

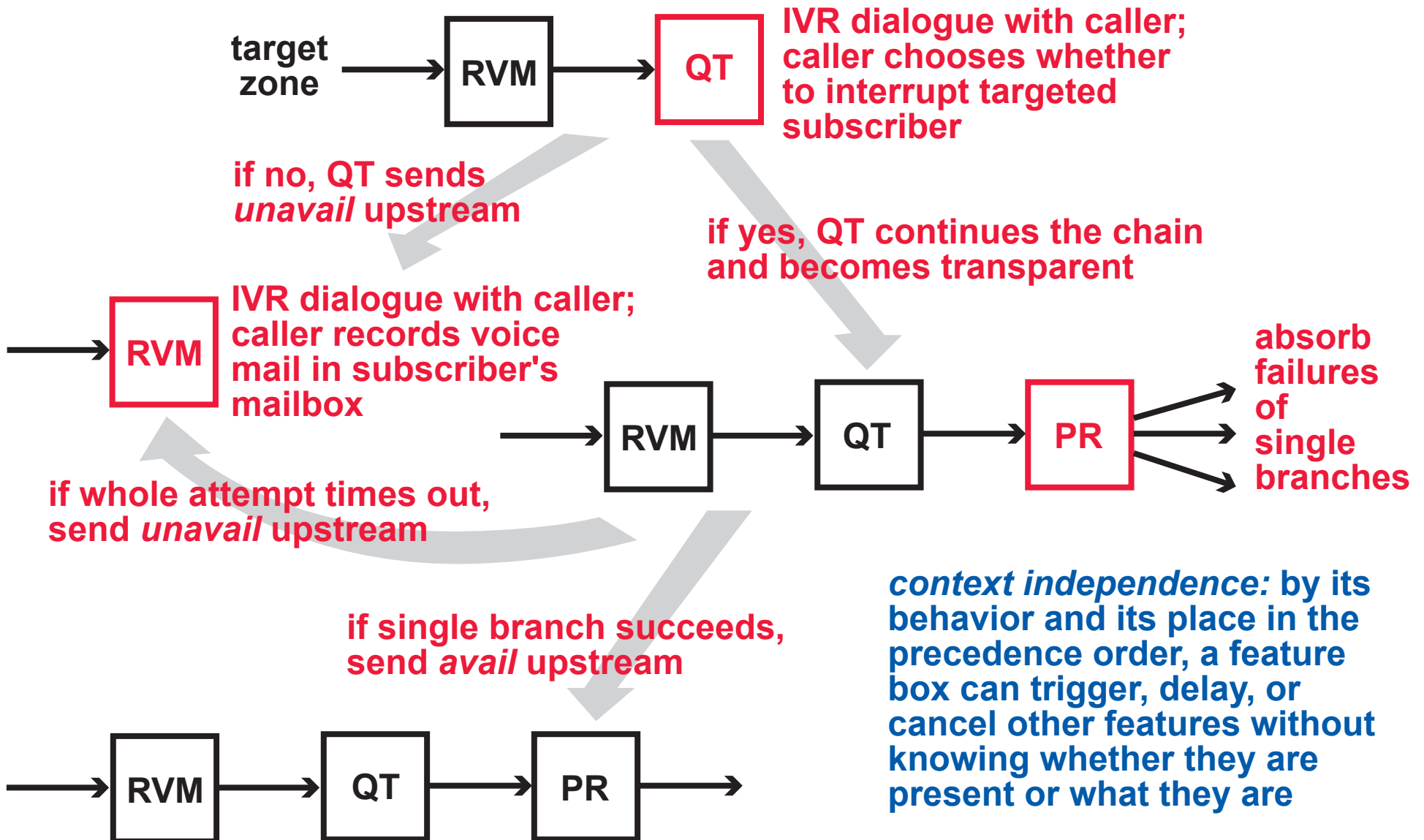
PART FIVE:
SOME VERIFICATION CHALLENGES

*a DFC case study with
several verification problems,
all concerning signaling properties
and event-based feature interactions*

