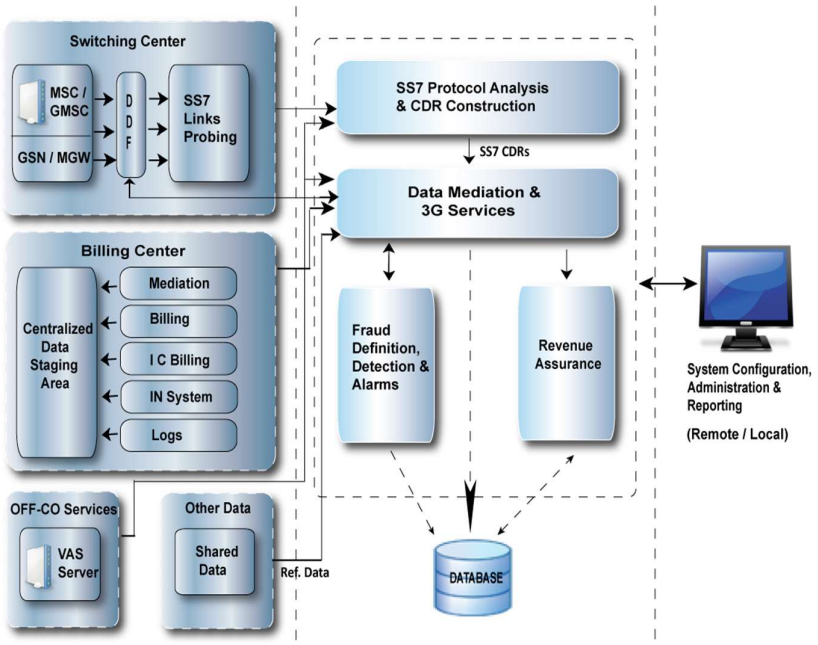
(f) Roaming Frauds

- Excessive Roaming Recharge
- TAP IN & TAP OUT
- NRTRDE Compliant Fraud Detection

Section 1.04 IProtect Architecture

iAcuity Telco Solution envisages the following interface architecture as per the diagram given below to collect data from various sources and process forfraud management.

IProtect collects data from all network elements of the network through data mediation. Apart from this the data is collected real-time from various MSCs. IProtect can also exchange FIGS related information with Network Elements. The fraudulent cases are routed to the analysts' terminals for appropriate action.

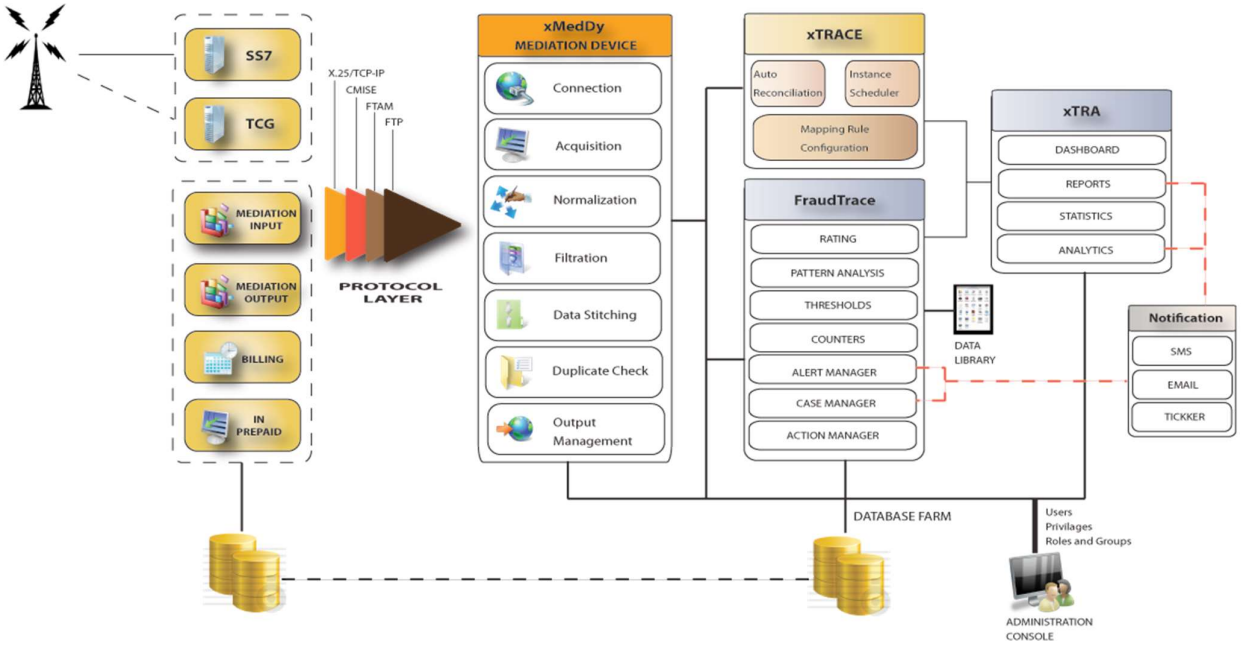


Section 1.05 Solution Description

iAcuity Telco Solution product IProtect is a very flexible & innovative fraud management system, to monitor traffic, highlighting all "anomalies" which indicate an incorrect use of services due to suspicious events and allows an automatic interruption of specific services to be implemented if particular conditions arise.

As service types and service operation are continually evolving, IProtect is highly flexible and it can be readily adapted to new and differing service modes and service pricing and can incorporate increasingly complex techniques and heuristics for the automatic identification of traffic anomalies.

System customization is achieved through a third generation language that allows the system to be configured rapidly to fit changing needs.



In addition, logging of all events and auxiliary data allows for a detailed analysis to be carried out off-line. This is useful in evaluating system behavior and in conducting "what if" scenarios, allowing for efficiency and economic return to be monitored constantly.

Since time to alarm generation is a major factor for the correct behavior of the system, it is important to retrieve data, as close as possible, to the source of service (for example, the switching center).

To this aim, the system can be configured to receive input from the closest available source (billing data, mediation device, switching centers); it reduces the latency between the time of generation of the event and the identification of the anomaly, bearing in mind that the time to alarm is directly proportional to the economic loss incurred for a missed identification.

Our approach is to deliver a flexible and configurable solution that supports you in achieving your objective. The solution must be able to evolve with the future needs of the customers. The solution achieves it in a number of ways E

- IProtect solution manages different incoming data flows in a real convergent way: due to the application architecture it is possible to increase the number data types that are analyzed according to needs and future development of the technology. It is not be necessary to change the fraud management platform or to develop ad hoc code.
- At the same time, the system can be configured with new rules as soon as new fraud techniques are discovered. Also in this case, the flexibility of the solution, with the easy to use console, allows the telecom operators to react to frauds without the need of developing a specific solution.

- IProtect main benefits are the following:
    - It is highly configurable according to new data input
    - Management of multiple input data format
    - Hardware and Software independent
    - Configurable data flows within the systems
    - Configurable internal record format Database is independent from data format (external and internal)
    - WEB interface, no clients maintenance, Multilingual
    - High scalability
    - Modularity of the solution
    - Secure access with smart card systems (if required)
    - Encryption on DB and secure connection with WEB
    - Short time required for Integration
    - Distributed configuration, even between multiple sites

IProtect is already running for wire line, wireless and UMTS carriers and are based on the state of the art technology and is available for SUN/Solaris, HP/HPUX, Linux and AIX platforms for the server side while the GUI is fully WEB based.

