Ingegneria del Software - Laboratorio
La costruzione razionale di una specifica di requisiti: il caso μ-SMA

Vincenzo Gervasi

20 febbraio 2000

1 Circe e la costruzione razionale di requisiti

Circe è un ambiente di supporto alla scrittura, analisi, validazione e misurazione di requisiti software in linguaggio naturale [2]. Sia l'interfaccia del sistema che le sue modalità operative sono strutturate in modo da non precludere alcuna forma di utilizzo dell'ambiente. In altre parole, Circe propone all'utente un'interfaccia "piatta", che l'utente del sistema può adattare allo stile di lavoro preferito e usare secondo le sue necessità.

Sebbene Circe si presti a forme diverse d'utilizzo, una certa disciplina nella fase di scrittura dei requisiti conduce solitamente a risultati di migliore qualità. In questo articolo viene presentata una possibile disciplina d'uso, che chiamiamo *costruzione razionale* dei requisiti. Il metodo viene presentato attraverso un esempio di applicazione a un caso concreto, in cui ciascun passo è corredato da una breve presentazione teorica che illustra i principi seguiti.

2 Il caso di studio

2.1 Tipologia del sistema

Baseremo i nostri esempi sul caso di studio, semplificazione di un sistema realmente esistente, di un sistema di monitoraggio ambientale.

I sistemi di monitoraggio costituiscono una classe particolare di sistemi di controllo. In tali sistemi, la componente di raccolta dati dai sensori, e la presentazione degli stessi agli utenti del sistema, sono dominanti rispetto alle azioni che il sistema deve compiere in risposta a stimoli esterni o dell'utente. Considerare un sistema di monitoraggio, tuttavia, non costituisce una sovrasemplificazione rispetto al caso completo dei sistemi di controllo, poiché in questo secondo caso la componente attiva (controllo) si presenta come l'esatto duale della componente passiva (monitoraggio).

Il nostro sistema di test presenta inoltre alcune interessanti caratteristiche legate agli aspetti temporali e alla robustezza rispetto ai fallimenti di componenti, (quest'ultima caratteristica esemplifica il trattamento di requisiti non-funzionali).

2.2 L'enunciato del problema

Il sistema μ-SMA viene descritto, in forma già sufficientemente completa, ma non precisa, dal seguente *Enunciato del problema*, fornito dal committente:

1. Il sistema di monitoraggio ambientale μ-SMA ha lo scopo di rilevare con continuità i parametri ambientali e metereologici su scala regionale, di segnalare tempestivamente l'eventuale superamento dei limiti di attenzione, di attivazione o di emergenza per ciascuno dei parametri monitorati, e di costituire un dettagliato archivio storico dell'evoluzione dei parametri ambientali.

2. Il sistema si articola su tre livelli: un Centro di Controllo Regionale (CCR), un insieme di Centri di Controllo Locali (CCL) e, per ciascuno di essi, un insieme di Centraline di Rilevamento (CdR). Il CCR monitorizza l'attività dei CCL e raccoglie i dati storici che questi ultimi gli inviano giornalmente; i CCL interrogano ogni cinque minuti tutte le CdR a essi collegate per raccogliere le relative misure. I CCL verificano inoltre il superamento dei limiti, che possono essere impostati dal personale di gestione e che sono tipicamente diversi a seconda della località in cui le CdR sono installate. Il superamento dei limiti di attenzione viene segnalato localmente al personale del CCL; il superamento degli altri limiti, ovvero il superamento continuato per oltre quattro ore dei limiti di attenzione, viene segnalato sia al CCL che al CCR.

3. Il μ-SMA deve essere in grado di continuare a operare ragionevolmente in presenza di guasti alle CdR (assenza di risposta alle interrogazioni del CCL, o risposta con valori fuori scala), che devono comunque essere segnalati al CCL. CCL e CCR sono realizzati con tecnologia ridondante e si suppongono affidabili, ma un collegamento CCL-CCR può non essere disponibile per un tempo massimo di 72 ore. In ogni caso, i dati storici devono essere preservati e trasmessi appena possibile; l'interruzione del collegamento deve essere segnalata non appena rilevata al personale del CCR.

4. Ogni CdR è caratterizzata da una marca, un modello, e un codice identificativo unico. Il CCL conosce per ogni CdR connessa il nome simbolico della grandezza misurata, l'unità di misura, e i limiti di scala per le misure accettabili.

5. Deve essere possibile in ogni momento aggiungere o rimuovere CdR a un CCL; allo stesso modo, deve essere possibile aggiungere o rimuovere CCL a un CCR. Ogni variazione della configurazione del sistema deve essere riportata nell'archivio storico.

6. Il sistema deve offrire al personale del CCL un'interfaccia utente che visualizzi con continuità le misure rilevate e gli eventuali allarmi dovuti al superamento delle varie soglie, nonché le indicazioni di malfunzionamenti nel sistema. Al personale del CCR devono essere segnalati soltanto gli allarmi (con l'indicazione della misura che eccede i livelli) e i malfunzionamenti.

Faremo spesso riferimento a quanto detto nell'enunciato, che rappresenta la nostra unica fonte di informazione sui desideri del committente; i casi in cui *introdurremo* informazione saranno evidenziati di volta in volta, e le informazioni introdotte dovranno essere soggette a verifica presso il committente.

3 La costruzione razionale dei requisiti

3.1 Principi generali

Il principio fondamentale che sottintende alla costruzione razionale dei requisiti è quello della *separation of concerns*, ovvero della separazione fra aspetti diversi del problema. Nella nostra applicazione, la separazione si concretizza nell'analisi distinta e progressiva di varie caratteristiche del sistema di cui si devono definire i requisiti.

In un caso tipico, sarà possibile analizzare separatamente, per esempio, gli aspetti di flusso di dati (chi invia cosa a chi) e quelli di ordinamento temporale degli eventi (quando accade qualcosa), oppure i dettagli dell'interfaccia utente (come viene mostrato qualcosa) e il funzionamento degli algoritmi (come viene calcolato un risultato).

La separazione di questi aspetti può essere intesa sia in senso *temporale* che in senso *spaziale*. Nel primo caso, i vari aspetti rilevanti vengono analizzati in sequenza, da un solo gruppo di analisti[1] che lavora aggiornando di volta in volta un unico documento di requisiti. Nel secondo caso, invece, i diversi aspetti possono essere affrontati separatamente da più gruppi di analisti, ciascuno specializzato in un sotto-dominio dell'applicazione. Questo secondo caso è più adatto al cosiddetto *modello a griglia*, in cui le competenze interne all'organizzazione sono raccolte per domini applicativi (per esempio: applicazioni bancarie) e, separatamente, per domini tecnologici (per esempio: sistemi distribuiti). In questo caso, ogni gruppo di analisti produrrà un documento di analisi parziale, che può poi essere consolidato in un solo documento con l'assistenza delle funzioni di validazione di CIRCE, quali l'identificazione di requisiti ridondanti.

Per il nostro caso di studio, considerata la ridotta complessità del sistema, faremo uso del primo modello: l'enunciato del problema verrà analizzato di volta in volta con l'ottica di estrarre le sole informazioni rilevanti per l'aspetto considerato, aggiornando via via un singolo documento di requisiti fino al completamento dell'analisi.

3.2 Designazioni e definizioni

È di fondamentale importanza distinguere fra *designazione*, ovvero l'attribuzione di un nome (univoco e condiviso) a un concetto tipico del dominio applicativo o del sistema che si sta specificando, e *definizione*, ovvero una convenzione che attribuisce un nome breve a un concetto complesso o a una relazione sulle designazioni.

Per esempio, con riferimento al paragrafo 1 del nostro enunciato, "parametro ambientale" *designa* un ente del dominio, che non viene ulteriormente analizzato, mentre nel paragrafo 3 "guasti alle CdR" *definisce* una situazione (la definizione è data immediatamente di seguito nel paragrafo).

In CIRCE, le designazioni possono solo essere introdotte come elementi di glossario, mentre per le definizioni possono essere adottate tre strategie:

1. introdurre esplicitamente nei requisiti la definizione corrispondente;
2. eliminare il termine definito e sostituirlo in ogni occorrenza con la relativa definizione;

[1] Il gruppo, ovviamente, può anche essere composto da una sola persona.

3. introdurre il termine definito nel glossario e non introdurre la sua definizione (può essere utile introdurla comunque come commento al termine di glossario).

In molti casi, la seconda o terza strategia è perfettamente applicabile, e riduce la possibilità di introdurre errori nel documento di requisiti: nel secondo caso, infatti, viene eliminato dai requisiti il termine definito, mentre nel terzo caso viene eliminata la sua definizione. In ogni caso si ottiene un documento più lineare. Anche noi adotteremo questa tecnica nel corso della nostra analisi.

3.3 Linguaggio e raffinamenti

L'approssimazione del linguaggio naturale definita da Circe include un certo numero di costrutti di astrazione/raffinamento che ricalcano l'uso comune del linguaggio come mezzo di astrazione. Questi costrutti possono essere utilmente applicati all'analisi dei requisiti ricalcando il diverso livello di comprensione che si ha a un dato momento delle proprietà del sistema di cui si vogliono analizzare i requisiti.

3.3.1 Azioni

Circe accetta la definizione di *azioni atomiche* denotate dal tag `/ACT`[2]. Un'azione di questo tipo è, per esempio,

```
muSMA monitorizza parametri/ACT.
```

che consente di "comprendere" il requisito

```
Il muSMA monitorizza i parametri.
```

Circe considera un'azione dichiarata come quella sopra in maniera atomica: non si hanno informazioni sugli elementi che costituiscono l'azione. Per esempio, da questa definizione non è possibile riconoscere il fatto che si sta parlando di una funzionalità del μ-SMA. Una versione meno astratta dello stesso concetto si può ottenere con il tag `/FUN`, che isola l'agente dalla funzione. La dichiarazione di glossario corrispondente sarebbe

```
muSMA.
monitorizza parametri/FUN.
```

che permette di esprimere lo stesso requisito dato sopra, ma consente a Circe di riconoscere che si sta descrivendo una funzionalità del μ-SMA. Un ulteriore raffinamento può essere ottenuto dettagliando l'azione, se questa è (o può essere ricondotta a) uno dei tipi di azione riconosciuto da Circe. Nel nostro caso, "monitorizza i parametri" indica probabilmente che il μ-SMA riceve i parametri da qualcuno (ed eventualmente li usa in altre elaborazioni non specificate). Questo fatto può essere espresso agevolmente dal requisito

```
muSMA riceve i parametri da qualcuno.
```

che introduce nel glossario i termini

[2] In versioni precedenti di Circe, questo tag era chiamato `/AZ`.

```
muSMA/IN.
parametri/INF.
qualcuno/OUT.
```

L'aggiunta di ulteriori dettagli, per esempio sul tipo di elaborazione che costituisce il "monitoraggio" e sulla destinazione dei risultati di tali elaborazioni, arricchirebbe ulteriormente i requisiti e il glossario (per esempio, `muSMA` diventerebbe `muSMA/IN/ELAB/OUT`.

Si noti ancora che ciascuna di queste forme esprime un requisito perfettamente valido, a diversi livelli di astrazione. Ovviamente, i requisiti più dettagliati forniscono più informazioni e possono essere oggetto di controlli di validazione più precisi.

3.3.2 Eventi

Analogamente a quanto visto sopra per le azioni, esiste una forma atomica per gli eventi, denotata dal tag `/EVT`. Così, per esempio, la voce di glossario

```
misura eccede limiti/EVT.
```

consente di scrivere requisiti come

```
Se la misura eccede i limiti, allora ...
```

Anche in questo caso, Circe non è in grado di penetrare la struttura dell'evento atomico per comprendere, nel nostro caso, che questo evento richiede la disponibilità dei dati *misura* e *limiti*. Per analogia con i linguaggi di programmazione, potremmo dire che la forma precedente corrisponde all'uso di un valore booleano, di cui però non si conoscono le modalità di calcolo:

```
IF misura_eccede_limiti THEN ...
```

Un primo raffinamento può essere ottenuto con l'uso del tag `/UNOP` (operatore unario), che esprime una proprietà su un valore (con tag `/INF`). L'esempio precedente potrebbe essere compreso anche dichiarando nel glossario

```
misura/INF.
eccede limiti/UNOP.
```

Questa forma consente a Circe di riconoscere l'uso di "misura" nella determinazione dell'evento, e corrisponde all'idioma

```
IF eccede_limiti(misura) THEN ...
```

in cui non è data l'implementazione di `eccede_misura()`. Un ulteriore livello di raffinamento lungo la stessa linea richiede l'uso del tag `/BINOP` (operatore binario), come nel caso seguente:

```
misura/INF.
limiti/INF.
eccede/BINOP.
```

che corrisponde al costrutto

```
IF eccede(misura,limiti) THEN ...
```

Schema MAS	Esempio	Descrizione
oggetto **è** modo	la porta è aperta	stato di un oggetto
richiedente **interrompe** servente	la periferica invia un'interruzione al sistema	trattamento delle interruzioni
in **riceve** inf **da** out	il sistema riceve il dato dalla periferica	ricezione di messaggi

Tabella 1: Alcuni schemi MAS per l'espressione di eventi.

Con questa dichiarazione, CIRCE può dedurre che sia "misura" che "limiti" vengono letti e usati per determinare se l'evento si verifica o meno. Tuttavia, l'implementazione di "eccede" non è nota: in questo caso particolare, è facile intuire che si tratta in realtà non di un generico operatore binario, ma di un operatore relazionale, che CIRCE supporta tramite il tag `/RELOP`:

```
misura/INF.
limiti/INF.
eccede/RELOP.
```

corrisponde alla forma più concreta

```
        IF misura > limiti THEN ...
```

in cui nulla rimane più da definire. Esistono inoltre molti altri tipi di eventi che possono essere espressi in forma astratta (tag `/EVT`) ma anche in forma più concreta. Alcuni di essi sono riportati nella tabella 1.

La descrizione di eventi può poi essere ulteriormente specializzata aggiungendo altre informazioni, per esempio sulle condizioni temporali. Esempi di requisiti di questo tipo sono

```
Quando la misura eccede i limiti per 3 minuti, allora ...
Se la misura eccede i limiti prima che ..., allora ...
```

Naturalmente, è anche possibile comporre gli eventi con i costrutti di tipo *and* e *or*, eventualmente facendo uso di liste, come nel caso seguente:

```
Se la misura eccede i limiti, e
- il sistema e' in modo monitoraggio, oppure
- il collegamento e' interrotto da piu' di 10 minuti,
allora ...
```

3.3.3 Dati

Anche per le descrizioni dei dati è possibile ricorrere a vari livelli di astrazione. Il riferimento più astratto a un dato è costituito dalla dichiarazione di un termine con tag `/INF`:

```
dati di guasto/INF.
```

Già con questa dichiarazione è possibile esprimere requisiti come

```
Il muSMA invia i dati del guasto all'archivio.
```

Una descrizione più raffinata può essere ottenuta dettagliando la struttura del guasto, che è (probabilmente) un dato composto. Il meccanismo linguistico usato da CIRCE prevede la dichiarazione di *attributi* dell'ente considerato, per esempio

```
guasto/INF: dati di guasto.
origine/ATTR.
istante/ATTR.
gravita'/ATTR: livello.
descrizione/ATTR.
```

sarà così possibile raffinare il requisito dato sopra scrivendo al suo posto

```
Il muSMA invia l'origine, l'istante, il livello e la descrizione
del guasto all'archivio.
```

Una caratteristica interessante degli attributi è che non necessariamente l'oggetto a cui si riferiscono deve esso stesso avere un tag `/INF`. Nell'esempio precedente, abbiamo dichiarato il guasto come un'informazione, con attributi `origine`, `istante`, `gravità` e `descrizione`; questa situazione corrisponde, in termini di linguaggi di programmazione, a un record `guasto` con i campi `origine`...`descrizione`: una soluzione familiare e soddisfacente per molti scopi. Ma avremmo anche potuto dichiarare il guasto come un evento, e considerare `origine` ...`descrizione` come attributi dell'evento:

```
guasto/EVT: si verifica un guasto.
origine/ATTR.
...
descrizione/ATTR.
```

e scrivere il requisito

```
Se si verifica un guasto, il muSMA invia l'origine, l'istante,
il livello e la descrizione del guasto all'archivio.
```

In questo caso, sarà CIRCE stesso a simulare la definizione di un'entità "descrittore di `guasto`", associata al guasto, nei modelli ove ciò sia necessario (per esempio, nei modelli di flusso dati).

