Automatic Verification of Wireless Control in a Mining Ventilation System

Maria D. Di Benedetto[1], Alessandro D'Innocenzo[1], Emmanuele Serra[1], Emmanuel Witrant[2]

***Abstract*— We address a wireless networked control problem for a mine ventilation system. Ventilation control is essential for the control of the operation of a mine for safety and energy optimization. The main control objective is to guarantee safety of the closed loop system. This test-case is simple enough to be computationally tractable, and yet it exposes the main difficulties encountered when using wireless networked systems for safety-critical applications. The focus of this paper is the formal verification of the operation of a closed loop control system for the so called secondary ventilation system that ensures air flow in the chambers of the mine where extraction takes place. The secondary ventilation system is modeled conservatively in the sense that if the formal verification process provides a positive answer then the system is guaranteed to work correctly while the converse is not necessarily true. For control, we use a simple threshold scheme. The overall closed-loop system is described by a hybrid model that takes into account the effects of time-delay, transmission errors and allows the precise formulation of the safety constraints. To ensure that the formal verification process is computationally tractable, we reason in the framework of temporal logics, and apply abstraction techniques and model checking tools that we developed previously.**

I. Introduction

Wireless networked control systems are considered a potential breakthrough for a number of applications in different industrial domains. Academia has focused on simple testbeds to demonstrate the quality of novel control and communication concepts and to understand the pitfalls of the techniques that were considered. However, to have an impact, we need to move to real industrial applications and to demonstrate the maturity of the technology while exposing the areas that need additional research. We identified an important potential application for wireless networks. This application is complex enough to expose the strengths and weaknesses of various control and communication approaches, while at the same time not prohibitive for the state of the art in the field. In particular, we focused on the ventilation control problem. Ventilation represents a significant portion of the power consumption cost for the ore extraction process. Thus improved ventilation control can have a major impact on cost and the environment at large. Because of the layout of a mine, wireless technology has the potential of solving cost and control accuracy problems that could not be tackled otherwise. We propose a conservative mathematical model of the secondary ventilation system of a mine, and propose a simple threshold control strategy for regulating gas concentrations in the extraction rooms. We make use of the hybrid system mathematical framework to model the closed loop system, while taking into account the effects of time-delay, transmission errors and safety constraints. Thus, we use abstraction techniques and tools that we developed in previous works [7], [6] to verify safety (with respect to gas concentrations) and temporal properties of the system, with a required precision.

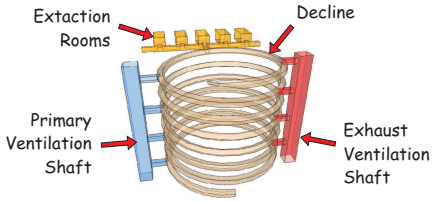

Fig. 1. Mine description.

The paper is structured as follows. In Section II, we describe the mining ventilation system. In Section III, we illustrate the existing ventilation system, define the control objectives and the proposed wireless control architecture. In Section IV we propose a mathematical model for the secondary systems. In Section V we propose a threshold control strategy, define a hybrid model of the closed loop system, and propose a procedure for automatic safety verification of the system.

II. Mining ventilation system

The main processes associated to ore extraction are drilling and blasting, ore transportation, and ore crushing. One supporting process is the ventilation in tunnels, clearly needed for the oxygen supply of the personnel and for the combustion process of vehicles (e.g. loader and dump trucks involved in ore transportation). The ventilation is achieved by a turbine and a heater on the surface and a vertical ventilation shaft as in Figure 1 (primary system), operated on a clockwise basis. Air pumped in from the surface is usually heated (in winter time at least), to avoid it to cause freezing down in the mine. From the primary ventilation shaft, a system of fans at each depth level of the mine pumps fresh air to the extraction rooms via tarpaulin tubes (secondary system): the secondary system is currently controlled based on manual demand by personnel entering a room. Bad quality air naturally flows because of pressure gradient from the extraction rooms back into the decline (which is a spiraling tunnel down as illustrated in Figure 1) and to the exhaust ventilation shaft, that is similar but separate from the primary ventilation shaft. The primary system has clear geometry and boundary conditions, while the secondary system is strongly varying in geometry (since rooms are blasted every day), characteristics (tarpaulin tube length and shape) and disturbances (trucks) even within the same mine. For these reasons, the secondary system is a typical hybrid environment, where the continuous variables

This work was partially supported by the HYCON Network of Excellence, contract number FP6-IST-511368

[1]Department of Electrical and Computer Engineering and Center of Excellence DEWS - University of L'Aquila, L'Aquila, Italy
email: {dibenede,adinnoce,serra}@ing.univaq.it
[2]Université Joseph Fourier / GIPSA-lab, Grenoble, France
email: emmanuel.witrant@gipsa-lab.inpg.fr

are given by gas concentrations and airflows, and the discrete variables are given by the number of working trucks in each extraction room.