- IProtect comes with a ticker application that can reside on desktop and pops up a visual and audible alert as and when a fraud case is raised

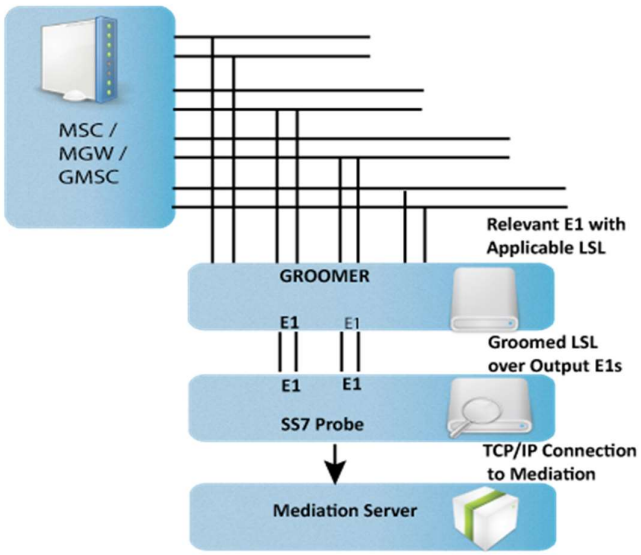
(a) Data Collection

The data that is acquired can be broadly categorized into

- FIGS data
- SS7 CDR
- Mediation CDR
- Billing CDR
- Customer account / profile details
- IN CDR
- Voucher management system
- Switch Transaction log
- OMC Transaction logs
- Switch subscribers' data
- Commercial Transaction Logs
- Subscribers data set from central site

(b) SS7 Data Collection

The real time fraud detection shallbe based on the CCS7 signaling links tapped from the network elements as shown Assumptions made are as follows regarding business requirements and network layout: E



(c) Reference Data

Reference data is stored in appropriate data structure suitable to be read by Data Analyzer module at the startup, in order to access the data with the required level of performance.

On the other hand, service usage data is sent by Acquisition to the Normalization module configured to translate incoming records in a unique normalized record format; translation rules are to be configured via GUI using the Modula native SQL Like language that gives the highest level of flexibility in introducing new data flows in the system (note that SQL Like language is widely used across several modules).

Normalized data flow is sent to the Rating module in charge to rate the event: Rating uses a flexible algorithm based rating method that allows to cover also sophisticated rating plans: also to add new rating plans is a matter of configuration so no classic development activities are needed.

Rated data is ingested by the Data Analyzer module, a generic, real time, rule based fraud engine: its extreme flexibility is gained through the extensive use of SQL Like language to define rules, patterns, etc. allowing configuring new rules and putting them on-line in the shortest time (even minutes). This approach is aimed to cover all known fraud techniques and to decrease the reaction time after a new fraud type is discovered.

At this point service usage data (i.e. CDR) signals and cases are stored in the data repository, this can be saving data on Oracle DB or on indexed file structure or on near line devices (DVD juke box) allowing, by means of performance retrieval techniques, access to recent and historical data during fraud investigation.

Data Analyzer produces signals that are correlated each other by Case Filter module in order to avoid case proliferation.

The web based interface offers three access channels to system data:

- Configuration interface
- Case Management Workflow
- Reporting and Monitoring

IProtect GUI is web based, allows secure connection (SSL), user profiling, smart card access control, external user DB interfacing (LDAP) and provides multilingual support.

System manages use of the data for the following functionality:

- Local Customer Info: Through this interface changes on local MSC subscriber data gets collected and checked against centralized subscriber database to highlight discrepancy.
- Net Operational Log: Through this interface logging information coming from MSC gets collected and analyzed highlighting potential fraudulent configuration actions.
- Call Events: These are collected via probes on CSSE7 signaling links to get all, relevant calling events, to track subscriber activity and actuate relevant fraud detection control on traffic.
- CCE Operational Log: Through this interface local customer care operation are collected and analyzed highlighting any potential fraudulent activity on subscriber configuration.
- Customer Info: Through this interface, subscriber relevant data is collected to align with subscriber database, via FMSE Coordination data interface, these updates are forwarded and shared with othernodes, same flows can be collected both from CRM local sub system and Billing local sub system. This will allow identification of any discrepancy.
- Rated CDRs: Through this interface all charged billing events gets collected (from local billing system) and further matched against traffic events highlighting major discrepancy.
- Billing Operational Log: Through this interface, all activities performed on billing system can be tracked in order to highlight any potentially fraudulent action aiming at fraudulent subscriber configuration.

Fraud analysts will be able to access the system via client workstations managing relevant cases according to the defined work lists.

Fraud analysts can take action against identified fraudster manually by (via standard IProtect WEBinterface), or automatically by the system as per the appropriate rules that are defined

(d) Off the Shelf Network Anomalies Handler

Ideally, fraudulent activity is to be identified whilst it is still in progress; this is known as 'real time' fraud detection. CDRs must be rated before being analyzed and this normally occurs as they pass through the billing & mediation system. For true real-time fraud detection IProtect must gather data directly from the network using SS7 probes as a mechanism able to interpret data as it transits: Those data can be fed into the IProtect and certain fraudulent activity (like abuse of test lines, call back fraud, long calls, etc.) can be identified as it occurs.

Some of the critical fraud types that can be detected are:

- **Prepaid Anomaly -** Including recharging of service (an interface to the voucher management system is required to collect information on the recharging activity of customers); Check on MSISDN not recharged after a configurable number of days.
- **IN Anomaly –** Reconciliation of call value & voucher recharge amount, to identify; IN call value more than voucher value; IN call validity more than the expiry date of the voucher; excess prepaid roaming usage; Masking IN CDRs; Tampering with IN rating logic
- **Subscription Anomaly –** A subscriber profile is created from his/her past usage data andaccount details to identify; Account creation using a faked name or address; usage more than 1.5 times the profile values. Applicable for postpaid services.
- **Internal Anomaly D** Illicit activation of unbilled services; Tampering with billing / rating system to result in zero value / zero duration calls; unauthorized bulk activation or deactivation; Multiple opening & closing of an account within a billing cycle. Applicable for both prepaid and postpaid services
- **Forwarding & Conference** Abnormal high usage of facilities, either on home network or while roaming, especially within first couple of days of service activation
- **Dealer Anomaly** Fraudulent activations to gain unearned commissions; Applicable for both prepaid and postpaid services
- **Technical Anomaly** **I**ncluding clip-on, PBX and wireless cloning; Applicable for both prepaid and postpaid services
- **Premium Rate Service** High number/value of calls being made to PRS list that is more than twice the normal PRS calling behavior. Applicable for both prepaid and postpaid services
- **Dialed Digit Patterns** Consecutive calls with related dialed digits, e.g. incrementing numbers, which might indicate computer based hacking of services; Applicable for both prepaid and postpaid services
- **Collision Anomaly** Whether the subscriber has made more than one call/event at the same time; Applicable for both prepaid and postpaid services

- **Velocity Check D** Detect consecutive calls/events where the travel time between the locations of the cells where the two calls/events originated is infeasible; Applicable for both prepaid and postpaid services

- **Usage of handset with multiple IMSI and vice versa D** As indications of possible attempts at cloning or manipulation of handsets. Applicable for both prepaid and postE paid services