3.3.4 Tempo

Anche per l'espressione di istanti e intervalli temporali CIRCE prevede meccanismi di astrazione linguistica. Le dichiarazioni fondamentali sono nel primo caso affidate al tag `/PIT` (point-in-time, un punto preciso sull'asse temporale) e nel secondo caso al tag `/TSPAN` (time span, un segmento sull'asse temporale). Esempi di istanti sono espressioni come "al momento del login", "mezzanotte del 31 dicembre 1999" e simili. Sono invece intervalli temporali espressioni come "tre minuti", "al più 5 millisecondi" o anche "un ragionevole tempo d'attesa". È così possibile scrivere requisiti come

```
Dopo al piu' 5 millisecondi da quando si verifica il guasto ...
```

Schema MAS	Interpretazione
tspan **da quando** evento	inizio(evento)+tspan
tspan **dopo che** evento	fine(evento)+tspan
tspan **dopo** evento	fine(evento)+tspan
tspan **prima di** evento	inizio(evento)-tspan
tspan **prima che** evento	inizio(evento)-tspan

Tabella 2: Alcuni schemi MAS per l'espressione di istanti.

Naturalmente, CIRCE non può penetrare definizioni atomiche di questo tipo per arricchire i modelli generati dai requisiti. A questo scopo, si possono usare molte altre forme per dichiarare informazione di carattere temporale. In primo luogo, in molti casi un evento (`/EVT`) può essere usato in maniera interscambiabile rispetto a un istante. CIRCE non definisce in maniera precisa questa equivalenza, lasciando ai singoli modelli la scelta a questo proposito. La maggior parte dei modelli considerano gli eventi come se si trattasse di eventi atomici (ovvero, di durata nulla); in taluni casi, i modelli assumono che un evento coincida con l'istante finale del suo completamento.

Si può essere più precisi usando uno degli schemi MAS che rappresentano istanti temporali, alcuni dei quali sono riportati in Tabella 2, che "ancorano" un intervallo temporale[3] all'inizio o alla fine di un evento dato.

4 Analisi dell'enunciato

In questa sezione analizzeremo razionalmente l'enunciato del problema, riportando tutte le informazioni che potremo raccogliere in ogni fase sotto forma di requisiti comprensibili a CIRCE.

Prenderemo in considerazione sei aspetti del sistema μ-SMA:

1. funzioni del sistema
2. confine del sistema e interazione con l'esterno
3. struttura interna del sistema e interazioni fra le parti
4. algoritmi e dati strutturati
5. interfaccia utente
6. aspetti temporali

Mentre la scelta di quali aspetti modellare è motivata dalle esigenze delle fasi di progetto e di implementazione (a cui devono essere fornite informazioni sufficienti per completare con successo i rispettivi compiti), la scelta del loro ordinamento è motivata da un criterio di astrazione/concretizzazione. Infatti, gli aspetti che vengono presi in considerazione per primi costituiscono già una versione coerente, benché ampiamente astratta, del sistema, e i modelli divengono più dettagliati man mano che si procede verso gli aspetti più concreti.

[3]Che può anche essere `immediatamente`, o un'espressione equivalente, a indicare un intervallo di lunghezza 0.

Procedendo in questo modo, è possibile arrestare lo sviluppo dei requisiti in qualunque momento e ottenere comunque un documento di requisiti consistente (ancorché non completo). Di maggiore importanza è poi il fatto che il documento di requisiti può essere presentato al committente, e da esso verificato, dopo che ciascuno degli aspetti sopraelencati è stato analizzato completamente, senza attendere il completamento dell'intero documento. Questa modalità offre l'opportunità di rilevare eventuali errori o errate interpretazioni prima di procedere troppo oltre nell'analisi.

4.1 Funzioni del sistema

Il primo livello di raffinamento consiste nel descrivere brevemente le funzionalità del sistema, senza per il momento entrare nel dettaglio delle loro modalità operative. Ciò consente di avere una visione sintetica di ciò che il sistema dovrà fare, ed è anche utile per un'eventuale strutturazione per funzioni del documento di requisiti.

Perché sia possibile definire quali sono le funzioni del sistema, occorrono due tipi di designazione: quella del sistema e quelle delle singole funzionalità.

In CIRCE, come detto, le designazioni corrispondono a elementi del glossario. Il termine che identifica il sistema dovrà avere il tag `/SYS` (significato: "questo è il sistema, o una sua parte, che si intende modellare"), mentre i termini che identificano le funzionalità dovranno avere tag `/FUN` (significato: "questo termine rappresenta una funzione del sistema").

Nel nostro caso di studio, sia l'identità del sistema che le sue funzioni sono già elencate nel primo paragrafo dell'enunciato:

1. **Il sistema di monitoraggio ambientale μ-SMA ha lo scopo di rilevare** con continuità **i parametri** ambientali e metereologici su scala regionale, **di segnalare** tempestivamente l'eventuale **superamento dei limiti** di attenzione, di attivazione o di emergenza per ciascuno **dei parametri** monitorati, **e di costituire un** dettagliato **archivio storico dell'evoluzione dei parametri** ambientali.

Dovremo dunque inserire nel glossario di CIRCE i termini seguenti:

```
# Il sistema
muSMA/SYS: sistema, sistema di monitoraggio ambientale.

# Le sue funzioni
Rileva i parametri/FUN: rileva i parametri ambientali e
                        meteorologici.
Segnala gli allarmi/FUN: segnala il superamento dei limiti.
Mantiene l'archivio storico/FUN: costituisce un archivio storico.
```

Si noti che la prima voce, `muSMA`, costituisce una designazione, mentre le funzioni sono definizioni, e il loro significato dovrà essere dettagliato nel seguito dell'analisi. Con questi termini definiti nel glossario possiamo introdurre il primo requisito, che sarà semplicemente[4]

[4]Usiamo in questo requisito lo schema MAS `soggetto/? funzione/FUN`, nonché quelli per le liste congiuntive di `/FUN`.

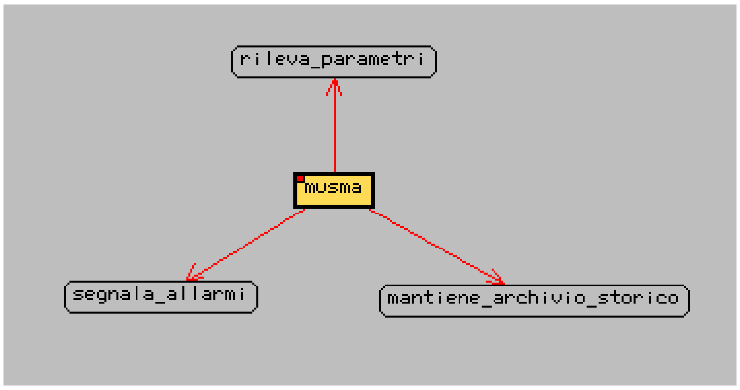


Figura 1: Vista delle funzionalità sul primo requisito.

`Il muSMA rileva i parametri ambientali e meteorologici, segnala il superamento dei limiti e costituisce un archivio storico.`

Ovviamente, questo solo requisito (che viene completamente compreso da Circe) non fornisce informazione sufficiente per la costruzione di modelli "interessanti", ma può comunque essere esaminato in forma grafica tramite la vista "Funzionalità"[5] (vedi figura 1).

Questo tipo di requisito, per quanto semplice, può essere utile quando le funzionalità del sistema sono descritte in punti disparati del documento, piuttosto che raccolte ordinatamente all'inizio come nel caso del nostro enunciato. Allo stesso modo, può essere utile verificare il modello Funzionalità di un documento ottenuto per composizione di specifiche parziali di requisiti, per accertarsi che tutte e sole le funzionalità desiderate del sistema siano state prese in considerazione in almeno uno dei documenti parziali (e che non vi siano sovrapposizioni, nel caso si sia scelto un partizionamento completo del problema).

1. `Il muSMA rileva i parametri ambientali e meteorologici, segnala il superamento dei limiti e costituisce un archivio storico.`

Tabella 3: Requisiti alla fine della prima fase

4.2 Confine del sistema e interazione con l'esterno

Il passo di raffinamento successivo consiste nell'identificare il *confine* del sistema, ovvero nel riconoscere in ciascuna delle interazioni del sistema quali componenti siano parte del sistema da specificare tramite i requisiti e quali non lo siano. Questa distinzione consente di identificare poi in maniera netta le interazioni del sistema con il suo ambiente.

[5] Questa vista è al momento ancora sperimentale, e potrebbe cambiare denominazione.

Il documento di requisiti che si ottiene dopo aver preso in esame questi aspetti costituisce un modello "a scatola nera" (*black box*) del sistema, ovvero un modello in cui nulla viene detto sulla composizione e sul funzionamento interno del sistema, mentre sono descritti i comportamento osservabili dall'esterno.[6]

Analizzeremo adesso singolarmente ogni paragrafo dell'enunciato del problema, marcando in grassetto i frammenti rilevanti per l'aspetto dell'analisi che stiamo trattando.

1. Il sistema di monitoraggio ambientale μ-SMA ha lo scopo di rilevare con continuità i parametri ambientali e metereologici su scala regionale, di segnalare tempestivamente l'eventuale superamento dei limiti di attenzione, di attivazione o di emergenza per ciascuno dei parametri monitorati, e di costituire un dettagliato archivio storico dell'evoluzione dei parametri ambientali.

Nulla ci dice questo paragrafo circa le interazioni del sistema, poiché non vengono indicate modalità per il rilevamento dei parametri ambientali (da chi il sistema riceve questi valori?), nè la destinazione delle segnalazioni di allarmi (a chi segnalare il superamento dei limiti?).

2. **Il sistema si articola su tre livelli: un Centro di Controllo Regionale (CCR), un insieme di Centri di Controllo Locali (CCL) e, per ciascuno di essi, un insieme di Centraline di Rilevamento (CdR).** Il CCR monitorizza l'attività dei CCL e raccoglie i dati storici che questi ultimi gli inviano giornalmente; **i CCL interrogano** ogni cinque minuti **tutte le CdR a essi collegate per raccogliere le relative misure.** I CCL verificano inoltre il superamento dei **limiti**, che **possono essere impostati dal personale di gestione** e che sono tipicamente diversi a seconda della località in cui le CdR sono installate. **Il superamento dei limiti** di attenzione viene segnalato localmente al personale del CCL; il superamento degli altri limiti, ovvero il superamento continuato per oltre quattro ore dei limiti di attenzione, **viene segnalato sia al CCL che al CCR**.

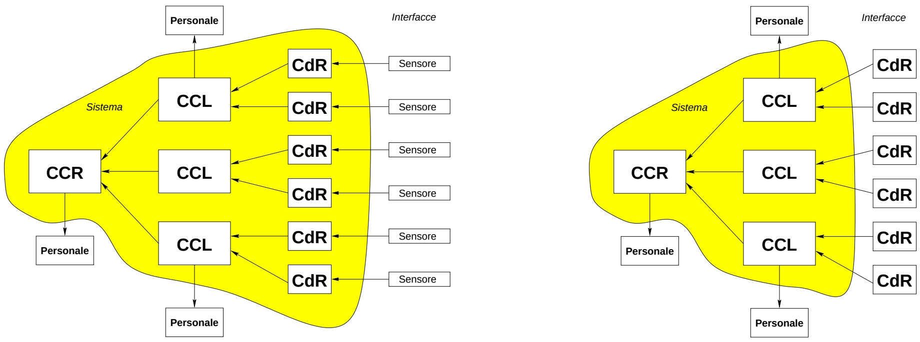
Da questo paragrafo ricaviamo alcune interessanti informazioni circa il confine del sistema. In particolare, appare che CCR, CCL e CdR siano parti del sistema, ma un esame più accurato rivela che CCR e CCL hanno un'interfaccia con l'esterno (con il personale), mentre le CdR sono oggetti "terminali", senza ulteriori interfacce. Se modellassimo semplicemente un sistema composto da CCR, CCL e CdR, avremmo descritto un sistema che *genera* al suo interno una serie di valori (i parametri ambientali) e, dopo alcune elaborazioni, li fornisce al personale di controllo. Questa soluzione è chiaramente inaccettabile e non risponde alle intenzioni del committente.

Abbiamo dunque due alternative per rendere il sistema coerente:

1. considerare le CdR come parti del sistema, e introdurre una nuova classe di enti esterni al sistema (probabilmente dei "sensori") da cui le CdR possono ottenere i parametri ambientali (figura 2(a)), oppure

2. considerare le CdR come enti esterni al sistema, e non indagare sul loro funzionamento interno (figura 2(b)).

[6] Si noti che quella che si ottiene è comunque una descrizione parziale e astratta del comportamento esterno del sistema: per esempio, non abbiamo ancora introdotto gli aspetti temporali.



(a) (b)

Figura 2: Due interpretazioni del confine del sistema.

Noi sceglieremo di adottare la seconda alternativa, che modella una situazione in cui le CdR sono preesistenti (possibilmente, componenti di produzione industriale) e a noi si chiede di realizzare soltanto il software di CCR e CCL. Questa alternativa ha anche il vantaggio rispetto alla prima, che sarebbe altrettanto praticabile, di semplificare il documento di requisiti, cosa che ci consentirà di analizzare taluni aspetti in maggior dettaglio. Coerentemente con la nostra scelta, nel seguito di questa sezione considereremo "CCR" e "CCL" come sinonimi di "muSMA", e "CdR" come elementi di interfaccia esterni al sistema. Annotiamo queste decisioni sotto forma di requisiti:

```
Il muSMA è composto da un CCR e da un numero qualunque di CCL.
Ogni CCL controlla un numero qualunque di CdR.
```

Cogliamo anche l'occasione per introdurre una *definizione* (non designazione) del "personale di gestione" citato nel paragrafo in considerazione:

```
Il personale del CCR e il personale del CCL sono personale.
```

Naturalmente, nel glossario dovremo introdurre i termini usati nei requisiti precedenti, ovvero (aggiornando anche `muSMA`, già presente)

```
muSMA/SYS/IN/OUT: sistema, sistema di monitoraggio ambientale.
CdR/IN/OUT: Centralina di Rilevamento.
CCL/IN/OUT/SYS: Centro di Controllo Locale.
CCR/IN/OUT/SYS: Centro di Controllo Regionale.
Personale/IN/OUT: operatore.
Personale del CCR/IN/OUT: operatore CCR.
Personale del CCL/IN/OUT: operatore CCL.
controllo/REL: controlla.
```

I frammenti successivi pongono minori problemi, e possono essere tradotti direttamente nei requisiti Circe seguenti:

```
Il muSMA interroga tutte le CdR collegate ottenendo le misure.
Il personale imposta i limiti del muSMA.
muSMA segnala il superamento dei limiti al personale.
```

Si noti in questi requisiti come abbiamo sostituito "Il μ-SMA interroga..." all'originale "Il CCL interroga...", come annunciato in precedenza. Perché CIRCE possa comprendere questi requisiti, il glossario dovrà essere espanso aggiungendo alcuni nuovi termini:

```
Limite/INF: limiti.
Superamento limite/INF: superamento limiti, superamento dei
                        limiti.
```

L'ultimo dei tre requisiti indicati sopra richiede qualche spiegazione. L'enunciato infatti reca "Il superamento dei limiti ... viene segnalato sia al CCL che al CCR". In questo requisito, per motivi che appariranno chiari più avanti, abbiamo sostituito "sia al CCL che al CCR" con "al personale", sostituzione che naturalmente deve essere verificata con il committente, ma che appare fondata sia dal punto di vista metodologico (il CCL e il CCR sono parti del sistema, e il sistema non può segnalare qualcosa a una sua parte) che concettuale (il personale in carico della gestione deve essere informato di eventi eccezionali).

