Middleware Improved Technology (MIT) to support dependability improvement in interdependent Critical Infrastructures

CRITIS '08

Roma - October 14, 2008

L. Lavalle (ENEA), A. Di Pietro (ENEA), M. Schembri (AIS), S. Geretshuber (IABG)

IRRIIS - FP6-2005–IST-4

Background: lessons learned

- System disturbance on 4 November 2006
  - It was triggered neither by technical failure nor by external event (such as extreme weather conditions)
  - “No specific attention was given by E.ON Netz to the fact that the protection devices have different settings on both sides of the Landesbergen-Wehrendorf line although this information was critical due to the very high flow on this line”.
  - “In some control areas, re-energization of customers was started by DSOs without proper knowledge of the situation in the overall UCTE system; some of them started reconnecting customers without coordination with their TSOs. This worsened the conditions for TSOs action to restore normal system conditions in a controllable way”.

- Blackout on 14 August 2003
  - “Cellular services were severely disrupted because most antenna sites were only provisioned with four to six hours of emergency battery power”.
  - “The state of Michigan scrambled to locate additional fuel supplies for telephone central office backup generators in anticipation of an extended loss of power”.

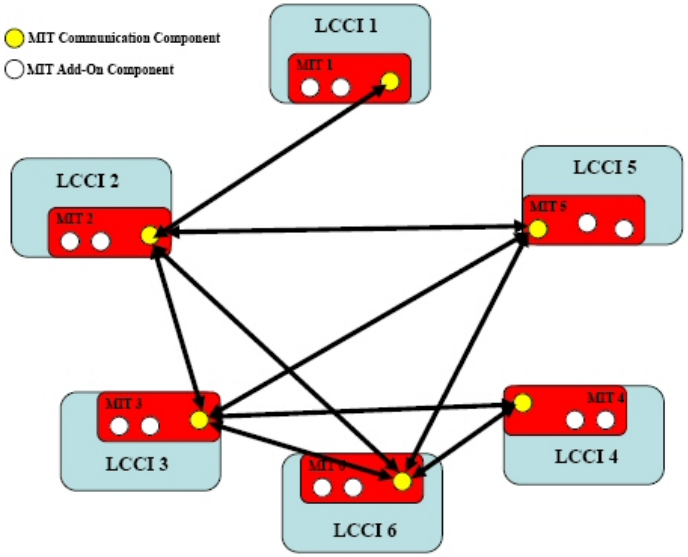
Needed MIT

- To mitigate interdependency effects we need:
  - To improve situational awareness
  - To support collaboration
  - To support risk assessment
- MIT is
  - A communication “platform” for automated information sharing
  - A set of additional tools to support risk assessment related to interdependency

Acceptable MIT: Constraints identified by stakeholders

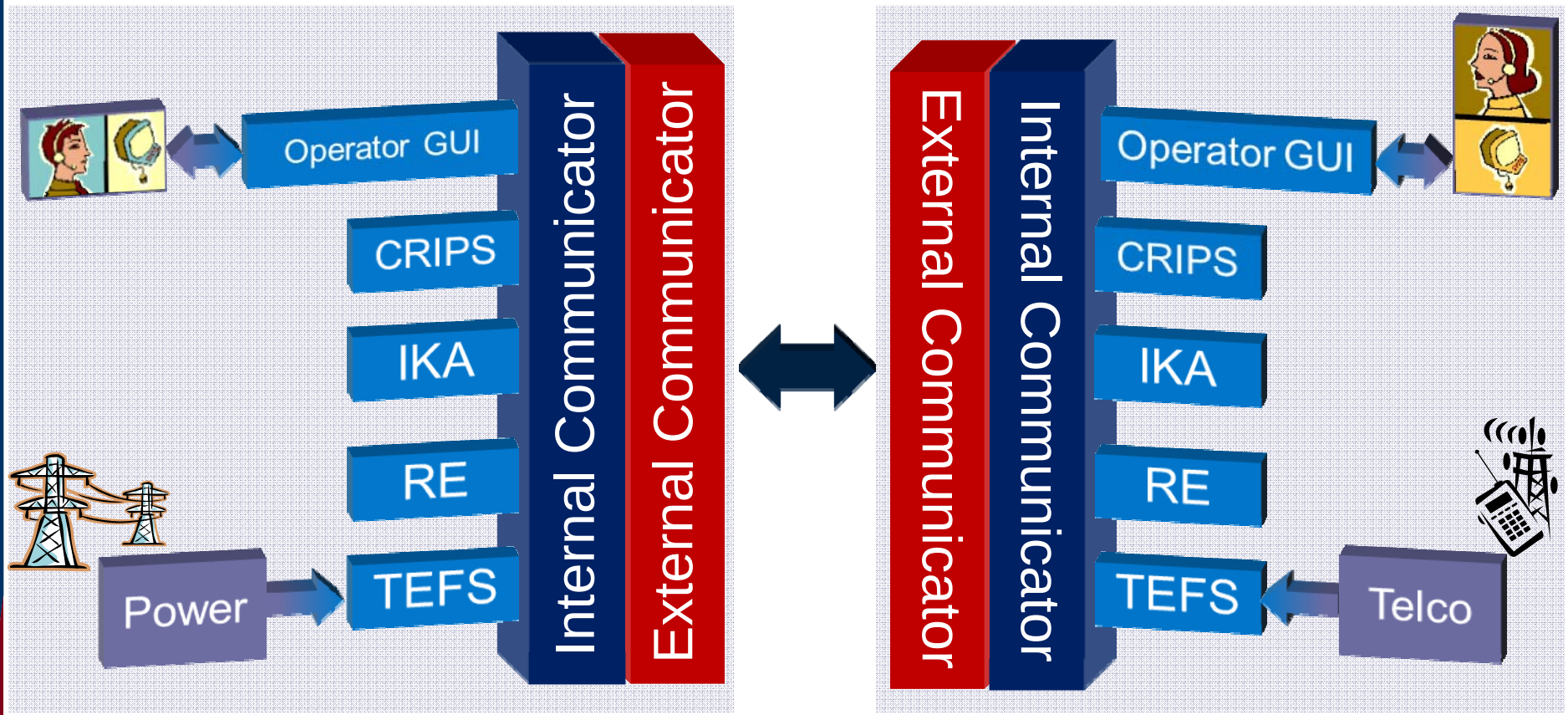
- MIT shall not require replacement of existing equipment or SW/HW modifications requiring re-certification of existing tools/equipment
- MIT shall be optional
- MIT shall work in existing working conditions
- MIT shall be designed to interface existing decision support tools
- MIT shall relieve the operator of duties unrelated to his CI management during emergencies
- Type and content of the information to be shared shall be agreed by the involved/interested CIs depending upon mutual interest.
- MIT shall process the information inside the CI and shall send just post-processed sanitised output