- **Hot lists & Black lists –** Known low usage origins / destinations; Acceptable high usage destinations; Known HOT origins / destinations and cell Ids; A/B number exclusion; calling card HOT destinations; Blacklisted IMEI / IMSI as known to the network; HOT and frequently called PRS numbers. Applicable for both prepaid and postpaid services

The system is able to generate alarms in particular cases that hide a potential fraud:

- A call record has been received for a service number or subscriber, unknown to the system, and detects ghost phones that are on the network, but not in billing system.
- When calls/events are made to certain specified numbers (e.g. black list numbers), number ranges, suspicious area (cell site) or countries.
- Changes in calling patterns per subscriber profile.
- Multiple subscribers with same usage pattern.
- Excessive usage based on the number of calls, value of calls and or usage beyond a subscriber's normal usage pattern.
- Call record received for a service number or subscriber who is using a class of service for which he/she is suspended;
- A number of short duration calls are made to the same destination;
- Excessive usage of "Call transfer" and "Call forward" features;
- A subscriber defined duration threshold is exceeded for an individual call/event;
- If a subscriber calls more than a specified number of different countries within a specified period of time;
- If more than a specified number of subscribers call the same phone number within a specified period of time;
- A subscriber is receiving only international calls from a specific destination;
- Particular recharging actions.

Alarms generated by IProtect can be delivered to the appropriate personnel using email, pagers and SMS, general monitoring systems or other means.

In addition, the system is able to generate automatic notification to a roaming partner if a roaming subscriber exceeds any thresholds generating the High Usage Report.

Section 1.06 Product Structure

The product structure is based on basic modules (that are able to work in parallel to increase system throughput) that create a processing "chain" integrated with the middleware. The system and its configuration can be fully controlled through a WEB based interface integrated with the system as a whole through J2EE compatible application servers.

The main modules composing IProtect are:

- Acquisition
- Normalization
- Rating
- Fraud Detection
- Case Management

(a) Acquisition Module

The Acquisition module enables the user to define and configure the parameters in order to acquire data for further actions.

Setting the parameters enables the user to define the data sources from which the system gathers information.

The Acquisition Module can be configured to read the following supported input data formats:

- Fixed and variable format ASCII
- Fixed & variable format Binary
- ASN.1
- XML
- IPDR
- Radius
- Mail log
- Http log
- LDAP
- OMC logs, GPRS, MMMSC etc.

The supported protocols are:

- FTP
- FTAM over X.25 / TCP/ IP
- CMISE/CMIP over X.25 / TCP/ IP
- Web services
- Mail
- Stream
- Acquisition via EAI bus (Tuxedo, WEB Methods, Tibco, Vitria, etc.)
- SS7

Several parameters can be configured:

- **Format name**: name assigned to identify the data source in the system;
- **Validity interval**: the period of time when the data source is considered valid and so the input path scans must be done;
- **Path**: where the files we want to process are physically located.
- **Polling period** among two sequential path scans.
- **Sequential check flag**: pointing the need to make a sequential check on the coming file;
- **Waiting interva**l of the sequential file (only when the sequential scan mode is active);
- **Last sequential value read** (automatically valued by the system when the sequential scan mode is active);
- **Position and length**, in the file name, of the specified date
- **Position and length**, in the file name, of the progressive number (used only when the sequential scan mode is active);
- **Header flag**: whether there is or not a record header in the file;
- **Footer flag**: whether there is or not a record footer in the file;

The “sequential file check” mode (whether activated) has the following working scheme:

- The Acquisition Module, when started, look for the file 000000; if this file is not present, at the moment, the module enters the sleep mode for a (configurable) number of seconds (polling period); then it will make a directory scan again; if in the second file scan the file is not yet found, an alarm is generated; it then skips to the next file searching;
- The searching cycle on the progressive file number is done in a range from 000000 to 999999. When the value is reached to 999999, the next progressive value will be set to 000000 automatically.
- If the Acquisition module receives a progressive number as an input (for example 000035) and the next file progressive number received is not sequential (for example 000041), it alerts the lack of all the missing files (in the example 000036, 000037, 000038, 000039 and 000040).
- Once the file has been computed (for example the file 000041), the module enters the sleep mode before doing another directory scan, that time waiting for the next file (000042);

- If the module receives as an input a file with a progressive number previously to that expected (forexample 000015 instead of 000042), it computes the file then alerting that the progressive is not right.
- Erroneous records shall be suspended and investigated via GUI either if the configuration is not complete or data is really to be trashed. In case the configuration has to be changed, this can be done via GUI and related data can be ingested again via Recycle Management module.

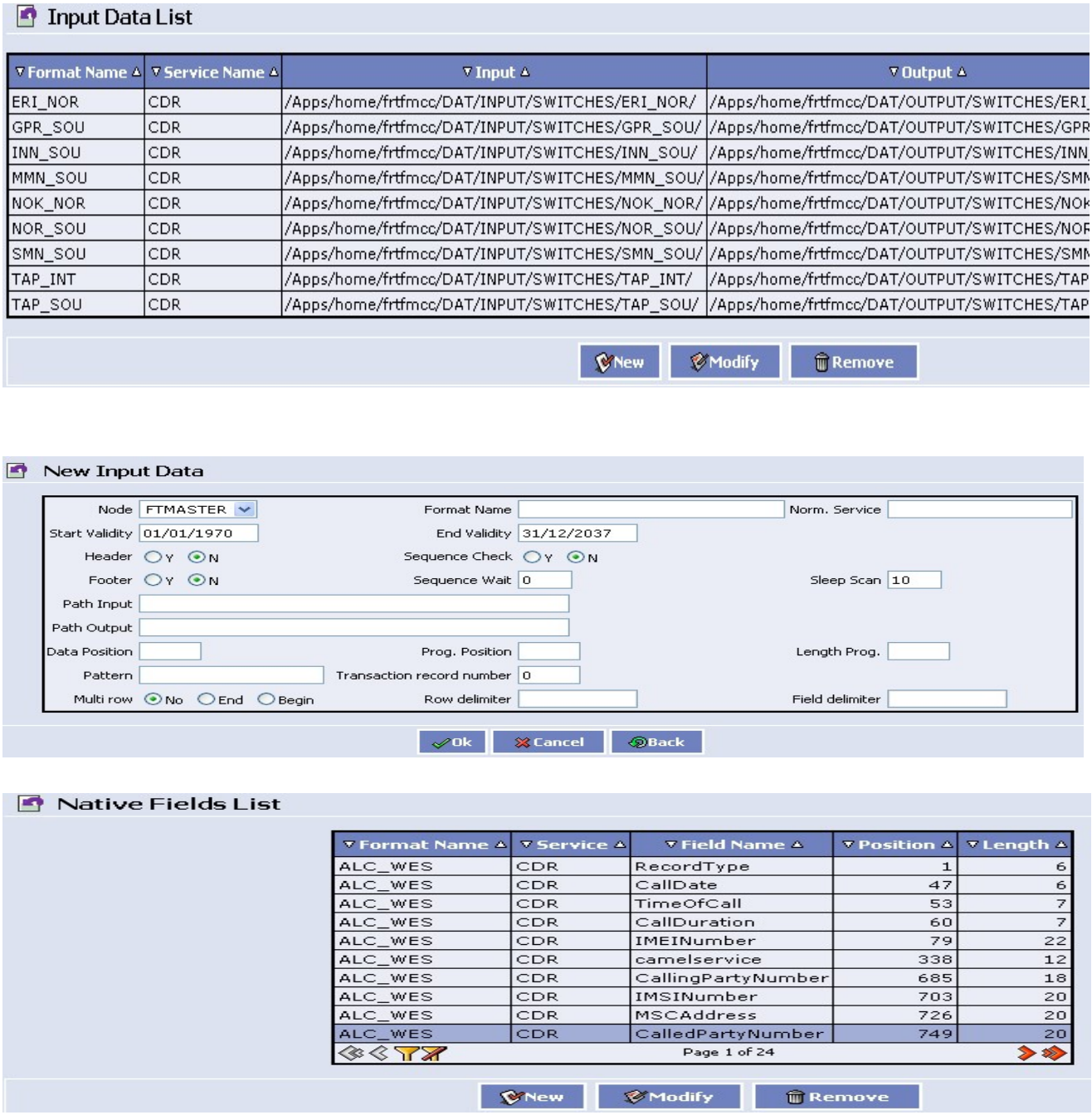


Figure – 8 Native Fields List Screen

Figure – 9 New Native Field Screen

(b) Normalization Module

The normalization module aims to convert the heterogeneous, native records into a unique, homogeneous, normalized record format.