Rimandiamo brevemente la discussione a questo riguardo, e prendiamo invece in considerazione il paragrafo successivo:

3. Il μ-SMA deve essere in grado di continuare a operare ragionevolmente in presenza di **guasti alle CdR** (assenza di risposta alle interrogazioni del CCL, o risposta con valori fuori scala), che **devono** comunque **essere segnalati al CCL**. CCL e CCR sono realizzati con tecnologia ridondante e si suppongono affidabili, ma un collegamento CCL-CCR può non essere disponibile per un tempo massimo di 72 ore. In ogni caso, i dati storici devono essere preservati e trasmessi appena possibile; **l'interruzione del collegamento deve essere segnalata** non appena rilevata **al personale del CCR**.

Questo paragrafo asserisce che i guasti delle CdR devono essere segnalati al CCL, ma definisce i guasti come (fra l'altro) "l'assenza di risposta alle interrogazioni del CCL". Appare dunque evidente che è il CCL stesso a rilevare i guasti delle CdR, e dunque non avrebbe senso che il CCL segnali a se stesso l'avvenuto guasto[7]. Interpreteremo allora l'enunciato come "... devono essere segnalati al *personale del* CCL" piuttosto che "... devono essere segnalati al CCL" (un caso insidioso di metonimia). Questa interpretazione, che comunque dovrebbe essere verificata con il committente, ben si allinea al secondo frammento interessante per i nostri scopi, che asserisce esplicitamente che l'interruzione del collegamento va segnalata al *personale* del CCR, e giustifica (anche se a posteriori) l'analoga sostituzione che abbiamo apportato sopra.
Ricaviamo dunque dall'enunciato i due requisiti seguenti:

```
muSMA segnala i guasti al personale del CCL.
muSMA segnala l'interruzione di collegamento al personale del CCR.
```

che introducono nel glossario i termini

```
Guasto/INF: guasti.
Interruzione di collegamento/INF.
```

[7] Questo è un tipico caso di ambiguità causato dall'uso di forme passive come "I guasti devono essere segnalati". L'uso di una forma attiva avrebbe imposto all'estensore dell'enunciato di dichiarare esplicitamente l'agente, e dunque a scrivere "Il CCL deve segnalare i guasti a ...", rendendo chiaro che il destinatario della segnalazione non poteva essere il CCL stesso. È per questo motivo che CIRCE impone che i requisiti siano tutti redatti in forma attiva.

Il quarto paragrafo non fornisce informazioni circa il confine del sistema:

4. Ogni CdR è caratterizzata da una marca, un modello, e un codice identificativo unico. Il CCL conosce per ogni CdR connessa il nome simbolico della grandezza misurata, l'unità di misura, e i limiti di scala per le misure accettabili.

ma quello successivo introduce alcuni elementi interessanti:

5. **Deve essere possibile in ogni momento aggiungere o rimuovere CdR a un CCL**; allo stesso modo, deve essere possibile aggiungere o rimuovere CCL a un CCR. Ogni variazione della configurazione del sistema deve essere riportata nell'archivio storico.

Scegliamo di analizzare in questo requisito soltanto la parte relativa all'aggiunta/rimozione di una CdR, consistentemente con la nostra decisione precedente di considerare le CdR come entità esterne al sistema. In tal senso, l'aggiunta/rimozione di una CdR è un evento significativo osservabile al confine del sistema, mentre l'aggiunta/rimozione di una CCL è un evento che influenza la struttura interna del sistema, ma non osservabile all'esterno. Allo stesso modo, la registrazione delle variazioni di configurazione è un evento interno, non osservabile all'esterno (lo sarebbe invece un ipotetico requisito sull'accesso del personale all'archivio storico).

Traendo ispirazione dal riferimento alle "variazioni di configurazione", e applicando un criterio di astrazione, modelliamo l'aggiunta/rimozione di componenti come variazioni a una "configurazione", che introduciamo nel glossario:

```
Configurazione/INF: configurazione del sistema.
```

da cui il requisito

```
muSMA riceve la configurazione dal personale.
```

Si noti che anche in questo caso abbiamo introdotto autonomamente un elemento importante, ovvero l'origine della comunicazione relativa alla configurazione. L'enunciato non ci assicura infatti che sia il personale (inteso come personale del CCR o del CCL) a impostare le variazioni di configurazione. D'altronde, questa interpretazione sembra la più plausibile, e non c'è nulla nell'enunciato che la renda inconsistente. Adotteremo dunque questa interpretazione, ricordandoci di verificarla con il committente. Per finire, consideriamo l'ultimo paragrafo dell'enunciato:

6. **Il sistema deve offrire al personale del CCL** un'interfaccia utente che visualizzi con continuità **le misure rilevate e gli eventuali allarmi dovuti al superamento delle varie soglie, nonché le indicazioni di malfunzionamenti nel sistema. Al personale del CCR devono essere segnalati soltanto gli allarmi** (con l'indicazione della misura che eccede i livelli) **e i malfunzionamenti**.

che può essere tradotto agevolmente con

```
Il personale del CCL ottiene le misure, il superamento limiti e i
guasti dal muSMA.
Il personale del CCR ottiene il superamento dei limiti e i guasti
dal muSMA.
```

```
1. Il muSMA rileva i parametri ambientali e meteorologici,
   segnala il superamento dei limiti e costituisce un
   archivio storico.

2. Il muSMA è composto da un CCR.

3. Il muSMA è composto da un numero qualunque di CCL.

4. Ogni CCL controlla un numero qualunque di CdR.

5. Il personale del CCR e il personale del CCL sono
   personale.

6. Il muSMA interroga tutte le CdR collegate ottenendo le
   misure.

7. Il personale imposta i limiti del muSMA.

8. Il muSMA segnala il superamento limiti al personale.

9. Il muSMA segnala i guasti al personale del CCL.

10. Il muSMA segnala l'interruzione di collegamento al
    personale del CCR.

11. Il muSMA riceve la configurazione dal personale.

12. Il personale del CCL ottiene le misure, il superamento
    limiti e i guasti dal muSMA.

13. Il personale del CCR ottiene il superamento limiti e i
    guasti dal muSMA.
```

Tabella 4: Requisiti alla fine della seconda fase

con cui introduciamo nel glossario

```
Guasto/INF: guasti, malfunzionamenti.
Interruzione di collegamento/INF.
```

Completata così l'introduzione dei requisiti relativi alle interazioni del sistema con l'esterno, è tempo di osservare i modelli prodotti da Circe e considerare i risultati dei controlli di validazione.

La struttura delle interazioni del sistema può essere osservata agevolmente nel Diagramma di comunicazione (figura 3): abbiamo un flusso di normale operatività fra il μ-SMA e le CdR (consistente nell'invio, su richiesta del μ-SMA, dei parametri ambientali rilevati), e alcuni flussi di controllo fra il μ-SMA e il personale, in termini generici ("personale") o più specializzati ("personale del CCR", "personale del CCL").

Il modello del μ-SMA che abbiamo descritto fino a questo punto è di necessità molto astratto; non abbiamo ancora analizzato gli aspetti strutturali e le funzio-

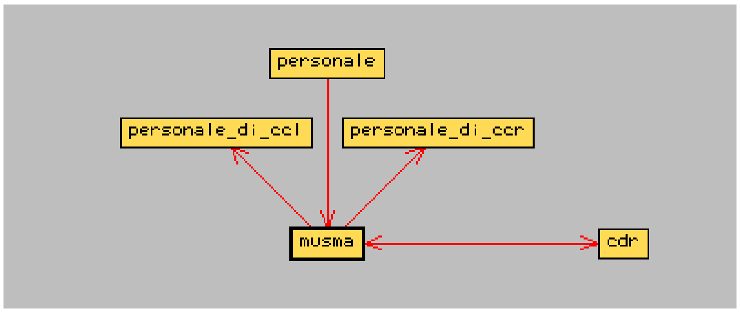


Figura 3: Il diagramma di comunicazione dopo il secondo raffinamento.

nalità interne del sistema, nè abbiamo dato dettagli di sorta sul comportamento dinamico del μ-SMA. Questo eccessivo livello di astrazione induce la costruzione di modelli incompleti, che vengono segnalati dalla vista di validazione Pandora. Ecco infatti gli avvisi emessi da Pandora:

Informazioni non definite

I valori di **superamento_limite**, **interruzione_di_collegamento** e **guasto** non vengono mai modificati dal sistema.

Una variabile che non viene mai modificata non è una variabile. Se si tratta di una costante, dovrebbe essere dichiarata con il tag /BLTIN nel glossario. Altrimenti, devi aggiungere qualche requisito che dica in che modo viene ottenuto il suo valore.

Viste rilevanti: Flusso dati HL, Flusso dati LL

Informazioni non utilizzate

I valori di **limite** e **configurazione** non vengono mai utilizzati dal sistema.

Una variabile che non viene mai usata come parametro in una elaborazione, non viene mai inviata all'esterno e non viene mai usata per prendere una decisione è probabilmente del tutto inutile. Se è così, puoi rimuovere questo termine dal glossario, e cancellare i requisiti ad esso relativi. Se, come è più probabile, la variabile rappresenta informazione utile, cerca di modellare più accuratamente il suo ciclo di vita, e dettaglia nei requisiti come, quando e perché viene usata.

Viste rilevanti: Flusso dati HL, Flusso dati LL

L'interpretazione di questi messaggi di avvertimento è immediata. Il fatto che non siano mai definiti i valori di `superamento_limite`, `interruzione_di_collegamento` e `guasto` è dovuto alla mancata individuazione nei requisiti delle circostanze in cui si ha un superamento dei limiti, e del modo in cui vengono rilevati le interruzioni di collegamento e i guasti da parte del μ-SMA. Analogamente, i requisiti non indicano come il μ-SMA debba usare i valori di `limite` e `configurazione`. L'eccessiva astrazione della nostra modellazione fino a questo punto è ben visibile nel diagramma di flusso dati (Fig. 4). Chiaramente, dovremmo specificare, per esempio, che il μ-SMA confronta le misure e i limiti

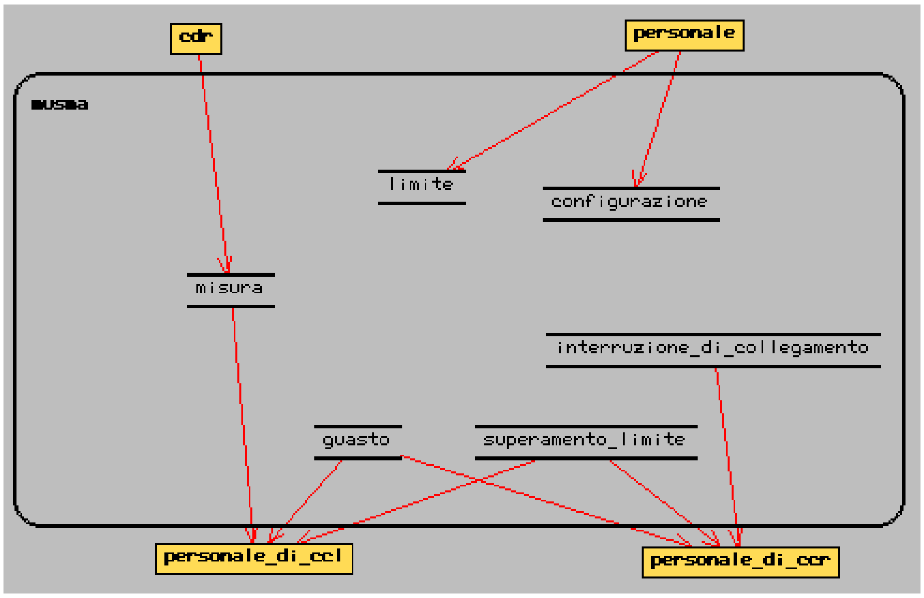


Figura 4: Il diagramma di flusso dopo il secondo raffinamento.

fissati per esse per decidere se si ha un superamento dei limiti, ma a questo arriveremo dopo aver descritto con maggiore precisione la struttura interna del sistema.

I controlli di validazione previsti da CIRCE sono di necessità incompleti: l'assenza di una segnalazione di errore esplicita non deve essere interpretata come la prova positiva dell'assenza di errori. Per esempio, i requisiti

```
8. Il muSMA segnala il superamento limiti al personale.
9. Il muSMA segnala i guasti al personale del CCL.
```

sono in realtà ridondanti rispetto ai più completi

```
 5. Il personale del CCR e il personale del CCL sono personale.
12. Il personale del CCL ottiene le misure, il superamento limiti
    e i guasti dal muSMA.
13. Il personale del CCR ottiene il superamento limiti e i guasti
    dal muSMA.
```

Infatti, il requisito 12 prevede che il superamento limiti sia segnalato al personale del CCL, mentre il 13 richiede che sia segnalato al personale del CCR. Come risulta dal requisito 5, il personale è composto proprio da personale del CCL e personale del CCR, quindi il requisito 8 è ridondante rispetto all'informazione combinata dei requisiti 5, 12 e 13. Questo tipo di deduzione è troppo complesso per CIRCE [8], e dunque la ridondanza "sfugge" ai controlli dello strumento.

[8]Non si tratta, ovviamente, di una limitazione concettuale, ma di una limitazione della versione attuale del sistema. Versioni future potrebbero certamente essere in grado di rilevare ridondanze di questo tipo. Rimane comunque valido il principio che ogni validazione automatica effettuata sui requisiti è soltanto una verifica che *un certo insieme di proprietà* siano

Il caso del requisito 9 (che si applica però anche al requisito 8) è leggermente diverso. Il requisito 12, infatti, specifica anch'esso che i guasti devono essere segnalati al personale del CCL, ma lo fa ponendo le segnalazioni di guasto all'interno di una lista comprendente anche le misure e il superamento limiti. Circe non può decidere autonomamente se questo raggruppamento o il particolare ordinamento della lista sia influente o meno, e quindi non può dichiarare la ridondanza del requisito 9 rispetto al 12. Per esempio, l'intenzione dell'estensore dei requisiti potrebbe essere quella di specificare tramite il requisito 12 la trasmissione di un unico pacchetto di dati, nell'ordine dato (è un caso estremamente comune in applicazioni di comunicazione, per esempio nella specifica di protocolli di rete), che è cosa ben diversa dall'invio di un pacchetto dati contenente la sola segnalazione di guasti.

In casi del genere, è necessario fare ricorso alla professionalità dell'analista (e a un po' di buon senso) per dare il giusto valore alle segnalazioni — e all'*assenza* di segnalazioni — da parte di Circe.

4.3 Struttura del sistema e interazioni fra le parti

In questo passo "esploderemo" il μ-SMA nei suoi componenti, e dettaglieremo le interazioni fra i componenti. In molte applicazioni, questo passo induce alcune scelte che potremmo definire di progettazione architetturale, ma nel nostro caso di studio la necessità di un partizionamento fisico (CCR, CCL e CdR sono fisicamente separati, e installati in siti diversi nell'ambito di una regione) induce naturalmente il partizionamento più ovvio, già indicato nell'enunciato.

Questo ci porta a raffinare un certo numero di requisiti già dati. In particolare, possiamo sostituire le occorrenze di μ-SMA con l'esatto componente coinvolto (CCR o CCL), e le occorrenze di personale con la classe di personale corretta (personale del CCR o personale del CCL). I raffinamenti relativi sono mostrati in tabella 5 (le relative variazioni al glossario sono facilmente ricavabili dal testo dei requisiti).

Come già abbiamo fatto per i passi precedenti, prenderemo ora in esame i paragrafi dell'enunciato rilevanti per i nostri scopi in questa fase, evidenziando di volta in volta i frammenti interessanti. In particolare, il paragrafo 2 reca:

2. Il sistema si articola su tre livelli: un Centro di Controllo Regionale (CCR), un insieme di Centri di Controllo Locali (CCL) e, per ciascuno di essi, un insieme di Centraline di Rilevamento (CdR). **Il CCR monitorizza l'attività dei CCL e raccoglie i dati storici che questi ultimi gli inviano** giornalmente; i CCL interrogano ogni cinque minuti tutte le CdR a essi collegate per raccogliere le relative misure. **I CCL verificano** inoltre **il superamento dei limiti**, che possono essere impostati dal personale di gestione e che sono tipicamente diversi a seconda della località in cui le CdR sono installate. Il superamento dei limiti di attenzione viene segnalato localmente al personale del CCL; il superamento degli altri limiti, ovvero il superamento continuato per oltre quattro ore dei limiti di attenzione, viene segnalato sia al CCL che al CCR.