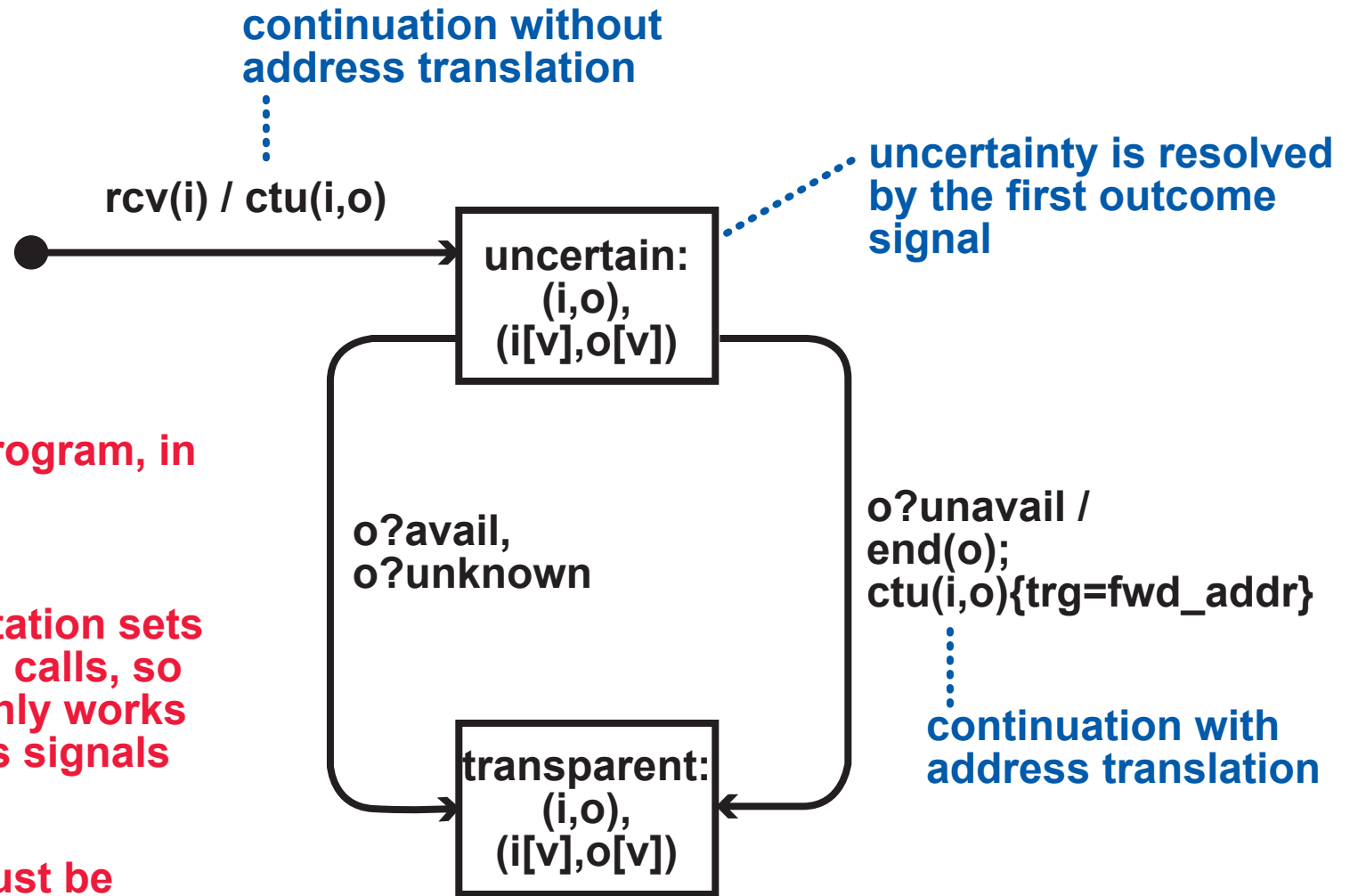
SIGNALING INTERACTIONS

transparency: a box behaves transparently when its functions are not needed

autonomy: each box has the power it needs to perform its functions independently



BOXTALK EXAMPLE: CALL FORWARDING ON BUSY



this is a Boxtalk program, in graphical syntax

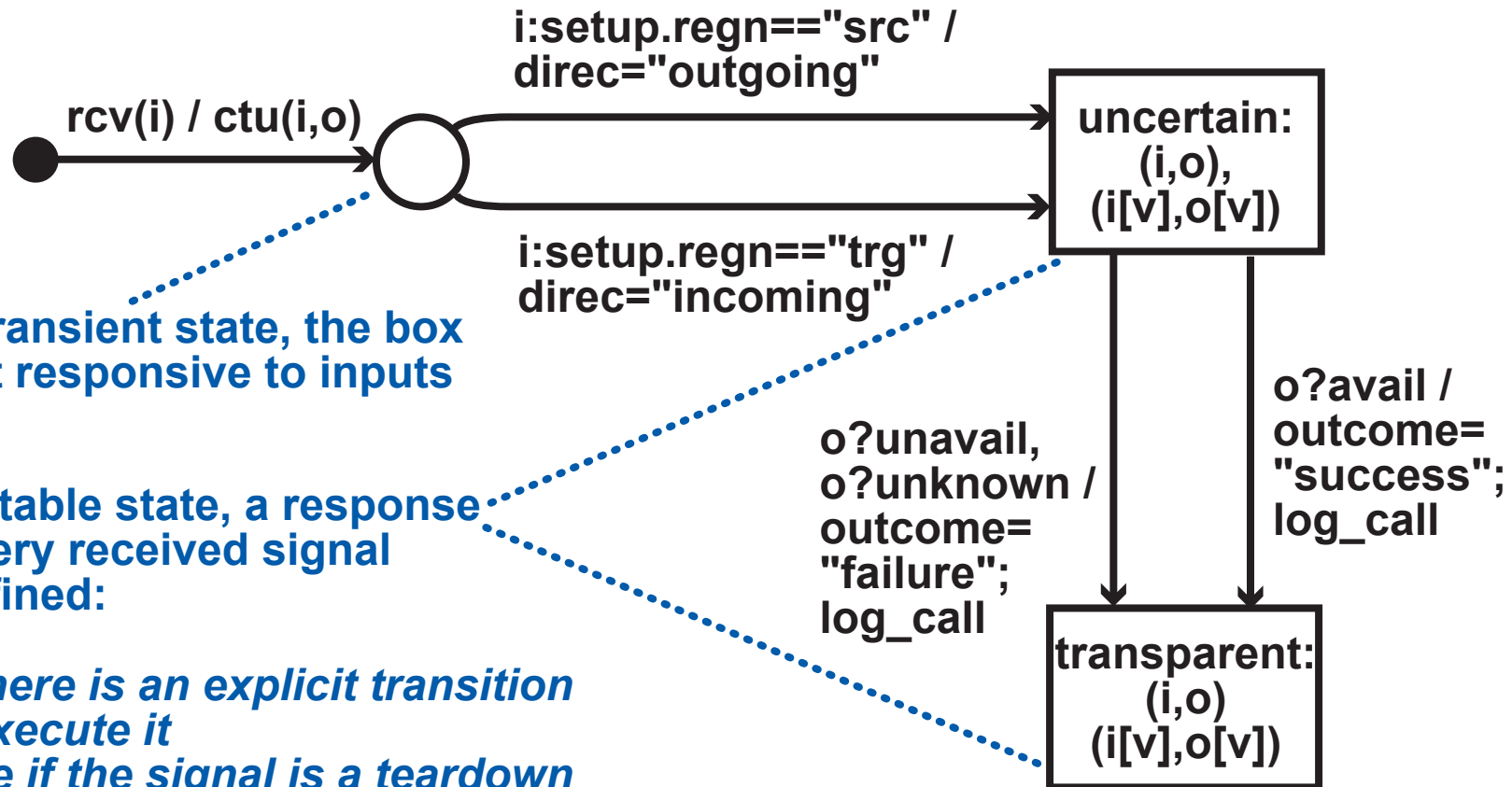
Boxtalk implementation sets up and tears down calls, so the programmer only works directly with status signals

each active call must be referred to by a call variable; each responsive state lists the variables of all active calls

a feature box should be INPUT-ENABLED, i.e., guaranteed to read every input signal in a prompt fashion

BOXTALK EXAMPLE: CALL LOGGER

this box can be used in a source or target zone



in a transient state, the box is not responsive to inputs

in a stable state, a response to every received signal is defined:

*if there is an explicit transition execute it
else if the signal is a teardown tear down all calls and quit
else if the source of the signal is linked send signal to all linked calls
else discard the signal*

A CASE STUDY

HISTORY

- these features are the relevant part of a feature set that was deployed by AT&T in a consumer trial of VoIP October 2003 to March 2004
- most of them are now in CallVantage, which is AT&T's VoIP service
- when the feature set was designed, the feature interactions were analyzed manually and heuristically

