

TELEMAC IST 2000-28156

Telemonitoring and Advanced Telecontrol of High-Yield Wastewater Treatment

*Final report on security issues  
in the light of experience in the project*

*Deliverable D5.1b*

---

*Deliverable type: Report*

*Number: D5.1b*

*Nature: Report*

*Date of delivery: 31st December 2004*

*Task: WP5.1*

*Responsible:*

*Simon Lambert*

*Business & Information Technology Department*

*CCLRC Rutherford Appleton Laboratory*

*Chilton*

*Didcot*

*Oxfordshire OX11 0QX*

*UK*

*Email: S.C.Lambert@rl.ac.uk*

*Other contributors:*

*Paolo Ratini*

*SPES srl*

*Via Broganelli 84*

*60044 Fabriano (AN), Italy*

*Email: Paolo.Ratini@spesonline.om*

*Laurent Lardon*

*INRA*

*LBE, Avenue des étangs*

*11100 Narbonne, France*

*Email: lardonl@ensam.inra.fr*

**Abstract:** This deliverable is the final report from task WP5.1, concerned with information security in the TELEMAC system. Following the earlier analysis reported in D5.1a, it analyses the measures that have been put into place during development of the TELEMAC system to deal with the security risks identified in that deliverable. Some methods from the IST project CORAS are used for the purpose. The conclusion is that the majority of security risks are adequately treated, though there are a few areas where further work would be desirable.

**TABLE OF CONTENTS**

<b><u>1</u></b>	<b><u>INTRODUCTION</u></b> .....	<b>4</b>
<b><u>2</u></b>	<b><u>SUMMARY OF EARLIER WORK ON SECURITY ISSUES</u></b> .....	<b>6</b>
<b><u>3</u></b>	<b><u>REVISITING THE EARLIER RISK ANALYSIS</u></b> .....	<b>8</b>
<b><u>4</u></b>	<b><u>APPROACH TO BE APPLIED</u></b> .....	<b>11</b>
4.1	<u>THE CORAS PROCESS APPLIED TO TELEMAC</u> .....	11
4.2	<u>ACTIVITIES IN RISK TREATMENT</u> .....	11
<b><u>5</u></b>	<b><u>APPLYING THE APPROACH</u></b> .....	<b>14</b>
<b><u>6</u></b>	<b><u>CONCLUSIONS</u></b> .....	<b>20</b>

## 1 Introduction

This deliverable is the final result of task WP5.1, which is concerned with information security in the TELEMAC system. TELEMAC, like many systems that support process automation or manufacturing, relies for many of its benefits on being a composite of distributed systems working together. The benefits for anaerobic digestion arise from access to a network of remote experts through the Telecontrol Centre (TCC) will make the running of the plants more efficient and less demanding of local expertise which is often not available. The drawback of course is that distributed systems are susceptible to network failure and attack, with potentially serious consequences.

In order to take account of this important issue, the TELEMAC project has dedicated a task, WP5.1, to analysis of security issues. As the Description of Work remarks, 'It is important to recognise that information security refers not only to network security, for example, the risks that arise through loss of data in case of network failure, but also to issues such as control of access, protection of sensitive data, data integrity, and authorisations to access resources according to roles.' To ensure correct treatment of these issues, two deliverables have been produced in the scope of this task. The first, D5.1a, was submitted in September 2002, one year into the project. It aimed to systematically identify major security concerns, to analyse and prioritise them, and to make recommendations for the future development within the project. Some approaches and methods from the IST project CORAS (A Platform for Risk Analysis of Security-Critical Systems, IST-2000-25031, January 2001–June 2003) were applied for this purpose.

The results of this analysis fed into the system development in the subsequent phases of the project. The leading partner concerned with developing the TELEMAC integrated system, SPES, took into account the recommendations of D5.1a and had ongoing discussions with the responsible partner, CCLRC. As will be summarised in section 5 of the present deliverable, a number of security measures were put in place during design and implementation, responding directly to the recommendations of D5.1a.

The present deliverable, D5.1b, has the main aim of validating the work done against the analyses and recommendations of D5.1a. D5.1a stated: 'The extent to which the security issues identified have been addressed during development will be assessed and reported in deliverable D5.1b, due towards the end of the project. It is expected that the findings of this deliverable will be continually refined in consultation with several partners in the project, particularly those with expertise in anaerobic WWTP and those involved in the system development.' Indeed this interaction has taken place: discussions have gone on between the partner principally responsible for software integration (SPES), those with special expertise in particular risks of the anaerobic digestion process (INRIA, INRA, ENEA) and the partner responsible for D5.1a and D5.1b (CCLRC).