L'informazione che il CCR monitorizza l'attività dei CCL rientra nell'analisi delle funzionalità del CCR, che possiamo ora svolgere per sottosistemi —

rispettate. Dato un simile insieme di proprietà, è sempre possibile immaginare un'applicazione per cui una proprietà non inclusa nell'insieme sia desiderabile, e costruire un insieme di requisiti che vìoli proprio quella proprietà.

Requisito originale	**Raffinamento**
6. Il muSMA interroga tutte le CdR collegate ottenendo le misure.	Un CCL interroga tutte le CdR collegate ottenendo le misure.
7. Il personale imposta i limiti del muSMA.	Il personale di un CCL imposta i limiti delle CdR del CCL.
8. Il muSMA segnala il superamento limiti al personale.	*rimosso, ridondante*
9. Il muSMA segnala i guasti al personale del CCL	*rimosso, ridondante*
10. Il muSMA segnala l'interruzione di collegamento al personale del CCR.	Il CCL segnala l'interruzione di collegamento CCL-CdR al personale del CCL. Il CCR segnala l'interruzione di collegamento CCR-CCL al personale del CCR.
11. Il muSMA riceve la configurazione dal personale.	Il CCL riceve la variazione di confiugrazione delle CdR dal personale del CCL. Il CCR riceve la variazione di configurazione dei CCL dal personale del CCR.
12. Il personale del CCL ottiene le misure, il superamento limiti e i guasti dal muSMA.	Il personale del CCL ottiene le misure, il superamento limiti e i guasti dal CCL.
13. Il personale del CCR ottiene il superamento limiti e i guasti dal muSMA.	Il personale del CCR ottiene il superamento limiti e i guasti dal CCR.

Tabella 5: Raffinamento dei requisiti per la terza fase.

analogamente a quanto abbiamo fatto per l'intero sistema nella sezione 4.1. Similmente, il fatto che i CCL verifichino il superamento dei limiti è (a questo stadio) una funzionalità non analizzata[9]. Per entrambi i casi possiamo dunque nuovamente usare una dichiarazione di funzionalità nel glossario, ovvero

```
monitorizza attività dei CCL/FUN.
verifica superamento limiti/FUN: verificano superamento di limiti.
```

L'interazione costituita dalla raccolta dei dati storici può invece essere immediatamente modellata in maggiore dettaglio come una comunicazione[10]. Otteniamo così i requisiti seguenti:

```
Il CCR monitorizza l'attività dei CCL.
I CCL verificano il superamento dei limiti.
I CCL inviano i dati storici al CCR.
```

in cui i dati storici compaiono nel glossario come

```
dati storici/INF.
```

In realtà, il primo di questi requisiti è ridondante, in quanto le funzionalità di monitoraggio (ricezione di misure, allarmi e variazioni alla configurazione, trattamento dei guasti) sono già descritte esplicitamente in altri requisiti. Il paragrafo 3 aggiunge qualche dettaglio sul collegamento fra CCL e CCR:

3. Il μ-SMA deve essere in grado di continuare a operare ragionevolmente in presenza di guasti alle CdR (assenza di risposta alle interrogazioni del CCL, o risposta con valori fuori scala), che devono comunque essere segnalati al CCL. CCL e CCR sono realizzati con tecnologia ridondante e si suppongono affidabili, ma **un collegamento CCL-CCR può non essere disponibile** per un tempo massimo di 72 ore. In ogni caso, i dati storici devono essere preservati e trasmessi appena possibile; l'interruzione del collegamento deve essere segnalata non appena rilevata al personale del CCR.

Potremmo modellare questo dettaglio in diversi modi, per esempio come un'osservazione sullo stato dell'entità "collegamento", ma la soluzione più semplice è probabilmente quella di definire un dato che rappresenti lo stato di collegamento e di applicarvi un operatore unario:

```
Un collegamento CCL-CCR puo' non essere disponibile.
```

a cui corrispondono, nel glossario, le voci seguenti:

```
collegamento CCL-CCR/INF.
non e' disponibile/UNOP: puo' non essere disponibile.
```

Proseguiamo la nostra analisi con il paragrafo 5 dell'enunciato del problema:

5. Deve essere possibile in ogni momento aggiungere o rimuovere CdR a un CCL; allo stesso modo, **deve essere possibile aggiungere o rimuovere CCL a un CCR**. **Ogni variazione della configurazione del sistema deve essere riportata nell'archivio storico**.

[9] Raffineremo queste funzionalità al passo successivo, quando dettaglieremo gli algoritmi e i dati strutturati usati dal μ-SMA.

[10] Naturalmente, sarebbe anche stato possibile definire la raccolta di dati storici come una funzionalità e raffinarla in un passo successivo; optiamo per una modellazione diretta al fine di ottenere una maggiore speditezza.

in cui le parti evidenziate corrispondono ai requisiti

```
Il CCR riceve la variazione di configurazione dei CCL dal
personale del CCR.
I CCL inviano le variazioni di configurazione delle CdR
all'archivio storico.
Il CCR invia le variazioni di configurazione dei CCL
all'archivio storico.
```

(si noti che il primo di questi requisiti è già stato introdotto per raffinamento dei requisiti ottenuti al passo precedente). Anche in questo caso, esistono diverse alternative per modellare l'archivio storico. Noi introduciamo la designazione

```
archivio storico/IN.
```

che dichiara l'archivio storico come un componente *attivo* capace di ricevere dati dall'esterno: non quindi un semplice deposito di dati, ma un componente software che potremmo identificare con un gestore di basi di dati (DBMS). Non attribuiamo all'archivio storico il tag `/SYS`, in quanto supponiamo che la progettazione di questo componente non faccia parte della nostra attività: in altri termini, modelliamo l'archivio come un componente prodotto da terze parti, di cui non siamo interessati a descrivere i dettagli interni. È anche interessante osservare che non abbiamo assegnato all'archivio il tag `/OUT`: assumiamo infatti che le operazioni di interrogazione dell'archivio siano esterne al μ-SMA in quanto sistema di monitoraggio, e vengano svolte tramite altri prodotti complementari.

Avremmo potuto anche dichiarare l'archivio storico come un deposito di informazioni, ovvero

```
archivio storico/INF.
```

e trattare l'aggiornamento dell'archivio come un'operazione su questi dati:

```
I CCL aggiungono le variazioni di configurazione delle CdR
all'archivio storico.
Il CCR aggiunge le variazioni di configurazione dei CCL
all'archivio storico.
```

tuttavia in questo caso l'archivio storico sarebbe stato modellato da un dato condiviso fra numerosi sistemi geograficamente distribuiti, una situazione che ci avrebbe costretti a dichiarare esplicitamente le politiche di condivisione e, in particolare, a introdurre un meccanismo per l'interrogazione dell'archivio (che altrimenti sarebbe stato un dato "morto", senza accessi in lettura).

Alla fine di questa fase, il μ-SMA è descritto dai requisiti in tabella 6. Circe costruisce in base a questi requisiti il diagramma di comunicazione in figura 5; si confronti questo diagramma con la nostra scelta originale in figura 2(b).

La figura 6 mostra invece il diagramma di flusso dati (ad alto livello) per i nostri requisiti. Si osservano adesso chiaramente due flussi distinti di informazioni: sulla sinistra, il flusso principale di monitoraggio, tramite cui le misure ottenute dalle CdR vengono mostrate al personale di gestione; sulla destra, il flusso secondario di controllo, tramite cui il personale imposta la configurazione del sistema e i limiti di accettabilità delle varie misure[11]. Rimangono naturalmente

[11] Si ricordi a questo proposito quanto detto a pagina 7: il deposito di dati "CdR" nel diagramma rappresenta il *descrittore* di una CdR, oggetto questo che ha fra i suoi attributi i limiti di accettabilità.

1. Il muSMA rileva i parametri ambientali e meteorologici, segnala il superamento dei limiti e costituisce un archivio storico. 2. Il muSMA è composto da un CCR. 3. Il muSMA è composto da un numero qualunque di CCL. 4. Ogni CCL controlla un numero qualunque di CdR. 5. Il personale del CCR e il personale del CCL sono personale. 6. Un CCL interroga tutte le CdR collegate ottenendo le misure. 7. Il personale di un CCL imposta i limiti delle CdR del CCL. 8. Un CCL segnala l'interruzione di collegamento CCL-CdR al personale del CCL. 9. Il CCR segnala l'interruzione di collegamento CCR-CCL al personale del CCR. 10. Un CCL riceve la variazione di configurazione CdR dal personale del CCL. 11. Il CCR riceve la variazione di configurazione CCL dal personale del CCR. 12. Il personale del CCL ottiene le misure, il superamento limiti, e i guasti dal CCL. 13. Il personale del CCR ottiene il superamento limiti e i guasti dal CCR. 14. I CCL inviano i dati storici al CCR. 15. I CCL verificano il superamento dei limiti. 16. Un collegamento CCL-CCR può non essere disponibile. 17. I CCL inviano le variazioni di configurazione CdR all'archivio storico. 18. Il CCR invia le variazioni di configurazione CCL all'archivio storico.

Tabella 6: Requisiti alla fine della terza fase

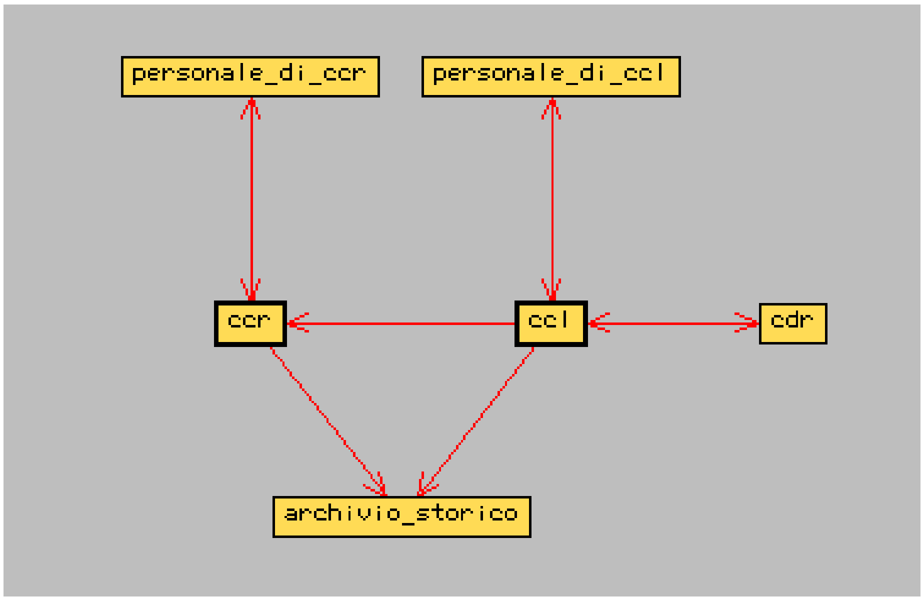


Figura 5: Il diagramma di comunicazione dopo il terzo raffinamento.

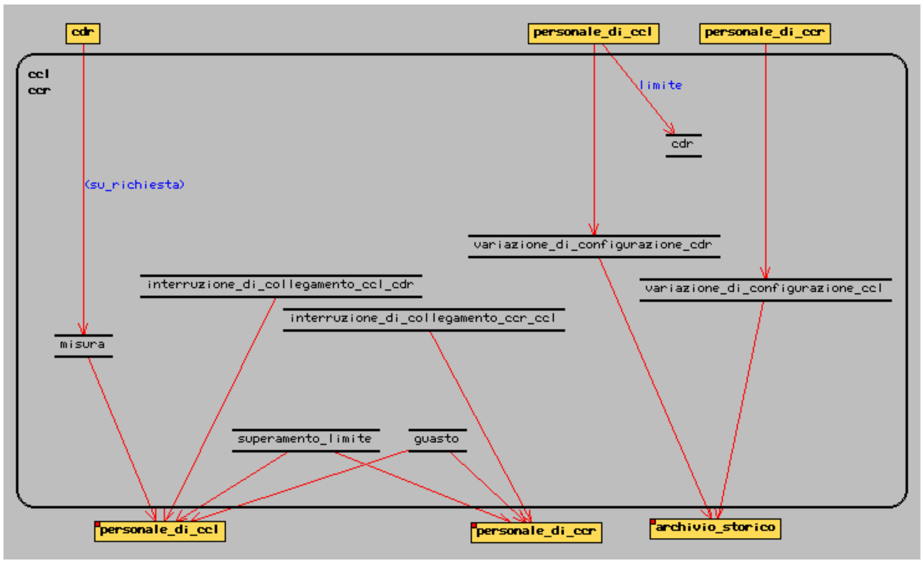


Figura 6: Il diagramma di flusso dati dopo il terzo raffinamento.

da definire molti altri dettagli, come peraltro segnalato da Pandora; in particolare, non abbiamo descritto come vengono rilevati i guasti e le interruzioni di collegamento, come viene valutato il "superamento limite" e che relazione ci sia fra questa condizione e i limiti di una CdR che il sistema riceve dal personale delle CCL. Questi dettagli saranno oggetto del nostro prossimo raffinamento.

4.4 Algoritmi e strutture dati

Con questo raffinamento ci proponiamo di descrivere con maggiore accuratezza la struttura dei dati che il nostro sistema tratta e le elaborazioni che esso compie su di essi. Per quanto riguarda i dati, ricordiamo che fino a questo punto il glossario per il μ-SMA contiene i seguenti termini con tag `/INF` (informazioni) e `/ATTR` (attributi):

```
misure/INF.
limiti/ATTR.
interruzione di collegamento CCL-CdR/INF.
interruzione di collegamento CCR-CCL/INF.
variazione di configurazione CdR/INF.
variazione di configurazione CCL/INF.
superamento limiti/INF.
guasti/INF.
dati storici/INF.
collegamento CCL-CCR/INF.
```

Procediamo adesso con il nostro consueto metodo, consistente nell'identificare testualmente sull'enunciato del problema i passi rilevanti per questa fase. Il primo paragrafo ci offre subito qualche dettaglio sulla natura dei limiti:

1. Il sistema di monitoraggio ambientale μ-SMA ha lo scopo di rilevare con continuità i parametri ambientali e metereologici su scala regionale, di segnalare tempestivamente l'eventuale superamento dei **limiti di attenzione, di attivazione o di emergenza** per ciascuno dei parametri monitorati, e di costituire un dettagliato archivio storico dell'evoluzione dei parametri ambientali.

a cui corrisponde il nuovo requisito

```
Il limite di attenzione, il limite di attivazione e il limite
di emergenza sono limiti.
```

e, naturalmente, l'introduzione di `limite di attenzione/INF`, `limite di attivazione/INF` e `limite di emergenza/INF` nel glossario. Il diverso trattamento a cui i diversi limiti fanno capo è descritto nel paragrafo

2. Il sistema si articola su tre livelli: un Centro di Controllo Regionale (CCR), un insieme di Centri di Controllo Locali (CCL) e, per ciascuno di essi, un insieme di Centraline di Rilevamento (CdR). Il CCR monitorizza l'attività dei CCL e raccoglie i dati storici che questi ultimi gli inviano giornalmente; i CCL interrogano ogni cinque minuti tutte le CdR a essi collegate per raccogliere le relative misure. **I CCL verificano inoltre il superamento dei limiti**, che possono essere impostati dal personale di gestione e che sono tipicamente diversi a seconda della località in cui le CdR sono installate. **Il superamento dei limiti di attenzione viene segnalato localmente al personale del CCL; il superamento degli altri limiti, ovvero il superamento** continuato per oltre

quattro ore **dei limiti di attenzione, viene segnalato sia al CCL che al CCR**.