For each native format defined on the system, a set of normalization rules can be specified in order to specify how the normalized record has to be constructed: the normalization rules can be modified during the system life: this is useful, for example, when, to cope with a modified situation, it is necessary to add new fields to the normalized record format.

For each field in the normalized record are defined as many rules as are the native formats defined in the system.

Each rule is defined as an expression in the SQL*Like language (a language with a SQL like syntax, purposely invented by iAcuity Telco Solution) where can be used constants (either numbers or strings), the set of available functions, the referenced fields of the native record using their name as it is defined in the system.

For each field in the normalized record, it is possible to define the following values.

- A symbolic name of the normalized field,
- The field position inside the record (1=first field),
- Field type (D=standard data, R=Routing Field, M=Metric),
- Low Range: once set, the record gets discarded if the field value is less than the set value. If not set, no control is made on this field;
- High Range: once set, the record gets discarded if the field value is higher than the set value. If not set, no control is made on this field;
- Values list: the record gets discarded if the field value is not present among the entities possible values, whose name is pointed in the field; if the values list is left empty no check is made.
- Default value: the value that must be used in the case it is not defined any value derivation rule starting from the fields of the input (native) record.

Once the record has been normalized, it is possible to send this record to the other modules that make the further processing.

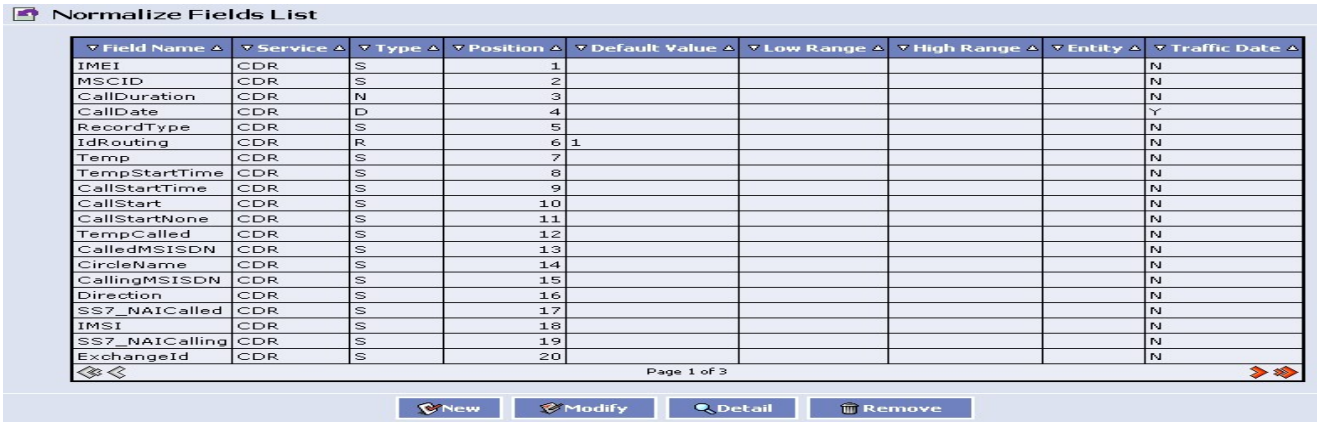
The Routing Rules definition is made in two steps. The first is the definition, inside the normalized record, of the routing field; this field will have an integer, from 1 on, that lets the record address one or more services.

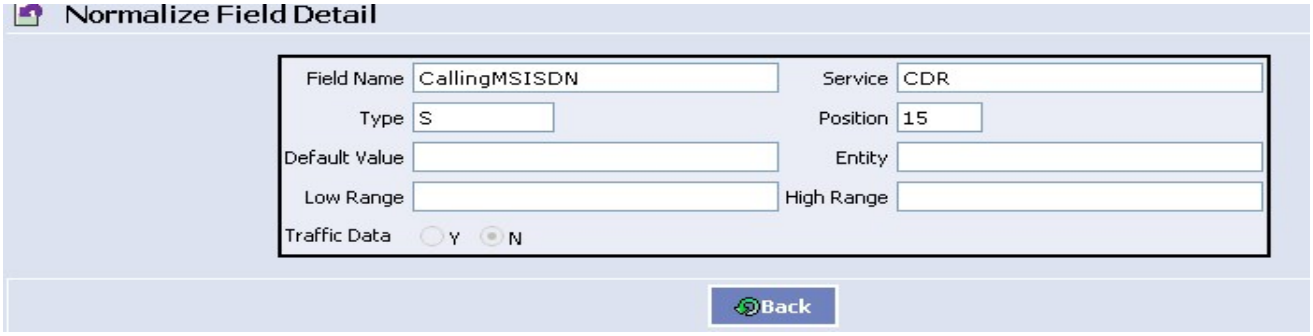
Since there can be more than one normalization service active, for each of them it is possible to define an independent routing table.

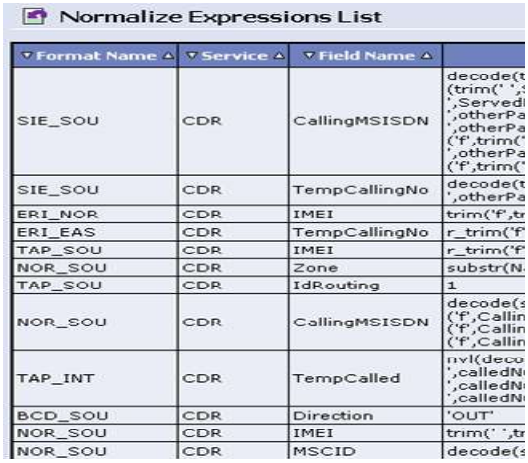
A routing rule is made by 2 values:

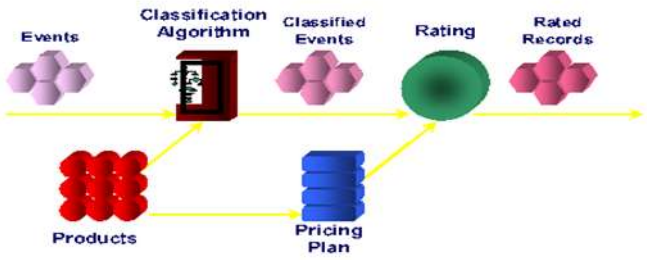
- Routing index: the value that can have the routing field in the normalized record;
- Service: the name of the data receiver service, that gets selected from a value list;
- Queue space: the logic space where you can find the record reception queue from the receiver service; this name is always equals to the name of the receiving service followed by "_QS".