The ventilation represents a significant portion of the power consumption cost for the ore extraction process. It is clear that investigating automatic control solutions is of great industrial interest, since the amount of pumped air can be minimized to save energy consumption. Moreover, introducing wireless networked control systems in the mine ventilation process can be motivated as follows. After all accessible ore has been retrieved from a mine level, the extraction rooms are filled and a new level further down along the decline is bored. All equipments, including the ventilation, have to be moved and re-configured in the new level. Hence mining is like a mobile process industry. Obviously there is a clear economic benefit in fast re-commissioning of the ventilation control system. In this context, the idea of having wireless access to the sensors as well as fan control inputs is quite natural. Moreover, wiring is unfeasible in the extraction rooms because of blasting and drilling operations.

III. Control objectives and proposed wireless control architecture

Currently, the ventilation is achieved by a turbine and a heater, operated on a clockwise basis, and a system of fans, controlled based on demand of air flow in different parts of the mine thanks to frequency converters. The inflow from the turbine has to provide air to fans that can be located very far from the ground (up to a kilometer deep) and that is usually heated (in winter time at least), to avoid that it causes freezing down in the mine. The fresh air is then carried to the extraction rooms thanks to tarpaulin tubes connected to the fans, which pump the air from the vertical shaft. The actual automation is operated in a clockwise way for the turbine and heater (i.e. they are run at maximum speed for a preset number of hours) and based on the vehicles demand combined with a timer for the fans. The secondary fan speed can assume only two values, and the fan is always working at least at low speed. When an extraction room is unused, the secondary fan is working at low speed. This is to guarantee a supply of fresh air for the whole mine. When the ore has to be loaded, two trucks (i.e a loader and a dump truck) are working in an extraction room. Since trucks consume O_2 and produce CO and CO_2 much more than humans, when a dumping truck is entering a room the employee has to communicate using walkie-talkies with the central control station to increase the fan speed to the high level in that room. To summarize, the actual control architecture is characterized by:

- no automatic control, but maximum ventilation power during ore extraction;
- no continuous monitoring of air quality;
- no wireless sensing;
- no localization system.

The overall objective of the mining ventilation control system is to provide good air quality in the extraction rooms. Thus, we specify the objective as the control air quality (O_2, NO_x and CO_x) in the extraction rooms. This is suitable to fulfill a cascade control configuration with the following two objectives:

- regulate turbine and heater to provide suitable air flow pressure at the ventilation fans in the tunnels;
- regulate ventilation fans to ensure air quality in extraction rooms.

It is clear that today's control architecture does not enable the fulfillment of these objectives, since there is no automatic control. We propose a wireless control architecture for fulfilling all the objectives listed above. We can consider

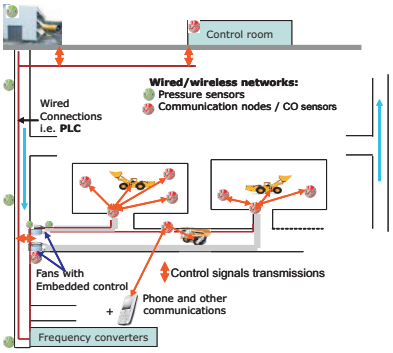

Fig. 2. Proposed decentralized automation based on both wireless and wired communications.

two control architectures: a *centralized architecture*, where all the control algorithms are run in the control room; and a *decentralized architecture*, where some intelligence is embedded at the fans locations and allows the fans regulation directly on the basis of the chemical sensors measurements. We choose the decentralized approach, for its simplicity and the higher performance level that is achievable in the presence of limited communications. Based on this control approach, the ventilation system can be described in two parts: one fixed installation, which is the primary air supply from the ground via a vertical shaft, and the secondary system, a mobile network of fans located underground. In this paper, we focus on the control of air quality in the secondary system.

The proposed wireless control architecture is depicted in Figure 2, where we introduced networked sensors in the access tunnels and in the extraction rooms. The sensors placed in the access tunnels can make use of the existing wired connections, while those in the extraction rooms have to be wireless, due to the blasting activities. The exchange of sensor measurements and control signals can occur thanks to wired links as well as wireless communication.

IV. Physical model for the secondary system

Because of the variety of room size and geometry, and of the tarpaulin tube characteristics (eg. length, diameter, curves, junctions), it is necessary to derive a flexible over-approximating mathematical model of the secondary system. We can derive such model by decomposing it in 2 different components:

1) The airflow model from the secondary fan to the extraction room via the tarpaulin tube;
2) The gas concentration dynamics in the extraction room.

A. Airflow model from the fan to the extraction room

We can derive a relation between the airflow velocities u_{fan} (near the fan) and u_{in} (at the tube endpoint, i.e. at the entrance of the extraction room). We can assume that the gradient of the temperature is 0 and that the airflow is incompressible. We limit our attention to the following aspects: the total loss η of airflow due to dissipation along the tarpaulin tube, and the total delay δ_t needed for the airflow velocity to propagate from the secondary fan to the endpoint of the tube. According to the above consideration, we get the following relation between u_{fan} and u_{in}:

$$u_{in}(t) = \eta u_{fan}\,(t - \delta_t) \tag{1}$$

In the following, we will show how to derive η and δ_t according to the characteristics of the tarpaulin tube.