However, in order to make this validation a meaningful exercise, it is also necessary for D5.1b to revisit some of the analyses that were made earlier. There have been some architectural changes since the earlier analyses were performed, and it is necessary to take these into account, so that there is a correspondence between the recommendations and the reality that has been implemented. The basis for this deliverable has been the final TELEMAC integrated system as reported in D5.3c ('Final functioning middleware and integrated systems on pilot sites ') and D5.3d ('Customisable software and final report on TELEMAC software'). The later-stage CORAS techniques have been applied, appropriate for assessing risk treatment options.

This deliverable is therefore intended to offer a clear assessment of the final state of the TELEMAC integrated system with respect to information security. It is not an academic exercise, but aims to show where the implemented system has responded to security risks and where any weak points might still remain.

As well as D5.3c and D5.3d, the deliverable. D4.5, the final supervision system module, is also relevant to the present deliverable. It includes an account of work on the use of hybrid (continuous and discrete) models which can be applied to situations where data might have been missing due to loss of connection to the TCC. This addresses one of the risks identified in the analysis. See also section 5 for connections to other deliverables.

## 2 Summary of earlier work on security issues

The deliverable D5.1a presented a characterisation of security properties and processes. These form a general framework for categorising and analysing security concerns. The security properties were listed as:

- confidentiality;
- integrity;
- availability;
- accountability;
- fairness.

This was followed by an introduction to the CORAS methods and approach. The basic CORAS risk management process is shown in Figure 1. From the perspective of D5.1a, the most important phases were identifying context, identifying risks and analysing/evaluating risks. The final phase, risk treatment, was only briefly touched on. It was pointed out that ‘At this stage of the TELEMAC project, the aim is to identify important risks and prioritise them, thus making recommendations for future system development.’

Deliverable D5.1a took the outline of the TELEMAC integrated system architecture as it then was and applied some particular risk analysis techniques. Risks were identified in terms of *assets*—not necessarily meaning physical or monetary assets, but also encompassing intangible assets such as loss of reputation. Risks were identified using the FMECA and HazOp methods, resulting in tables of specific risks. Using FMECA, failures in system entities and their consequences were identified. Using HazOp, deviations in communications between components with their causes and consequences were analysed.

A digression was made on specific risks in the anaerobic digestion process, concentrating on failures and the associated costs. For example, the costs resulting from a decrease in COD removal efficiency due to erratic plant management were estimated. The conclusion was that there is a considerable variety of consequences that are possible from the specific risks to the operation of an anaerobic WWTP. Some of these can be quantified more readily than others. Some risks, though not directly quantifiable, may ultimately have effects that can be measured: for example, the effects on a company’s share price if it is perceived to be careless with regard to environmental protection.

The conclusions of the deliverable were presented as a table and a set of general recommendations for system development. These recommendations are reproduced here for reference.

- The consequences of failure of individual TELEMAC components (hardware and software) at the plant should be studied, to see how robust the overall system is.
- Attention should be paid to poorly performing components; this is related to validation of the system, being considered elsewhere in the project.
- Another validation-related issue is the stability of the behaviour of the system in case of short-duration loss of access by the local technician or TCC.
- Authentication mechanisms for access by a remote expert should be put in place. Possibly data transmitted should be encrypted.

On this basis the system development and integration proceeded, resulting in the final system as presented in D5.3c and D5.3d.