Ciò ci induce a raffinare il precedente requisito 15 (che, ricordiamo, si affidava a una dichiarazione astratta di funzionalità attraverso il tag `/FUN`) in questo modo[12]:

```
Il CCL calcola il superamento limiti in base alla misura e ai
limiti della CdR.
```

Inoltre, dobbiamo introdurre il collegamento mancante fra il CCL (che rileva il superamento dei limiti) e il CCR (che, in base al requisito 13, deve essere in grado di segnalare il superamento limiti ai suoi utenti). Non tutti i casi di superamento limiti vengono segnalati al CCR, ma solo quelli più gravi, come descritto nell'enunciato. Poiché questa descrizione fa riferimento ad aspetti temporali, che non abbiamo ancora trattato in maniera razionale, ci manteniamo astratti, introducendo nel glossario un operatore unario

```
rilevante per il CCR/UNOP: e' rilevante per il CCR.
```

che ci permette di scrivere il requisito

```
Se il superamento limiti e' rilevante per il CCR, il CCL invia
il superamento limiti al CCR.
```

Il paragrafo successivo ci dà l'opportunità di introdurre una definizione esplicita dei guasti (si veda pagina 3):

3. Il μ-SMA deve essere in grado di continuare a operare ragionevolmente in presenza di **guasti alle CdR (assenza di risposta alle interrogazioni del CCL, o risposta con valori fuori scala)**, che devono comunque essere segnalati al CCL. CCL e CCR sono realizzati con tecnologia ridondante e si suppongono affidabili, ma un collegamento CCL-CCR può non essere disponibile per un tempo massimo di 72 ore. In ogni caso, i dati storici devono essere preservati e trasmessi appena possibile; l'interruzione del collegamento deve essere segnalata non appena rilevata al personale del CCR.

L'assenza di risposta alle interrogazioni del CCL è un tipico sintomo di guasto alla linea di comunicazione, che modelleremo con un attributo `stato` del collegamento CCL-CdR; la risposta con valori fuori scala viene invece determinata confrontando la misura letta con i limiti di scala della CdR. Otteniamo dunque il requisito

```
Il CCL rileva i guasti in base alla misura, ai limiti di scala
della CdR e allo stato del collegamento CCL-CdR.
```

Inoltre, i guasti rilevati devono essere segnalati al CCR, affinché questo possa informare il proprio personale come richiesto dal requisito 13:

```
Il CCL invia i guasti al CCR.
```

[12] All'introduzione di questo requisito corrisponde un aggiornamento della designazione di `CCL` nel glossario, a cui va aggiunto il tag `/ELAB` che indica "oggetto capace di compiere elaborazioni". Lo stesso accadrà per il `CCR` e, per mantenere la validità della gerarchia di classificazione, per `muSMA`.

Il paragrafo successivo dell'enunciato, da cui finora non abbiamo attinto alcunché, è interamente dedicato alla descrizione di dati strutturati:

4. Ogni CdR è caratterizzata da una marca, un modello, e un codice identificativo unico. Il CCL conosce per ogni CdR connessa il nome simbolico della grandezza misurata, l'unità di misura, e i limiti di scala per le misure accettabili.

La prima parte può essere tradotta direttamente con il requisito

```
Ogni CdR ha attributi una marca, un modello e un codice
identificativo unico.
```

in cui gli attributi sono dichiarati nel glossario come

```
marca/ATTR.
modello/ATTR.
codice/ATTR: codice identificativo unico.
```

La seconda parte non ci dice come fa il CCL a "conoscere" gli altri dati relativi alla CdR. Possiamo assumere che questi dati siano immessi dal personale, riservandoci di verificare con il committente la correttezza di questa assunzione:

```
Il CCL riceve dal personale del CCL il nome simbolico della
grandezza misurata, l'unita' di misura della grandezza misurata
e i limiti di scala della CdR.
```

a cui corrispondono nel glossario le dichiarazioni

```
nome simbolico/ATTR: nome simbolico di grandezza misurata.
unita' di misura/ATTR: unita' di misura della grandezza misurata.
limiti di scala/ATTR.
```

Abbiamo così esaurito l'analisi dell'enunciato (non ci sono altri frammenti rilevanti per questa fase), ma non l'opera di raffinamento. Dobbiamo infatti ancora dettagliare il trattamento delle variazioni di configurazione (finora sappiamo soltanto che vengono registrate nell'archivio storico, ma non come vengano usate) e la composizione dei dati storici. Per quanto riguarda le configurazioni, possiamo semplicemente scrivere

```
Il CCL modifica la configurazione in base alla variazione di
configurazione delle CdR.
Il CCR modifica la configurazione in base alla variazione di
configurazione dei CCL.
```

mentre l'archivio locale dei dati storici verrà mantenuto con la funzionalità descritta nel requisito

```
Il CCL aggiunge le misure ai dati storici.
```

(si noti che in questo requisito usiamo la voce di glossario `dati storici/INF`, modellando questo archivio come un deposito di informazioni anziché come un'entità attiva — vedi pagina 21).

Alla conclusione di questa fase, i requisiti completati appaiono come riportato nelle tabelle 7 e 8. Il documento di requisiti non è ancora completamente consistente: Pandora segnala infatti, fra l'altro, il mancato utilizzo delle configurazioni (che noi sappiamo essere usate dal CCL nel ciclo di interrogazione delle

1. Il muSMA rileva i parametri ambientali e meteorologici, segnala il superamento dei limiti e costituisce un archivio storico.

2. Il muSMA è composto da un CCR.

3. Il muSMA è composto da un numero qualunque di CCL.

4. Ogni CCL controlla un numero qualunque di CdR.

5. Il personale del CCR e il personale del CCL sono personale.

6. Un CCL interroga tutte le CdR collegate ottenendo le misure.

7. Il personale di un CCL imposta i limiti delle CdR del CCL.

8. Un CCL segnala l'interruzione di collegamento CCL-CdR al personale del CCL.

9. Il CCR segnala l'interruzione di collegamento CCR-CCL al personale del CCR.

10. Un CCL riceve la variazione di configurazione CdR dal personale del CCL.

11. Il CCR riceve la variazione di configurazione CCL dal personale del CCR.

12. Il personale del CCL ottiene le misure, il superamento limiti, e i guasti dal CCL.

13. Il CCL calcola il superamento limiti in base alla misura e ai limiti della CdR.

14. Il CCL rileva i guasti in base alla misura, ai limiti di scala della CdR e allo stato del collegamento CCL-CdR.

15. Il CCL invia i guasti al CCR.

16. Se il superamento limiti è rilevante per il CCR, il CCL invia il superamento limiti al CCR.

Tabella 7: Requisiti alla fine della quarta fase (segue).

```
17. Il personale del CCR ottiene il superamento limiti e i
    guasti dal CCR.

18. I CCL inviano i dati storici al CCR.

19. Il CCL aggiunge le misure ai dati storici.

20. Un collegamento CCL-CCR può non essere disponibile.

21. I CCL inviano le variazioni di configurazione CdR
    all'archivio storico.

22. Il CCR invia le variazioni di configurazione CCL
    all'archivio storico.

23. Il CCL modifica la configurazione in base alla variazione
    di configurazione delle CdR.

24. Il CCR modifica la configurazione in base alla variazione
    di configurazione dei CCL.

25. Il limite di attenzione, il limite di attivazione e il
    limite di emergenza sono limiti.

26. Ogni CdR ha attributi una marca, un modello, e un codice
    identificativo unico.

27. Il CCL riceve dal personale del CCL il nome simbolico
    della grandezza misurata, l'unità di misura della
    grandezza misurata e i limiti di scala della CdR.
```

Tabella 8: (segue) Requisiti alla fine della quarta fase.

CdR, e dal CCR nel ciclo di interrogazione dei CCL), la mancata definizione dei "collegamenti" e delle "interruzioni del collegamento", e il mancato uso del nome simbolico e del nome dell'unità di misura per le CdR. Per i due ultimi casi, possiamo immaginare che queste informazioni servano esclusivamente a decorare la visualizzazione dell'interfaccia utente, e non siano oggetto di elaborazioni. Per i casi restanti, possiamo per il momento considerare sottointeso il loro uso, e procedere alle fasi di raffinamento successive. Il diagramma di flusso dati del nostro sistema a questo punto è visibile in figura 7. Si tratta questa volta di un diagramma di flusso a basso livello, e in cui sono state nascoste le etichette sugli archi per diminuire l'affollamento grafico. È comunque ben visibile, nella parte destra, il flusso di dati del CCR, e su quella sinistra il flusso del generico CCL.

4.5 Interfaccia utente

L'enunciato del problema è (opportunamente) molto avaro di dettagli relativi all'interfaccia utente. Gli unici riferimenti a questo aspetto sono nel paragrafo 6:

6. Il sistema deve offrire al personale del CCL un'interfaccia utente che visualizzi

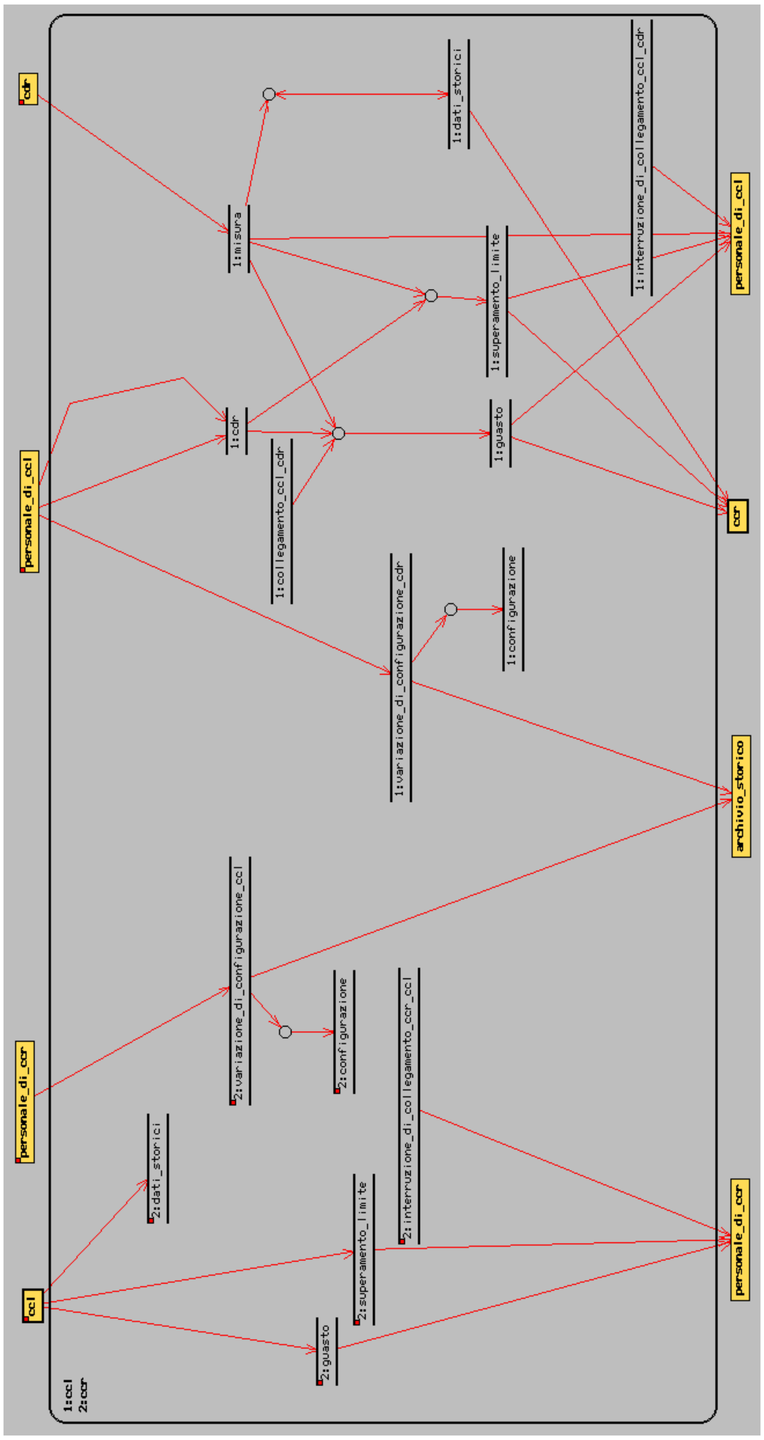


Figura 7: Il diagramma di flusso dati dopo il quarto raffinamento.

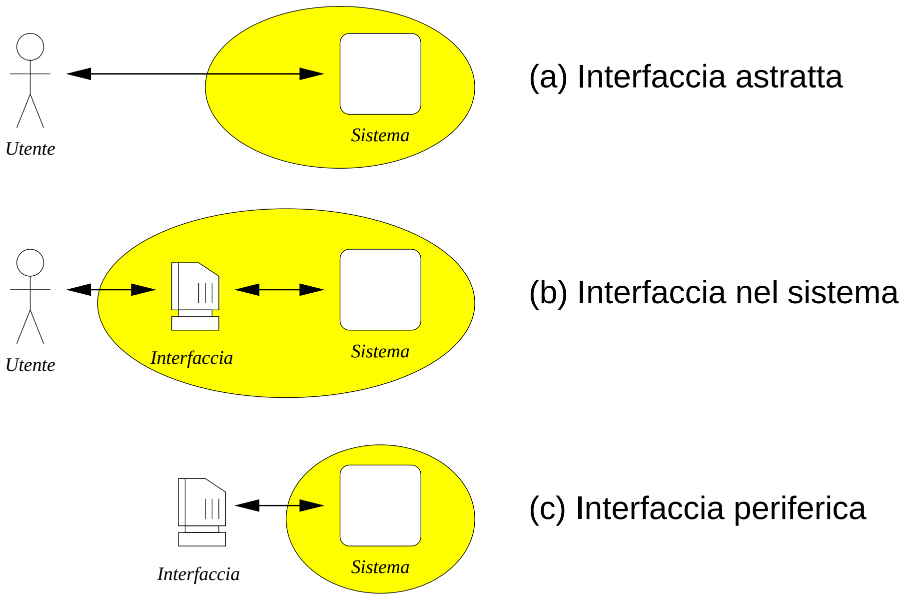


Figura 8: Tre alternative per la descrizione dell'interfaccia utente.

> con continuità le misure rilevate e gli eventuali allarmi dovuti al superamento delle varie soglie, nonché le indicazioni di malfunzionamenti nel sistema. Al personale del CCR devono essere segnalati soltanto gli allarmi (con l'indicazione della misura che eccede i livelli) e i malfunzionamenti.

Sebbene Circe disponga di strumenti linguistici e tecnologici per la modellazione dell'interfaccia utente (inclusa la generazione di codice Java e di prototipi eseguibili), le informazioni disponibili sono troppo ridotte perché i requisiti per l'interfaccia utente possano essere ottenuti in maniera razionale.

Per questo motivo, non tratteremo in questo documento della progettazione di un'interfaccia utente per il μ-SMA, rimandando il lettore a [3] per i dettagli tecnici e a [1] per una serie di esempi già implementati.

Esamineremo però una delle principali scelte di modellazione che hanno impatto sui requisiti per l'interfaccia utente, ovvero dove porre il confine fra sistema e utente. Analogamento a quanto discusso per i sensori nella sezione 4.2, abbiamo un certo numero di alternative, che corrispondono a dichiarazioni di glossario diverse. Il caso più semplice è quello illustrato in figura 8(a): il sistema dialoga direttamente con i suoi utenti umani; l'interfaccia utente non è descritta ed è completamente astratta. Questo è il caso dei nostri requisiti 7–13. Questo approccio ha il pregio della concisione e delle chiarezza, ma è poco dettagliato e non fornisce alcuna indicazione al progettista dell'interfaccia utente su quali siano i desideri del committente a questo riguardo.

Lo schema di figura 8(b) è molto più dettagliato: in questo caso, l'interfaccia utente è vista come un componente del sistema, che a sua volta dialoga con l'utente. Vengono descritte tutte le interazioni fra il nucleo del sistema e l'interfaccia utente (per esempio: "Il sistema invia all'interfaccia utente le misure da visualizzare"), ma anche le interazioni fra quest'ultima e l'utente (per esempio: "Quando l'utente preme il pulsante 'aggiorna', l'interfaccia utente richiede le misure al sistema") e le caratteristiche grafiche ed elaborative dell'interfaccia utente stessa. Inutile dire che una descrizione così dettagliata è generalmente *molto* lunga, e spesso tende ad essere sovraspecificata, esprimendo nei requisiti vincoli che non hanno corrispondenza nelle intenzioni del committente.