The **loss of airflow** due to curves and length of the tube can be modeled using tabulated standard loss parameters as follows. The action of the fan produces a variation of pressure ΔH, which is partly dissipated along the tarpaulin tube (distributed losses ξ_d) and in the curves (concentrated losses ξ_c), and partly converted to airflow. Conservation of energy implies that:

$$\Delta H = \xi_d + \xi_c + \rho\frac{u_{in}^2}{2} - \rho\frac{u_{fan}^2}{2} \tag{2}$$

where ρ is air density. We can express the distributed losses by:

$$\xi_d = \frac{1}{2}\frac{L_t}{D_t}\rho u_{avg}^2 f \tag{3}$$

where L_t and D_t are, respectively, the length and the diameter of the tarpaulin tube, f models friction losses, and u_{avg} is the average velocity of the fluid in the tube. We take into account the concentrated losses introduced by the curves by considering an *effective* length $L_e = \sigma L_t$, $\sigma > 1$. The value of the coefficient σ is tabulated, and depends on the curve ray and on the tube diameter. Moreover, in equation (3), we can replace u_{avg} with u_{fan} obtaining an over-approximation of the losses:

$$\xi = \xi_d + \xi_c = \frac{1}{2}\frac{L_e}{D_t}\rho u_{fan}^2 f \tag{4}$$

If the fluid is inviscid then its flow is turbulent (i.e. the Reynolds number Re is very high), then equation (4) can be further simplified considering that the friction losses can be expressed as follows [10]:

$$f = (1.82\log_{10} Re - 1.64)^{-2} = \left(\frac{1}{1.82\log_{10} Re - 1.64}\right)^2 \tag{5}$$

thus by replacing expression (4) in equation (2) and solving for the variable u_{in} we obtain:

$$u_{in} = \sqrt{\frac{2}{\rho}\left[\Delta H - \frac{1}{2}\frac{L_e}{D_t}\rho\left(\frac{u_{fan}}{1.82\log_{10} Re - 1.64}\right)^2\right] + u_{fan}^2} \tag{6}$$

Assume that the sections of the fan, of the tarpaulin tube and of the tube opening at the room entrance are all circular with diameter D_t. For standard conditions of dry air at 21 °C, the system resistance curve can be expressed by:

$$\chi = \frac{F^2}{(1.29 S_t)^2} \tag{7}$$

where χ are the total losses expressed in $[Pa]$, S_t is the section of the tarpaulin tube, and F is the volumetric flow rate expressed in $\left[\frac{m^3}{s}\right]$. Considering that the airflow velocity u_{fan} is the ratio between the volumetric flow rate F and the section S_t, we can find a relation between the static pressure and the airflow velocity:

$$u_{fan} = \frac{F}{S_t} \Rightarrow u_{fan}^2 = \frac{F^2}{S_t^2} = 1.29^2 \Delta H \Rightarrow \Delta H = 0.6\ u_{fan}^2 \tag{8}$$

This formula comes out by choosing the operating point for the secondary fan, which indicates the volumetric flow through the system at a particular fan static pressure. In the operating point, the static pressure ΔH matches the total losses χ, and it can be determined by the fan performance curve and the system resistance curve intersection. While the fan performance curve describes the performance of a particular fan, the system resistance curve describes the characteristics of airflow through the system. By replacing equation (8) in the equation (6), we obtain $u_{in} = \eta u_{fan}$.

The **delay** δ_t introduced by a tube of length L_t is the time needed for the airflow at the secondary fan level to propagate to the end of the tarpaulin tube. This airflow is considered inviscid and incompressible, and modeled as a time-varying delay $\delta_t(t)$. Indeed, considering a Poiseuille laminar flow and the previous hypotheses, the flow speed $u(t,x)$ and temperature $T(t,x)$ are obtained from Navier-Stokes equations (see, for example, [8] or similar textbooks for details) as

$$\frac{\partial}{\partial t}\begin{bmatrix} u \\ T \end{bmatrix} + \begin{bmatrix} u & r \\ \mu T & u \end{bmatrix}\frac{\partial}{\partial x}\begin{bmatrix} u \\ T \end{bmatrix} = 0 \tag{9}$$

where $u(t,x)$ and $T(t,x)$ are the airflow velocity at time t and position $x \in [0, L_t]$, r is the gas constant per unit of mass, and μ is the ratio of specific heat coefficients. Note that $u(t, L_t) = u_{in}(t)$, and $u(t,0) = u_{fan}(t)$. The characteristic velocities $v(t,x)$ are then the solutions of

$$\det\begin{vmatrix} -v+u & r \\ \mu T & -v+u \end{vmatrix} = 0 \tag{10}$$

$$\Leftrightarrow v_{1,2}(t,x) = u(t,x) \pm \sqrt{\mu r T(t,x)} \tag{11}$$

We are interested in the down-flow time-delay, which is approximated from the previous equation as

$$\delta_t(t) \approx \frac{L_t}{\bar{u}(t) + \sqrt{\mu r \bar{T}(t)}} \tag{12}$$

where $\bar{u}(t)$ and $\bar{T}(t)$ are the space-averaged flow speed and temperature, respectively.