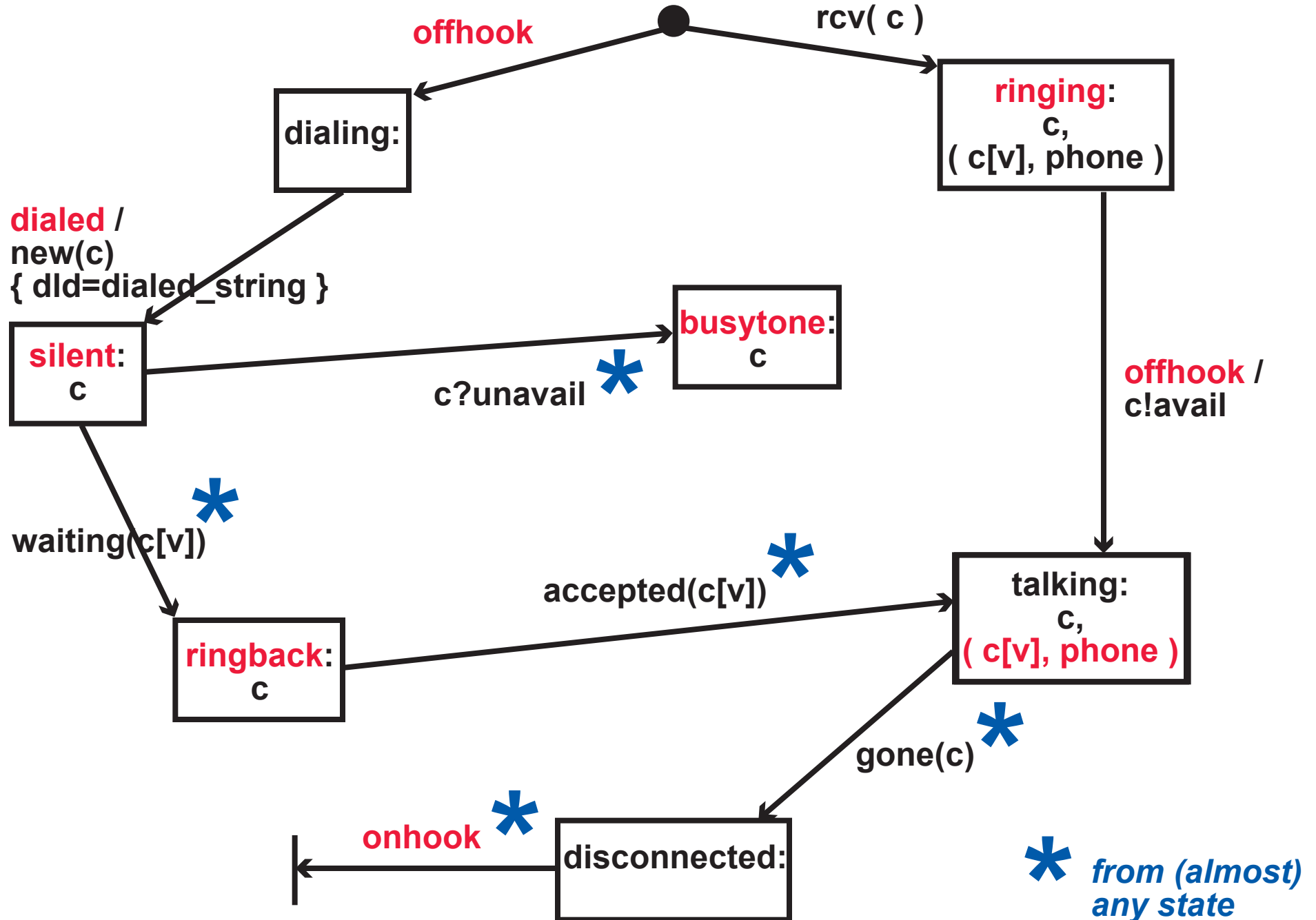
BOUNDARIES

- the only devices are "black phones"
- no source feature boxes
- no bound feature boxes
- a feature box can only use the *new* method to place a call to a resource
- a feature box cannot use the *rev* method

WHAT CAN HAPPEN THAT IS INTERESTING?

