Estimating the probability of undetected failure of pasteurization process control using Fault Tree Analysis

J. Hein M. van Lieverloo[1], Cornelis P. Willig[2], Martijn B. Fox[1] and Marjon H.J. Wells-Bennik[1]

[1] NIZO food research, Kerhemseweg 2, 6718 ZB Ede, the Netherlands (hein.van.lieverloo@nizo.nl)
[2] Dependable Industrial Automation Consultancy, Herman Heijermanslaan 2, 21056 ES Heemstede, the Netherlands (cornelis.willig@diac.nl)

Keywords: Process control; Boolean Monte Carlo analysis; process optimization, cost-benefit analysis.

Abstract

Dairies rely on process control to warrant the temperatures and holding times required for pasteurization. It is possible to quantify the probability of simultaneous failure of primary as well as process safety control components, using Fault Tree Analysis (FTA), thus quantitatively validating this Critical Control Point. FTA of a case study pasteurization process using generic component failure rate data showed that a former configuration on average would lead to the top event ‘undetected contamination’ every 5 years. The five base events most contributing to this failure rate all concerned milk flow control. The failure rate dropped to once every 1050 years when a second flow meter was installed, serving as a flow guard that automatically initiates recirculation to the raw milk tank when flow deviates from set point values. After this cost-effective change of process control, other base events (leaking regenerative heaters, PLC cards) became most important. The failure rates are estimates from a basic model excluding so-called ‘common cause failures’ (e.g. PLC failure) that usually increase failure rates. Fault Tree Analysis is a tool well applicable to quantify the low probabilities of calamities in pasteurization and other critical food processing, to identify the most important process components and to find the optimal balance of costs, safety and quality.

Introduction

Most strains of *L. monocytogenes* are very sensitive to regular pasteurization conditions (Van Asselt & Zwietering, 2006). However, if pasteurization fails undetected (and therefore unchecked), milk may be contaminated. Growth models show that some bacteria, e.g. *Listeria monocytogenes*, readily grow in pasteurized milk (Te Giffel and Zwietering, 1996) and any contamination during or after pasteurization will lead to a high probability of exceeding the EU food safety objective of < 100 cfu/g at the time of consumption (Van Lieverloo et al., 2007). Contamination incidents such as the USA Whittier Farms post-pasteurization outbreak end of 2007 show the need for rigorous control of any post-pasteurization recontamination (Anonymous, 2008). The dairy industry strives for undetectably low probabilities of recontamination of milk, preferably zero. This poses the challenge of estimating actual levels of recontamination.

Other industries (aircraft, nuclear, petrochemical) that accept extremely low probabilities of barely unacceptable events (explosions, contamination) use Fault Tree Analysis (FTA) to estimate probabilities of both primary as well as secondary safety systems failing at the same time.

Materials and methods

FTA is a Boolean Monte Carlo Analysis where known probabilities of base events (failing valves, thermometers, computers etc.) are used to calculate the probability of the top event (Andrews and Moss, 2002), in this case the undetected contamination of milk. This FTA focused on cross-contamination between raw and pasteurized milk, low temperature and low heating time. The basics of an FTA are the simulation of the effects of failures of base components ('base events') by linking these events using AND and OR gates. When either of two or more events occurring lead to another event, these events are linked using an OR gate. When two or more events must occur simultaneously or consecutively to lead to another event, this occurrence is described by an AND gate. Figure 1 shows the symbols used to present a fault tree in a diagram.

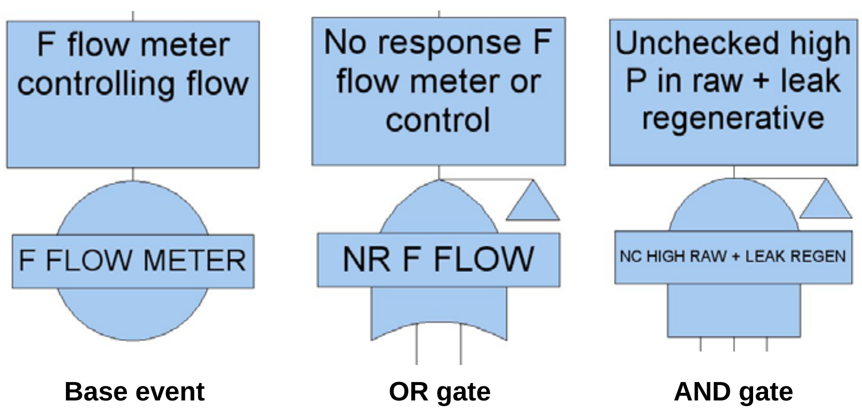

Figure 1: Most common symbols in a fault tree. The triangles are used to indicate replicated branches.or to indicate a link within the fault tree paging display.

Boolean algebra rules apply to calculations of probabilities of events described by an OR or AND gate. Roughly, the probabilities of base events connected by an OR gate are added and probabilities of base events connected by an AND gate are multiplied, but actual Boolean algebra is more complex (Andrews and Moss, 2002) and was performed by the software (FaultTree+ by Isograph Ltd). Several models can be used to describe the probabilities of base events. Most commonly used are fixed models, assuming equal failure probability during the lifetime of the component (excluding burn-in and wear-out periods). Another common model applies to components and personnel (operators) that may only fail 'on demand' as they are not continuously operating. The failure models can either be point estimates or probability density functions, the latter case allowing for a Boolean Monte Carlo analysis.