Finally, we can relate a given airflow u_{in}^* to the fan velocity $\dot{\theta}_{fan}^H$ needed to produce an airflow u_{in}^* at the endpoint of the tarpaulin tube. We still assume that in the proximity of the fan the air temperature in the ventilation shaft and in tarpaulin tube is constant, and the airflow is incompressible. Thus, the airflow is only due to pressure difference. We recall that the airflow speed in proximity of the fan is u_{fan}, and ΔH is the fan static pressure (expressed in [Pa]). The data sheet of the fan, which can be found in [11], relates the fan static pressure ΔH to u_{fan} for different values of the fan speed (expressed in RPM). Thus, given u_{in}^*, we can compute the needed values of u_{fan}^* and ΔH^* using equations (6) and (8). Using the data sheet, we directly obtain the needed fan speed $\dot{\theta}_{fan}^*$. The boundary conditions given by the air pressure in the primary ventilation shaft affect the fan performance curves by means of a vertical translation.

B. Gas concentration dynamics in the extraction room.

Let $c(h,t)$ be the concentration of a gas, where h is the distance from the floor. In the presence of full turbulence the steady state concentration is constant w.r.t. h. In absence of turbulence (and according to the buoyancy characteristic of gases at different temperatures) the steady state concentration of a volatile (resp. heavy) gas stratifies on the top (resp. bottom) of a room. The presence in the room of vehicles and air inflow/outflow generates a moderate turbulence. Hence, we can reasonably choose a smooth shape to model the gas concentration in the room.

We are interested here in deriving the dynamics of

$$C(z,t) = \frac{1}{z}\int_0^z c(h,t)dh, \tag{13}$$

that is the averaged concentration between $h = 0$ and $h = z$ of a particular gas in the room. To this aim, we consider the air inflow and outflow, that are positioned at heights h_{in}, h_{out} respectively. Another aspect to consider in the model is the gas generation (consumption) due to the vehicles in the extraction room. For a fixed number of vehicles, we consider the gas generation (consumption) as a positive (negative) constant G_E expressed in $[kg/s]$, which does not affect the overall air mass in the room. The pollutant dynamics is set thanks to the mass conservation law:

$$\begin{aligned} \dot{m}(t) &= \dot{m}_{in}(t) - \dot{m}_{out}(t) \\ &= G_E + u_{in}(t)S_{in}c_{atm} - u_{out}(t)S_{out}C(h_{out}, t) \end{aligned} \tag{14}$$

where $\dot{m}_{in}(t)$ is the incoming pollutant mass rate due to the engines and to the atmosphere gas concentration c_{atm} given by appropriate specifications (we neglect human contribution); when we consider gases that are not present in the air, such as carbon monoxide, $c_{atm} = 0$. Moreover, $\dot{m}_{out}(t)$ is the outflow pollutant mass rate, S_{in} and S_{out} are the sections of the input and output opening, $C(h_{out}, t)$ is the space averaged concentration from the room floor to the height of the air outflow, $u_{in}(t)$ and $u_{out}(t)$ are the airflow velocities of the input and output airflow. Dividing (14) by the room volume V_R, and supposing incompressibility of the mass flow rate, we obtain the concentration dynamics:

$$\dot{C}(H_R, t) = \frac{G_E}{V_R} + \frac{u_{in}(t)S_{in}c_{atm}}{V_R} - \frac{u_{in}(t)S_{in}}{V_R}C(h_{out}, t) \tag{15}$$

The concentration $c(h, t)$ can be modeled by means of a sigmoid function

$$c(h, t) = \frac{\alpha(t)}{1 + e^{-\beta(t)(h-\gamma(t)H_R)}} \tag{16}$$

where H_R is the room height, $\alpha(t)$ is expressed in $\left[\frac{kg}{m^3}\right]$ and depends on the quantity of gas in the room while both $\beta(t)$ (expressed in $[m^{-1}]$) and $\gamma(t)$ (dimensionless) depend on the buoyancy characteristics of the gas, the flow momentum at the trucks exhausts, the temperature and the number of trucks in the room (the last two being the most important). In particular, the sign of $\beta(t)$ is determined by the volatility of the gas: it is positive (resp. negative) if the gas is lighter (resp. heavier) than air. The functions $\alpha(t)$, $\beta(t)$ and $\gamma(t)$ have to be experimentally identified in the extraction room for each gas, by means of a fitting operation [12] between the concentration curve obtained from the measures in the room and the curve obtained from the sigmoid function (16). As a rough approximation, we can use a hybrid representation here, supposing that we have β_k and γ_k, where k is the number of trucks in the room (we do not consider the transient dynamics of these parameters). By replacing the sigmoid function in the integral (13) we obtain:

$$C(z, t) = \frac{\alpha(t)}{\beta_k z} \ln\left(\frac{e^{\beta_k(z-\gamma_k H_R)} + 1}{e^{-\beta_k \gamma_k H_R} + 1}\right) \tag{17}$$

Computing equation (17) for $z = H_R$ and solving it for the variable $\alpha(t)$ we obtain

$$\alpha(t) = \frac{\beta_k H_R}{\ln\left(\frac{e^{\beta_k(1-\gamma_k)H_R+1}}{e^{-\beta_k\gamma_k H_R+1}}\right)} C(H_R, t) \tag{18}$$