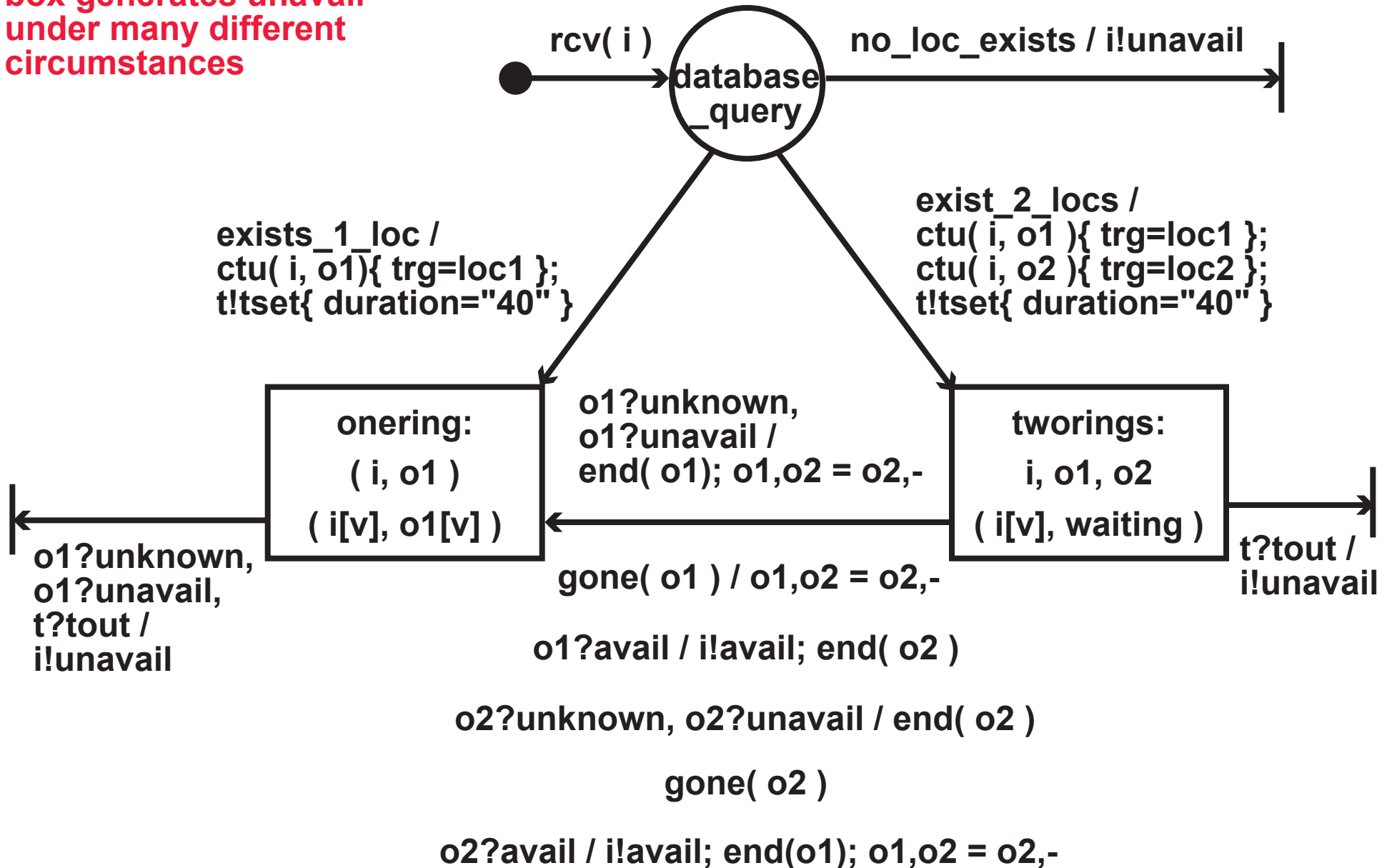
- a target region can contain several target zones
- a usage can reach an interface box, or stop at some feature box
- a usage can fork
- a usage can have multiple, sequential extensions downstream of a feature box

BOUND BOX: BLACK PHONE INTERFACE (SIMPLIFIED)



FREE BOX: PARALLEL FIND ME

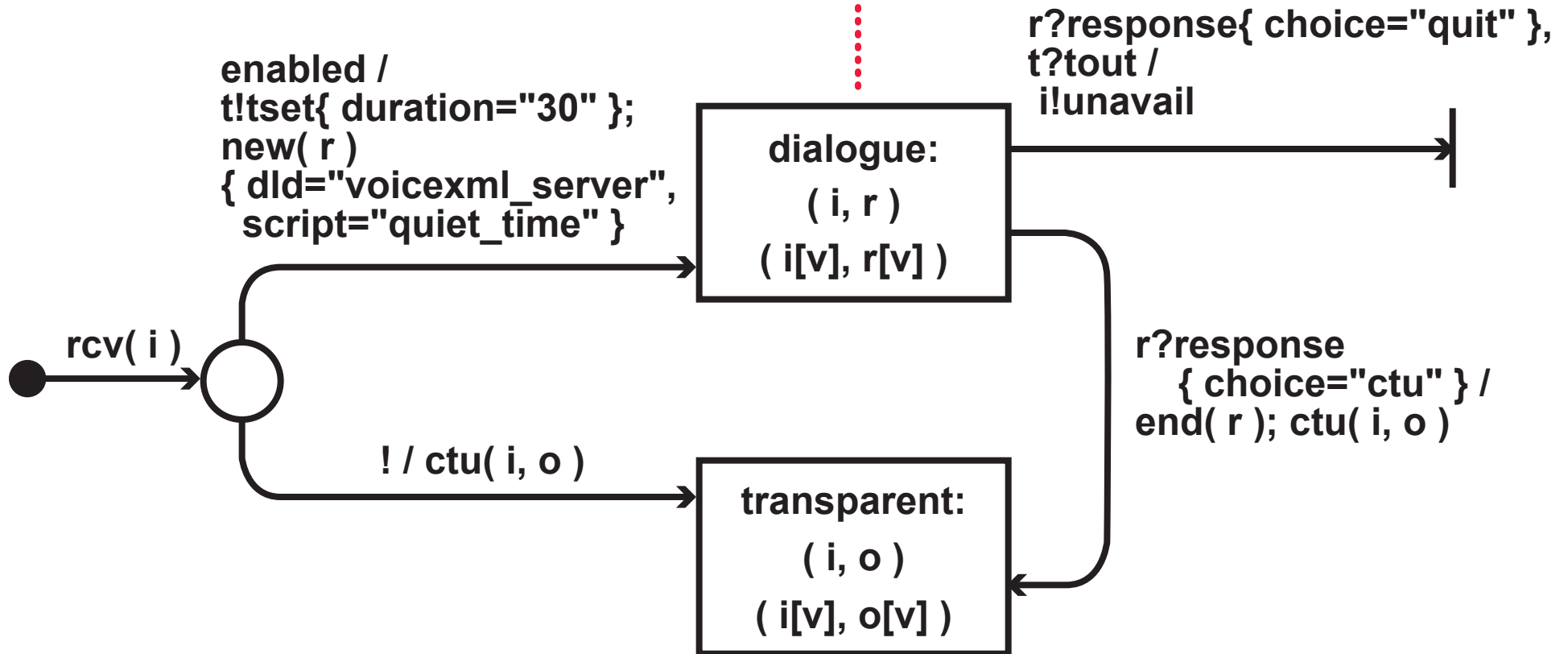
box generates unavail
under many different
circumstances