Una soluzione intermedia consiste nel considerare l'interfaccia utente come una periferica esterna al sistema (figura 8(c)). In questo caso, i requisiti descrivono solo le interazioni fra il sistema e l'interfaccia utente (per esempio: "Il sistema invia le misure all'interfaccia utente", e "Il sistema riceve dall'interfaccia utente il comando di aggiornamento"), e tralasciano — affidandola a una fase di progettazione successiva, e possibilmente alla professionalità di uno specialista in interfaccia uomo-macchina — la descrizione visuale e dinamica dell'interazione fra l'interfaccia utente e l'utente umano.

Come già annunciato, opteremo in questo esercizio per la soluzione di figura 8(a), che non richiede l'aggiunta di ulteriori dettagli ai requisiti che già abbiamo dato. Passiamo dunque senza indugio al prossimo e ultimo passo di raffinamento.

4.6 Aspetti temporali

Come ultimo passo nel nostro processo di costruzione razionale dei requisiti per il μ-SMA considereremo adesso gli aspetti temporali citati nell'enunciato del problema. In tutti i casi, le informazioni temporali costituiscono un raffinamento semplice di un requisito già esistente, e non sarà necessario introdurre nuovi requisiti.

Sin dalla prima specifica ad altissimo livello (sezione 4.1) avevamo omesso di considerare alcuni frammenti del primo paragrafo:

1. Il sistema di monitoraggio ambientale μ-SMA ha lo scopo di rilevare **con continuità** i parametri ambientali e metereologici su scala regionale, di segnalare **tempestivamente** l'eventuale superamento dei limiti di attenzione, di attivazione o di emergenza per ciascuno dei parametri monitorati, e di costituire un dettagliato archivio storico dell'evoluzione dei parametri ambientali.

La rilevazione *con continuità* dei parametri ambientali è evidentemente soltanto un *desiderata*, poiché qualunque sistema digitale, come è il μ-SMA, può soltanto trattare dati discreti. Intendiamo dunque questo desiderio del committente come "il sistema deve rilevare i parametri ambientali con frequenza superiore a quella tipica dell'evoluzione dei fenomeni osservati". Una rapida occhiata in avanti al paragrafo 2 ci consente di stabilire che nel nostro caso questa frequenza è pari a cinque minuti. Possiamo dunque raffinare il requisito 6 scrivendo

```
Un CCL interroga tutte le CdR collegate ottenendo le misure ogni
cinque minuti.
```

Naturalmente, se non avessimo avuto l'informazione addizionale circa i cinque minuti avremmo anche potuto lasciare astratto l'intervallo di campionamento, inserendo nel glossario un termine

```
tempo di campionamento/TSPAN.
```

e dichiarando che l'interrogazione deve avvenire `ogni tempo di campionamento` anziché `ogni cinque minuti`. Sempre nel paragrafo 2 troviamo un altro riferimento interessante:

2. ...Il CCR monitorizza l'attività dei CCL e raccoglie i dati storici che questi ultimi gli inviano **giornalmente**; ...

Questo *giornalmente* è alquanto vago, e si presta alle più varie interpretazioni. Per esempio, potrebbe essere inteso come "tutti i giorni, a una data ora del giorno" oppure come "ogni 24 ore", o meglio "24 ore dopo l'ultimo invio" (che può essere ritardato da guasti alla linea di comunicazione), o ancora "almeno una volta al giorno". Potremmo raffinare il requisito 18 scrivendo semplicemente

```
I CCL inviano i dati storici al CCR ogni 24 ore.
```

ma è più precisa (e forse più elegante) la soluzione seguente:

```
24 ore dopo che il CCL ha inviato i dati storici al CCR,
quando lo stato del collegamento CCR-CCL e' uguale a "operativo",
il CCL invia i dati storici al CCR.
```

che specifica un ciclo di trasmissione in quattro punti:

1. invia i dati storici al CCR.
2. attendi che siano trascorse 24 ore.
3. se il collegamento è operativo, vai al punto 1.
4. (attendi un ragionevole intervallo, e) vai al punto 3.

Questa politica ci permette di soddisfare anche un'altra richiesta dell'enunciato, che al paragrafo 3 reca:

3. ...In ogni caso, i dati storici devono essere preservati e trasmessi **appena possibile**; ...

Tornando al paragrafo 2, troviamo ancora:

2. Il superamento dei limiti di attenzione viene segnalato localmente al personale del CCL; il superamento degli altri limiti, ovvero il superamento continuato **per oltre quattro ore** dei limiti di attenzione, viene segnalato sia al CCL che al CCR.

Dovremo dunque raffinare il requisito 16, in cui avevamo lasciata astratta la determinazione della rilevanza del superamento limiti, scrivendo al suo posto un requisito come il seguente:

```
Se
- il limite superato del superamento limiti e' uguale al limite
  di attenzione della CdR per quattro ore, o
- il limite superato del superamento limiti e' uguale al limite
  di attivazione della CdR, oppure
- il limite superato del superamento limiti e' uguale al limite
  di emergenza della CdR,
allora il CCL invia il superamento limiti al CCR entro il tempo di
segnalazione allarmi.
```

dove la clausola "entro il tempo di segnalazione allarmi" ci consente di soddisfare la richiesta del primo paragrafo dell'enunciato di segnalare *tempestivamente* il superamento dei limiti. Abbiamo applicato a questo requisito la tecnica descritta in precedenza per lasciare astratta l'esatta tempistica, inserendo nel glossario

```
tempo di segnalazione allarmi/TSPAN.
```

Il nostro ultimo raffinamento riguarderà il requisito 20, in cui preciseremo (in accordo col paragrafo 3 dell'enunciato) la durata massima dell'interruzione del collegamento:

```
Un collegamento CCL-CCR puo' non essere disponibile per
al piu' 72 ore.
```

Con questo ultimo passo abbiamo pressoché esaurito il contenuto informativo dell'enunciato del problema, come dimostrato dalle annotazioni all'enunciato riportate in appendice B.

Il risultato finale del passo di estrazione dell'informazione, ovvero l'elenco dei requisiti con il glossario relativo, è riportato nell'appendice A.

Il processo di analisi dovrà ora continuare con una verifica presso il committente di tutte le assunzioni fatte fino a questo punto, seguita dall'eventuale aggiornamento e completamento dei requisiti in base alle nuove informazioni fornite. A questo completamento farà poi seguito la fase di progettazione, che potrebbe utilmente partire dai modelli diagrammatici prodotti da CIRCE.

5 Completamento dei requisiti

L'enunciato del problema, seppure già sufficientemente dettagliato, non fornisce informazione sufficiente per costruire una specifica dei requisiti completa. In questa sezione, mostreremo quali suggerimenti possono essere ottenuti da CIRCE circa l'assenza di informazioni rilevanti per la fase di progettazione, e completeremo i requisiti aggiungendo i completamenti "più probabili" per le varie assenze.

Naturalmente, tutte le decisioni prese in questa fase andranno verificate con il committente, per garantire la corrispondenza fra le nostre assunzioni e le sue intenzioni.

5.1 Segnalazioni di PANDORA

La vista PANDORA è destinata a raccogliere e presentare varie segnalazioni di errore e di avvertimento da parte di CIRCE. Se esaminiamo le segnalazioni di PANDORA relative al nostro ultimo raffinamento dei requisiti, troviamo fra le altre due insiemi di segnalazioni relative al flusso dei dati:

Informazioni non definite

I valori di **interruzione_di_collegamento_ccr-ccl**, **interruzione_di_collegamento_ccl-cdr**, **cdr.limite_di_attenzione**, **cdr.limiti_di_scala**, **cdr.limite_di_attivazione**, **cdr.limite_di_emergenza**, **cdr.limite**,

collegamento_ccl-cdr e **collegamento_ccl-ccr** non vengono mai modificati dal sistema.

Una variabile che non viene mai modificata non è una variabile. Se si tratta di una costante, dovrebbe essere dichiarata con il tag `/BLTIN` *nel glossario. Altrimenti, devi aggiungere qualche requisito che dica in che modo viene ottenuto il suo valore.*

VISTE RILEVANTI: Flusso dati HL, Flusso dati LL.

Informazioni non utilizzate

I valori di **configurazione**, **cdr.unità_di_misura** e **cdr.nome_simbolico** non vengono mai utilizzati dal sistema.

Una variabile che non viene mai usata come parametro in una elaborazione, non viene mai inviata all'esterno e non viene mai usata per prendere una decisione è probabilmente del tutto inutile. Se è così, puoi rimuovere questo termine dal glossario, e cancellare i requisiti ad esso relativi. Se, come è più probabile, la variabile rappresenta informazione utile, cerca di modellare più accuratamente il suo ciclo di vita, e dettaglia nei requisiti come, quando e perché viene usata.

VISTE RILEVANTI: Flusso dati HL, Flusso dati LL.

Il significato di queste due segnalazioni è il seguente.

1. Nel primo caso, CIRCE non trova nei nostri requisiti per il μ-SMA una descrizione su
   (a) come vengono rilevate le interruzioni di collegamento fra CdR e CCL e fra CCL e CCR;
   (b) come viene definito lo stato del collegamento fra CdR e CCL e fra CCL e CCR;
   (c) come vengono stabiliti i valori per i limiti di attenzione, di attivazione, di emergenza e di scala di una CdR;
   (d) come vengono stabiliti i valori per i "limiti" di una CdR.
2. Nel secondo caso, invece, CIRCE non trova nessun uso plausibile per
   (a) il nome simbolico di una CdR e l'unità di misura della grandezza misurata;
   (b) la configurazione (dei CCL e del CCR).

Di queste segnalazioni, solo 2(a) può essere ignorata (supponendo che il nome simbolico e l'unità di misura non siano oggetto di nessuna elaborazione, ma siano soltanto usati a scopo di visualizzazione dall'interfaccia utente — che, come detto, non descriveremo).

5.1.1 Stato dei collegamenti

Le segnalazioni 1(a) e 1(b) riguardano la determinazione da parte dei vari sottosistemi di quale sia lo stato di un collegamento. Riportiamo qui di seguito i requisiti relativi:

8. Il CCL segnala l'interruzione di collegamento CCL-CdR al personale del CCL.

9. Il CCR segnala l'interruzione di collegamento CCR-CCL al personale del CCR entro il tempo di segnalazione interruzioni di collegamento CCR-CCL.

10. 24 ore dopo che il CCL ha inviato i dati storici al CCR, se lo stato del collegamento CCR-CCL è uguale a "operativo", il CCL invia i dati storici al CCR.

15. Il CCL rileva i guasti in base alla misura, ai limiti di scala della CdR e allo stato del collegamento CCL-CdR.

20. Un collegamento CCL-CCR può non essere disponibile per al più 72 ore.

Come si vede, esiste innanzitutto una dualità fra le *interruzioni di collegamento* e lo *stato del collegamento*. Questa dualità trae origine dall'enunciato del problema, che introduceva entrambi i termini, ma un minimo di riflessione convincerà che si tratta in realtà di una descrizione ridondante per un fenomeno semplice: ogni collegamento ha uno stato osservabile, che può essere "operativo" oppure "non disponibile". Questa semplice proprietà può essere espressa in CIRCE dichiarando nel glossario

```
collegamento CCR-CCL/HASSTATE: collegamento CCL-CCR.
collegamento CdR-CCL/HASSTATE: collegamento CCL-CdR.
operativo/MODE.
non disponibile/MODE.
```

Con queste nuove definizioni, i requisiti precedenti diventano

8. Quando il collegamento CCL-CdR diventa non disponibile, il CCL invia un avviso di collegamento interrotto al personale del CCL.

9. Quando il collegamento CCR-CCL diventa non disponibile, il CCR invia un avviso di collegamento interrotto al personale del CCR entro il tempo di segnalazione interruzioni di collegamento CCR-CCL.

10. 24 ore dopo che il CCL ha inviato i dati storici al CCR, se il collegamento CCR-CCL è operativo, il CCL invia i dati storici al CCR.

15. Il CCL rileva i guasti in base alla misura, ai limiti di scala della CdR e allo stato del collegamento CCL-CdR.

20. Il collegamento CCL-CCR diventa operativo entro 72 ore da quando esso era diventato non disponibile.

In questa nuova formulazione, l'*avviso di collegamento interrotto* diventa una costante (in effetti, si tratta di un messaggio di errore), e può quindi essere dichiarata `/INF/BLTIN`.

5.1.2 Limiti delle CdR

I requisiti rilevanti per le segnalazioni 1(c) e 1(d), in quanto relativi ai *limiti* (in generale) sono i seguenti:

7. Il personale di un CCL imposta i limiti delle CdR del CCL.

14. Il CCL calcola il superamento limiti in base alla misura e ai limiti della CdR.

17. Se

    (a) il limite superato del superamento limiti è uguale al limite di attenzione della CdR per quattro ore, o

    (b) il limite superato del superamento limiti è uguale al limite di attivazione della CdR, oppure

    (c) il limite superato del superamento limiti è uguale al limite di emergenza della CdR,

    allora il CCL invia il superamento limiti al CCR entro il tempo di segnalazione allarmi.

25. Il limite di attenzione, il limite di attivazione e il limite di emergenza sono limiti.

Come si vede, l'asimmetria segnalata da PANDORA è dovuta al fatto che l'impostazione dei limiti di attenzione, attivazione ed emergenza è descritta in termini generici dal requisito 7, mentre il loro uso è descritto in dettaglio nel requisito 17.

La segnalazione di PANDORA potrebbe quindi essere ignorata, sulla base della nostra interpretazione della relazione di classificazione descritta dal requisito 25. In realtà, l'interpretazione più stretta richiederebbe non una relazione di classificazione, bensì una serie di attributi di secondo livello. In altre parole, "limiti" non deve essere una classe avente per istanze i vari tipi di limiti[13], bensì un attributo composto avente come campi i limiti specifici. L'espressione completa per riferirsi a un limite specifico dovrebbe dunque essere "il campo *limiti di attivazione* dell'attributo *limiti* di una CdR". Una simile formulazione è però eccessivamente verbosa, e poco comprensibile.

Meglio allora rinunciare alla generalizzazione "limiti", peraltro usata esclusivamente nei requisiti 7 e 14, e scrivere invece

7. Il personale di un CCL imposta il limite di attenzione, il limite di attivazione e il limite di emergenza delle CdR del CCL.

14. Il CCL calcola il superamento limiti in base alla misura, al limite di attenzione, al limite di attivazione e al limite di emergenza della CdR.

facendo così cadere il requisito 25 e rimuovendo il termine "limiti" dal glossario.

[13] In questo caso, il requisito 7 potrebbe essere inteso come "...imposta una qualunque istanza dei limiti", mentre la nostra intenzione è che venga impostato esattamente ciascuno dei tre limiti di attenzione, attivazione ed emergenza.

5.1.3 Gestione delle configurazioni

La segnalazione 2(b), l'ultima che dobbiamo analizzare, indica che i requisiti non descrivono l'uso che si fa del dato *configurazione*. In effetti, gli unici requisiti che trattano della configurazione sono i seguenti:

23. Il CCL modifica la configurazione in base alla variazione di configurazione delle CdR.

24. Il CCR modifica la configurazione in base alla variazione di configurazione dei CCL.

In realtà, la configurazione viene utilizzata in maniera implicita da diversi requisiti, per esempio

6. Un CCL interroga tutte le CdR collegate ...

dove *tutte le CdR collegate* dovrebbe essere sostituito da *tutte le CdR che la configurazione segnala come collegate*. Tuttavia, purché questa interpretazione sia chiara e possibilmente documentata (per esempio, attraverso commenti alla dichiarazione di *configurazione* nel glossario), non è necessario ricorrere alla forma più esplicita. Possiamo dunque ignorare la segnalazione di PANDORA (almeno fino alla fase di implementazione).

Si noti comunque che il piccolo problema sollevato da *tutte le CdR collegate* è anche identificato da altre viste: per esempio, la vista "Termini residui" segnala *tutte* e *collegate* come termini usati nei requisiti ma non dichiarati nel glossario, mentre la vista "Comprensione" riporta gli stessi termini come [Non compresi] nel rapporto sulla comprensione.