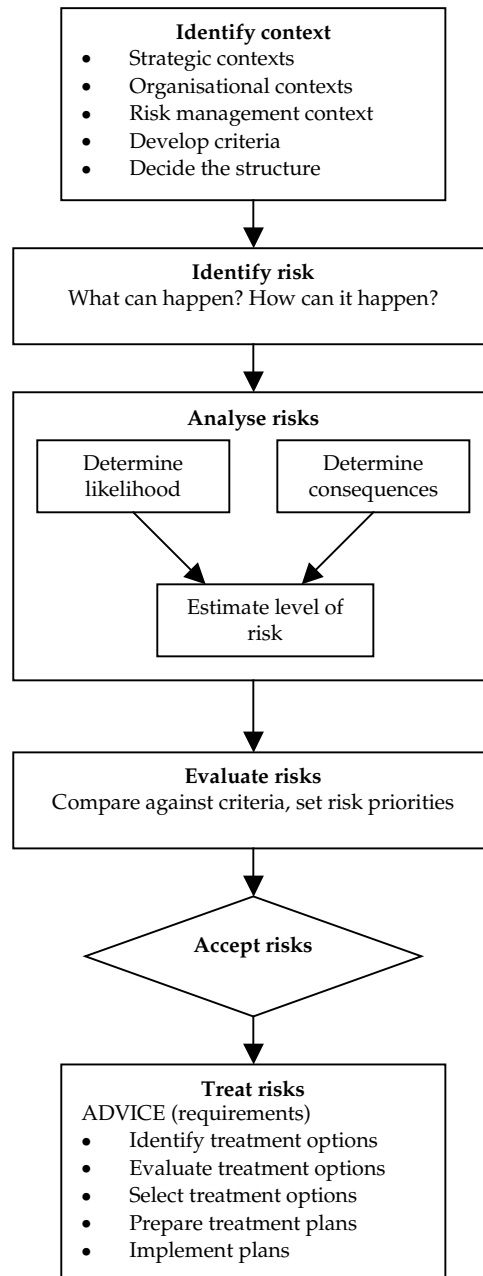


Figure 1: The basic CORAS risk management process

### 3 Revisiting the earlier risk analysis

Since deliverable D5.1a was produced, the architecture of the TELEMAC integrated system has been refined in the light of experience in the project. The abstracted TELEMAC system architecture presented as Figure 2 in D5.1a placed more emphasis on the existence of components such as sensors, actuators and models, and less on the communication between physically separate subsystems. In particular, as explained in D5.3c, there are two variants of the Pellucid integrated system, according to whether or not there is a pre-existing control system at the plant. Furthermore, the idea of remote MySQL queries to the databases (local and remote) was introduced. This has strong advantages, explained in section 3.2 of D5.3c, but introduces new aspects into the security analysis.

Figure 2 illustrates the final form of the abstracted TELEMAC system architecture, combining the two variants mentioned above. A number of points are worth noting.

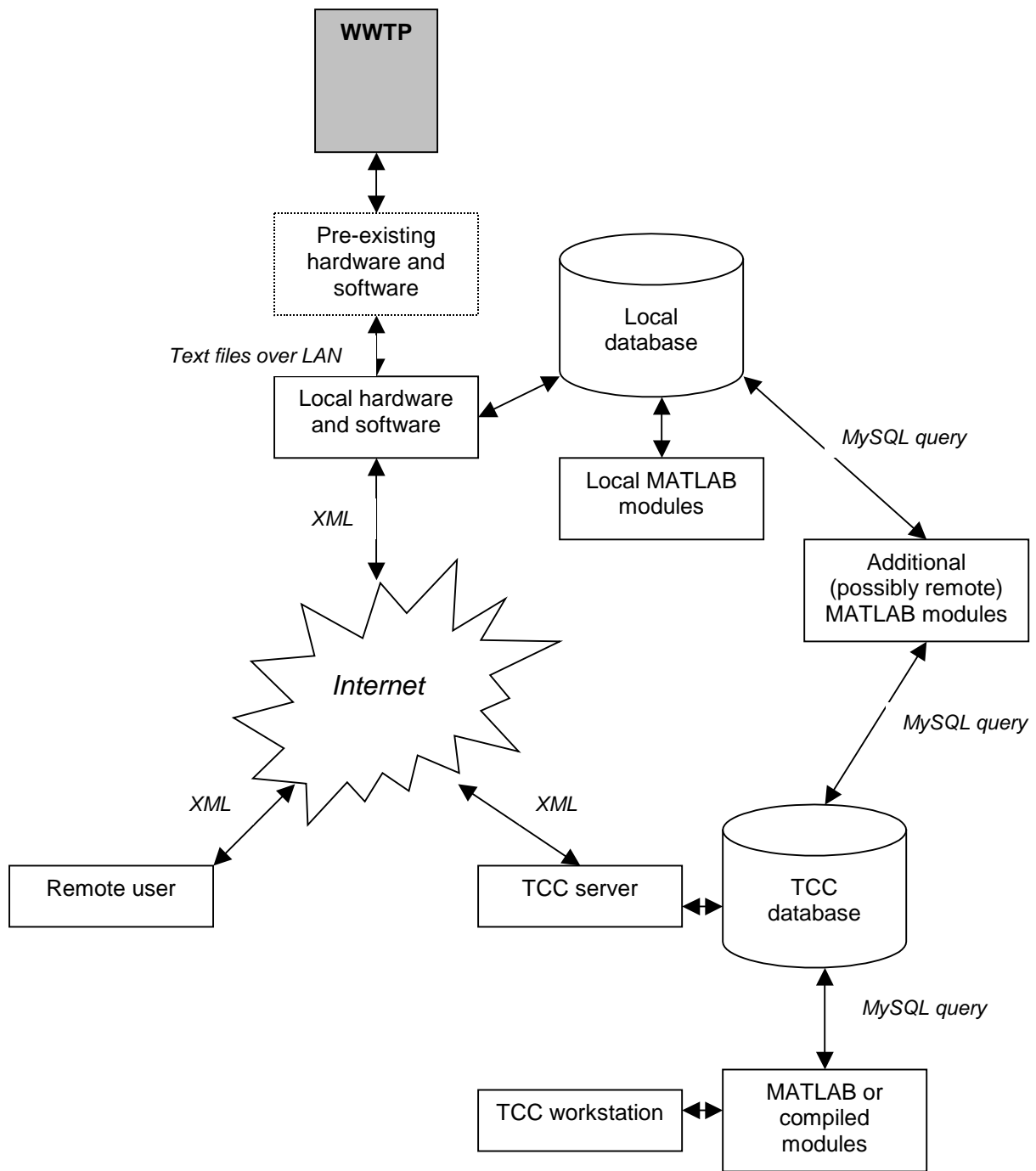
- The components labelled ‘MATLAB modules’ have been introduced explicitly in this version of the diagram. The local MATLAB modules are those that implement the standard TELEMAC supervision and control functions at the local level (that is, without involvement of the TCC). The additional MATLAB modules may be running either locally or remotely (not necessarily at the TCC)—this gives additional flexibility for testing the modules as well as running them without needing installation on the local plant. The MATLAB modules at the remote level are those that perform TCC-level functions, a typical example being data mining.
- As well as communication over Internet, using XML as the exchange format, the diagram takes into account the possible use of MySQL query at both local and remote levels. In effect, this offers an alternative means of communication between TELEMAC components.
- As in the original scheme, the local database stores data only for the associated plant; the TCC database stores data for multiple plants and over longer timescales.