By replacing expression (18) in equation (16) and computing the space averaged concentration between 0 and h_{out} we obtain

$$\begin{aligned} C(h_{out}, t) = &\frac{\beta_k H_R}{\ln\left(\frac{e^{\beta_k(1-\gamma_k)H_R+1}}{e^{-\beta_k\gamma_k H_R+1}}\right)} C(H_R, t)\times \\ &\times \frac{1}{h_{out}} \int_0^{h_{out}} \frac{1}{1 + e^{-\beta_k(h-\gamma_k H_R)}} dh \end{aligned} \tag{19}$$

Finally, by replacing the expressions of $C(h_{out}, t)$ and $u_{in}(t)$ in equation (15), we obtain

$$\begin{aligned} \dot{C}(H_R, t) = &\frac{G_E}{V_R} + \frac{S_{in}c_{atm}\eta}{V_R} u_{fan}(t - \delta_t(t)) + \\ &+ \frac{S_{in}\eta}{V_R} u_{fan}(t - \delta_t(t)) \frac{\beta_k H_R}{\ln\left(\frac{e^{\beta_k(1-\gamma_k)H_R+1}}{e^{-\beta_k\gamma_k H_R+1}}\right)} C(H_R, t)\times \\ &\times \frac{1}{h_{out}} \int_0^{h_{out}} \frac{1}{1 + e^{-\beta_k(h-\gamma_k H_R)}} dh \end{aligned} \tag{20}$$

Note that η depends on the airflow velocity in the tube, because the Reynolds number does.

V. Safety control strategy for the secondary system

Given the model of the secondary system defined in equation (20), we consider the following control specifications.

1) **Safety:** the gas concentrations cannot enter an unsafe set (a *red alert* zone), given by standard air quality for humans.
2) **Comfortable air quality:** the gas concentrations may enter, only for a bounded amount of time, an inefficient set (a *yellow alert* zone) where safety air quality for humans is satisfied but may be uncomfortable.

The two properties above intuitively state the following: we guarantee that the oxygen concentration is always over the minimum safe threshold for humans, and we require that, whenever a disturbance (e.g. the entrance of a truck in a room) makes the oxygen concentration go under a threshold of optimality (comfortable air quality), this only happens for a short amount of time.

Our aim is to automatically verify whether the controlled system satisfies the aforementioned safety/comfort properties. Thus, we first need to model the two specifications as formulae. The first *strong* specification (that is a classical safety property) can be modeled using the CTL temporal logic [5], while the second *relaxed* specification can be modeled using the TCTL temporal logic [1]. Clearly, we have to verify that both specifications are satisfied.

Because of the hybrid nature of the problem (e.g. number of trucks in an extraction room), it is extremely hard to exhaustively verify on the model (20) whether the specifications above are satisfied for any discrete and continuous disturbance. For this reason, we first obtain a reasonable hybrid model with affine dynamics of our closed-loop system, then we construct a timed automaton abstraction of the hybrid automaton, which preserves CTL and TCTL temporal properties. Timed automata can generally be abstracted into finite state systems [4], and this makes model checking decidable.

We first define a hybrid model with affine dynamics of our closed-loop system under the following assumptions:

Assumption 1. As already discussed, at present, the fan speed can assume only two values, and the fan is always working at least at low speed. When an extraction room is unused, the secondary fan is working at low speed. This is to guarantee a supply of fresh air for the whole mine. When the ore has to be loaded, two trucks are working in an extraction room (i.e a loader and a dump truck). Since trucks consume O_2 and produce CO and CO_2 much more than humans, when a dumping truck is entering a room the employee has to communicate by radio with the central control station, to

increase the fan speed to the high level. We consider the fan speed level as our control input, and we suppose that it can assume a finite number of possible values. This is motivated by the fact that we do not need an accurate control on the gas concentrations, since we can tolerate moderate oscillations. We think that a continuous and very accurate control might be expensive and wasteful because of the huge dimensions and inertia of the fans. As a first approach, we consider w.l.o.g. only two speed levels (as currently happens in the mine), namely $\dot{\theta}_{fan} \in \{\dot{\theta}^L_{fan}, \dot{\theta}^H_{fan}\}$. The low level is necessary for safety reasons, to have a continuous inlet of fresh air. The high level is necessary to allow adequate air change, when trucks are working in a room. Depending on the maximum gas emission/consumption of the trucks, we can chose a desired airflow u^H_{in} at the endpoint of the tarpaulin tube and derive the corresponding fan velocity $\dot{\theta}^H_{fan}$ as illustrated in Section IV.

Assumption 2. It often happens that the employees forget to communicate to the central control station that they are exiting the room, thus the fans remain at high speed level even if they are unused. The main waste of energy of the secondary system seems to be imputable to the absence of gas concentration feedback and to the excess of ventilation of the unused extraction rooms. One possible approach is using localization of trucks to increase air supply only in employed rooms. However, in this case we do not have feedback on the gas concentration. For this reason, we can use sensors to get feedback of the gas concentration, and use it to design a control strategy. We consider a threshold control strategy: we can switch fans to low and high speed levels when the gas concentrations hit some given thresholds.

