Communicating via CAFCR; illustrated by security example

-

Gerrit Muller

University of South-Eastern Norway-NISE

Hasbergsvei 36 P.O. Box 235, NO-3603 Kongsberg Norway

gaudisite@gmail.com

Abstract

One of the main bottlenecks of developing complex products is communication between the many involved stakeholders. The "CAFCR" model is explained as one of the means to help communicating. The views of the "CAFCR" model are integrated amongst others by many qualities. This is illustrated by means of a mobile infotainment product and zooming in on the quality security.
The bilateral communication is analyzed and the importance of interaction for fruitful communication is explained

1 Introduction

The communication aspect of architecting is discussed by means of an example product: mobile infotainment, see figure 1. This product is much more than only the tangible appliance: portable infotainment device, a long food chain to connect the appliance with the outside world is needed. The product can be used to watch movies or other content anywhere anytime, or to browse and update a calender and many more applications.
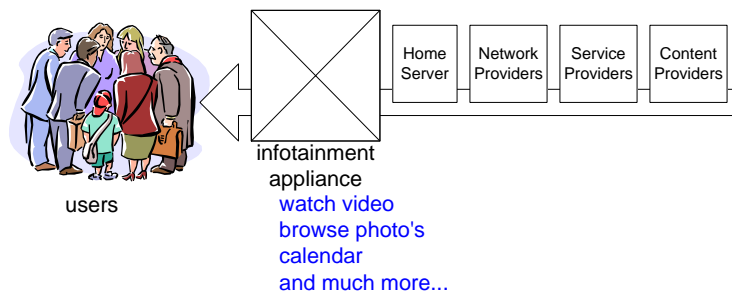

Figure 1: Example product: mobile infotainment

To make the example even more specific, the focus will be on security aspects. Of course many more aspects are important for this type of product, but security is especially interesting for communication due to the wide range of (often conflicting) concerns with respect to security.
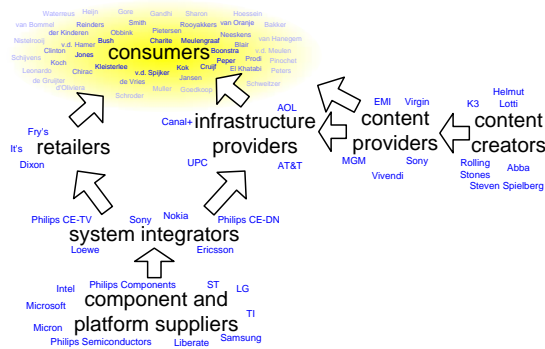
2 Stakeholders

Figure 2: Value chain

The producer of the appliance for mobile infotainment is part of a much larger value chain, see figure 2. The food chain starts at the suppliers of components and platforms, such as Philips Semiconductors, Intel, Symbian and many more. These components are integrated by the appliance makers, such as Philips Consumer Electronics, Sony, Nokia or Samsung. Via a distribution chain of retailers and providers the appliance is delivered to a wide variety of consumers.

Complementary to this part of the value chain are an infrastructure value chain and content value chain. All kinds of players in these chains are mutually dependent: without content no appliance, but also without appliances no content.
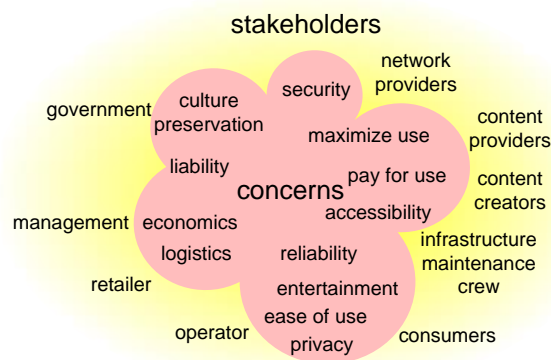

Figure 3: Stakeholders and concerns

Many stakeholders are involved in the creation of mobile infotainment. All of these stakeholders have multiple concerns, see figure 3. Although they use the