Recall that the CORAS process consists of five stages:

Identify context – Identify risks – Analyse risks – Evaluate risks – Treat risks

In D5.1a, most emphasis was placed on the first three stages, and to a lesser extent the fourth stage. The last stage, ‘Treat risks’, was addressed by making recommendations on prioritisation of the risks to be addressed during the TELEMAC system development.

In the present deliverable, the results of analysis and evaluation will be revisited and modified to reflect the changes to the architecture. The key result is a table of grouped risks with their severity. The risks have been grouped in order to make them more manageable; the detailed analyses performed with such methods as FMECA and HazOp result in lengthy lists of risks (deviations, failures, ...), and in order to analyse these further it is necessary to impose some structure on them. The approach taken for this deliverable has been to take the table of grouped risks from D5.1a and modify it directly, rather than repeating the detailed analyses. This is considered satisfactory for the purpose.



**Figure 2: Revised abstracted TELEMAC system architecture**

The following table shows the grouped risks assessed in the light of the revisions to the architecture. Note that it does not cover risks arising from components outside the TELEMAC system itself. This was explained in terms of system boundaries in D5.1a: the anaerobic digester itself is not part of the system being considered, nor is the pre-existing control system, nor are the human actors in the system—the local technician, telecontroller and (possibly) remote expert.

<b>Risk theme</b>	<b>Severity</b>	<b>Remarks</b>
TELEMAC component failure (local level, including MATLAB modules)	Medium–high	
Communication failure at local level	High	Unlikely in the case of processes running on the same hardware
Poorly performing TELEMAC components at local level	Medium–high	The detection of poor performance is addressed in deliverables D4.3, D4.4 and D4.5
Unauthorised access at local level	High	An unqualified or malicious person controlling the plant locally could have serious effects
Loss of communication WWTP–TCC	Medium	Decision to locate as much diagnostic/control functionality as possible at local plant will alleviate effects
TELEMAC component failure (remote level)	Low–medium	As above
Poorly performing TELEMAC components at TCC	Low–medium	As above
Functioning of TCC server compromised	Medium–high	For example, hacking or denial of service attacks
Loss of communication with databases by remote MATLAB modules	Low	Remote MATLAB modules unlikely to be critical to system functioning (being tested, additional service)
Unauthorised access at TCC	High	
Interception or hijacking of session TCC–WWTP by external party	Medium–high	Implications for revealing data to outside world Hijacking differs from interception in that the external party is actually changing the communication, rather than just intercepting it Possible severe consequences, but considered unlikely
Loss of communication remote expert–TCC	Low	Remote expert has no direct access to local plants
Impersonation of remote expert by external party, or hijacking of session	Low–medium	As above, but confidential data might be revealed

Note that the first column of the table has been renamed ‘Risk theme’ rather than ‘Risk group’ as in D5.1a. This is more compatible with CORAS terminology (‘risks are classified into themes, based on the common characteristics of the risks. The reason for doing this classification is that it is more effective and efficient to address risk themes than it is to address each risk individually’ (CORAS D4.1, ‘Process Guidelines’).