Assumption 3. One problem in using sensors to estimate gas concentration is that rooms are blasted every day, and sensors might be damaged during blast operations. For this reason a possible solution is using a wireless sensor network that can be easily displaced and removed within the room and measure the gas concentrations. We assume here that the network design guarantees that the measured concentration is affected by a bounded estimation error $\varepsilon > 0$, and an estimation and communication delay bounded by a value $\delta_c > 0$. As discussed in Section II, the main wiring problem in the mine is in the extraction room. Thus, we reasonably assume that the threshold is checked on a gateway sensor positioned in the room, and that the control signal is transmitted to the fan on a cable. On the basis of these assumptions, the secondary control system can be modeled as a non deterministic affine hybrid automaton. Non deterministic guard conditions determined by $\varepsilon > 0$ model the estimation error, while a clock variable models estimation, communication and actuation delays $\delta = \delta_c + \delta_t$.

We consider a three dimensional continuous state space $x(t) \in \mathbb{R}^3$, where the first component is the concentration of oxygen $x_1(t) = c_{O_2}(t)$, the second is the concentration of carbon monoxide $x_2(t) = c_{CO}(t)$, and the third is the concentration of carbon dioxide $x_3(t) = c_{CO_2}(t)$ in the extraction room. The dynamics of this three dimensional system are obtained by replying the differential equation (20) for each gas:

$$\dot{x}_i(t) = a_i x_i(t) + b_i, i \in \{1, 2, 3\}$$

with the coefficients a_i, b_i defined in Section IV. The constants a_i depend both on the buoyancy characteristics of the i-th gas and on the concentration of the i-th gas in the room, while the constants b_i depend on the i-th gas emission/consumption of the trucks and on the input volumetric airflow.

Since there are two speed levels, each constant a_i, b_i can assume two values (respectively a^L_i, a^H_i and b^L_i, b^H_i). Let $g_{l,1}, g_{h,2}, g_{h,3}$ be the thresholds on the gas concentrations that trigger the increase of the fan speed, and $g_{h,1}, g_{l,2}, g_{l,3}$ be the thresholds on the gas concentrations that trigger the decrease of the fan speed. In our hybrid model of the controlled secondary system we will consider the worst case value for the disturbance introduced by the trucks, namely when there are two working trucks in the extraction room. The hybrid model is now described, using the notations introduced in [7].

- $Q = \{q_1, q_2, q_3, q_4\}$ is the set of discrete states that models the two speed levels of the fan and the two actuation delays when we switch from one speed to the other and viceversa. In particular, q_1 models the low speed state, q_2 models the low to high switch delay, q_3 models the high speed state and q_4 models the high to low switch delay.
- $X = \mathbb{R}^4$ where x_1, x_2 and x_3 represent, respectively, the concentration of oxygen, carbon monoxide and carbon dioxide, while x_4 is a clock state variable.
- $Init = \{(q_1, x_0)\}$ is the set of initial conditions.
- $E = \{(q_1, q_2), (q_2, q_3), (q_3, q_4), (q_4, q_1)\}$ is the set of discrete transitions.
- The continuous dynamics for the discrete states are given by

$$\begin{pmatrix} \dot{x}_1(t) \\ \dot{x}_2(t) \\ \dot{x}_3(t) \\ \dot{x}_4(t) \end{pmatrix} = \left(\begin{bmatrix} a^\nu_1 & 0 & 0 \\ 0 & a^\nu_2 & 0 \\ 0 & 0 & a^\nu_3 \end{bmatrix} \begin{pmatrix} x_1(t) \\ x_2(t) \\ x_3(t) \end{pmatrix} + \begin{pmatrix} b^\nu_1 \\ b^\nu_2 \\ b^\nu_3 \end{pmatrix} \right), \quad 1$$

  where $\nu = L$ for states q_3, q_4 while $\nu = H$ for states q_1, q_2.
- Invariant, guard and reset are defined as follows:

$$\begin{aligned}
&Inv(q_1) = \{x \in \mathbb{R}^4 | x_1 > g_{l,1} - \varepsilon \wedge x_2 < g_{h,2} + \varepsilon \wedge x_3 < g_{h,3} + \varepsilon \wedge x_4 > 0\} \\
&Inv(q_2) = \{x \in \mathbb{R}^4 | x_4 < \delta\} \\
&Inv(q_3) = \{x \in \mathbb{R}^4 | x_1 < g_{h,1} + \varepsilon \wedge x_2 > g_{l,2} - \varepsilon \wedge x_3 > g_{l,3} - \varepsilon \wedge x_4 > 0\} \\
&Inv(q_4) = \{x \in \mathbb{R}^4 | x_4 < \delta\} \\
&G(q_1, q_2) = \left\{x \in \mathbb{R}^4 | x_1 \leqslant g_{l,1} - \varepsilon \wedge x_2 \geqslant g_{h,2} + \varepsilon \wedge x_3 \geqslant g_{h,3} + \varepsilon\right\} \\
&G(q_2, q_3) = \left\{x \in \mathbb{R}^4 | x_4 \geqslant \delta\right\} \\
&G(q_3, q_4) = \left\{x \in \mathbb{R}^4 | x_1 \geqslant g_{h,1} + \varepsilon \wedge x_2 \leqslant g_{l,2} - \varepsilon \wedge x_3 \leqslant g_{l,3} - \varepsilon\right\} \\
&G(q_4, q_1) = \left\{x \in \mathbb{R}^4 | x_4 \geqslant \delta\right\} \\
&\forall e \in E, R(e, x(t)) = (x_1(t), x_2(t), x_3(t), 0)'
\end{aligned}$$