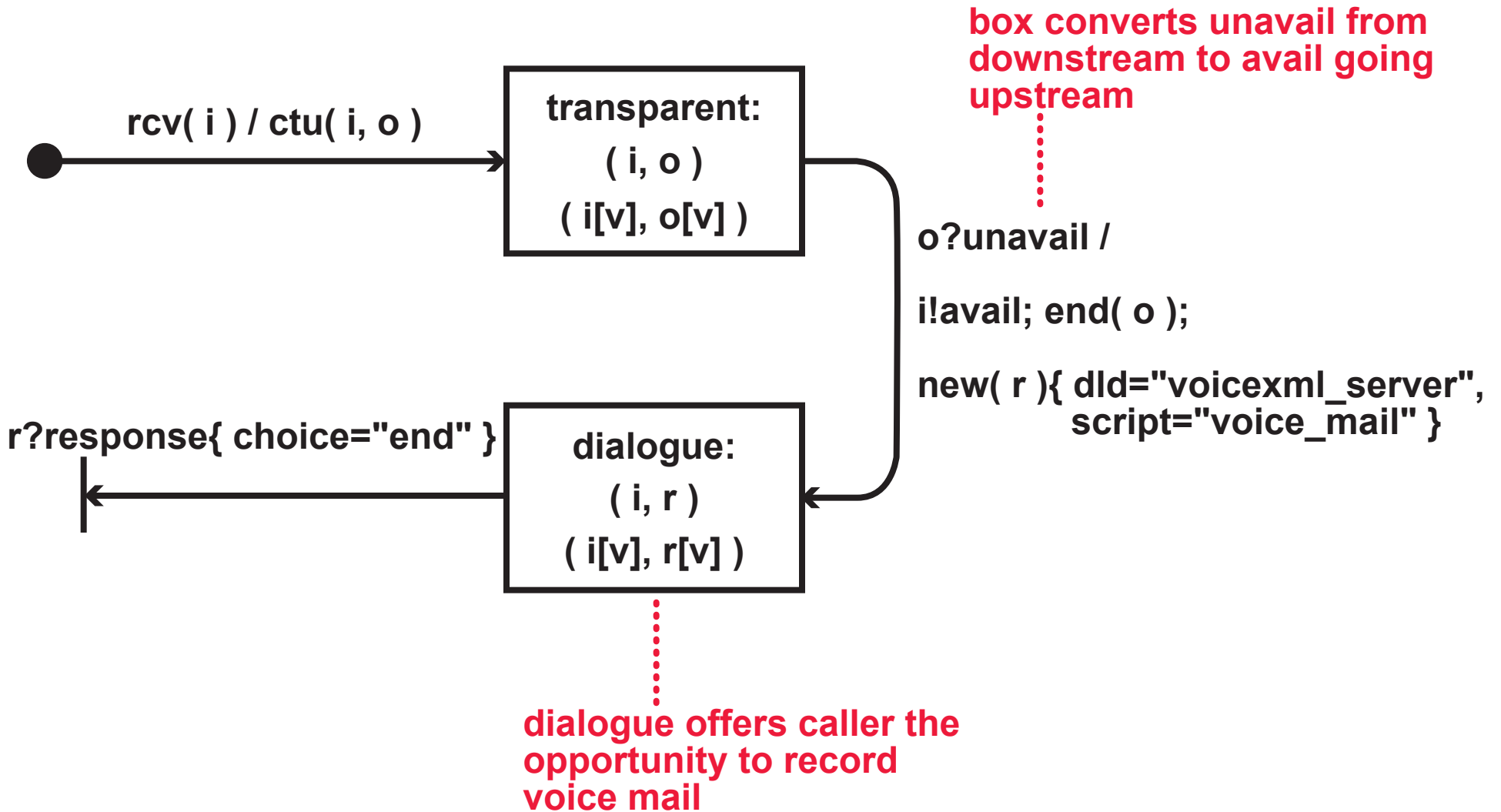
FREE BOX: QUIET TIME

dialogue says that the subscriber wishes not to be disturbed, prompts caller to leave a message (choice "quit") or interrupt the subscriber (choice "ctu")