Note that two risk themes from the table in D5.1a have been omitted in this new table: ‘Loss of local technician’s access’ and ‘Loss of telecontroller’s access’. This is because they may be treated under TELEMAC component failure at the local/remote level—for example, user interface failure or inability to log on.

The next step is to apply the CORAS risk treatment methods to these risk groups, with a view to comparing the options with what has actually been implemented in the project.

## 4 Approach to be applied

### 4.1 The CORAS process applied to TELEMAC

The IST project CORAS (IST-2000-25031) developed a framework to support security risk analysis. The aim was not to invent new ways of conducting risk management (risk analysis), but rather to base the process guidelines on well-known risk management and information security standards. The framework is based on the synthesis between:

- an appropriate combination of risk analysis methods adapted to the security critical systems domain;
- viewpoint-oriented modelling following the RM-ODP standard and realised using graphical semiformal methods.

In order to facilitate the effective use of the CORAS framework, the CORAS project developed a corresponding process. This is an integrated risk management and development process, which describes the context in which the CORAS framework is used. Within TELEMAC, the full CORAS process has not been used. Instead, a selection of methods have been applied at appropriate stages of the development lifecycle.

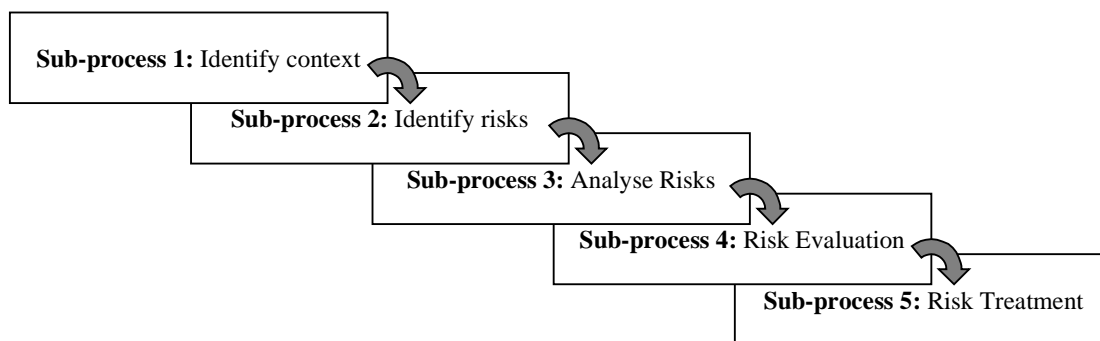


Figure 3: Overview of the CORAS risk management process

In a system development undertaken according to the full CORAS process, risk treatment would be performed as an integral part of the development during the elaboration and construction phases. In TELEMAC, the situation is somewhat different. The design and implementation of the system has been carried out with regard to the risks identified in D5.1a, and taking advantage of some common methods for security and risk reduction, as will be explained in section 5. D5.1a took the CORAS process up to the stage of risk evaluation, and now the final system will be compared with the results from the risk treatment sub-process. The aim is not to give the developed system a ‘pass’ or ‘fail’ mark, but simply to throw light on which risks are adequately covered and which may require further treatment during the exploitation phase following the project.

### 4.2 Activities in risk treatment

The risk treatment sub-process comprises two activities:

- Activity 5.1: Identify treatment options
- Activity 5.2: Assess alternative approaches

#### Activity 5.1: Identify treatment options

**Objective:** This activity includes the development of candidate approaches for mitigating the high-priority risks and themes. Candidate approaches, which are not necessarily mutually or appropriate in all circumstances, include the following:

- *Risk avoidance:* risk can be avoided by deciding not to proceed with the activity likely to generate risk.
- *Reduction of likelihood:* the likelihood of occurrence of ‘risk’ events may be reduced by reducing threats or vulnerabilities.
- *Reduction of consequences:* the consequences of ‘risk’ events may be reduced by reducing threats or vulnerabilities or modification of the asset at risk in some other way.
- *Risk transference:* another party can bear or share some part of the risk. Mechanisms include the use of contracts, insurance agreements and organizational structures.
- *Risk retention:* after unacceptable risks have been reduced or transferred, there may be residual risks that are retained.