MIT Architecture



- Constraints identified by stakeholders have been taken into account
- Communication is conceptually peer-to-peer
- MIT will be installed in the Control Centre, but in a separate machine
- Communication Components + Add-On Components.

MIT with other CI(s)



MIT Communication Components

- Function: to exchange data with MIT installed on neighbouring CIs
- Features:
  - Information Message
    - to send information on occurring events, taking into account service details, planned Quality of Service and probability of occurrence
  - Negotiation Message
    - to negotiate downtimes of services with other CIs
- Additional Info:
  - Same Communication Components for all the CIs

MIT Add-On Components

- **Internal assessment**
  - To provide the operator with a clear and as much as possible thorough (and useful!) picture of his own CI
  - To get information needed by neighbouring CIs about the local infrastructure status
- **Risk assessment**
  - To correlate the internal status of the CI with the status of neighbouring CIs
  - To estimate the probability of occurrence of undesirable event based on both internal and neighbouring status
  - To share risk information with interested neighbouring CIs
- **Emergency management**
  - To support the operator during an emergency.
  - To support the local CI operator in the negotiation process with operators of the neighbouring CIs during an emergency.

Tool to Extract Functional Status

- Function: To interface with SCADA and existing tools in the Control Centre and merge their output in order to have a clear and complete picture
- Features:
  - Basic source of information for TEFS is SCADA system with its underlying database
  - Interfaces SimCIP
- Additional Info:
  - Mandatory to provide information to dependent CIs
  - We have a TEFS for each domain
  - Different approach if neighbouring CIs belong or not to the same domain

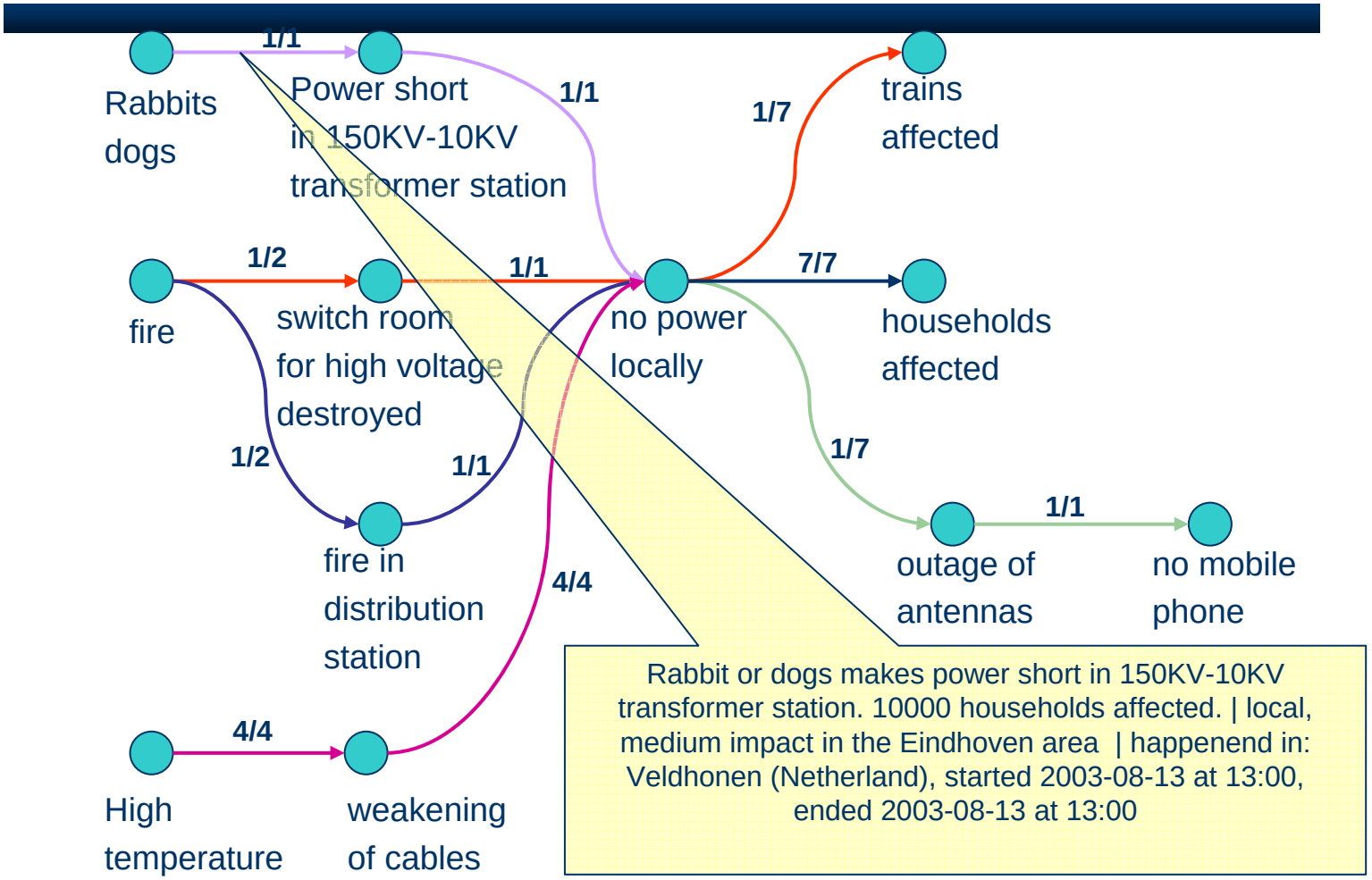
Risk Estimator

- Function: to assess immediate and potential risk of degradation/outage of services that are critical for its own mission
- Features:
  - Gets information from local and neighbouring CI
  - Estimates the risk taking into account
    - Probability
    - Severity of consequences
  - Shows level of risk on a “map”, taking into account both value and trend
- Additional Info:
  - We are exploring different approaches to make a good estimation
  - Allows “experts” to refine correlation information