It is possible to assign several receiving services for the same value in the Routing field: if, during the evaluation of the receiver service of the normalized service, it is not possible to find any receiving service, the record gets discarded.









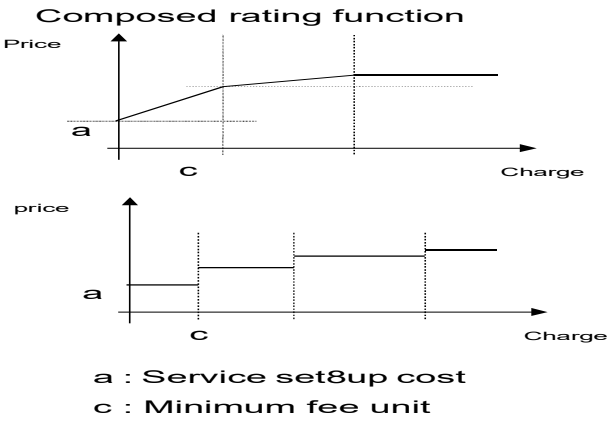
(c) Rating Module

The Rating Algorithm enables the user to define the calculation procedure for the ranking and valorization of the generic records, by taking into consideration all the framework information and the rating element definitions.

The algorithm is an ordered sequence of steps, each of which allows the user to make a calculation or a data association, or to check on the program execution: the step number defines the line number and the order according to the lines executed.

Each line includes an operator: some operators yield a result (a variable) that may be used in the next algorithm steps or to define the value assigned to a field of a rated record.

The variables defined and rated during the rating algorithm process are one type like variables, similarto "records" but different from the fields of the normalized record and more similar to string type variables. The variable type depends both on the operator used and on the data the operator works on.



Rating Module has the following key features:

- Event based
- Convergent
- Flexible classification algorithm
- Configurable rating and discount curves
- Multiple rating with no record duplication
- Configuration oriented (no development)

The Rating module enables each record to be rated by considering all aspects that may affect the costing process (e.g. in the case of a phone call: call type, chosen tariff plan, date and hour of call, duration, existing promotions, discounts, etc.)

A correct rating is reached by identifying a series of values for calculation. These can be identified in 3 ways:

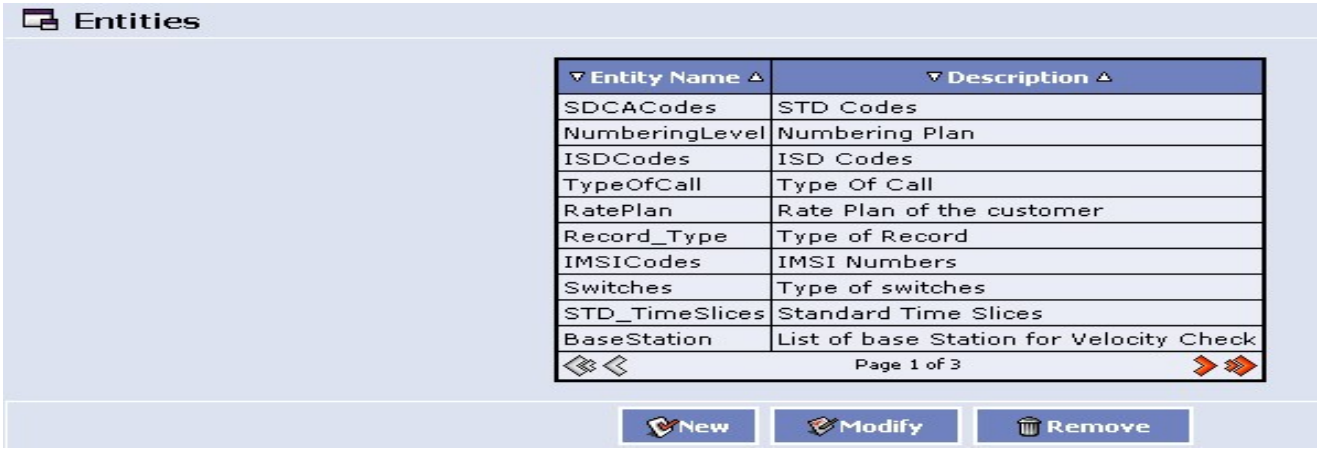
- The value is included in the normalized record and therefore immediately available.
- The value can be found by searching a value list using a particular value E taken from the normalized record E as a key with the most detailed information.
- The value is obtained through the "relations" and the combination of values gathered in the two previous steps.
- This last method can also be applied to values previously obtained by "relation".
- The system models these procedures by defining:
- Entity: values lists that can be used for mode 2;
- Relations: sets on Descartes products that can be used on mode 3;
- Rate plans: expressed as sequences of calling time (calling time start hour/end hour, day type, etc.); a cost per minute value is given to every plan;
- Holidays list: to keep record of holidays (Sundays are included by default; Saturdays may be included);
- Rating algorithm: defines the sequence of elementary steps that ensure the correct identification of the elements used in the record rating.

(d) Entities

An entity is a list of values, identifiable with a name and compiled in such a way that every element has a number of other values as well.

Every element of an entity has the following fixed attributes:

- Name: the unique name of a particular element in an entity. It is the key through which search for the corresponding value derived from the normalized record may be carried out.
- Description: a generic description of the element that helps to identify the element.
- Every entity is thus identifiable as a set of elements, each of which has specific features.



(e) Relations

A relation is a set of subsets on a Descartes product defined between Entities AND/OR Relations. The system allows the user to choose the framework and composition of a relation, based on all the objects configured in the system.

The simplest relation is the one dimensional relation: in this case, given a set of values (e.g. an entity) all its elements is grouped in a homogeneous way (e.g. the central entities get grouped by geographic regions), and every subset of central entities can be given a name (e.g. Central North, Central South, Central Islands); finally the set of group names, which forms the set of values of a relation, can generally be given the name of a Region.

(f) Rating Plan

Each element may be associated to a relation, such as the following:

- A Rating Plan, containing the cost per unit of calling time;
- A set of configurable and individually named User Attributes (maximum 10), each of which is based on a value that may be specified.

Rating Algorithm

Step	Result	Operator	Subject	Parameter 1	Parameter 2	Parameter 3	Paramete
276	CallType	SET	Constant	'ISD'			
277	CallDuration	SET	Constant	'60'			
278	DestLocationISD	MATCH	ISDCodes	CalledMSISDN	I		
279	ISDZone	RELATE	ISDZones	DestLocationISD			
280	ISDChargeClassSMS	RELATE	OutChargClassSMSISD	InOperatorType	ISDZone		
281	CallCharge	RATE	ISDChargeClassSMS	CallStartTime	CallDuration	CALL_START_TRH.Value	
282		STOP					
283	DestLocation	MATCH	SDCACodes	CalledMSISDN	I		
284	DestNodal	RELATE	Parent_Nodal	DestLocation			
285	DestCircle	RELATE	Parent_Circle	DestNodal			
286	OutOpType	MATCH	NumberingLevel	CalledMSISDN	I		
287	OutOperatorType	RELATE	OutOperType	OutOpType			
288	OutOperatorName	RELATE	OperNames	OutOpType			
289		IF		296	290		
290	CallType	SET	Constant	'LOCAL'			
291	IaorIe	MATCH	TypeOfCall	'A'	E		
292	CallDuration	SET	Constant	'60'			
293	LocalChargeClassSMS	RELATE	OutChargClassSMSLoc	InOperatorType	OutOperatorType	IaorIe	RTP
294	CallCharge	RATE	LocalChargeClassSMS	CallStartTime	CallDuration	CALL_START_TRH.Value	
295		STOP					
296	CallType	SET	Constant	'STD'			