The results of the model include the failure rate (reciprocal of Mean Time To Failure MTTF) and the unavailability ('down-time') of the system. The relative contribution of base events to the unreliability was calculated as the Fussel-Vesely importance ranking (Andrews and Moss, 2002), corrected to 100%. In this basic FTA, no variability was included and calculations were performed using point estimates of failure rates. It is important to emphasize that these values are not actual failure data, as the actual component failure rates probably most likely are lower than then generic failure data used. Maintenance data will be used to optimize the data of important components.

Results and discussion

The case study fault tree of the pasteurization process with the top event 'undetected contamination' is shown in Figure 2. Calculating the model results in a mean failure rate of the top event of once every 5 years. In the Fussel-Vesely importance ranking, five basic events concerning flow control top the list (Table 1). The base event with the highest importance, 'No response to failure of flow meter or flow control' occurs four times in the fault tree (Figure 2). In the former configuration of the process, the flow was controlled by one flow meter, leaving the detection of flow failures (failing pump, failing flow meter or failing PLC cards) to observing operators. The failure rate dropped to once every 1050 years when a second flow meter was installed, serving as a flow guard that automatically initiates recirculation to the raw milk tank when flow deviates from set point values (Figure 3). After this change, other base events (PLC cards, leak of regenerative heat exchanger) became most important (Table 2) and the configuration became more balanced from a cost-benefit point-of-view.

Table 1: Importance ranking of base events for top event 'undetected contamination' of the **former configuration** of the case study pasteurization process (using generic failure rate data)

Relative importance	Base event
49.9 %	No response to failure of flow meter or flow control (some operator experience). Failure on demand rate set fixed at 0.5.
12.47 %	Failure of PLC input card responding to flow meter input [a]
12.47 %	Failure of the speed control unit of the raw milk pump [a]
12.47 %	Failure of the PLC output card controlling raw milk pump speed [a]
12.47 %	Failure of the flow meter controlling flow via the raw milk pump [a]

[a] failure rate fixed at once in 10 years, MMTR 8 hours
MTTR = mean time to repair (from failure to running)

Table 2: Importance ranking of base events for top event 'undetected contamination' of the **new configuration** of the case study pasteurization process (using generic failure rate data)

Relative importance	Base event
18.47%	Failure of PLC output card initiating recirculation to raw milk [a]
12.35%	Leakage of regenerative (dormant failure rate of once per three years, inspection interval three years, MTTR 8 hours)
8.22%	Failure of PLC output card relaying high temperature differences between start and end of the holding section (> 1 °C) [a]
6.44%	Failure of the steam kettle [b]
4.29%	Failure of the flow guard meter [a]
4.29%	Failure of PLC input card flow guard meter [a]
3.99%	Block of flow after regenerative (raw side) fixed at once per year
3.22%	Failure of the speed control on the raw milk pump [a]
3.22%	Failure of flow meter [a]
3.22%	Failure of PLC input card flow [a]
3.22%	Failure of PLC output card flow meter [a]

[a] failure rate fixed at once in 10 years, MMTR 8 hours
[b] failure rate fixed at once in 10 years, MMTR 8 hours
MTTR = mean time to repair (from failure to running)