**Methods, Techniques and Tools:** The identification of candidate approached for the treatment of risks and themes involves the consideration of existing and missing policies and practices, threats, assets, vulnerabilities and available technologies.

**Modelling:** Supports the formalization of new requirements and policies. May also be used to specify needs with respect to testing and monitoring.

**Input:** Priority list of risks and themes, threat list, assets list, existing security policies

**Output:** Treatment options for each risk/theme

**Persons involved:** Security experts, system administrators, management.

#### **Activity 5.2: Assess alternative approaches**

**Objective:** In this activity, after candidate mitigation approaches have been agreed upon, a search for potential solutions is conducted.

**Methods, Techniques and Tools:** Alternatives should be rated with criteria such as the following:

- ability to address information security requirements.
- ability to address information security risks.
- applicability to the organization’s existing information infrastructure.
- associated cost.
- impact to the organization.

**Modelling:** Provides a foundation for the assessment.

**Input:** information security requirements, candidate approaches, cost of solutions.

**Output:** list of potential solutions.

**Persons involved:** security experts, system administrators, management.

Within each of the treatment options the following approaches are possible:

- Changes to security requirements;
- Changes to security policy (including organisational routines);
- Changes to the system architecture (including security architecture);
- Strategies for testing;
- Strategies for monitoring, for example in the form of intrusion detection.

The following table is provided for evaluating risk treatments. Each risk theme may have one or more treatment options, implemented through particular approaches. These options will meet the evaluation criteria to various degrees, by reducing the risk in certain ways. They will have particular costs and benefits.

<b>Risk Theme (or Risk)</b>	<b>Treatment option</b>	<b>Approach</b>	<b>Evaluation criteria met</b>	<b>Risk Theme/Risk reduction</b>	<b>Benefit</b>	<b>Cost</b>
<..>	<..>	<..>	<Yes, No, Partly, N/A>	<Reduction>	<Benefit>	<Cost>

In the context of TELEMAC, the treatment options considered are those that have actually been adopted during the system development.

## 5 Applying the approach

Before applying the approach in detail, some general remarks will be made about the security measures that haven been put in place during the TELEMAC integration.

- Remote users log on with a user name and password. Attempted logins are recorded, including the IP address.
- The database records actions that have been performed, providing an audit trail.
- The local software has some access control to regulate access of different local users to different features.
- The TCC server could be set up with a firewall. Two ports must be opened: port 80 (standard HTTP) and port 3306 (for query to MySQL database). Access to the MySQL database is password controlled.
- If there is a loss of connection, there are two possibilities: either an auto-restore of the previous configuration, or the operator is alerted and sets the parameters himself.
- XML is received by the plant from the TCC in complete form, and is compliant with the structure of the database, so it is intrinsically safe—there can be no arbitrary interruption.
- If MATLAB crashes it could in theory crash the C++ shell. A monitor system called WatchDog checks for this occurrence, saves the parameters and restarts the machine.

Furthermore, three particular components have has special consideration to issues of risk and security.

- Anasense sensor: the risk is reduced by the very robust design of the sensor (D2.4). In case the sensor is down it should be detected by the supervision system (D4.3), and the local operator should manage the problem. Other strategies are then deployed based on the remaining working sensors (gas sensors, pH, ...) and based on sensor network analysis (see D4.4).
- Gas sensor: likewise the design is very robust (D2.4). The sensor accuracy is on-line estimated (D2.2). In case the sensor is down it should be detected by the supervision system (D4.3) and an alert to the local operator will be sent.
- Implemented algorithms: the results provided by the automatic controllers or by the software sensors are on-line estimated. If they turn out to be not appropriately working they are automatically disconnected and another algorithm is chosen. If none of the algorithms achieves a convincing working mode the process automatically goes down to open loop and an alert to a remote expert is sent (deliverable D4.3).

Bearing these in mind, we will now proceed to evaluate the risk treatments using the tabular form introduced above. The table has been reset for greater legibility.

<b>R1</b>	
<b>Risk theme</b>	TELEMAC component failure (local level, including MATLAB modules)
<b>Treatment option</b>	1. Reduction of likelihood 2. Reduction of consequences
<b>Approach</b>	1. Validation of components at local level prior to integration 2. Automatic restart of TELEMAC system in event of crash
<b>Evaluation criteria met</b>	Partly
<b>Risk reduction</b>	1. Provides some assurance of robustness of components in isolation.