Rated Record

Field Name	Position	Format Type	Type	Default Value	Description	Attribute Code	Type Relationship	Entity
InterconnectFlag	38	%s	D					
INVoucherId	45	%s	D					
N_IMEI	4	%s	K					
OwnerCaller_VVC	33	%s	K		OwnerCaller for Velocity Check			BASE_C
JulianEventDateTime	24	%s	K					VCC_DA
IN_AmountBalance	43	%s	D					
Home_Circle	51	%s	D					
N_GPRS_Dlink_Uplink	54	%s	D					
Location	29	%s	D		Location for Velocity Check			
VCC_Flag	31	%s	D		Event Flag for Velocity Check			VCC_FL

Page 1 of 6

New Modify Remove

(g) Groups Management

This function enables User Groups to be defined, and to carry out checks on the groups by assigning rules to each one according to each one's particular features.

The following table shows a brief description of group parameters.

Field Name	Description
Group name	Defines the symbolic name of the group, this name is available in the information associated to the notification as detailE1.
Description	Allows brief description of group.
Priority	Defines verification order of assignations within same group.
Rule	Defines User Group automatic assignation rules for the lines identified by the traffic, based on general features (zone of origin, origin source).

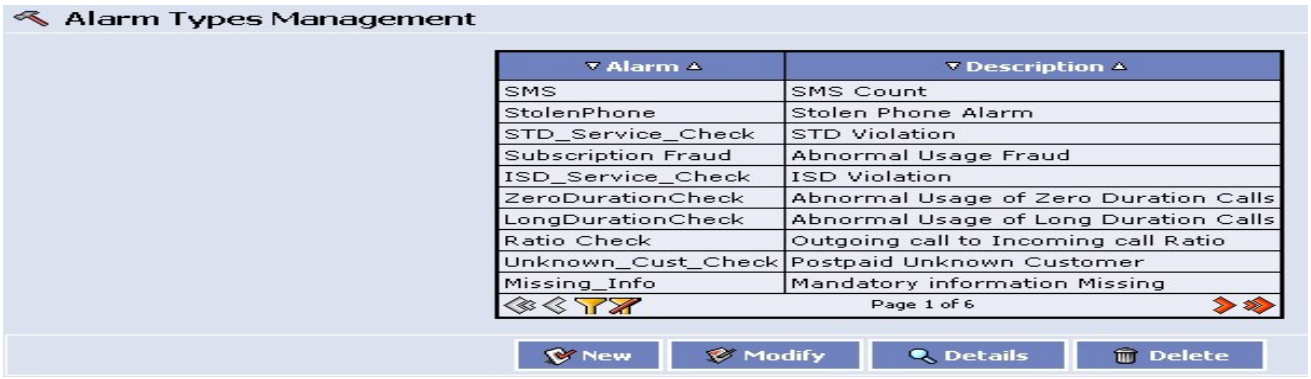
(h) Actions management

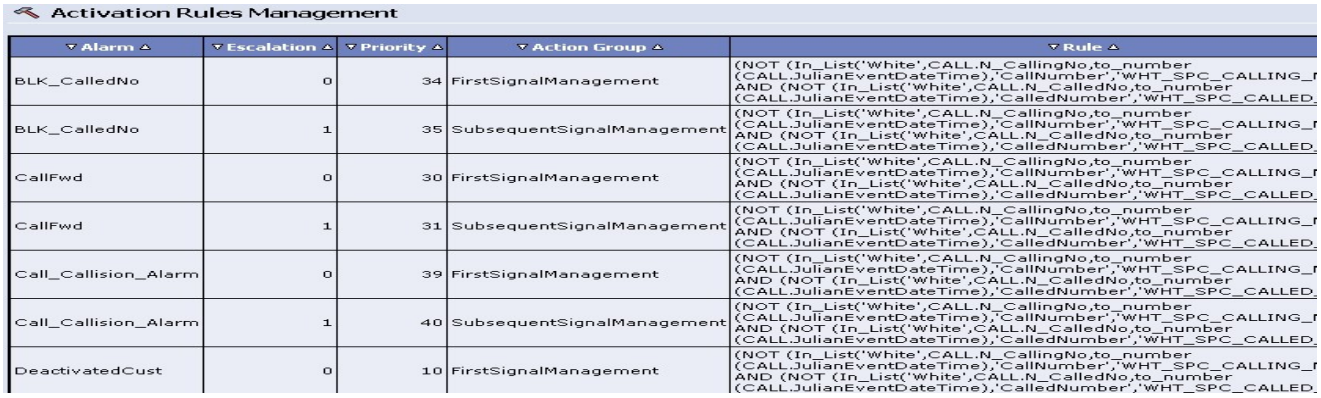
Through this function the Actions to be carried out in the event of fraud alerts are defined. Each alarm's escalation level is linked to Boolean rules that manage and activate it, in growing priority order. The Management of Alarms includes the implementation of one of the following groups of atomic actions:

- Escalate E Increment of the escalation level associated with a user for the specific notification.
- Notify E Opens a fraud case, which the operator might have to work on.
- Reset Escalate E Zero sets the escalation level associated with the user for the specific notification.
- Send specific emails with notification data to configurable recipients.
- External Call E The system provides a dossier of notification data to any external configurable procedures
- No Operation

The following table shows, for each available field, the field name, whether it is required, and a brief description of its function.

Field Name	Description
Alarm	Type of alarm, in priority order.
Priority	Defines action verification order within same group.
Escalation	Level attributed to each set of actions, to enable system to select appropriate set of elementary actions to carry out, given same conditions.
Group	Defines Action's group of belonging.
Rule	SQL like language Boolean expression which, if verified, determines the action to carry out for the group of belonging.





(i) Fraud Detection

(i) Counters

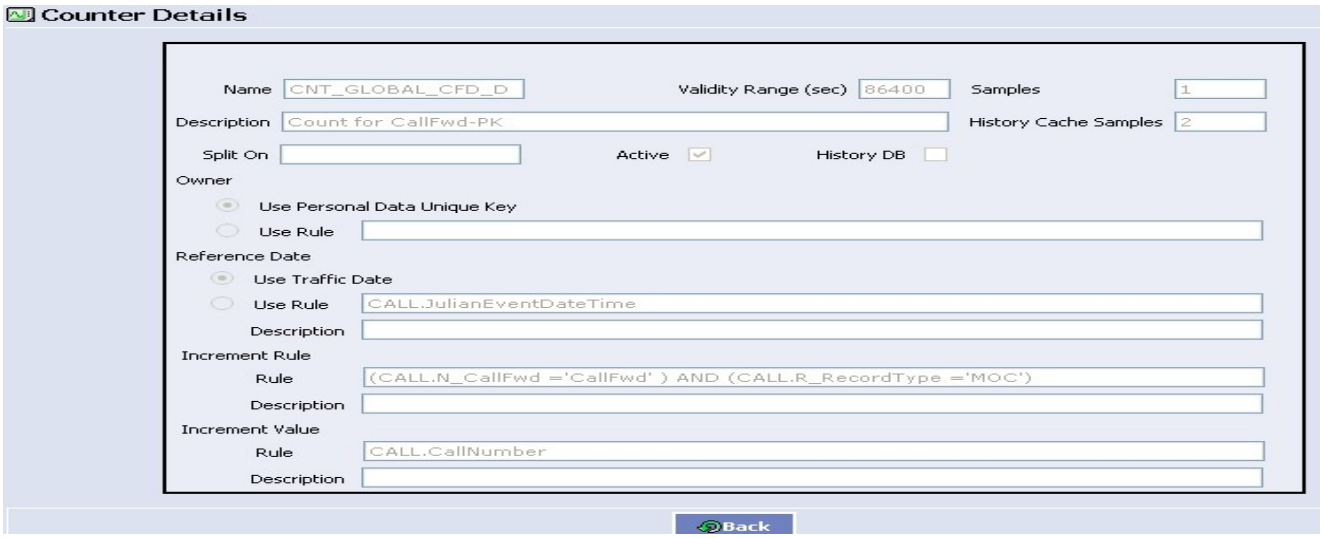
The system's counters totalize the grouped values following an "Owner" key. This allows different sizes to be checked, that are linked to the Monitored flow of events (i.e. number of events, economical value of events, etc.).