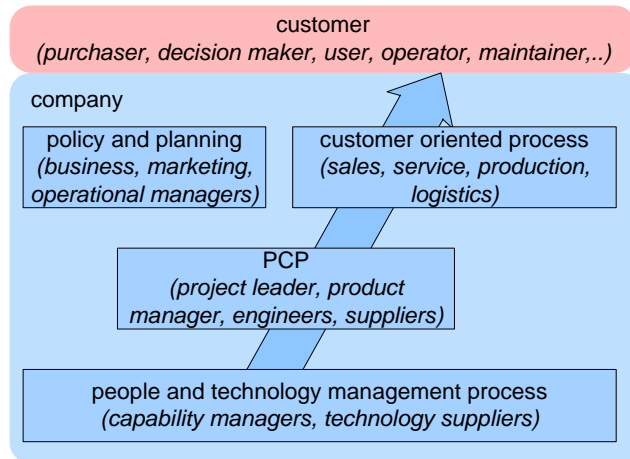same label for a given concern, every stakeholder has its own specific interest and view on such a concern.

Figure 4: Internal stakeholders

Figure 3 shows predominantly the external stakeholders, but many (company-) internal stakeholders are involved as well, as modeled in figure 4. The internal stakeholders are supportive for the overall business goal, their organization to support such a new product is part of the creation of a new product.

3   The "CAFCR" model and qualities

A useful top level decomposition of an architecture is provided by the so-called "CAFCR" model, as shown in figure 5. The *customer objectives* view and the *application* view provide the **why** from the customer. The *functional* view describes the **what** of the product, which includes (despite the name) also the *non functional* requirements. The **how** of the product is described in the *conceptual* and *realization* view, where the conceptual view is changing less in time than the fast changing realization (Moore's law!).
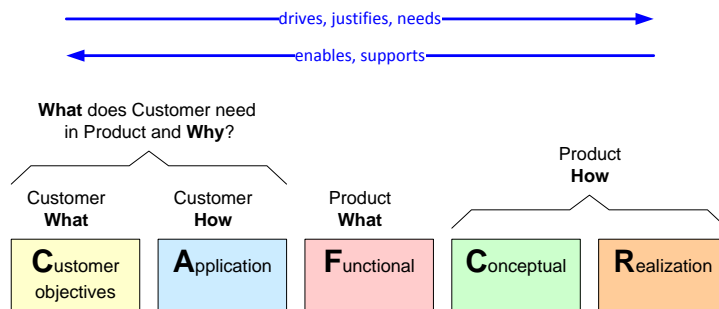

Figure 5: The "CAFCR" model

The job of the architect is to integrate these views in a consistent and balanced way. Architects do this job by *frequent viewpoint hopping*, looking at the problem from many different viewpoints, sampling the problem and solution space in order to build up an understanding of the business. Top down (objective driven, based on intention and context understanding) in combination with bottom up (constraint aware, identifying opportunities, know how based), see figure 6.

In other words the views must be used concurrently, not top down like the waterfall model. However in the end, a consistent story must be available, where the justification and the needs are expressed in the customer side, while the technical solution side enables and support the customer side.

The model is used to provide a next level of reference models and methods [4]. Although the 5 views are presented here as sharp disjunct views, many subsequent models and methods don't fit entirely in one single view. This in itself not a problem, the model is a means to build up understanding, it is not a goal in itself.

"**The** customer" is a tremendous abstraction. Many players are involved in the value chain, while in many cases a player is a small company, where multiple people are involved. Figure 7 shows an example of the people involved in a small company. Note that most of these people have different interests with respect to the system.