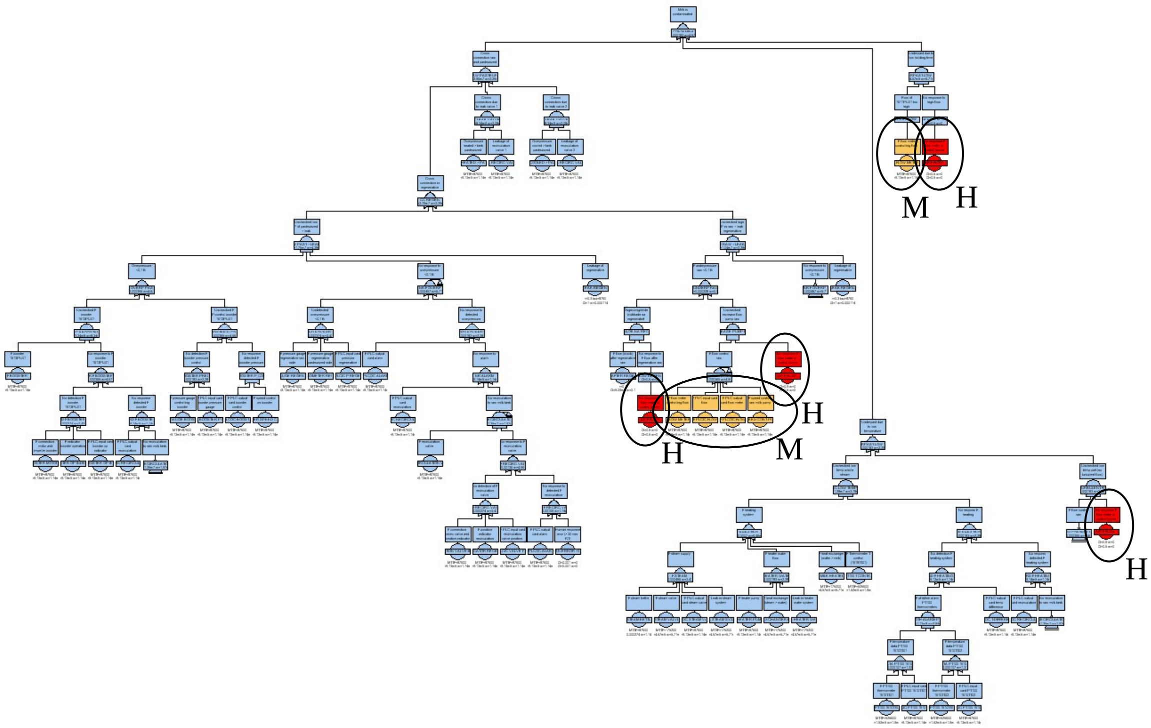

Figure 2: Fault tree of the former case study pasteurization process configuration. The most important base events (see Table 1) are marked H (high = 'No response to failure of flow meter or flow control', occurring four times in the tree) and M (middle).

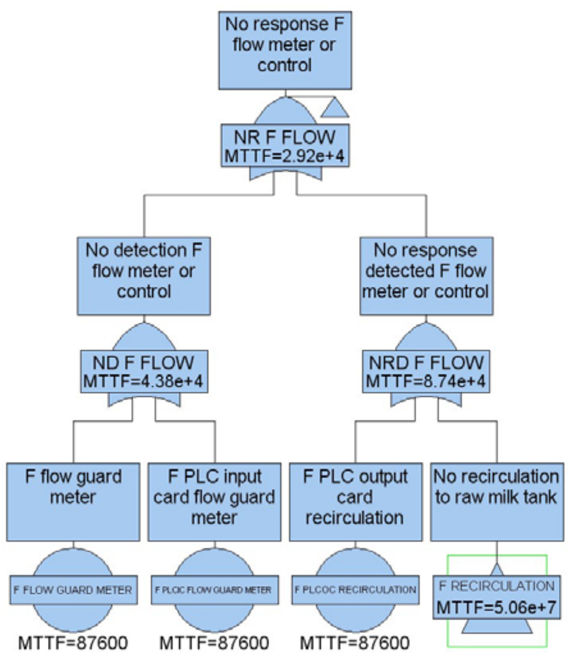

Figure 3: Fault tree branch of the optimized part of the case study pasteurization process configuration. A guarding flow meter automatically initiates recirculation to the raw milk tank when the flow control system (pump, flow meter, PLC cards) fails. MMTF (mean time to failure) is the reciprocal of the failure rate. The triangle bottom right refers to a deeper branch.

The actual failure rate of the new configuration probably is higher than once every 1000 years, as this failure rate is estimated by a basic model. Common cause failure models will be added to the model to account for the effect of e.g. a PLC failing entirely or the effect of common age, brand and maintenance plans for similar parts (valves, thermometers etc.).
The failure rates of the events with the highest importance rankings will be varied to evaluate the effect of variability and uncertainty on the model results, thus turning the model into a Boolean Monte Carlo analysis.

Conclusion

It is possible to estimate the probability of pasteurization process control failure with an acceptable level of certainty. Moreover, it is possible to pin-point the weakest link in the safety control, prioritizing it for optimization if the level contamination needs to be lowered. It is also possible to assess whether the relative contribution to unreliability (and unavailability) of all safety systems are consistent with their relative capital and operational expenditures. Thus, FTA provides companies with a tool to optimize the safety as well as the cost-effectiveness of their pasteurization process.

Literature

Andrews, J.D. and Moss, T.R. (2002) Reliability and risk assessment. 2nd ed. Professional Engineering Publishing Ltd. London and Bury St Edmunds, United Kingdom, 540 p.

Anonymous (2008) Environmental and milk products test positive for *Listeria*. Milk processing plant will remain closed until cleared by health officials. Press release January 17, 2008. The Official Website of the Office of Health and Human Services (EOHHS), Commonwealth of Massachusetts. http://www.mass.gov/?pageID=eohhs2pressrelease&L=1&L0=Home&sid=Eeohhs2&b=pressrelease&f=080117_whittier_farms&csid=Eeohhs2

Te Giffel, M.C. and Zwietering M.H. (1999) Validation of predictive models describing the growth of Listeria. Int. J. Food Microbiol. 46: 135-149

Van Asselt ED, Zwietering MH (2006) A systematic approach to determine global thermal inactivation parameters for various food pathogens – Int. J. Food Microbiol 107(1), 73-82

Van Lieverloo, J.H.M., Fox, M., Schutyser, M., Te Giffel, M.C. and De Jong, P. (2007) Evolving from high through low uncertainty risk assessments for dairy products using kinetic, stochastic and fault tree modelling. Proc. 5th Int. Conf. Predictive Modeling in Foods, Athens, 16-19 September 2007.