The threshold control strategy is defined by the guards $g_{l,1}$, $g_{l,2}$, $g_{l,3}$, $g_{h,1}$, $g_{h,2}$ and $g_{h,3}$. We now automatically verify, by using the theoretical results introduced in [6] and the tool that we have developed in [7], if *for a given control strategy* the hybrid automaton defined above (which models the closed-loop secondary system according to our control strategy) satisfies **Safety** and **Comfort** properties. More precisely, define the Safety specification introduced above as a CTL formula ψ_s, and define the comfortable air quality specification as a TCTL formula $\psi_c(t_{max})$, with t_{max} the maximum time the system is allowed to dwell in uncomfortable air quality.

Unfortunately, model checking is in general undecidable even for affine hybrid automata. An important technique used to cope with complexity is *abstraction*. In recent papers [7], [6] we proposed and implemented an algorithm to construct an abstraction of a hybrid automaton with affine dynamics, which preserves temporal properties expressed by CTL and TCTL formulae. The abstract model belongs to a subclass of timed automata, called *durational graph*. Durational graphs are a special class of timed automata [3], [2] where the continuous variables are *clocks* that increase with constant slope. Resets are restricted to clock resets to 0.

The following result is directly implied by the results developed in [6]:

Proposition 1: Given a hybrid automaton $\mathcal{H}$ and a durational graph $\mathcal{G}$ such that $\mathcal{H}$ and $\mathcal{G}$ are bisimilar with precision φ ($\mathcal{H} \approx_\varphi \mathcal{G}$), then:

i. If the specification ψ_s is satisfied for the system $\mathcal{G}$, then it is satisfied for the system $\mathcal{H}$;
ii. If the specification $\psi_c(t_{max})$ is satisfied for the system $\mathcal{G}$, then $\psi_c(t_{max} + \varphi)$ is satisfied for the system $\mathcal{H}$.

According to the above proposition, we can verify properties of the affine hybrid automaton by checking properties on the durational graph abstraction, using model checking tools for timed automata (e.g. *KRONOS* [13], *UPPAAL* [9]). If for an initial choice of the threshold the system is not verified to be safe, we can iteratively run the verification procedure for tighter thresholds until safety and comfort are both satisfied.

The abstraction algorithm's graphical output is illustrated in Figure 3, and intuitively works as follows: the set of initial conditions

of the gas concentrations (blue polytope) is partitioned in a finite number of polytopes according to the continuous dynamics and the guard sets. The property of each element of the partition is that, for each pair of initial conditions x_1^0, x_2^0 belonging to it, the arrival times t_1, t_2 to the guard satisfy $|t_1 - t_2| < \varphi$. This procedure is iterated to all guard sets (green and red polytopes) of the hybrid automaton. Each partition element is translated into a discrete state of the abstracting durational graph. The resulting durational graph $\mathcal{G}$ satisfies $\mathcal{H} \approx_\varphi \mathcal{G}$, and thus Proposition 1 holds. If the abstraction does not satisfy the required safety and comfort properties, it is not possible to determine if the original system does. However, since the verification process is automatic, it is possible by iterative search to choose different thresholds, in order to guarantee that the specifications are satisfied.

By executing the automatic verification procedure on our hybrid model using the thresholds $g_{l,1} = 0.2955$, $g_{l,2} = 0.5 \cdot 10^{-3}$, $g_{l,3} = 0.0885$, $g_{h,1} = 0.2975$, $g_{h,2} = 2.5 \cdot 10^{-3}$, $g_{h,3} = 0.091$ (in $[Kg/m^3]$) and an abstraction precision $\varphi = 1s$, we verified on the abstraction $\mathcal{G}$ that ψ_s is satisfied, and $\psi_c(t_{max})$ is satisfied for $t_{max} = 61s$. Since our abstraction has been constructed with precision $\varphi = 1s$, then Proposition 1 implies that **(1) the original hybrid system is safe and (2) the maximum time of uncomfortable air quality is bounded by 62 s**.