The 5 CAFCR views become more useful when the information in one view

Gerrit Muller   University of South-Eastern Norway-NISE
Communicating via CAFCR; illustrated by security example
September 9, 2018   version: 0.1   page: 4
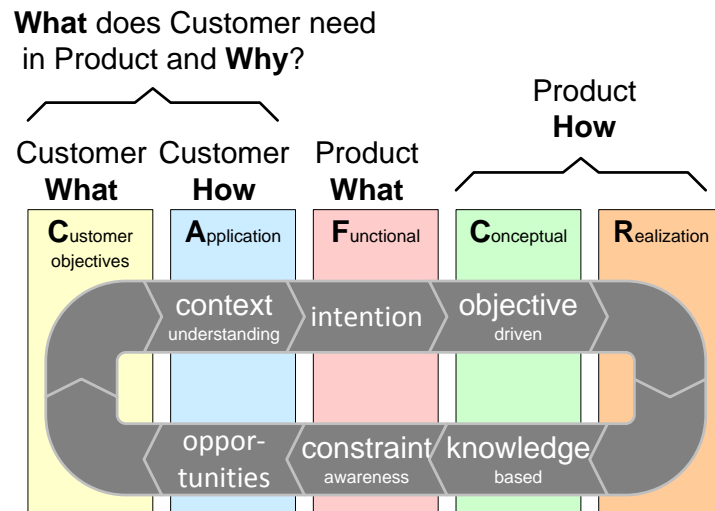
Figure 6: Five viewpoints for an architecture. The task of the architect is to integrate all these viewpoints, in order to get a *valuable*, *usable* and *feasible* product.

is used in relation with neighboring views. One of the starting points is the use of the stakeholder concerns. Many stakeholder concerns are abstracted in a large set of more generic qualities. These qualities are meaningful in every view in their own way. Figure 8 shows the qualities as cross cutting needles through the CAFCR views.

4 Zooming in on security

As an example figure 9 shows security issues for all the views. The green (upper) issues are the desired characteristics, specifications and mechanisms. The red issues are the threats with respect to security. An excellent illustration of the security example can be found in [2].

Customer objectives view

One of the typical customer objective with respect to security is to keep sensitive information secure, in other words only a limited set of trusted people has access. The other people (non trusted) should not be able to see (or worse to alter) this information.

Application view

The customer will perform many activities to obtain security: from selecting trustful people to appointing special guards and administrators who deploy a security policy. Such a policy will involve classification of people with respect to need of

CEO: Chief Executive Officer
CFO: Chief Financial Officer
CIO: Chief Information Officer
CMO: Chief Marketing Officer
CTO: Chief Technology Officer

CFO   CIO
CMO   CEO   CTO
decision maker(s)   purchaser

Who is **the** customer?

department head

chain of retailers

content provider

network provider

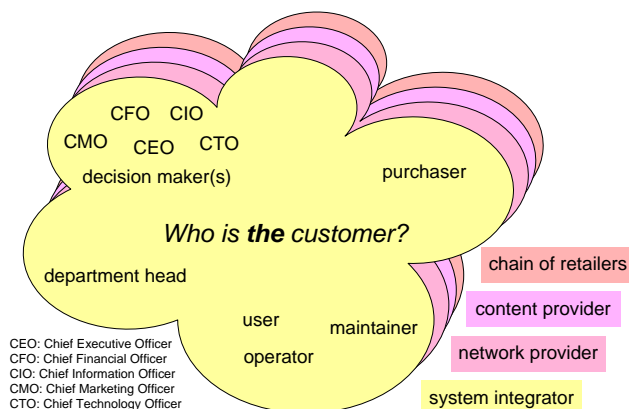user   maintainer

operator

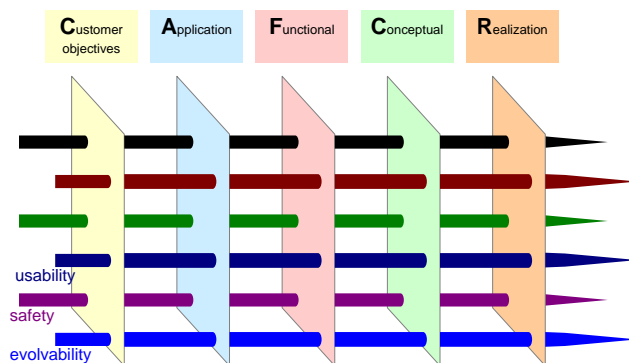system integrator

Figure 7: The abstracted customer

Figure 8: The quality needles are generic integrating concepts through the 5 CAFCR views