Incident Knowledge Analyser

- Function: to exploit stored experience and identify if current situation has some similarity with one of the precondition which led to a disruption of operation in the past
- Features:
  - checks immediately whether on-going failures are notified as causes of major incidents in the past.
  - extracts possible known cascading effects of on-going failures.
  - stores new incidents
- Additional Info:
  - Mind Map
  - Enable experience sharing
  - It can incorporate other knowledge

Incident Knowledge Analyser Mind Map

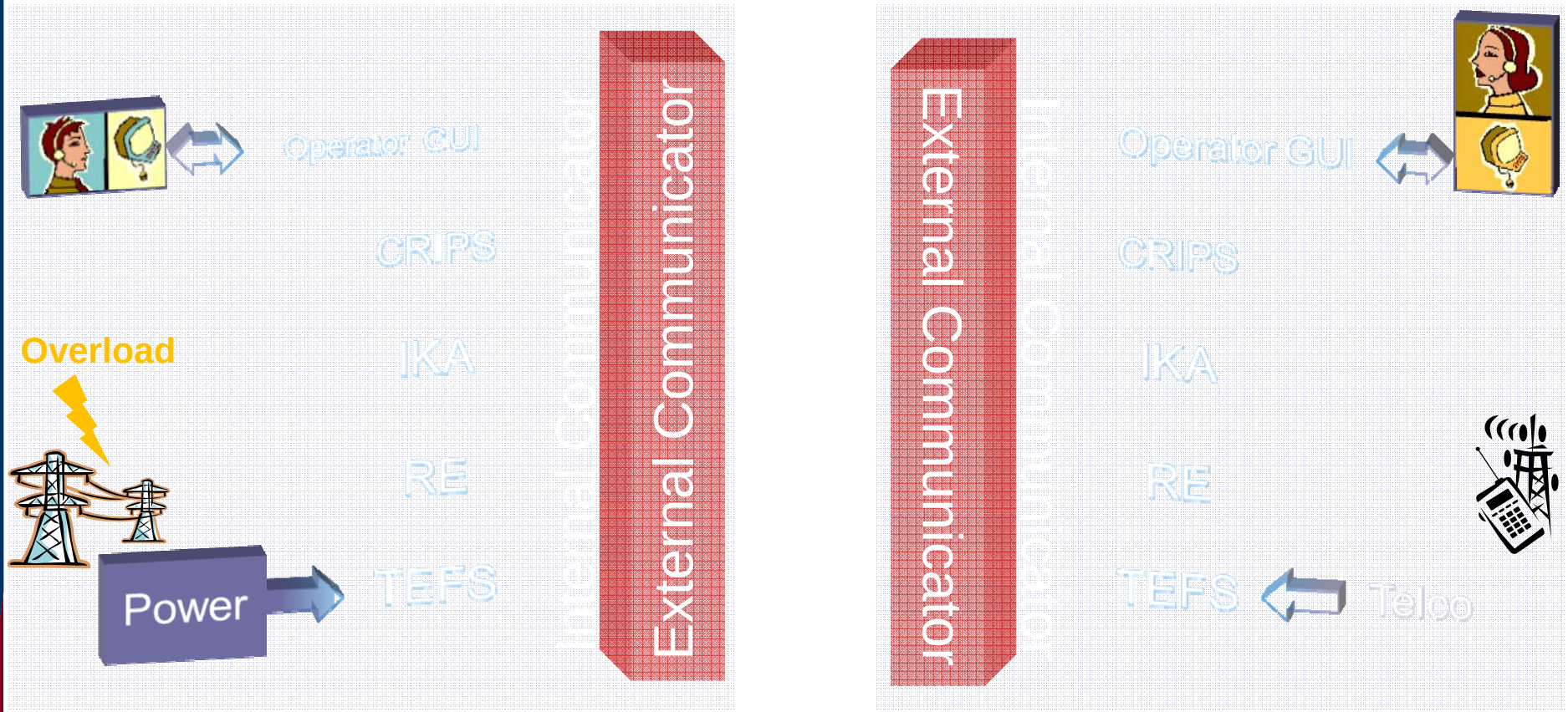


CRIPS

- CRIPS is a Knowledge Based Expert System
- CRIPS supports operators by
  - Assessing of the current situation based on
    - dependency structures
    - insights gained during exercises
    - experiences from incidents