	However, their functioning as a whole is not known. There might be unexpected interferences, or the failure of a sensor (for example) might cause more serious consequences in controllers. 2. Ensures that the system is never totally unavailable.
<b>Benefit</b>	Confidence in robustness of individual components at local level and basic recoverability of the local system.
<b>Cost</b>	Cost mostly borne in TELEMAC project itself, though some testing will be required for future installations.

<b>R2</b>	
<b>Risk theme</b>	Communication failure at local level
<b>Treatment option</b>	Risk retention
<b>Approach</b>	No special measures taken to ensure communication at the local level
<b>Evaluation criteria met</b>	Yes
<b>Risk reduction</b>	Although the severity of this risk was assessed as high, it is considered of low probability. In fact the WatchDog system mentioned above provides some protection against a complete failure and crash of the system.
<b>Benefit</b>	N/A
<b>Cost</b>	None

<b>R3</b>	
<b>Risk theme</b>	Poorly performing TELEMAC components at local level
<b>Treatment option</b>	Reduction of likelihood
<b>Approach</b>	As for the first risk in this set, the key is validation of individual components. The same caveat applies about interactions. However, the work done in the project in WP1 on experimentation and validation gives confidence in the functioning of the overall system. There is automatic assessment of the component performances (deliverable D4.3) and warning an expert in case of threshold reached.
<b>Evaluation criteria met</b>	Partly
<b>Risk reduction</b>	Provides some assurance of quality of performance of components in isolation, and that there is a mechanism for handling poor performance.
<b>Benefit</b>	Confidence in performance of individual components at local level.
<b>Cost</b>	Cost mostly borne in TELEMAC project itself, though some testing will be required for future installations.

<b>R4</b>	
<b>Risk theme</b>	Unauthorised access at local level
<b>Treatment option</b>	Reduction of likelihood
<b>Approach</b>	Implementation of access control and management of the log table with respect to the undertaken actions (deliverable D5.3c)
<b>Evaluation criteria met</b>	Yes

<b>Risk reduction</b>	Setting aside human factors (guessing or revealing passwords), this provides adequate security against malicious intrusion attempts.
<b>Benefit</b>	Protection against intrusion and consequent damaging or unpredictable actions.
<b>Cost</b>	Already incorporated in TELEMAC system

<b>R5</b>	
<b>Risk theme</b>	Loss of communication WWTP–TCC
<b>Treatment option</b>	Reduction of consequences
<b>Approach</b>	Decision to locate maximum expertise at local plant rather than remotely Audit trail of actions taken Integrity of XML transmitted Implementation of a backup connection via modem
<b>Evaluation criteria met</b>	Partly
<b>Risk reduction</b>	Local plant is able to run (possibly) at reduced efficiency in case of prolonged loss of communication from TCC. Actions may be reconstructed. There is no danger of database corruption from incomplete transmissions. The risk of having at the same time internet and phone connection down has been estimated as very low.
<b>Benefit</b>	Assurance of integrity of local plant in case of communication failure.
<b>Cost</b>	Already incorporated in TELEMAC system

<b>R6</b>	
<b>Risk theme</b>	TELEMAC component failure (remote level)
<b>Treatment option</b>	Reduction of likelihood
<b>Approach</b>	Validation of components at remote level prior to integration
<b>Evaluation criteria met</b>	Partly
<b>Risk reduction</b>	Provides some assurance of robustness of components in isolation. However, their functioning as a whole is not known. There might be unexpected interferences, though since the responsibilities of the TCC components are less than those at the local level, the potential for damaging results is correspondingly less.
<b>Benefit</b>	Confidence in robustness of individual components at remote level.
<b>Cost</b>	Cost mostly borne in TELEMAC project itself, though some testing will be required for future installations.

<b>R7</b>	
<b>Risk theme</b>	Poorly performing TELEMAC components at TCC
<b>Treatment option</b>	1. Reduction of likelihood 2. Reduction of consequences
<b>Approach</b>	1. The key is validation of individual components. An additional complexity arises from the TCC's ability to handle multiple plants: though this should be an improvement, it is possible that in some circumstances it might be a

	weakness, for example, incorrect generalisation across plants. 2. Local operator has final authority on actions taken on his plant.
<b>Evaluation criteria met</b>	Partly
<b>Risk reduction</b>	1. Provides some assurance of quality of performance of components in isolation. 2. Provides final measure for preventing damaging actions.
<b>Benefit</b>	Confidence in performance of individual components at remote level, and in ability to prevent damaging actions initiated remotely.
<b>Cost</b>	Cost mostly borne in TELEMAC project itself, though some testing will be required for future installations.