information and trustfulness and classification of information with respect to the level of security. To recognize *trusted* people authentication is required by means of badges, passwords and in the future additional biometrics. Physical security by means of buildings, gates, locks et cetera is also part of the customers security policy.

The security is threatened in many ways, from burglary to fraud, but also from simple issues like people forgetting their password and writing it on a yellow sticker. Social contacts of trusted people can unwillingly expose sensitive information, for instance two managers discussing business in a business lounge, while the competition is listening at the next table.

A frequent threat for security is formed by unworkable procedures. For instance the forced change of passwords every month, resulting in many people writing

Customer objectives	Application	Functional	Conceptual	Realization
sensitive information	selection classification	functions for	cryptography	*specific*
	people	administration	firewall	algorithms
	information	authentication	security zones	interfaces
trusted	authentication	intrusion detection	authentication	libraries
	badges	logging	registry	servers
	passwords	quantification	logging	storage
	locks / walls			protocols
	guards			
	administrators			

desired characteristics, specifications & mechanisms

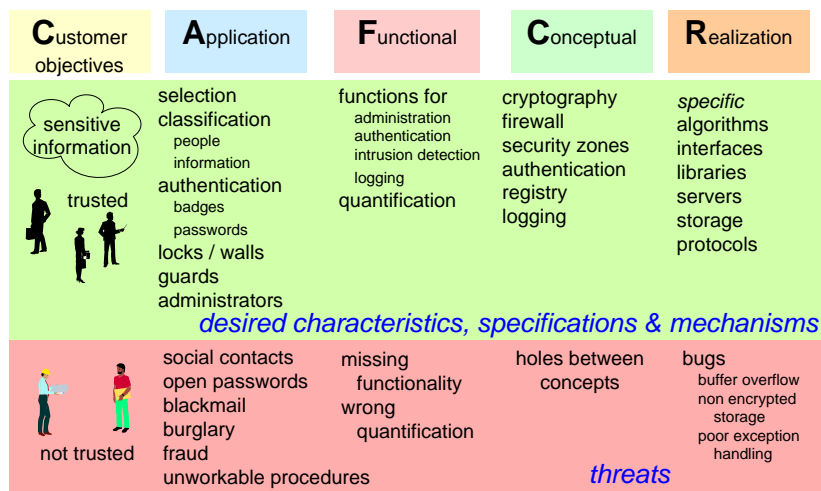|				
	social contacts	missing	holes between	bugs
	open passwords	functionality	concepts	buffer overflow
	blackmail	wrong		non encrypted
	burglary	quantification		storage
not trusted	fraud			poor exception
	unworkable procedures			handling

threats

Figure 9: Example security through all views

down the password.

An interesting article is [1], which shows how secret security procedures, in this case for passenger screening at airports, is more vulnerable. It describes a method for terrorists how to reverse engineer the procedures empirically, which turns the effectiveness of the system from valuable to dangerous.

Functional view

The system under consideration will have to fit in the customers security. Functions for authentication and adminstration are required. The performance of the system needs to be expressed explicitly, for instance the required confidence level of encryption or the speed of authentication.

Security threats are mostly caused by missing functionality or wrong quantification. This threat will surface in the actual use, where the users will find work around compromising the security with the work around.

Conceptual view

Many techological concepts have been invented to make systems secure, for example cryptography, firewalls, security zones, authentication, registry, and logging. Every concept covers a limited set of aspects of security. For instance cryptography makes stored or transmitted data non-interpretable for non trusted people.