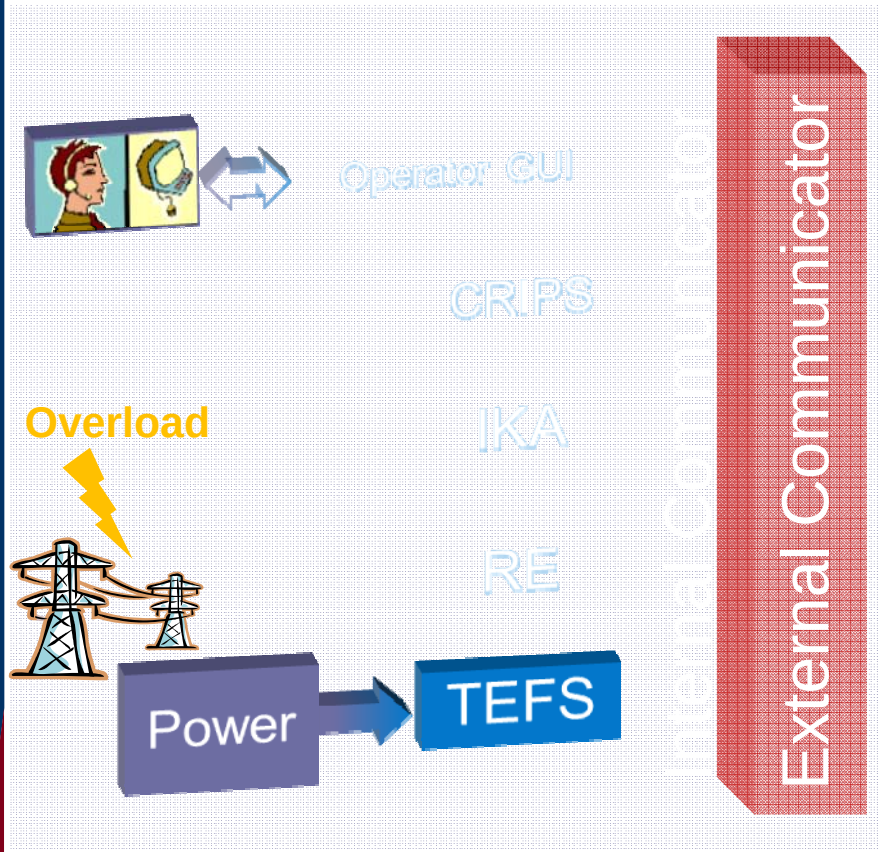
    } = **Expert knowledge**
  - Suggesting measures/decisions based on this assessment