<b>R8</b>	
<b>Risk theme</b>	Functioning of TCC server compromised
<b>Treatment option</b>	Reduction of likelihood
<b>Approach</b>	Use of firewall with TCC server
<b>Evaluation criteria met</b>	Yes
<b>Risk reduction</b>	Prevents most attempts to compromise TCC server, e.g. hacking.
<b>Benefit</b>	Assurance of integrity of TCC server from outside attacks
<b>Cost</b>	Low—standard precaution

<b>R9</b>	
<b>Risk theme</b>	Loss of communication with databases by remote MATLAB modules
<b>Treatment option</b>	Reduction of consequences
<b>Approach</b>	The MATLAB module is not allowed to intervene remotely if it is involved in the control loop. No special measures taken if the MATLAB modules are used to provide advice or software sensor predictions.
<b>Evaluation criteria met</b>	Yes
<b>Risk reduction</b>	Any remote MATLAB modules are unlikely to be critical to system functioning; for example they might be in a testing phase, or providing an additional service that may help to improve efficiency.
<b>Benefit</b>	Assurance of integrity in case of loss of MATLAB module.
<b>Cost</b>	Already incorporated in TELEMAC system

<b>R10</b>	
<b>Risk theme</b>	Unauthorised access at TCC
<b>Treatment option</b>	Reduction of likelihood
<b>Approach</b>	Password control of access Monitoring of the log files with respect to the undertaken action (D5.3c)
<b>Evaluation criteria met</b>	Yes

<b>Risk reduction</b>	Setting aside human factors (guessing or revealing passwords), this provides adequate security against malicious intrusion attempts.
<b>Benefit</b>	Protection against intrusion and consequent damaging or unpredictable actions.
<b>Cost</b>	Already incorporated in TELEMAC system

<b>R11</b>	
<b>Risk theme</b>	Interception or hijacking of session TCC–WWTP by external party
<b>Treatment option</b>	Risk retention
<b>Approach</b>	No special measures taken, apart from management of the log files with respect to the undertaken action (D5.3c)
<b>Evaluation criteria met</b>	Yes
<b>Risk reduction</b>	This risk is considered highly unlikely
<b>Benefit</b>	N/A
<b>Cost</b>	None

<b>R12</b>	
<b>Risk theme</b>	Loss of Internet communication remote expert–TCC
<b>Treatment option</b>	Reduction of consequences
<b>Approach</b>	Remote expert does not have direct access to local plants The developed software runs under any web browser; even if the remote expert loses his laptop he should be able to find a computer with a browser (D5.2a). In case Internet connection is not available, the plant can still be monitored with a mobile phone using the WAP access (D4.2).
<b>Evaluation criteria met</b>	Yes
<b>Risk reduction</b>	Remote expert cannot be directly manipulating plant when communication lost
<b>Benefit</b>	Assurance of integrity of plant when remote expert is active
<b>Cost</b>	Some restriction on actions of remote expert

<b>R13</b>	
<b>Risk theme</b>	Impersonation of remote expert by external party, or hijacking of session
<b>Treatment option</b>	Reduction of likelihood
<b>Approach</b>	Use of passwords Attempted logins recorded Monitoring of the log files with respect to the undertaken action (D5.3c)
<b>Evaluation criteria met</b>	Yes
<b>Risk reduction</b>	The standard security measures taken make it unlikely that an unauthorised person can represent the remote expert. Audit trail allows reconstruction of

	actions if necessary.
<b>Benefit</b>	Low likelihood of disclosure of data or damaging actions on plant arising from remote expert.
<b>Cost</b>	Already incorporated in TELEMAC system

## 6 Conclusions

From an examination of the tables presented in the foregoing section, it can be seen that the majority of evaluation criteria for risk treatment are met. This means that on the whole the security measures put in place by the TELEMAC project are adequate for the purpose. However there are a number of areas where some security concerns remain, and these should be addressed during the exploitation phase after the end of the TELEMAC project. These areas are as follows.

1. How to assure correct (or at least safe) functioning of the TELEMAC components as a whole (rather than individual components). This applies at both local and remote (TCC) levels. In a complex system such as TELEMAC, there is potential for unpredictable interaction between components. This should be addressed in two ways: (a) by putting in place failsafe mechanisms to ensure that a safe behaviour can be guaranteed even in the worst case; (b) studying the specific interactions, their causes and effects with a view to reducing likelihood and consequences.
2. How to balance the need for safe running in the case of loss communication with the TCC against the benefits that TCC control can offer.