5.2 Segnalazioni di altre viste

Alcune altre viste di validazione di CIRCE segnalano potenziali errori nei requisiti di cui occorre tenere conto.

Per esempio, la vista "Errori automa" riporta la seguente segnalazione:

> collegamento_ccl-cdr ha un solo stato ("non_disponibile").

Questa imperfezione può essere risolta dichiarando esplicitamente gli stati possibili per il collegamento CCL-CdR. Per simmetria, dichiareremo inoltre gli stati possibili per il collegamento CCR-CCL, ottenendo così due nuovi requisiti:

- Un collegamento CCL-CdR può essere operativo o non disponibile.
- Un collegamento CCR-CCL può essere operativo o non disponibile.

La nostra traduzione è stata accurata e metodica, e le rimanenti viste di validazione non segnalano particolari errori. Un'ispezione completa orientata alla verifica di conformità dei requisiti dovrebbe comunque includere almeno le viste indicate in Tabella 9.

Cogliendo i suggerimenti della vista Comprensione, e al solo scopo di migliorare lo stile dei requisiti, possiamo anche trasformare tutti i requisiti che si limitano a descrivere comunicazioni in forma passiva (usando il verbo "riceve") in requisiti attivi (con "invia"). Per esempio, il requisito

11. Il CCL riceve la variazione di configurazione CdR dal personale del CCL.

Vista	Aspetti controllati
Errori automa	stati degli oggetti, transizioni fra stati
Errori selettori	espressioni selettive[14]
Sussunzione	proposte di sussunzione di relazioni e attributi da singole istanze a classi
Pandora	collezione di segnalazioni varie e consigli per la risoluzione dei problemi
Comprensione	rapporto sulla comprensione del testo, segnalazione di parti non comprese
Termini residui	uso di termini non inseriti nel glossario (e non predefiniti)
Uso termini	presenza nel glossario di termini non usati nei requisiti
Requisiti non atomici	presenza di requisiti non atomici, che potrebbero essere scomposti in requisiti atomici
Requisiti ridondanti	presenza di requisiti ridondanti, che potrebbero essere eliminati senza perdita di informazione

Tabella 9: Principali viste di validazione offerte da CIRCE.

può essere scritto nella forma alternativa, ed equivalente,

11. Il personale del CCL invia la variazione di configurazione CdR al CCL.

La differenza fra le due forme è sottile: in termini generali, la *ricezione* di un dato costituisce un evento, mentre l'*invio* di un dato costituisce un'azione. La trasformazione in forma attiva ha dunque lo scopo di sostituire la descrizione di un evento osservato da un componente del sistema (nel nostro caso, dal CCL) con la descrizione di un comportamento attivo di un'altra entità, che può essere un componente del sistema o meno (come è nel nostro caso). L'unico requisito di tipo evento che non può essere riportato a forma attiva è il seguente:

20. Il collegamento CCL-CCR diventa operativo entro 72 ore da quando esso era diventato non disponibile.

Ciò non è sorprendente, in quanto questo "requisito" descrive un vincolo su eventi che avvengono nel mondo esterno al sistema, il quale non è in alcun modo coinvolto nelle transizioni fra *operativo* e *non disponibile* del collegamento CCL-CCR. In effetti, questo requisito ha l'unico scopo di fornire delle assicurazioni circa il dimensionamento massimo di eventuali buffer di comunicazioni (deve essere possibile memorizzare l'intero traffico non trasmesso per al massimo tre giorni). Enunciati di questo tipo potrebbero essere omessi dal documento di requisiti per il μ-SMA, e trasmessi direttamente alle fasi di progettazione e implementazione.

Tuttavia, per favorire la documentabilità dei nostri requisiti, può essere preferibile lasciare comunque il requisito nel documento, e ignorare invece la segnalazione della vista Comprensione. Questa sarà la strada che seguiremo.

5.3 Analisi dei modelli

Le modifiche che abbiamo apportato ai requisiti dietro suggerimento di PANDORA e delle altre viste di validazione hanno avuto l'effetto di rendere il documento accettabile rispetto ai test di conformità condotti da CIRCE. Questo è una proprietà importante, che deve sempre essere garantita da un buon documento di requisiti, ma non è condizione sufficiente perché un documento di requisiti sia considerato di buona qualità.

Altre migliorie ai requisiti possono essere ottenute esaminando i modelli grafici e testuali prodotti da CIRCE.

5.3.1 Modelli funzionali

In Figura 9 è possibile osservare il modello di flusso dati a basso livello ottenuto dopo i passi di completamento che abbiamo compiuto finora. Si può verificare come la rappresentazione del flusso dati coincida largamento con la nostra intuizione, e in particolare, procedendo da sinistra a destra:

- Il CCL invia al CCR le segnalazioni di guasto, di superamento limite, e i dati storici. Le prime due vengono mostrate al personale del CCR, mentre i dati storici non vengono ulteriormente trasmessi o elaborati[15] Al personale del CCR viene anche inviato un avviso di collegamento interrotto (quando viene rilevata un'interruzione del collegamento CCR-CCL).

- Il personale del CCR invia al CCR le variazioni di configurazione, che il CCR usa per aggiornare la configurazione corrente (che non viene usata esplicitamente, ma di questo abbiamo già discusso nella Sezione 5.1.3). Le variazioni di configurazione vengono anche registrate nell'archivio storico, come richiesto dall'enunciato del problema.

- Il personale del CCL invia anch'esso le variazioni di configurazione, che vengono trattate dal CCL analogamente a quanto fatto dal CCR. Inoltre, il personale invia (in due distinte operazioni)

  1. il nome simbolico, l'unità di misura e i limiti di scala di una CdR;
  2. il limite di attenzione, di attivazione e di emergenza di una CdR.

  Il nome simbolico e l'unità di misura non vengono mai usati, come avevamo già rilevato. I limiti di scala vengono usati (in effetti, comparati con le misura) per rilevare i guasti. Altri casi di guasto derivano dall'interruzione del collegamento CCL-CdR. In ogni caso, il guasto viene segnalato sia al personale del CCL che al CCR (come detto sopra). Un probabile difetto della nostra modellazione risiede nel fatto che un "avviso di collegamento interrotto" viene inviato *indipendentemente* dalla segnalazione di guasto al solo personale del CCL: appare così che in caso di interruzione del collegamento CCL-CdR, il personale riceva ben *due* segnalazioni: una generica di guasto (a cui saranno presumibilmente associati i dettagli sulla causa) e una specifica di collegamento interrotto. I due avvisi sono con ogni probabilità ridondanti, ma senza l'assistenza del committente non è possibile decidere quale dei due possa essere eliminato.

[15] Questa, naturalmente, è un'anomalia; probabilmente i dati storici dovrebbero essere inviati all'archivio storico. Tuttavia, l'enunciato del problema si limita a dire che il CCR "raccoglie i dati storici che gli vengono inviati", senza menzionare il rapporto fra questa raccolta e l'archivio storico, che in altri punti è citato esplicitamente. Una decisione finale sulla correttezza di questa modellazione non può essere presa senza consultare il committente.

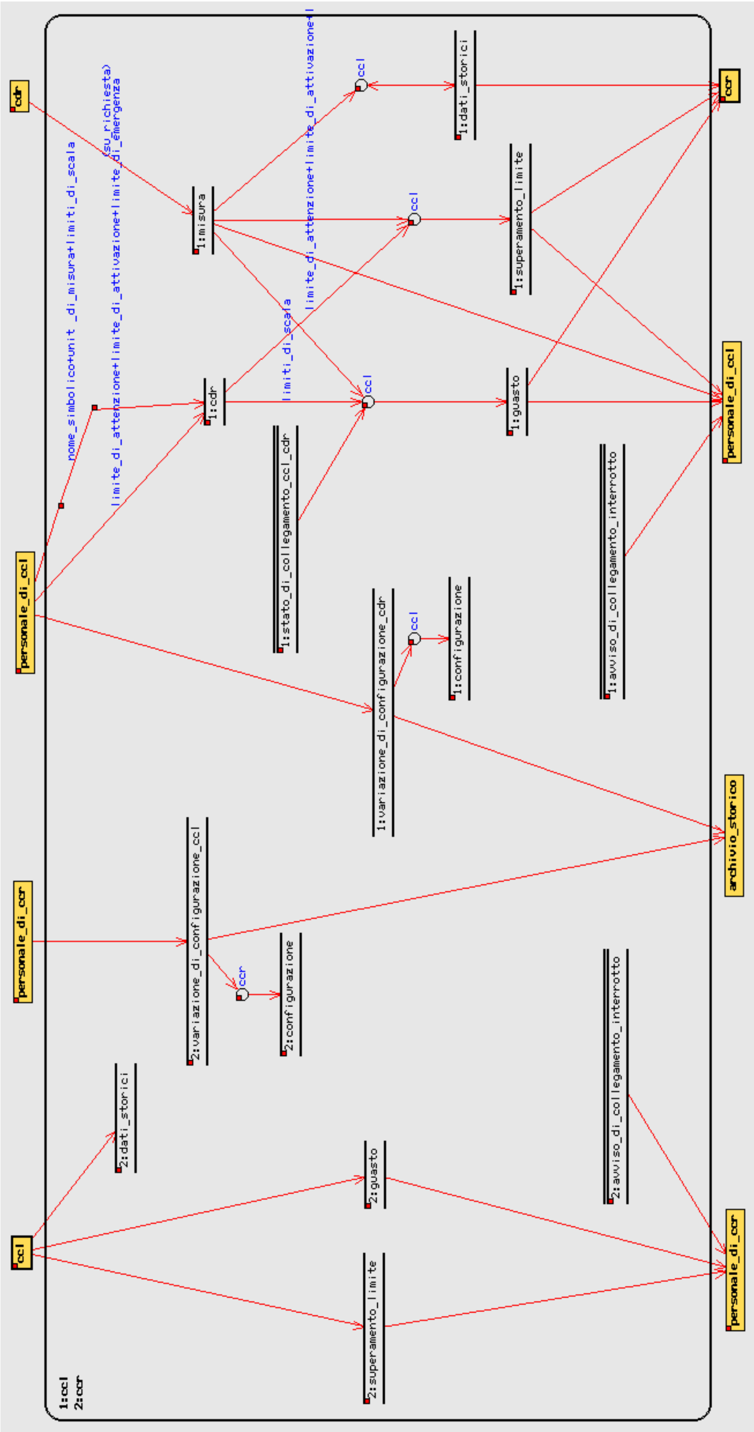


Figura 9: Il diagramma di flusso dati dopo i primi due passi di completamento.

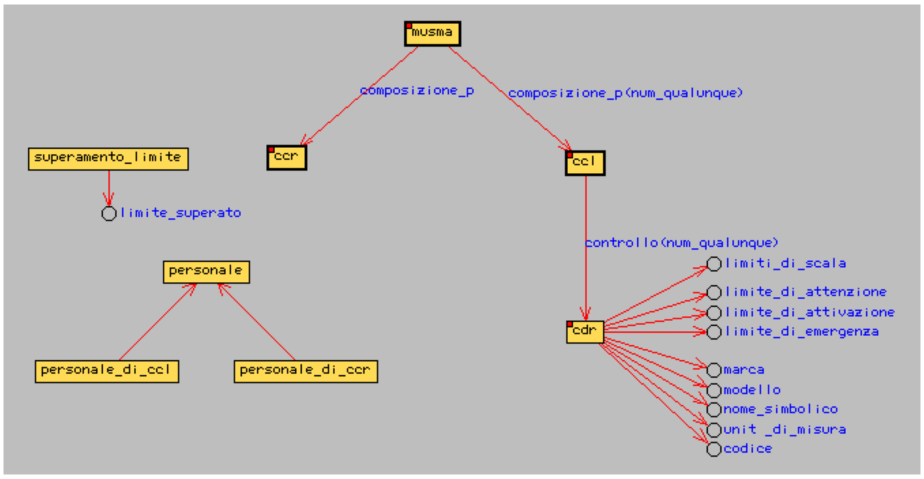


Figura 10: Il diagramma Entità-Relazioni dopo il completamento.

- Per finire, ogni CdR invia al proprio CCL la lettura delle misure. La misura viene comparata con i limiti di scala della CdR, come abbiamo detto, per identificare i guasti, ma anche con i limiti di attenzione, attivazione ed emergenza della CdR per verificare l'eventuale superamento dei limiti. Se si è verificato, il superamento limiti viene segnalato sia al personale del CCL che al CCR, come già visto. Le misure concorrono inoltre a costruire i dati storici, che vengono (periodicamente, quando possibile) inviati al CCL.

Il fatto che il modello coincida con la nostra intuizione, la stabilità del modello delle comunicazioni (che non è mutato rispetto a quello ottenuto dal terzo raffinamento dei requisiti, Figura 5) e il soddisfacimento dei controlli di validità effettuati da Circe sono altrettanti fattori che ci inducono a considerare gli aspetti funzionali della nostra descrizione del μ-SMA ormai sufficientemente definiti.

5.3.2 Modelli degli oggetti

La struttura degli oggetti del nostro sistema è piuttosto semplice, ma un'ispezione diretta del modello degli oggetti può comunque rivelare dettagli interessanti. Il diagramma entità-relazioni del μ-SMA è riportato in Figura 10.

Come atteso, il μ-SMA risulta composto da un CCR e da un numero qualunque di CCR, ciascuno dei quali controlla un numero qualunque di CdR. Ogni CdR ha un certo numero di attributi:

- i limiti di scala;
- i limiti di attenzione, attivazione ed emergenza;
- una marca, un modello, un nome simbolico, un'unità di misura e un codice unico.

In particolare, l'ultimo gruppo di attributi potrebbe attirare la nostra attenzione: il diagramma di flusso dati in Figura 9 mostra infatti che il nome simbolico

Eventi e condizioni	**Azioni**
collegamento_ccl-ccr è operativo	ccl invia dati_storici a ccr
limite_superato di superamento_limite uguale limite_di_attenzione di cdr per 4 ore o limite_superato di superamento_limite uguale limite_di_attivazione o limite_di_emergenza di cdr	ccl invia superamento_limite a ccr entro tempo_di_segnalazione_allarmi
collegamento_ccl-cdr diventa non_disponibile	ccl invia avviso_di_collegamento_interrotto a personale_di_ccl
collegamento_ccl-ccr diventa non_disponibile	ccr invia avviso_di_collegamento_interrotto a personale_di_ccr entro tempo_di_segnalazione_interruzioni_di_collegamento_ccr-ccl

Tabella 10: Il modello Eventi-Azioni dei requisiti completi.

e l'unità di misura, nonché tutti i limiti, vengono impostati per ogni CdR dal personale del CCL relativo. Al contrario, la marca, il modello e il codice unico non vengono mai impostati (dobbiamo dunque supporre che essi vengano impostati in fabbrica per ogni CdR e siano inalterabili) e non sono mai utilizzati. Questi attributi potrebbero quindi essere rimossi dal documento di requisiti, ma probabilmente saranno utili in fase di implementazione (il codice unico, per esempio, potrebbe servire come indirizzo di unità sulla rete di collegamento). Anche in questo caso, la nostra comprensione può essere verificata con il committente; decidiamo comunque di mantenere questi attributi nel documento di requisiti a scopo di documentazione.

L'unico attributo del superamento limiti (un indicatore di quale limite sia stato superato) e la gerarchia di classificazione del personale sono esattamente come attesi e non richiedono particolari attenzioni.

5.3.3 Modelli dinamici

La componente dinamica del μ-SMA non è particolarmente estesa. Si tratta infatti essenzialmente di un sistema di flusso dati (e, in particolare, di un sistema di monitoraggio, quindi con il flusso dei dati principalmente unidirezionale). Le uniche eccezioni al normale flusso di funzionamento riguardano il superamento dei limiti e il trattamento delle interruzioni di collegamento, come riportato dal modello Eventi-Azioni riportato in Tabella 10.