Communicating Risk using MIT



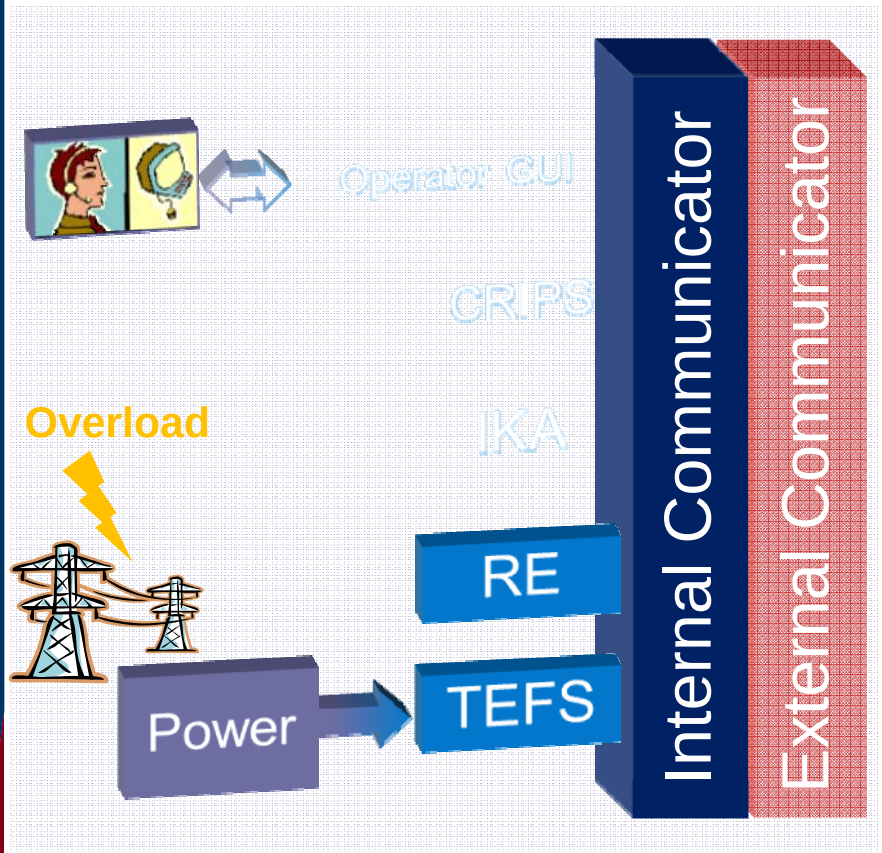
Overload in SCADA at Power LCCI

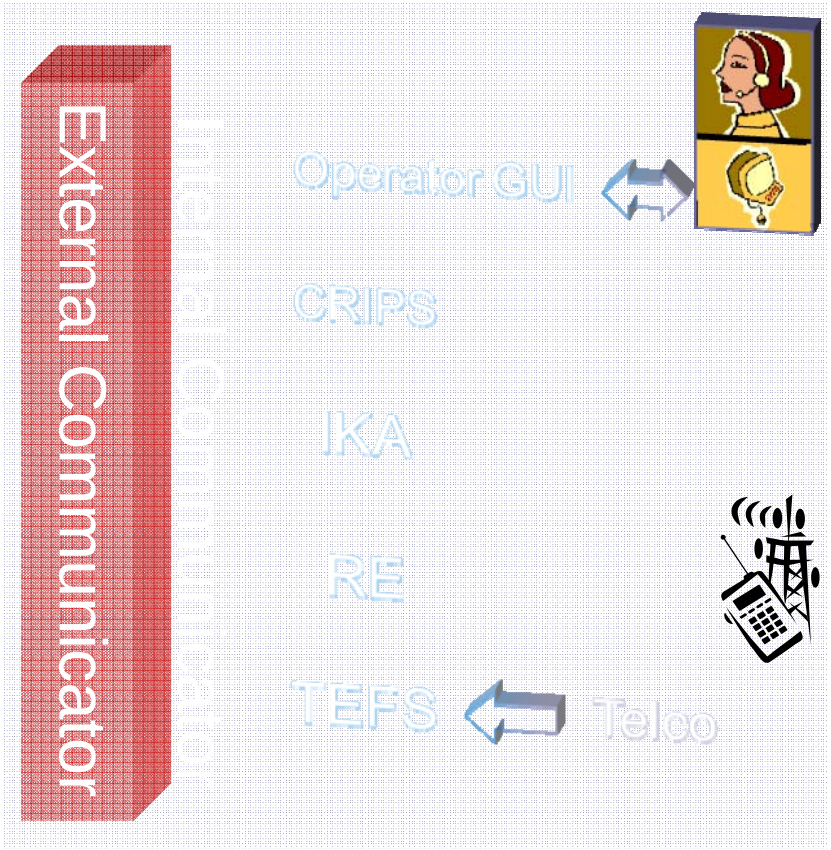
Communicating Risk using MIT



Overload detected by TEFS

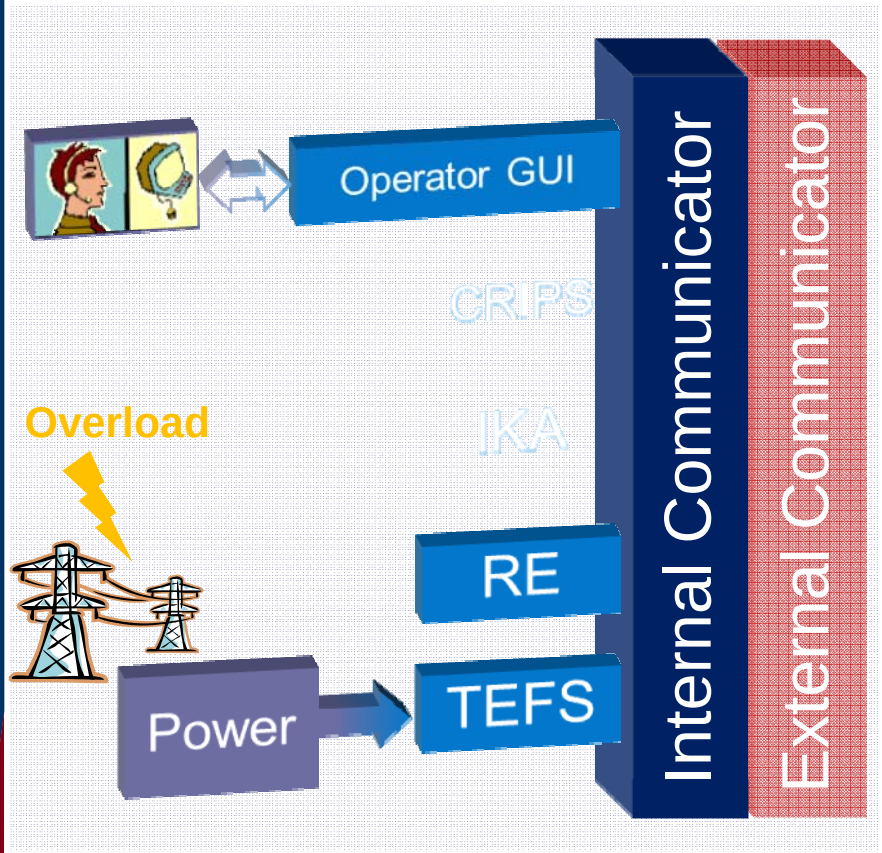
Communicating Risk using MIT