Problems in the conceptual view are mostly due to the non ideal combination of concepts. For instance cryptography requires keys. Authentication is used to access and validate keys. The interface between cryptography and authentication is a risky issue. Another risky issue is the transfer of keys. All interfaces between the concepts are suspicious areas, where poor design easily threatens the security.

Realization view

Gerrit Muller
Communicating via CAFCR; illustrated by security example
September 9, 2018   version: 0.1

University of South-Eastern Norway-NISE

page: 7

The concepts are realized in hardware and software with specific algorithms, interfaces in specific libraries, running at specific clients and servers et cetera. Every specific hardware and software element involved in the security concepts in itself must be secure, in order to have a secure system.

A secure realization is far from trivial. Nearly all systems have bugs. Well known security related bugs are buffer overflow bugs, which are exploited by hackers to gain access. Another example is storage of very critical security data, such as passwords and encryption keys, in non encrypted form. In general exception handling is a source of security threats in security.

Security conclusion

Security is a quality which is heavily determined by the customers way of working (application view). To enable a security policy of the customer a well designed and implemented system is required with security functionality fitting in this policy.

In practice the security policy of customers is a large source of problems. Heavy security features in the system will never solve such a shortcoming. Another common source of security problems is poor design and implementation, causing a fair policy to be corrupted by the non secure system.
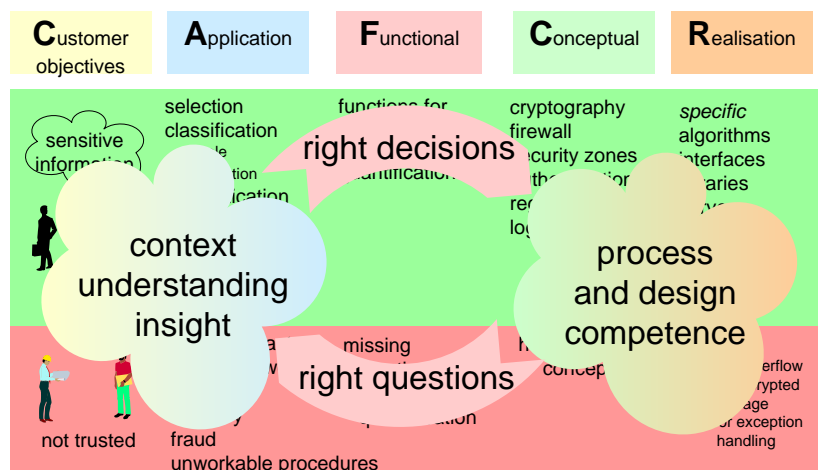

Figure 10: Role of views

Figure 10 visualize the reasoning with respect to security over the different views. Only if sufficient understanding of the context is combined with good process and design competences an acceptable result can be obtained.

Note that a very much simplified view on security is presented, with the main purpose of illustration. A real security view will be more extensive than described here.

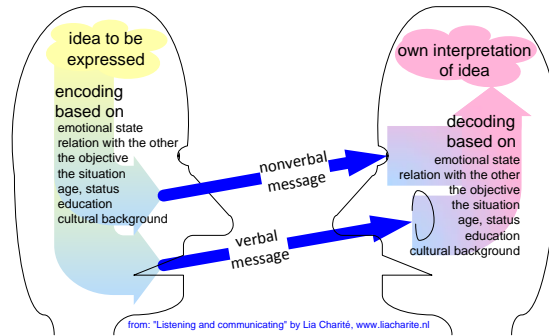# 5 The wonder of communication

Figure 11: Active listening: the art of the receiver to decode the message

If someone wants to transfer an idea to another person, then this idea is encoded in a message. This message is encoded by a variety of means, ranging from the verbal message to the non verbal message such as facial expression(s), gestures and voice modulation. The encoding of this message depends on many personal aspects of the *speaker*, see figure 11. The receiver of this message has to decode this message and makes his own interpretation, also based on many personal aspects of the *receiver*.