The counters' main features are:

- The Owner E an identifier that totalizes the increments for each Owner E can be a Customer Code, an IP address or a telephone number.
- An incremental rule through which the timing of the counter's increment is set (e.g. increase a counter only if the event shows a traffic flow towards a particular destination or group of destinations, or the cost of the single event is higher than a certain value)
- An incremental value through which the incremental amount can be set. The value can be a single unit, so it simply calculates the events, or an economical value associated with the event (e.g. if the event is a consumer event, the increment is equal to the cost of the consumer event, whereas if the event is a recharging event, it is a negative value equal to E in absolute terms E the amount of the recharged event);
- A period of aggregation of events, which defines the period of time over which the events are totalized.

The following table shows, for each available field in the Define Counter window, the field name, whether it is required, and a brief description of its function.

Field Name	Description
Name	Defines symbolic name of counter; the name is usable in SQL like language to question the counter to obtain the current value.
Code	Defines the Counter's numerical code.
Validity Period	Duration in minutes of period within which events are totalized on the basis of the incremental value defined in the same Counter. Duration is linked to start of calculation.
Description	Allows a brief comment on the Counter to be inserted.
Start Calculation	Includes an SQL like language expression, which returns a date hour string (DDEMMEYYYY HH:MM: SS format, with HH range from 00 E 23): defines the time reference point from which the duration of the period of the Counter is calculated. The rule can be defined by using all the variables listed in <Variables>, the functions listed in <Functions> and the operators listed in <Operators>; when the Pattern line is selected, the selection of an item from one of these lists causes links it to the end of the SQL like language expression defined up to that moment.
Incremental Rule	Contains a Boolean SQL like language expression, which, if true, allows the totaling of the incremental value on the counter to be carried out; if not, the counter is not incremented. The rule can be defined using all the variables listed in <Variables>, the functions listed in <Functions, and the operators listed in <Operators>; when the Pattern line is selected, the selection of an item from one of these lists links it to the end of the SQL like language expression defined up to that moment.
Incremental Value	Includes a numerical SQL like language expression, which yields the value whose counter is to be incremented if the increment is verified. The rule can be defined using all the variables listed in <Variables>, the functions listed in <Functions, and the operators listed in <Operators>; when the pattern line is selected, the selection of an item from one of these lists links it to the end of the SQL like language expression defined up to that moment.
Owner	Includes an SQL like language expression, which returns a string that is used as aggregating key of the Counter increments. The numerical increments are totalized only if they share a common Owner. E.g. if the events record telephone calls, you can define a Counter for each group of called numbers which coincide with the first six numbers. The rule can be defined using all the variables listed in <Variables>, the functions listed in <Functions, and the operators listed in <Operators>; when the Pattern line is selected, the selection of an item from one of these lists links it to the end of the SQL like language expression defined up to that moment.



(ii) Black Lists

IProtect allows setting up black lists in order to define known fraudster. The following table shows a brief description of each parameter of a black list:

Field name	Description
Code	Defines Black List's identification code.
Name	Defines Black List's name.
Subject	Defines type of Black List (i.e: black list customer, black list business customers, etc.).
Priority	Defines verification order of specific Black List.
Description	Allows brief description of Black List.
Validity start	Defines operation's start of validity.
Validity end	Defines operation's end of validity.
Notes	Allows explanatory notes to be inserted.

(iii) Patterns

Patterns check new series of values E such as the following E starting from the single event (i.e. a telephone call):

- Personal details associated to the event
- Whether the personal data / event / item belongs to Black List
- Value of particular counters, which can be associated to the event.

If a check is verified, a Pattern notification is generated which, in accordance with the rules defined in Actions Management, can generate a fraud case, which alerts operators.

Alarm details include:

- DetailE1: Pattern name
- DetailE2: Pattern code
- DetailE3: Verified SQL like language rule
- DetailE4: System date and time when notification was emitted
- DetailE5: ** Not used
- DetailE6: ** Not used

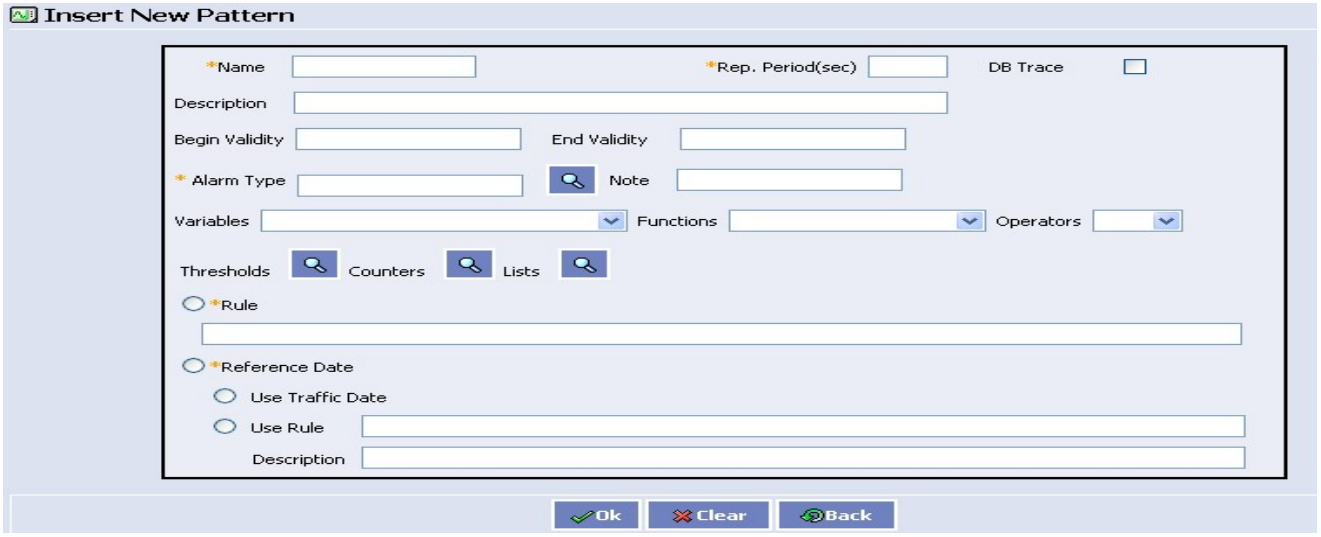
The system verifies the Patterns according to the following steps:

- It examines the Group Patterns ordered according to each one's priority and Rule Code.
- If the rule associated with the Pattern is not verified, it defines the next Pattern within the group.
- If the rule associated with the Pattern is verified, an alarm is triggered; the system defines the first Pattern of the next group, even if there are still patterns to be verified within the current group.