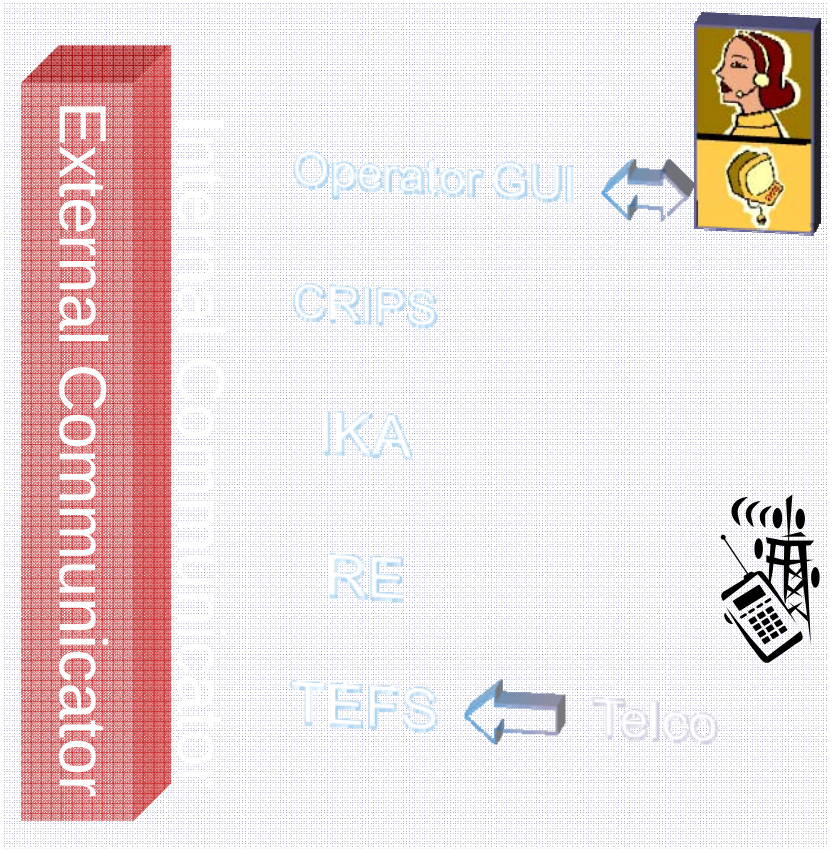




Risk estimator obtains TEFS value and makes necessary risk calculation

Communicating Risk using MIT



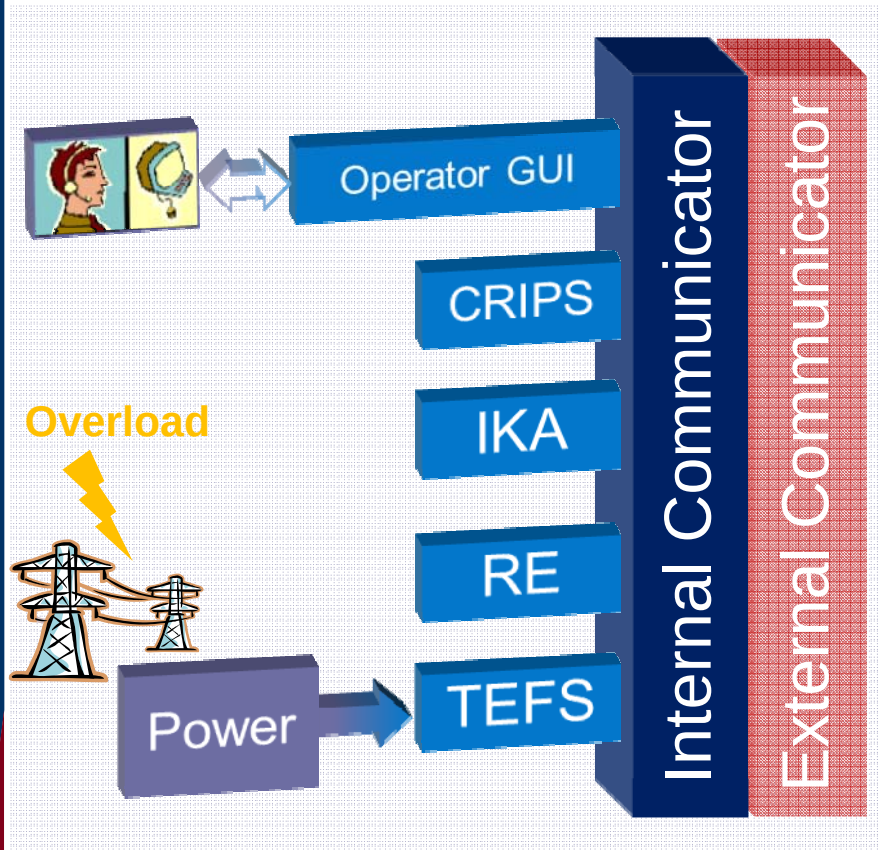


Operator can see risk value for its services through Operator GUI

Communicating Risk using MIT

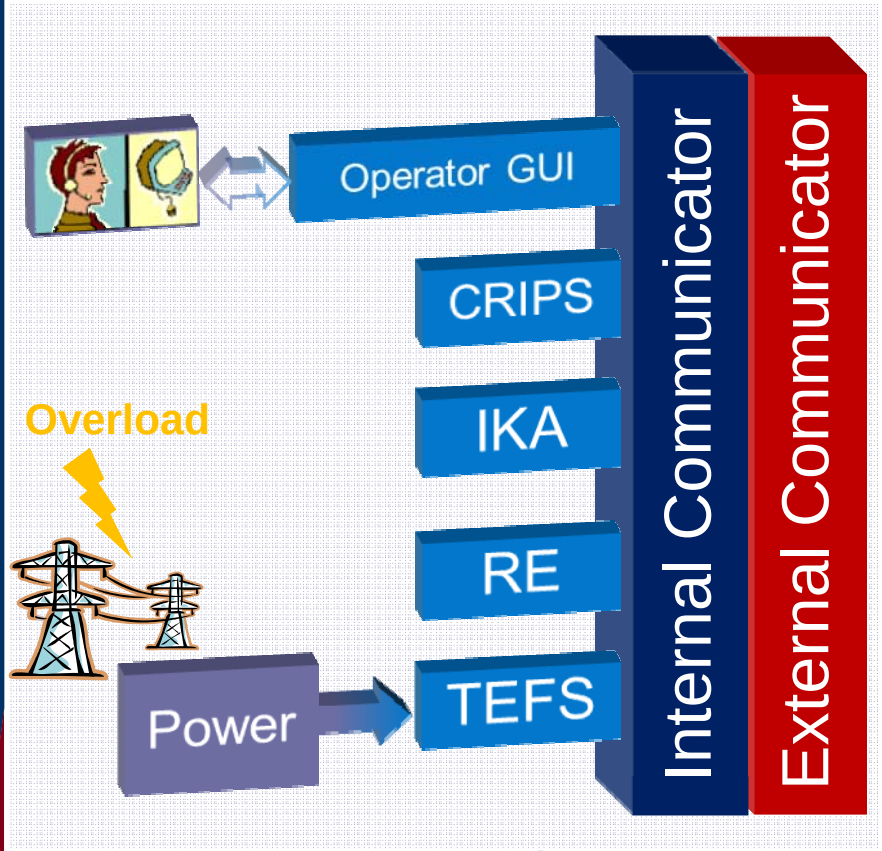