È sufficiente un'ispezione diretta a questo modello per convincersi che il comportamento del sistema descritto dai requisiti coincide con quello inteso. Si noti comunque che le azioni che vengono eseguite incondizionatamente, per esempio l'invio dei dati storici ogni 24 ore, non vengono mostrate in questo modello.

6 Conclusioni

In questo caso di studio abbiamo mostrato come usare i costrutti di astrazione linguistica di Circe per sviluppare un documento di requisiti in maniera razionale. Abbiamo modellato in maniera incrementale i diversi aspetti rilevanti per un caso di studio semplificato, ma realistico, fino a ottenere dei requisiti sufficientemente dettagliati.

Abbiamo poi considerato le segnalazioni di inconsistenza da parte degli strumenti di validazione contenuti in CIRCE e l'interpretazione dei modelli che esso è in grado di estrarre dai requisiti testuali per perfezionare, completare e correggere il risultato della nostra analisi dell'enunciato del problema.

Il documento ottenuto non è certamente completo, ed è tutt'altro che perfetto: c'è largo spazio per miglioramenti, per ulteriori raffinamenti e per l'assunzione di decisioni architetturali e sistemistiche più stringenti. Tuttavia, il documento finale incorpora praticamente tutta l'informazione contenuta nell'enunciato del problema, e non molto potrebbe essere aggiunto senza un'effettiva interazione con il committente.

Ulteriori miglioramenti possono essere lasciati come utile esercizio per chi voglia acquisire maggiore dimestichezza con gli aspetti operativi e interattivi dell'ambiente di supporto. I lettori interessati possono fare riferimento a [1], che raccoglie numerosi esempi di analisi dei requisiti per il μ-SMA, completi di progettazione OMT e di implementazione di un prototipo in Java.

A Requisiti e glossario estratti dall'enunciato

In questa sezione riportiamo *verbatim* le viste sui requisiti e sul glossario prodotte da Circe. Tutte le viste si riferiscono all'ultimo raffinamento dei requisiti estratti direttamente dall'enunciato del problema.

A.1 Requisiti

```
 1. Il muSMA rileva i parametri ambientali e meteorologici, segnala il
    superamento dei limiti e costituisce un archivio storico.

 2. Il muSMA è composto da un CCR.
 3. Il muSMA è composto da un numero qualunque di CCL.
 4. Ogni CCL controlla un numero qualunque di CdR.
 5. Il personale del CCR e il personale del CCL sono personale.

 6. Un CCL interroga tutte le CdR collegate ottenendo le misure ogni cinque
    minuti.

 7. Il personale di un CCL imposta i limiti delle CdR del CCL.

 8. CCL segnala l'interruzione di collegamento CCL-CdR al personale del CCL.
 9. Il CCR segnala l'interruzione di collegamento CCR-CCL al personale del
    CCR entro il tempo di segnalazione interruzioni di collegamento CCR-CCL.

10. 24 ore dopo che il CCL ha inviato i dati storici al CCR, se lo stato
    del collegamento CCR-CCL è uguale a "operativo", il CCL invia i dati
    storici al CCR.

11. CCL riceve la variazione di configurazione CdR dal personale del CCL.
12. CCR riceve la variazione di configurazione CCL dal personale del CCR.

13. Il personale del CCL ottiene
    - le misure
    - il superamento limiti, e
    - i guasti dal CCL.

14. Il CCL calcola il superamento limiti in base alla misura e ai limiti
    della CdR.
15. Il CCL rileva i guasti in base alla misura, ai limiti di
    scala della CdR e allo stato del collegamento CCL-CdR.

16. Il CCL invia i guasti al CCR.

17. Se
    - il limite superato del superamento limiti è uguale al limite di
      attenzione della CdR per quattro ore, o
    - il limite superato del superamento limiti è uguale al limite di
      attivazione della CdR, oppure
    - il limite superato del superamento limiti è uguale al limite di
```

  emergenza della CdR,
allora il CCL invia il superamento limiti al CCR entro il tempo di segnalazione allarmi.

18. Il personale del CCR ottiene
    - il superamento limiti e
    - i guasti
    dal CCR.

19. Il CCL aggiunge le misure ai dati storici.

20. Un collegamento CCL-CCR può non essere disponibile per al più 72 ore.
21. I CCL inviano le variazioni di configurazione CdR all'archivio storico.
22. Il CCR invia le variazioni di configurazione CCL all'archivio storico.

23. Il CCL modifica la configurazione in base alla variazione di configurazione delle CdR.
24. Il CCR modifica la configurazione in base alla variazione di configurazione dei CCL.

25. Il limite di attenzione, il limite di attivazione e il limite di emergenza sono limiti.

26. Ogni CdR ha attributi una marca, un modello e un codice identificativo unico.

27. Il CCL riceve dal personale del CCL il nome simbolico della grandezza misurata, l'unità di misura della grandezza misurata e i limiti di scala della CdR.

A.2 Glossario

Sistemi comunicanti

a. archivio storico/in.
b. ccl/in/out/sys/elab.
c. ccr/in/out/sys/elab.
d. cdr/in/out.
e. musma/sys/in/out.
f. personale/in/out/elab.
g. personale di ccl/in/out/elab.
h. personale di ccr/in/out/elab.

Informazioni

a. collegamento ccl-ccr/inf: collegamento ccr-ccl.
b. collegamento ccl-cdr/inf: collegamento cdr-ccl.
c. configurazione/inf.
d. dati storici/inf.
e. guasto/inf: guasti.
f. interruzione di collegamento ccl-cdr/inf.
g. interruzione di collegamento ccr-ccl/inf.

h. misura/inf: misure.
i. operativo/inf/bltin.
j. superamento limite/inf: superamento limiti.
k. variazione di configurazione ccl/inf:
variazioni di configurazione ccl,
variazione di configurazione di ccl.
l. variazione di configurazione cdr/inf:
variazioni di configurazione cdr,
variazione di configurazione di cdr.

Attributi
a. codice/attr: codice identificativo unico.
b. limite/attr: limiti.
c. limite di attenzione/attr.
d. limite di attivazione/attr.
e. limite di emergenza/attr.
f. limite superato/attr.
g. limiti di scala/attr: limite di scala.
h. marca/attr.
i. modello/attr.
j. nome simbolico/attr: nome simbolico di grandezza misurata.
k. stato/attr.
l. unità di misura/attr: unità di misura di grandezza misurata.

Ordinali
a. a più 72/num.

Relazioni e operazioni
a. controllo/rel: controlla.
b. non è disponibile/unop: può non essere disponibile.
c. rilevante per ccr/unop: è rilevante per ccr.

Parti del sistema
a. ccl/in/out/sys/elab.
b. ccr/in/out/sys/elab.
c. musma/sys/in/out.

Tempo
a. tempo di segnalazione allarmi/tinterv.
b. tempo di segnalazione interruzioni di collegamento ccr-ccl/tinterv.

Altri
a. elabora: rileva.
b. invia: ha inviato.
c. mantiene archivio storico/fun: costituisce archivio storico.
d. rileva parametri/fun:
rileva parametri ambientali e meteorologici.
e. segnala allarmi/fun: segnala superamento di limiti.

B Materiale residuo nell'enunciato

Nel corso della costruzione dei requisiti abbiamo progressivamente preso in considerazione pressoché tutto il materiale testuale fornito come enunciato del problema. Qui di seguito vengono invece evidenziate le parti che **non** sono state prese in considerazione. Si noti come si tratti spesso di materiale ridondante o privo di contenuto informativo, oppure di requisiti negativi (per esempio: "il CCL si suppone affidabile" può essere interpretato come "il CCL non avrà guasti"; se i nostri requisiti non parlano di guasti al CCL, questa condizione è automaticamente soddisfatta dal documento di requisiti).

1. Il sistema di monitoraggio ambientale μ-SMA ha lo scopo di rilevare con continuità i parametri **ambientali e metereologici su scala regionale**, di segnalare tempestivamente **l'eventuale** superamento dei limiti di attenzione, di attivazione o di emergenza per ciascuno dei parametri monitorati, e di costituire un **dettagliato** archivio storico dell'evoluzione dei parametri **ambientali**.

2. Il sistema si articola su tre livelli: un Centro di Controllo Regionale (CCR), un insieme di Centri di Controllo Locali (CCL) e, per ciascuno di essi, un insieme di Centraline di Rilevamento (CdR). Il CCR monitorizza l'attività dei CCL e raccoglie i dati storici che questi ultimi gli inviano giornalmente; i CCL interrogano ogni cinque minuti tutte le CdR a essi collegate per raccogliere le relative misure. I CCL verificano inoltre il superamento dei limiti, che possono essere impostati dal personale di gestione **e che sono tipicamente diversi a seconda della località in cui le CdR sono installate**. Il superamento dei limiti di attenzione viene segnalato localmente al personale del CCL; il superamento degli altri limiti, ovvero il superamento continuato per oltre quattro ore dei limiti di attenzione, viene segnalato sia al CCL che al CCR.

3. **Il μ-SMA deve essere in grado di continuare a operare ragionevolmente in presenza di** guasti alle CdR (assenza di risposta alle interrogazioni del CCL, o risposta con valori fuori scala), **che** devono **comunque** essere segnalati al CCL. **CCL e CCR sono realizzati con tecnologia ridondante e si suppongono affidabili, ma** un collegamento CCL-CCR può non essere disponibile per un tempo massimo di 72 ore. In ogni caso, i dati storici devono essere preservati e trasmessi appena possibile; l'interruzione del collegamento deve essere segnalata non appena rilevata al personale del CCR.

4. Ogni CdR è caratterizzata da una marca, un modello, e un codice identificativo unico. Il CCL conosce per ogni CdR connessa il nome simbolico della grandezza misurata, l'unità di misura, e i limiti di scala per le misure accettabili.

5. Deve essere possibile in ogni momento aggiungere o rimuovere CdR a un CCL; allo stesso modo, deve essere possibile aggiungere o rimuovere CCL a un CCR. Ogni variazione della configurazione del sistema deve essere riportata nell'archivio storico.

6. Il sistema deve offrire al personale del CCL un'interfaccia utente che visualizzi con continuità le misure rilevate e gli eventuali allarmi dovuti al superamento delle varie soglie, nonché le indicazioni di malfunzionamenti nel sistema. Al personale del CCR devono essere segnalati soltanto gli allarmi (con l'indicazione della misura che eccede i livelli) e i malfunzionamenti.

C Requisiti e glossario finali

In questa sezione riportiamo *verbatim* le viste sui requisiti e sul glossario prodotte da CIRCE. Tutte le viste si riferiscono all'ultimo raffinamento dei requisiti, completati in seguito alle segnalazioni delle viste di validazione e all'ispezione diretta dei modelli di CIRCE.

C.1 Requisiti

```
1. Il muSMA rileva i parametri ambientali e meteorologici, segnala
   il superamento dei limiti e costituisce un archivio storico.

2. Il muSMA è composto da un CCR.
3. Il muSMA è composto da un numero qualunque di CCL.
4. Ogni CCL controlla un numero qualunque di CdR.
5. Il personale del CCR e il personale del CCL sono personale.

6. Un CCL interroga tutte le CdR collegate ottenendo le misure ogni
   cinque minuti.
7. Il personale di un CCL imposta il limite di attenzione, il limite
   di attivazione e il limite di emergenza delle CdR del CCL.

8. Quando il collegamento CCL-CdR diventa non disponibile, il CCL
   invia un avviso di collegamento interrotto al personale del CCL.
9. Quando il collegamento CCR-CCL diventa non disponibile, il CCR
   invia un avviso di collegamento interrotto al personale del CCR
   entro il tempo di segnalazione interruzioni di collegamento CCR-CCL.
10. 24 ore dopo che il CCL ha inviato i dati storici al CCR, se il
    collegamento CCR-CCL è operativo, il CCL invia i dati storici al CCR.

11. Il personale del CCL invia la variazione di configurazione CdR al CCL.
12. Il personale del CCR invia la variazione di configurazione CCL al CCR.

13. Il CCL segnala al personale del CCL
    - le misure
    - il superamento limiti, e
    - i guasti.

14. Il CCL calcola il superamento limiti in base alla misura e al
    limite di attenzione, al limite di attivazione e al limite di
    emergenza della CdR.

15. Il CCL rileva i guasti in base alla misura, ai limiti di scala
    della CdR e allo stato del collegamento CCL-CdR.

16. Il CCL invia i guasti al CCR.

17. Se
    - il limite superato del superamento limiti è uguale al limite
      di attenzione della CdR per quattro ore, o
```

- il limite superato del superamento limiti è uguale al limite
  di attivazione o il limite di emergenza della CdR,
allora il CCL invia il superamento limiti al CCR entro il tempo
di segnalazione allarmi.

18. Il CCR segnala al personale del CCR
    - il superamento limiti e
    - i guasti.

19. Il CCL aggiunge le misure ai dati storici.

20. Il collegamento CCL-CCR diventa operativo entro 72 ore da quando
    esso era diventato non disponibile.

21. I CCL inviano le variazioni di configurazione CdR all'archivio storico.
22. Il CCR invia le variazioni di configurazione CCL all'archivio storico.

23. Il CCL modifica la configurazione in base alla variazione di
    configurazione delle CdR.
24. Il CCR modifica la configurazione in base alla variazione di
    configurazione dei CCL.

25. Ogni CdR ha attributi una marca, un modello e un codice
    identificativo unico.

26. Il personale del CCL invia al CCL
    - il nome simbolico della grandezza misurata,
    - l'unità di misura della grandezza misurata, e
    - i limiti di scala
    della CdR.

27. Un collegamento CCL-CdR può essere operativo o non disponibile.
28. Un collegamento CCR-CCL può essere operativo o non disponibile.

C.2 Glossario

Sistemi comunicanti
   a. archivio storico/in.
   b. ccl/in/out/sys/elab.
   c. ccr/in/out/sys/elab.
   d. cdr/in/out.
   e. musma/sys/in/out.
   f. personale/in/out.
   g. personale di ccl/in/out/elab.
   h. personale di ccr/in/out/elab.

Informazioni
   a. avviso di collegamento interrotto/inf/bltin.

b. configurazione/inf.
c. dati storici/inf.
d. guasto/inf: guasti.
e. misura/inf: misure.
f. superamento limite/inf: superamento limiti.
g. variazione di configurazione ccl/inf: variazioni di configurazione ccl, variazione di configurazione di ccl.
h. variazione di configurazione cdr/inf: variazioni di configurazione cdr, variazione di configurazione di cdr.

Attributi

a. codice/attr: codice identificativo unico.
b. limite di attenzione/attr.
c. limite di attivazione/attr.
d. limite di emergenza/attr.
e. limite superato/attr.
f. limiti di scala/attr: limite di scala.
g. marca/attr.
h. modello/attr.
i. nome simbolico/attr: nome simbolico di grandezza misurata.
j. stato/attr.
k. unità di misura/attr: unità di misura di grandezza misurata.

Relazioni e operazioni

a. controllo/rel: controlla.

Stati

a. non disponibile/mode.
b. operativo/mode.

Parti del sistema

a. ccl/in/out/sys/elab.
b. ccr/in/out/sys/elab.
c. musma/sys/in/out.

Tempo

a. tempo di segnalazione allarmi/tinterv.
b. tempo di segnalazione interruzioni di collegamento ccr-ccl/tinterv.

Altri

a. collegamento ccl-ccr/hasstate: collegamento ccr-ccl.
b. collegamento ccl-cdr/hasstate: collegamento cdr-ccl.
c. diventa: è diventato, era diventato.
d. elabora: rileva.
e. invia: ha inviato.
f. mantiene archivio storico/fun: costituisce archivio storico.
g. rileva parametri/fun: rileva parametri ambientali e meteorologici.
h. segnala allarmi/fun: segnala superamento di limiti.

Riferimenti bibliografici

[1] V. Ambriola and V. Gervasi. Progetti degli studenti partecipanti al corso ISLP 99. URL: http://bilbo.di.unipi.it/ISLP99.

[2] V. Ambriola and V. Gervasi. Processing natural language requirements. In *Proceedings of ASE 1997*, pages 36–45. IEEE Press, 1997.

[3] M. Arioli. Note su GUIGenerator, 1999. Dispense per il corso di Ingegneria del software: laboratorio di progettazione.

Indice