From technical point of view a pure miracle is happening in communication: sender and receiver use entirely different configured encoders and decoders and nevertheless we are able to convey messages to others.
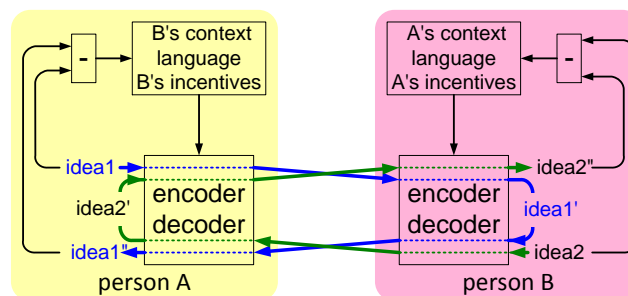

Figure 12: Intense interaction needed for mutual understanding

The mechanism behind this miracle can be understood by extending the model of sender and receiver as in figure 12. The mutual understanding is built up in an

interactive calibration process. By phrasing and rephrasing examples, illustrations and explantions the coding and decoding information is calibrated.
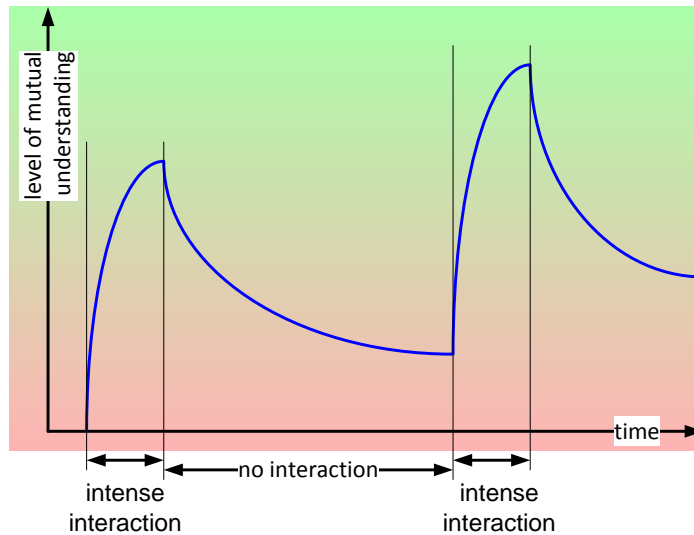

Figure 13: Mutual understanding as function of time

The calibration information is very dynamic, part of the coding depends on volatile issues, such as mood, and context. During interaction the mutual understanding improves, while it degrades as long as no interaction takes place, as visualized in figure 13.

Note that glossaries of terms, unified notations and all these kind of measures do not fundamentally address the communication difficulties explained here. In fact standardized terminology and notations are minor[1] in comparison with the human differences which have to be bridged continuously.

---

[1]Dogmatic applied unification of terms and notations work in my experience often counterproductive. Problems or viewpoints which are more easily expressed in other terms are disallowed due to the unification obsession, where active participation is required to obtain understanding that exceeds terms and notations.

6 Story telling

Story telling is a method to enable communication between people with different points of view. The method is a means to get discussions quickly a concrete and factual.
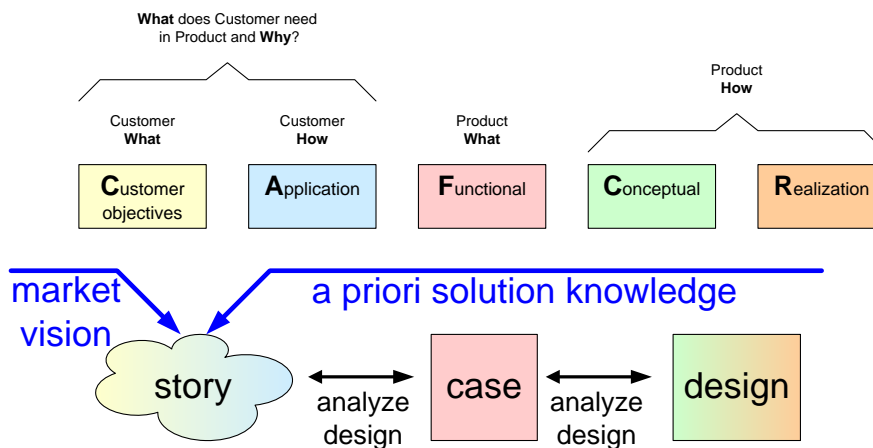