Using the IKA, operator analyses situation by checking whether the event has happened in the past and what consequences it had.

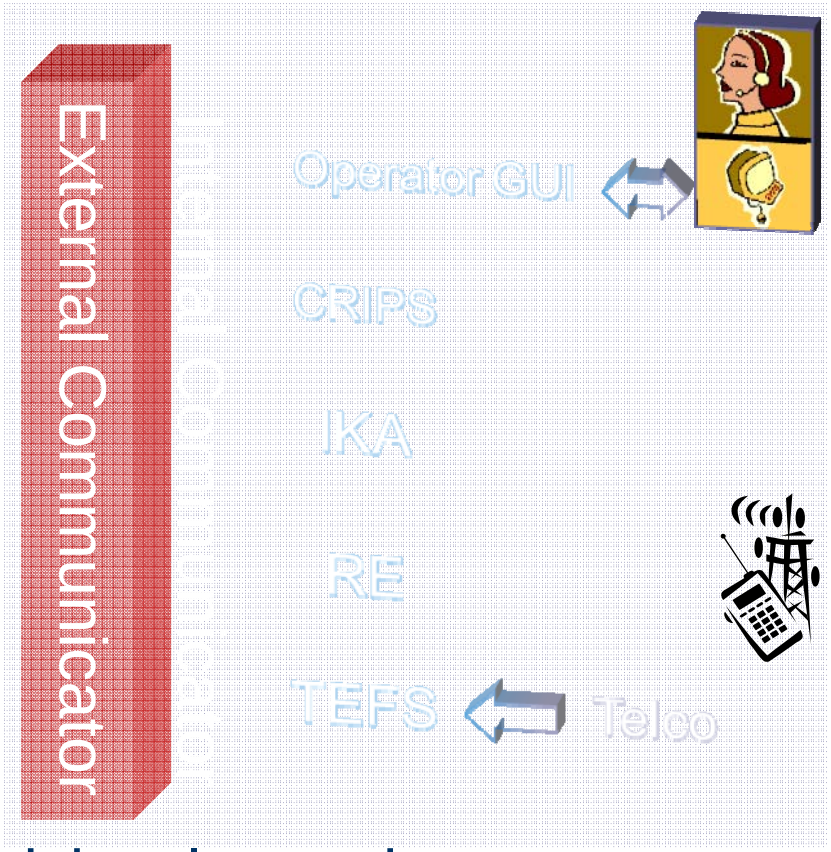
Communicating Risk using MIT



Using CRIPS, operator is suggested certain actions based on the rules built into CRIPS.