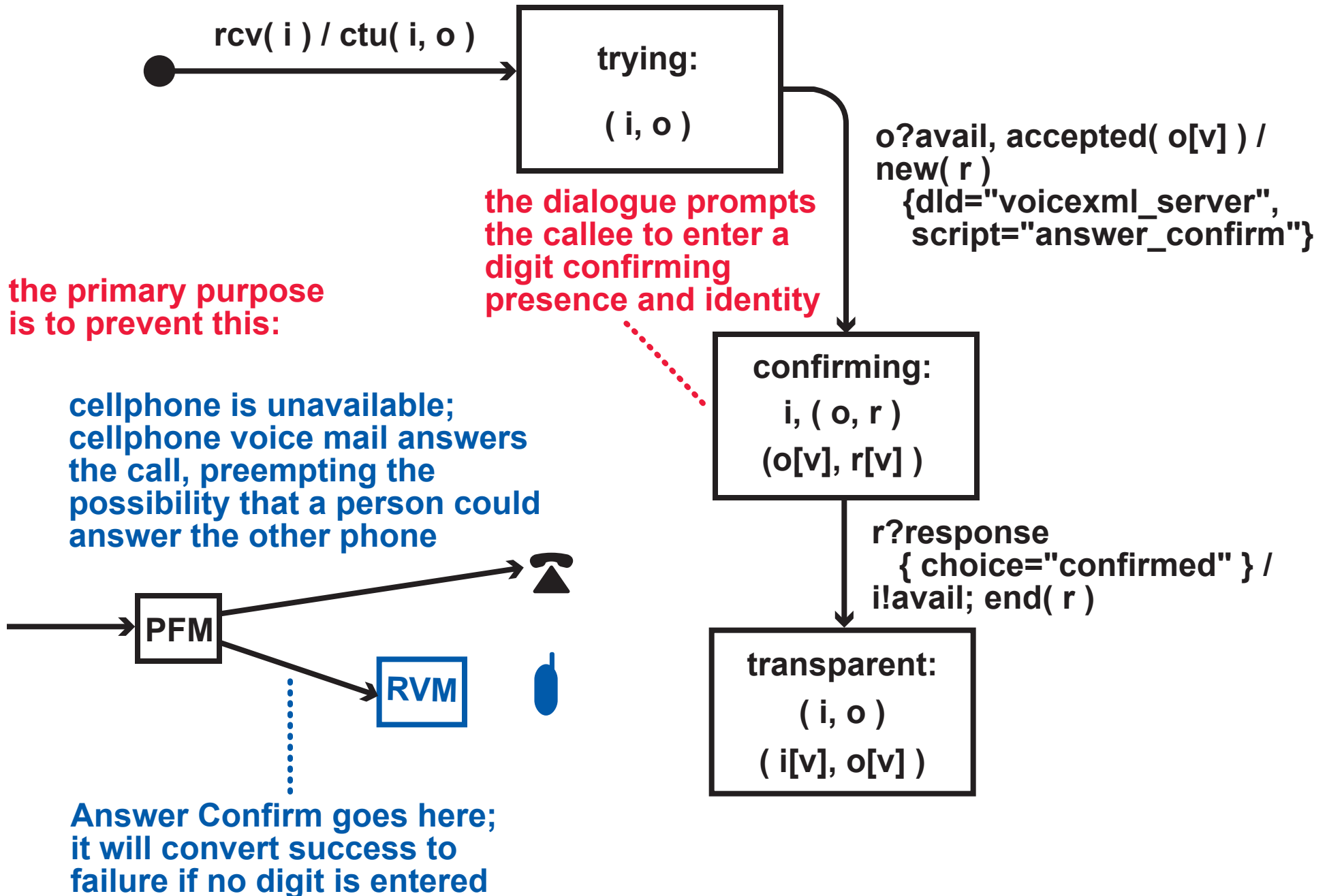
box generates unavail



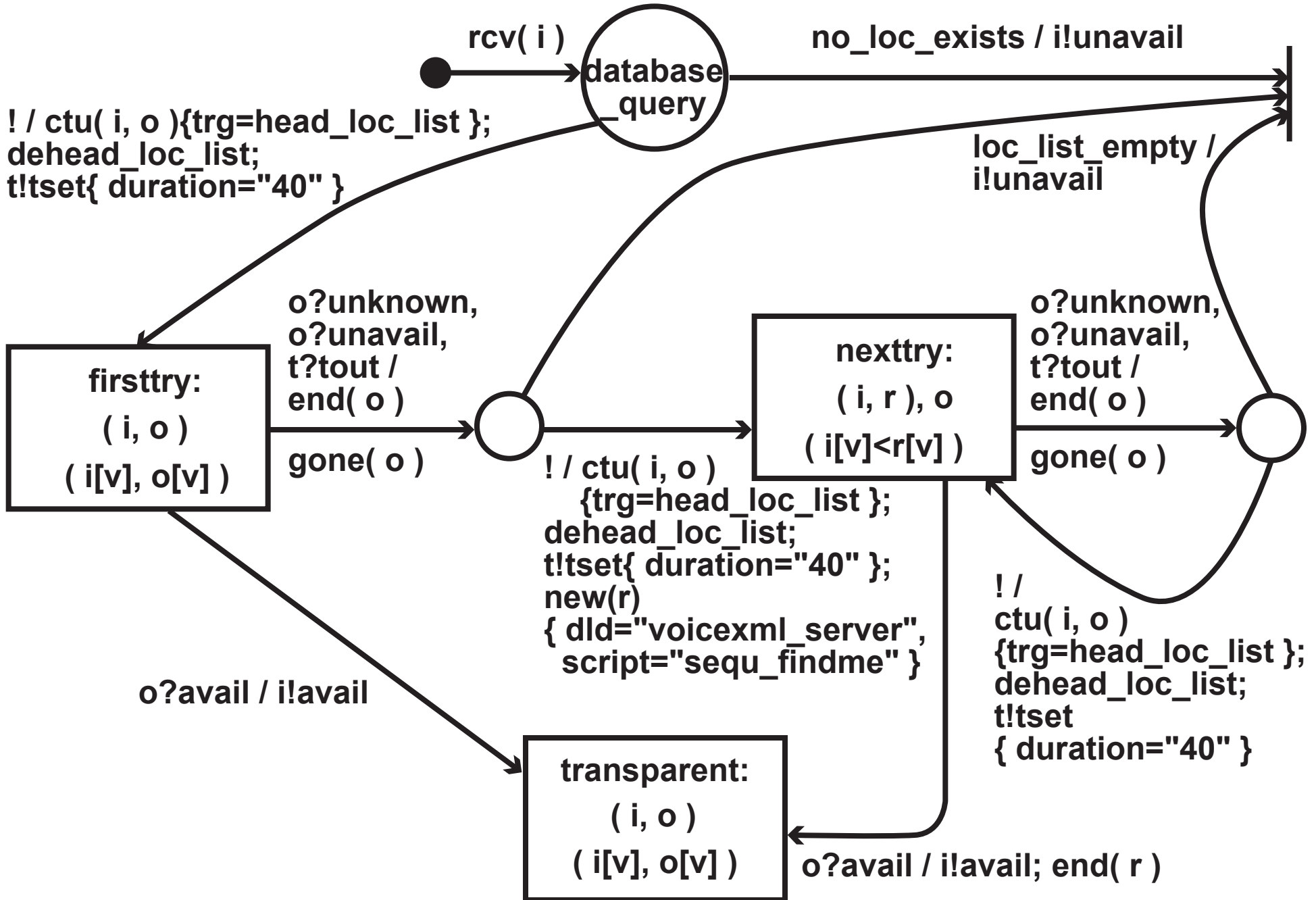
FREE BOX: RECEIVE VOICE MAIL



FREE BOX: ANSWER CONFIRM



FREE BOX: SEQUENTIAL FIND ME



VERIFICATION CHALLENGES

A COMPLETE SPECIFICATION OF A FEATURE SET BASED ON THESE PROGRAMS MUST ALSO INCLUDE:

- a precedence partial order on the feature box types AC, PFM, QT, RVM, SFM
- constraints on which addresses can subscribe to which features
- constraints on the addresses used by Find Me features

WE CONSIDER THE INTERACTIONS AMONG THESE FEATURES THAT ARE GOVERNED BY GENERAL PRINCIPLES, NOT PERSONAL CHOICE

CHALLENGES

- Within the boundaries of this study, what are the correctness criteria for feature sets?
- Complete the specification of a feature set based on these programs, and prove that it satisfies the correctness criteria.
- Devise constraints on box behavior, precedence, subscriptions, and operational data that guarantee the correctness criteria.
- Prove that the design constraints guarantee correctness.
- Show that the design constraints allow reasonable features to do their jobs.

I DO NOT KNOW THE ANSWERS!