Figure 14: Story telling method

Figure 14 positions the story in the customer objectives view and application view. A good story combines a clear market vision with a priori realization know how. The story itself must be expressed entirely in customer terms, no solution jargon is allowed.

A story is a short single page story, preferably illustrated with sketches of the most relevant elements of the story, for instance the appliance being used.

The story is used to get case data in the functional view. All functions, performance figures and quality attributes are extracted from the story. This case data is used to make a design exploration.

The strength of the method is early focus on concrete actual problems and solutions. Once sufficient factual specification and design depth is obtained, it becomes time to determine useful generic concepts.
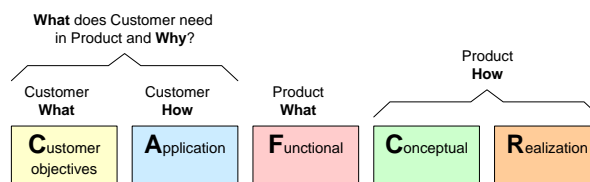
7 Summary

The previous chapters have shown that many stakeholders with many different concerns are involved. Also is shown how difficult a bilateral communication is. The challenge of developing a complex product, such as the mobile infotainment, is to communicate with many different stakeholders over many different subjects. Figure 15 summarizes this by showing a small subset of stakeholders, one of their most primary thoughts and the bad consequences if this thought is followed without taking other concerns into account.

stakeholder	primary thought	threat
consumer	privacy	kill usability
content provider	DRM, consumer == pirate	kill usability kill market
Chief Financial Officer	how to stay in control	kill usability
operational manager	result in time, accessibility	security
web engineer	PHP only supports alphanumerical password	poor password protection
crypto engineer	128 bit keys	no attention for key handling process

Figure 15: How do these stakeholders communicate?

Figure 16 summarizes the contribution of the "CAFCR" model in the communication.

CAFCR, as shared reference, enables:
+ Positioning of concerns, problems and solutions
+ Checklists per view
+ Reasoning top down and bottom up

Figure 16: Summary

8   Acknowledgements

Henk Koning helped by providing inputs in the initial setup of the presentation. The definition of active listening and the diagram of bilateral communication are reused from a presentation given by my wife Lia Muller for her psycho-social study. Peter van den Hamer proposed several textual improvements.

References

[1] Samidh Chakrabarti and Aaron Strauss. Carnival booth: An algorithm for defeating the computer-assisted passenger screening system. `http://swissnet.ai.mit.edu/6805/student-papers/spring02-papers/caps.htm`, 2002. Shows that security systems based on secret designs are more vulnerable and less secure.

[2] Charles C. Mann. Homeland insecurity. *The Atlantic Monthly*, pages 81–102, September 2002. Volume 290, No. 2T; Very nice interview with Bruce Schneier about security and the human factor.

[3] Gerrit Muller. The system architecture homepage. `http://www.gaudisite.nl/index.html`, 1999.

[4] Gerrit Muller. Architectural reasoning explained. `http://www.gaudisite.nl/ArchitecturalReasoningBook.pdf`, 2002.

History
Version: 0.1, date: October 17, 2002 changed by: Gerrit Muller
- added section on story telling
- textual improvements

Version: 0, date: October 11, 2002 changed by: Gerrit Muller
- Created, no changelog yet