In any case, for the Pattern to be verified, the validity period must include the date of the traffic event (CDR), and the Pattern for the group to which the line belongs must be active.

The following table shows a brief description of each parameter of a pattern.

Field Name	Description
Name	Defines the symbolic name of the Pattern; this name is available in the information associated to the notification as detailE1.
Rule Code	Defines numeric Pattern code: given the same group and priority it chooses the Pattern verification order.
Int. Rep.	Defines the period of time (in seconds), after which the escalation level associated with the notification of the owner (line, contract, etc.), is reEset to zero. The reference time, from which the seconds are counted, corresponds to the date and time of the event, which generated the first notification.
Description	Allows brief description of Pattern.
Priority	Defines verification order of Patterns within the same group.
Group	Defines Pattern's group of belonging.
Validity start	Defines start of validity time from which Pattern check is activated.
Validity end	Defines end of validity time after which Pattern check is not activated any more.
Owner	Includes an SQL like language expression through which a reference point is built. Here notifications are both accumulated and generated during the checks of the rule associated with the Pattern. The expression, which can return a generic personal data item (line code, contract's or costumer's, etc.) or more complex information, is defined by using the variables listed in <Variables>, the functions listed in <Functions> and the operators listed in <Operators>. When the Pattern line is selected, the choice of an item from one of the lists links it to the end of the defined SQL like language expression.

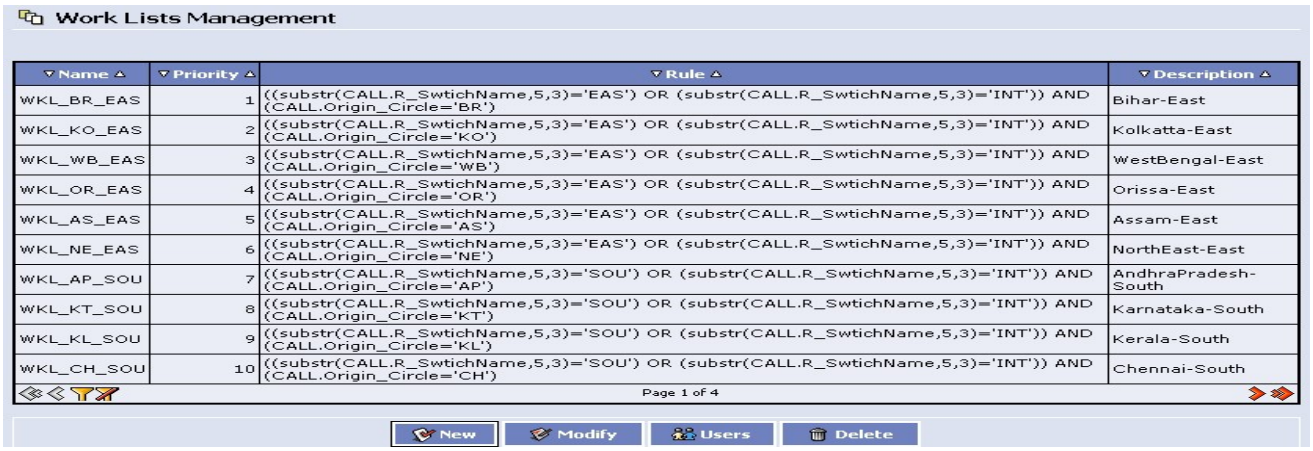


(iv) Work lists

IProtect allows setting up work lists, to manage the fraud cases generated by the system E can be viewed and defined.

The following table shows a brief description of each parameter of a work list.

Field Name	Description
Name	Defines the name of a Worklist.
Variables	Allows variables from a defined list to be inserted.
Alarms	Allows alarms from a defined list to be inserted.
Rule	Allows a rule from a defined list to be inserted.
Priority	Allows a priority from a defined list to be inserted.
Operators	Allows an operator from a defined list to be inserted.



 CONFIDENTIAL

(j) Case Management Workflow Module

Case Management Workflow Module offers a complete web based interface to the analyst team in charge to verify and investigate fraud cases generated. It is possible (as in all Modula GUI's) to set up specific user profiles associating to the profiles single features within the product and associate users to user profiles (user and profiles structure can be synchronized with the centralized access authorization system).

This flexibility allows to perfectly tailoring Case Workflow structure to carrier organization and to fraud analysts team composition.

Generated cases are taken by analysts offering them powerful and performance data traffic search engine with multiple search key support, black list access along with a complete work list (queues) support that allows each analyst to correctly manage the history of his cases assigning severity level of fraud case and tracking the case life through its different steps, escalate if needed, overriding alarms.

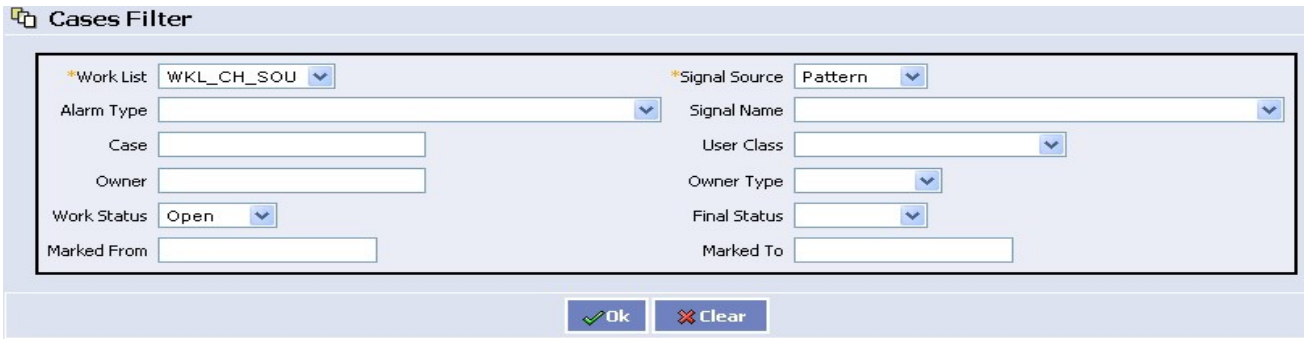
Through an alarm interface it is also configurable to trigger alarms when severity level is exceeded through electronic devices to selected users.

It is also possible to establish escalation procedures based on case severity and automatically assign cases to fraud analysts based on various criteria (e.g. market, type of case, type of customer, fraud analyst experience level) as well as adding resolution descriptions once cases are closed.

Case management workflows allows to collect cases in "dossiers", improving operators capability in relate cases basing on case similarity, and managing a set of them as a unique object, the dossier.

Via case management GUI operators can track cases/dossiers, taking actions such as additional payments, service barring etc., marking the dossier for follow-up.

The capability of the system to define work lists for operators, automatically assigning cases to a specific work list depending on case characteristics, allows to efficiently subdividing workload on operators basing also on operators skills (e.g. international fraud operators, national frauds operators, etc.).



India
360 Kalyandas Udyog Bhavan,
Prabhadevi,
Mumbai - 400025.

Email: info@iacuitytelco.com www.iacuitytelco.com

.

CONFIDENTIAL