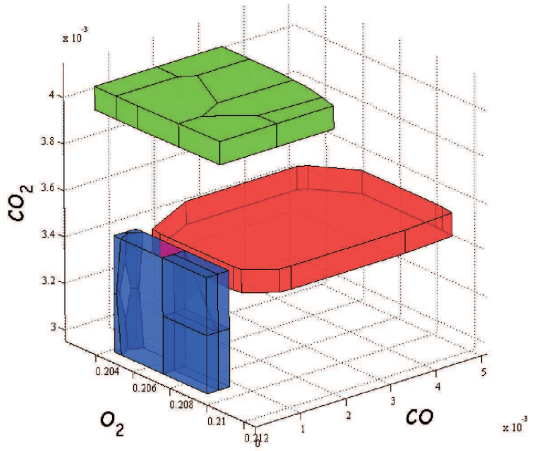

Fig. 3. Matlab simulations and screenshot of the abstraction algorithm output. Polytopes represent set of initial conditions and the projections of their executions with the guard sets.

For completeness, we also show in Figure 4 some Matlab simulations of the closed loop system. For the initial condition chosen for this simulation, safety and comfort are verified using the plots. The advantage of automatic verification is that the same two properties can be verified in *one shot* for the whole set of initial conditions.

VI. Conclusions

In this work, we addressed a wireless networked control problem for a mining ventilation application. We developed a conservative mathematical model of the mine secondary ventilation system and a threshold control strategy, and modelled the closed loop system as an affine hybrid system. We expressed control specifications regarding Safety and Comfort of air quality in the framework of temporal logics. We used abstraction techniques and tools that we developed in some previous work to construct an abstraction that inherits the properties of interest of the original hybrid system with a desired precision. We then show how to automatically verify whether Safety and Comfort specifications are satisfied. Future work aims at extending automatic verification results to more complex control strategies.

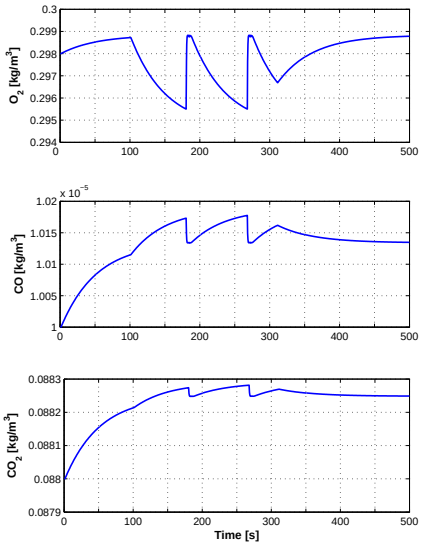

Fig. 4. Matlab Simulations.

References

[1] R. Alur, C. Courcoubetis, and D.L. Dill. Model–checking in dense real–time. *Information and Computation*, 104(1):2–34, 1993.

[2] R. Alur, C. Courcoubetis, N. Halbwachs, T.A. Henzinger, P.H. Ho, X. Nicollin, A. Olivero, J. Sifakis, and S. Yovine. The algorithmic analysis of hybrid systems. *Theoretical Computer Science*, 138:3–34, 1995.

[3] R. Alur and D.L. Dill. A theory of timed automata. *Theoretical Computer Science*, 126:183–235, 1994.

[4] R. Alur, T. Henzinger, G. Lafferriere, and G.J. Pappas. Discrete abstractions of hybrid systems. *Proccedings of the IEEE*, 88(2):971–984, July 2000.

[5] E.M. Clarke, O. Grumberg, and D.A. Peled. *Model Checking*. The MIT Press, Cambridge, Massachusetts, 2002.

[6] A. D'Innocenzo, A. A. Julius, M. D. Di Benedetto, and G.J. Pappas. Approximate timed abstractions of hybrid automata. In *Proceedings of the 46^{th} IEEE Conference on Decision and Control. New Orleans, Louisiana, USA.*, 12–14 December 2007.

[7] A. D'Innocenzo, A. A. Julius, G. J. Pappas, M. D. Di Benedetto, and S. Di Gennaro. Verification of temporal properties on hybrid automata by simulation relations. In *Proceedings of the 46^{th} IEEE Conference on Decision and Control. New Orleans, Louisiana, USA.*, 12–14 December 2007.

[8] C. Hirsch. *Numerical Computation of Internal & External Flows: the Fundamentals of Computational Fluid Dynamics*. Butterworth-Heinemann (Elsevier), 2^{nd} edition, 2007.

[9] K. G. Larsen, P. Pettersson, and W. Yi. UPPAAL in a nutshell. *International Journal on Software Tools for Technology Transfer*, 1(1):134–152, December 1997.

[10] Poh-Seng Lee, Suresh V. Garimella, and Dong Liu. Investigation of heat transfer in rectangular microchannels. *International Journal of Heat and Mass Transfer*, 48:16881704, 2005.

[11] E. Widzyk-Capehart and B. Watson. Agnew gold mine expansion mine ventilation evaluation using VentSim. In *Proc. of the 7^{th} International Mine Ventilation Congress*, 2001.

[12] E. Witrant, E. Joffrin, S. Brémond, G. Giruzzi, D. Mazon, O. Barana, and P. Moreau. A control-oriented model of the current profile in tokamak plasma. *Plasma Phys. Control. Fusion*, 49:1075–1105, 2007.

[13] S. Yovine. Kronos: A verification tool for real-time systems. *International Journal of Software Tools for Technology Transfer, Springer-Verlag*, 1(1):123–133, October 1997.