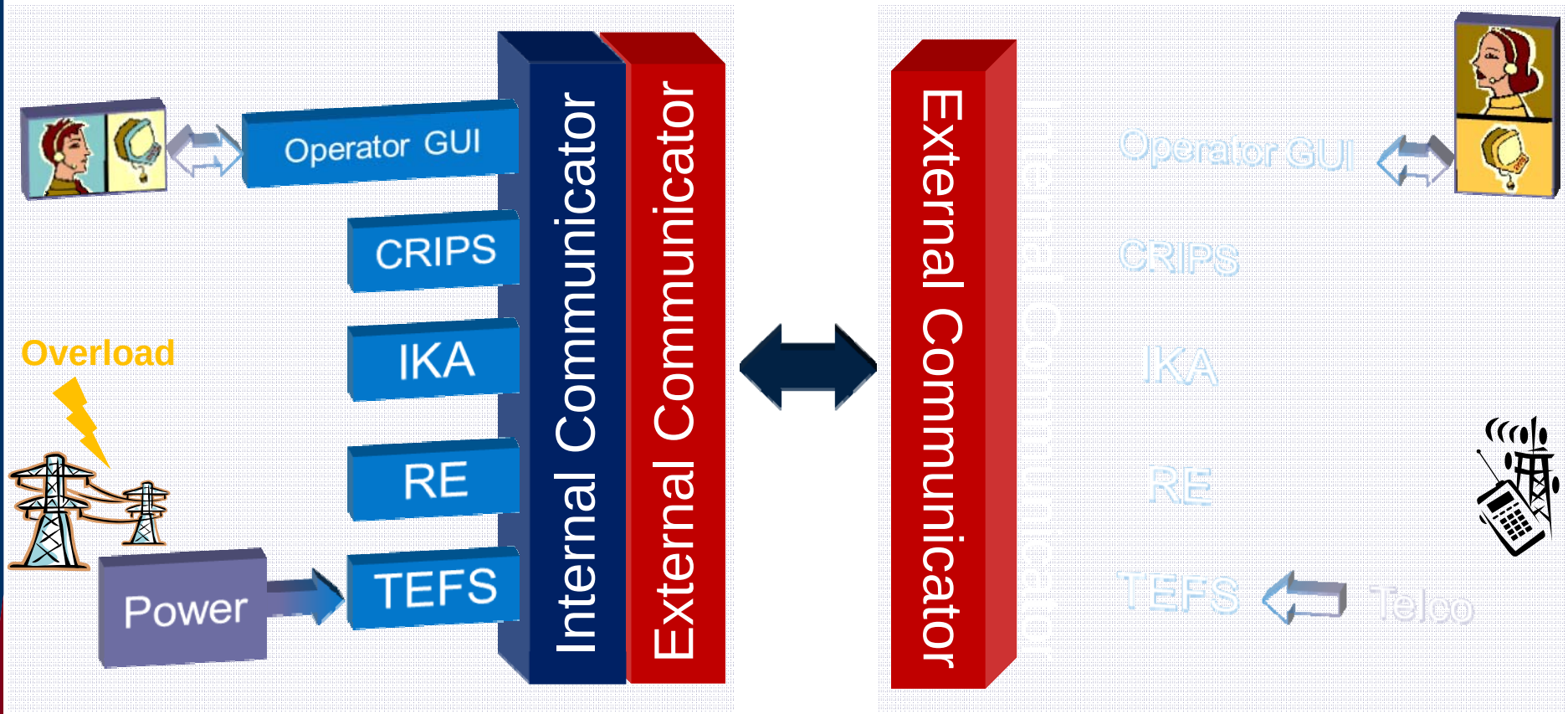
Communicating Risk using MIT





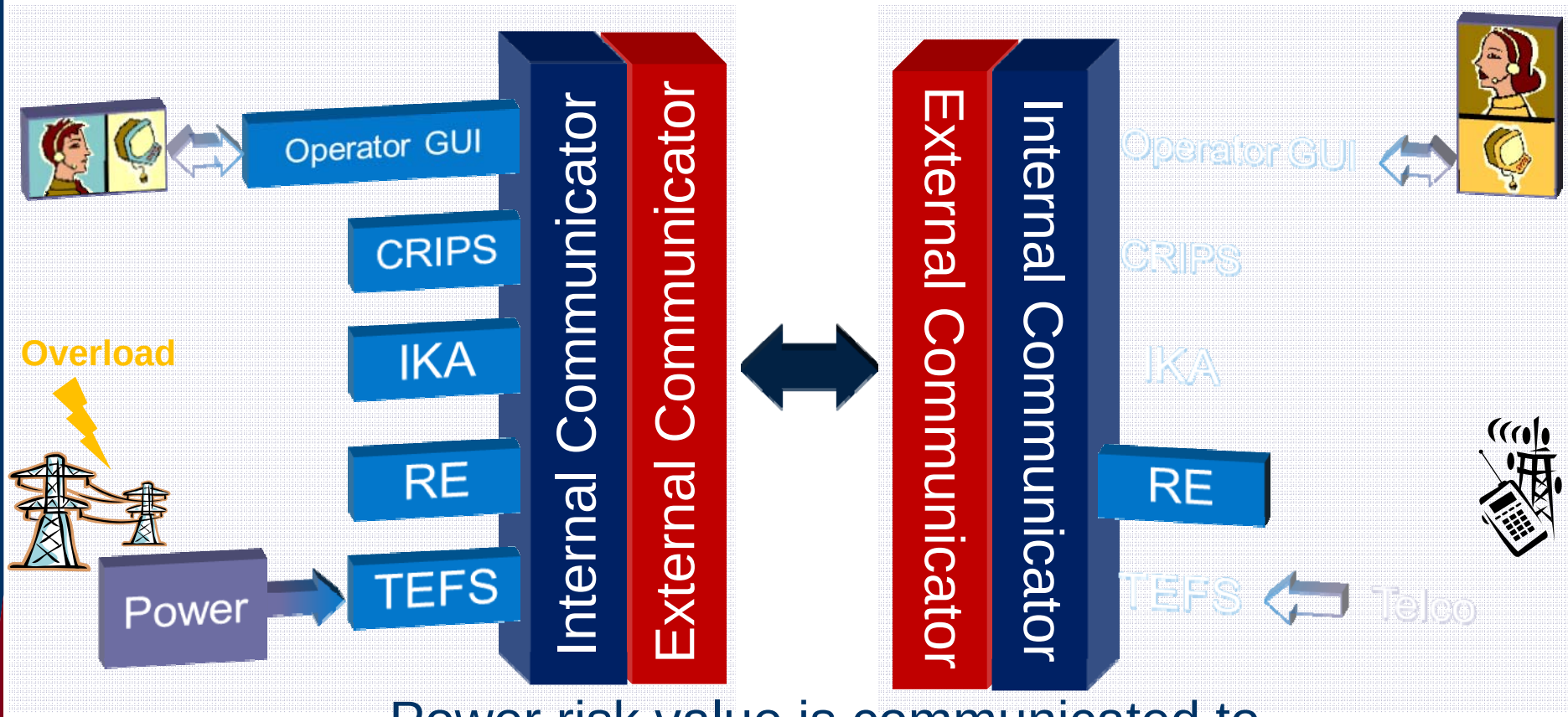
Operator confirms risk value and chooses to send it to subscribed LCCIs.

Communicating Risk using MIT



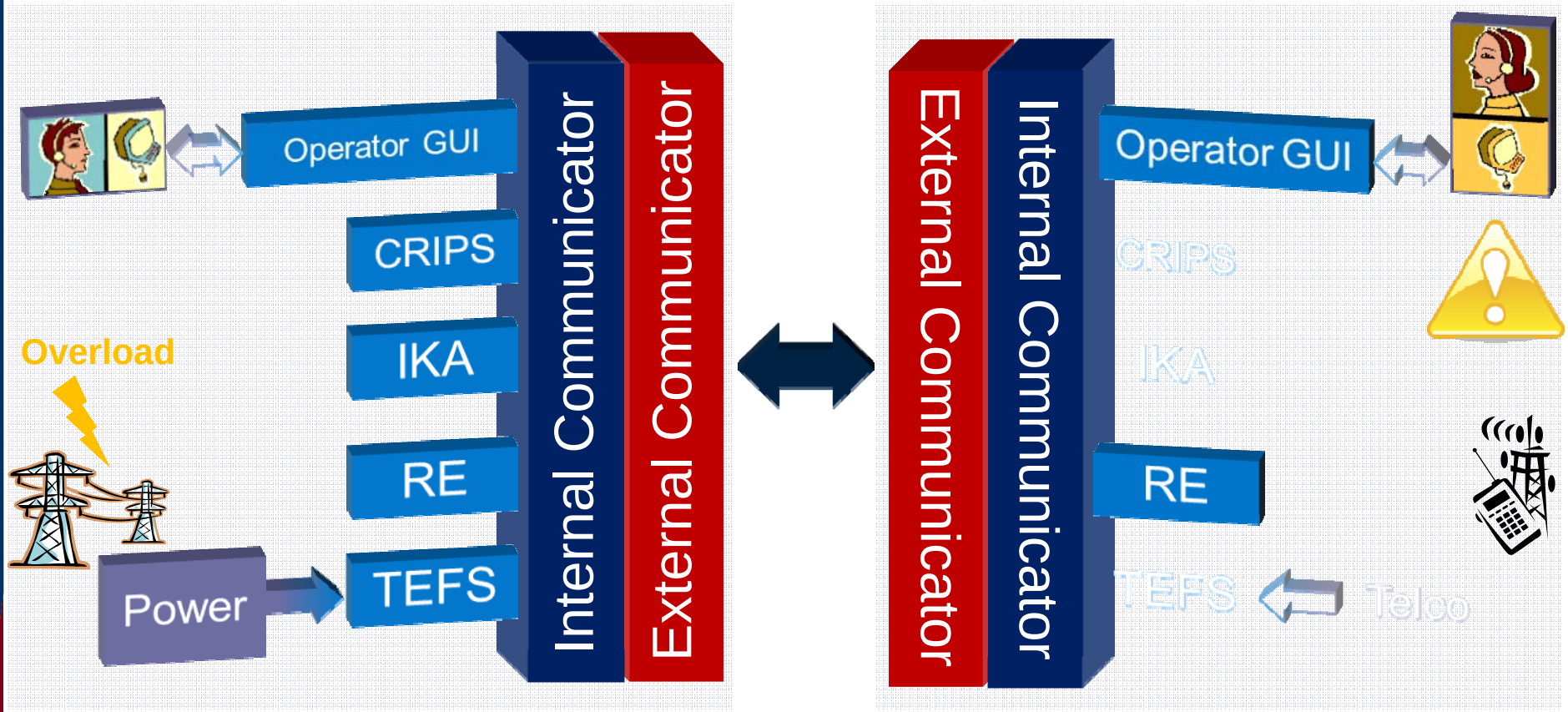
Effected LCCI receives risk value

Communicating Risk using MIT



Power risk value is communicated to the telco RE to calculate the effect on its own Services.

Communicating Risk using MIT



Telco Operator is warned of the effect of risk at power LCCI on its services through the Operator GUI

THANK YOU

IRRIIS - FP6-2005–IST-4